

Common Criteria

Installation Supplement and Administrator Guide

August 2024

www.lexmark.com

Contents

Change history....4

Overview and first steps....6

Overview....6
Physical configuration....8

Configuring the printer....10

Configuration checklist....10
Enabling nonvolatile memory encryption using Out of Service Erase....11
Enabling service nonvolatile memory encryption....12
Disabling the Wi-Fi interface....12
Disabling the host USB....12
Disabling ThinPrint....12
Disabling flash drive access....13
Disabling the AirPrint software feature....13
Hiding protected home screen icons....13
Holding all jobs....13
Erasing temporary data files....13
Creating and modifying digital certificates....14
Setting up Internet Protocol Security (IPsec)....16
Shutting down port access....17
Configuring time source settings....17
Configuring security audit logging....18
Configuring e-mail....20
Setting the fax storage location....21
Configuring fax....21
Configuring security reset jumper behavior....22
Configuring the minimum password length....22
Configuring login restrictions....23
Configuring print permissions....23
Disabling the Intelligent Storage Drive....23
Setting up local accounts....24
Setting up local groups and permissions....24
Setting up network accounts....25

User access....31
Controlling access to device functions....32

Troubleshooting....34

Login issues....34
LDAP issues....36

Audit log....37

Erasing keys in flash memory....39

Out of service erase....40

User responsibilities....41

Notices....42

Index....43

Change history

June 2024

- Added information on creating and modifying digital certificates.

April 2024

- Added information on Out of service erase.
- Updated information on audit log.
- Updated information on configuring the printer.

March 2024

- Updated the list of supported printers.

June 2023

- Added information on enabling service nonvolatile encryption.
- Added information on enabling nonvolatile memory encryption using Out of Service Erase.
- Added information on disabling the Wi-Fi interface.
- Updated the list of supported printers.

December 2022

- Added information on erasing keys in flash memory.

November 2022

- Updated the list of supported printers.
- Added information on the Lexmark Trusted Platform Module (TPM).
- Updated the information on preshared keys.
- Updated the steps on checking physical interfaces and installed firmware.
- Deleted the information on configuring printer hard disk encryption because hard disk encryption is now automatic.
- Added information on disabling the intelligent storage drive.

February 2018

- Added information on the following to conform to the Hard Copy Device Protection Profile:
  - Updating firmware
  - Configuring the time source settings
  - Configuring the minimum password length
  - Configuring login restrictions
  - Password requirements for local accounts
  - Setting up Internet Protocol Security (IPsec)
  - Configuring the screen timeout

- Updated the list of supported printers.

October 2016

- Added information on the following:
  - Disabling flash drive access
  - Configuring print permissions
  - Access controls and their required level of protection

May 2016

- Initial document release for multifunction products with a tablet-like touch-screen display.

Overview and first steps

Overview

This guide describes how to configure a supported Lexmark™ printer to conform to the Common Criteria certified target of evaluation. Carefully follow the instructions in this guide to make sure that the printer meets the requirements of the evaluation.

This guide is intended for use by service providers and network administrators responsible for the management of security appliances and software in their network environment. A working knowledge of printers is required for effective use of this guide.

Some settings can be configured using either the *Embedded Web Server* or the printer control panel. Where applicable, instructions for both methods are included.

For information on setting up the printer or using printer features, see the printer *User's Guide*.

Note: The printer *User's Guide* and the *Embedded Web Server Administrator's Guide* are available at **support.lexmark.com**.

Supported printers

Multifunction products (MFPs)

- Lexmark CX532adwe, with and without hard disk
- Lexmark CX635adwe, with and without hard disk
- Lexmark MX532adwe, with and without hard disk
- Lexmark MX632adwe, with and without hard disk

Single-function printers (SFPs)

- Lexmark CS632dwe
- Lexmark MS632dwe

Note: MFPs support copy, email, fax, and printing features. Printers with a hard disk support hard disk features. Some of the features described in this guide are not available in all printers.

Operating environment

The instructions provided in this guide are based on the following assumptions and objectives:

- The printer is installed in a cooperative, nonhostile environment that is physically secured or monitored and protected from unauthorized access to printer external interfaces.
- The administration platform and local area network are physically and logically secured.
- Authorized administrators are trained and capable of performing tasks related to the installation, configuration, operation, and maintenance of the network environment. This includes—but is not limited to —operating systems, network protocols, and security policies and procedures.
- Authorized administrators are trusted to use their access rights appropriately.
- Audit records exported from the printer to another trusted location are accessible to authorized personnel for periodic review and are secured from unauthorized access.

- The operating environment can identify and authenticate users whose accounts are defined externally (LDAP, Kerberos, and so on).
- When an administrator configures *Network Time Protocol* (NTP), the operating environment provides reliable time stamps.
- Users are aware of and are trained to follow the security policies and procedures of their organization. Users are authorized to use the printer according to these policies and procedures.

Understanding the home screen

The screen on the front of the printer is touch sensitive and can be used to access printer functions and navigate settings and configuration menus.



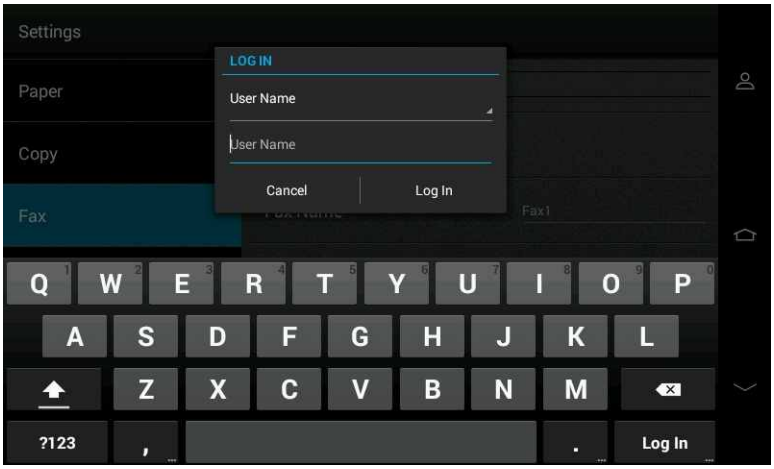
Touch **Settings** to access settings and configuration menus for the printer.

Notes:

- Access to printer menus may be restricted to administrators only.
- By default, the secured applications or functions are hidden from the printer home screen.

Using the keyboard on the display

Some printer settings require one or more alphanumeric entries, such as server addresses, user names, and passwords. When an alphanumeric entry is needed, a keyboard appears.



As you touch the letters and numbers, your selections appear in a corresponding field at the top of the screen. The keyboard on the display may also contain other icons, such as Done, Next, or Submit.

To type a single uppercase or shift character, touch , and then touch the letter or number. To turn on Caps Lock, double-tap , and then continue typing. Caps Lock remains engaged until you touch it again.

Touch  to delete a single character, or press and hold it to delete everything that you have typed.

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the top of the printer home screen.
   - From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
2. Open a Web browser, and then type the printer IP address.

Physical configuration

Physical configuration checklist

Before beginning configuration tasks, do the following:

1. Make sure that no optional interfaces are installed.
2. If the device does not have a Trusted Platform Module (TPM), then install the Lexmark TPM option.
3. Check the firmware version.
4. Attach a lock to the printer.

Checking physical interfaces and installed firmware

1. Make sure that only one network interface is installed in the printer. There must be no optional network, parallel, or serial interfaces.
2. If the device supports Wi-Fi, then disable the Wi-Fi interface.
3. Turn on the printer using the power switch.
4. From the home screen, touch **Settings** > **Reports** > **Menu Settings Page**. The printer prints several pages of device information.
5. In the Installed Features section, make sure that no Pluggable Firmware Option (PFO) cards are installed.
6. If you have not yet installed hard disk or fax options, then install them before proceeding.
7. If the device does not have a Trusted Platform Module (TPM), then install the Lexmark TPM option.
8. To check the firmware version, under the Device Information section, locate **`Base =`**.

   Note: To make sure that the Base value is correct and up-to-date, contact your Lexmark representative.

Updating firmware

1. From the Embedded Web Server, click **Settings** > **Device** > **Update Firmware**.
2. Browse to the required flash file.
3. Click **Upload**.

   Note: For more information on updating the device firmware, contact your Lexmark representative.

Attaching a lock

Warning—Potential Damage: After a lock is attached, the metal plate and controller board cannot be removed. The security jumper cannot be accessed without causing visible damage to the device.

Before you begin, make sure that the printer case is closed.

Locate the security slot, and then attach a lock. It is the same type of security slot found on most laptop computers. You can typically find it at the back of the printer near an outside edge.

Configuring the printer

You can achieve an evaluated configuration on a non-network (standalone) printer in just a few steps.

Configuration checklist

This checklist outlines the steps in configuring the settings needed to achieve the evaluated configuration for a standalone printer.

- ☐ Enable nonvolatile memory encryption using Out of Service Erase.
- ☐ Enable service nonvolatile memory encryption.
- ☐ Disable the Wi-Fi interface.
- ☐ Disable the intelligent storage drive.
- ☐ Disable the host USB interface.
- ☐ Disable ThinPrint.
- ☐ Disable flash drive access.
- ☐ Disable SNMP.
- ☐ Disable the home screen icons.
- ☐ Require all jobs to be held.
- ☐ Erase temporary data files.
- ☐ Create and modify digital certificates.
- ☐ Set up Internet Protocol Security (IPsec).
- ☐ Shut down the port access.
- ☐ Configure the time source settings.
- ☐ Configure the security audit logging settings.
- ☐ Configure the email settings.
- ☐ Set the fax storage location.
- ☐ Configure the fax settings.
- ☐ Configure the security reset jumper behavior.

- ☐ Configure the login restrictions.
- ☐ Configure the print permissions.
- ☐ Set up local accounts.
- ☐ Set up local groups and permissions.
- ☐ Set up network accounts.
- ☐ Set the default login methods.
- ☐ Configure the minimum password length.

Enabling nonvolatile memory encryption using Out of Service Erase

Using the Embedded Web Server

For printers with two-line LCD, use this method.

1. From the Embedded Web Server, click **Settings** > **Device** > **Maintenance**.
2. Locate Erase Printer Memory, and then select **Sanitize all information on nonvolatile memory**.
3. Select **Start initial setup wizard**.
4. Click **Start**.

Notes:

- The Nonvolatile memory encryption option is disabled by default.
- When enabled, there is no option to disable the encryption.

Using the control panel

1. From the home screen, touch **Settings** > **Device** > **Maintenance** > **Out of Service Erase**.
2. Select **Sanitize all information on nonvolatile memory**, and then touch **Erase**.
3. Select **Start initial setup wizard**.
4. Touch **Next** > **Start**.

Notes:

- The Nonvolatile memory encryption option is disabled by default.
- When enabled, there is no option to disable the encryption.

Enabling service nonvolatile memory encryption

Using the Embedded Web Server

For printers with two-line LCD, use this method.

1. From the Embedded Web Server, click **Settings** > **Device** > **Maintenance** > **Configuration Menu** > **Device Operations**.
2. Locate Encrypt Service Nonvolatile Memory, and then click **Start**.
3. Click **Continue**.

Notes:

- The Encrypt Service Nonvolatile Memory option is disabled by default.
- When enabled, there is no option to disable the encryption.

Using the control panel

1. From the home screen, touch **Settings** > **Device** > **Maintenance** > **Configuration Menu** > **Device Operations**.
2. Locate Encrypt Service Nonvolatile Memory, and then touch **Start**.
3. Touch **Continue**.

Notes:

- The Encrypt Service Nonvolatile Memory option is disabled by default.
- When enabled, there is no option to disable the encryption.

Disabling the Wi-Fi interface

1. From the home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
2. Set Active Adapter to **Standard Network**.

Disabling the host USB

1. From the home screen, touch **Settings** > **Network/Ports** > **USB**.
2. Set Enable USB Port to **Off**.
3. From the Enable USB Port dialog box, touch **Yes** to reboot the printer.

Disabling ThinPrint

1. From the home screen, touch **Settings** > **Network/Ports** > **ThinPrint**.
2. Set Enable ThinPrint to **Off**.

Disabling flash drive access

1. From the home screen, touch **Settings** > **Device** > **Preferences**.
2. Set Flash Drive Access to **Disabled**.

Disabling the AirPrint software feature

1. From the home screen, touch **Settings** > **Network/Ports** > **AirPrint**.
2. Set Enable AirPrint to **Off**.

Hiding protected home screen icons

1. From the home screen, touch **Settings** > **Security** > **Miscellaneous**.
2. Set Protected Features to **Hide**.

Holding all jobs

1. From the home screen, touch **Settings** > **Security** > **Confidential Print Setup**.
2. Set “Require All Jobs to be Held” to **On**.
3. Set the Confidential Job Expiration value.

   Note: Off is not a recommended setting.

Erasing temporary data files

1. From the home screen, touch **Settings** > **Security** > **Erase Temporary Data Files**.
2. Set Stored in onboard memory to **On**.
3. From the Stored on hard disk menu, select **3 Pass Erase**.

   Note: This setting performs a 3-Pass overwrite of the data: 0xAA, 0x55, and then a random value (DoD 5220-22.M).

Creating and modifying digital certificates

Certificates are needed for domain controller verification and for SSL support in LDAP. Each certificate must be in a separate PEM (.cer) file.

Setting certificate defaults

These settings apply to new certificates generated in Certificate Management.

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. Click **Configure Certificate Defaults**, and then specify the values for the following fields:
   - **Common Name**—Type a name for the printer. Leave this field blank if you want to use the printer host name as the common name.
   - **Organization Name**—Type the name of the company or organization issuing the certificate.
   - **Unit Name**—Type the name of the unit within the company or organization issuing the certificate.
   - **Country/Region**—Type the country or region where the company or organization issuing the certificate is located. You can type only up to two characters.
   - **Province Name**—Type the province where the company or organization issuing the certificate is located.
   - **City Name**—Type the city where the company or organization issuing the certificate is located.
   - **Subject Alternate Name**—Type the alternate name and prefix that conforms to RFC 2459. For example, **`IP:123.123.123.123`**. Leave this field blank if you want to use the IPv4 address.

   Note: You can type up to 128 characters in all fields, except in **Country/Region**.
3. Click **Save**.
4. Create a ZIP bundle containing a file called **`bundle.xml`** with the following contents:

```
<?xml version="1.0" encoding="UTF-8"?>
<bundle>
<deviceSettings>
<setting name="printer.certMgr.RSAKeyLength">3072</setting>
</deviceSettings>
</bundle>
```

   Note: You can use any file name for the ZIP bundle.
5. From the Embedded Web Server, click the **Import Configuration** button, browse to your ZIP file, and then click **Import**.

Creating a certificate

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.
2. From the Device Certificates section, click **Generate**, and then specify the values for the following fields:
   - **Friendly Name**—Type a name for the certificate. You can type up to 64 characters.
   - **Common Name**—Type a name for the printer. Leave this field blank if you want to use the printer host name as the common name.
   - **Organization Name**—Type the name of the company or organization issuing the certificate.
   - **Unit Name**—Type the name of the unit within the company or organization issuing the certificate.
   - **Country/Region**—Type the country or region where the company or organization issuing the certificate is located. You can type only up to two characters.
   - **Province Name**—Type the province where the company or organization issuing the certificate is located.

- **City Name**—Type the city where the company or organization issuing the certificate is located.
- **Subject Alternate Name**—Type the alternate name and prefix that conforms to RFC 2459. For example, **`IP:123.123.123.123`**. Leave this field blank if you want to use the IPv4 address.

Note: You can type up to 128 characters in all fields, except in **Country/Region** and **Friendly Name**.

3 Click **Generate**.

Viewing, downloading, and deleting a certificate

1 From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.

2 From the Device Certificates list, click a certificate.

3 From the View Certificate window, do one of the following:

- To remove a previously saved certificate, click **Delete**.
- To download or save the certificate as a PEM (.cer) file, click **Download To File**.
- To download or save the signing request as a CSR file, click **Download Signing Request**.
- To upload a previously signed certificate, click **Install Signed Certificate**, browse to the certificate source file, and then click **Save**.

Notes:

- If Extended Validation is checked, then the device verifies that a valid CA chain is installed on the device and the certificate's revocation status via OCSP. If either of these checks fails, including an unreachable OCSP responder (defined in the certificate's Authority Information Access extension), then the installation of the signed device certificate fails.
- The device certificate with Friendly Name **default** should be signed by a CA (i.e. not self-signed). This signature ensures that the device certificate will not be regenerated if the IP address or hostname changes, preventing the previous certificate from becoming obsolete.

Installing a Certificate Authority (CA) certificate

A CA certificate is required when using Smart Card Authentication.

1 From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management**.

2 From the Manage CA Certificates section, click **Upload CA**, and then browse to the PEM (.cer) file.

Sample certificate:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBs
…
l3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

3 Reboot the printer.

Understanding the extendedKeyUsage field

The device validates the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

- Client certificates presented for TLS I have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

Setting up Internet Protocol Security (IPsec)

IPsec encrypts IP packets as they are transmitted over the network between devices. It does not handle authentication or restrict access.

Note: An IPsec-trusted communications channel must be configured between the printer and all the network services that are used, including authentication, audit, email, and NTP servers.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **IPSec**.
2. Select **Enable IPSec**.
3. Set Base Configuration to **Secure**.

   Note: Secure mode only allows cryptographic algorithm AES-CBC-256 and Secure Hash Algorithm (SHA)-based HMAC algorithms HMAC-SHA-256 and HMAC-SHA-384 in the ESP and IKE protocols. In addition, secure mode allows connections only to the configured IPsec endpoints, and no plain-text connections.
4. In the IKE SA Lifetime (Hours) menu, select a value from 1 to 24.
5. In the IPSec SA Lifetime (Hours) menu, select a value from 1 to 8.
6. Configure the authenticated connections.
   - From the Pre-Shared Key Authenticated Connections section, type the IP address of the client device that you want to connect to the printer.
   - From the Certificate Authenticated Connections section, type the IP address of the client device that you want to connect to the printer.

   Notes:

   - If you are using preshared key (PSK) authentication, then type the corresponding key. Retain the key to use later when configuring client devices. Preshared keys may have up to 256 characters, composed of a combination of uppercase and lowercase letters, numbers, and special characters. For adequate security, preshared keys must have at least 22 characters.
   - If you are using certificate authentication, then the device verifies the endpoint certificate's revocation status via OCSP. If the certificate has been revoked, then it is rejected and authentication fails. If the certificate status is good, the OCSP responder (defined in the endpoint certificate's Authority Information Access extension) is unreachable, or any other OCSP error occurs, the certificate is accepted and authentication continues.
7. Click **Save**.

Shutting down port access

Disabling virtual ports helps prevent intruders from accessing the printer using a network connection.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP** > **TCP/IP Port Access**.
2. Clear the following check boxes:
   - TCP 21 (FTP)
   - UDP 69 (TFTP)
   - UDP 137 (WINS)
   - UDP 161 (SNMP)
   - UDP 162 (SNMP Traps)
   - TCP 631 (IPP)
   - TCP 5001 (IPDS)
   - UDP 5353 (mDNS)
   - UDP 9300/UDP 9301/UDP 9302 (NPAP)
   - TCP 9500/TCP 9501 (NPAP)
   - TCP 9600 (IPDS)
   - ThinPrint
   - UDP 3702/TCP 65001 (WS-Discovery)
   - TCP 65002 (WSD Print Service)
   - TCP 65003 (WSD-Eventing)
   - TCP 65004 (WSD Scan Service)
3. Click **Save**.

Configuring time source settings

An accurate system clock is necessary to make sure that the audit log time stamps are accurate. You can set the system clock manually, or automatically using Network Time Protocol (NTP). We recommend using the NTP method.

Configuring NTP settings

Use NTP to sync printer date and time settings automatically with a trusted clock.

Note: Before configuring the NTP settings, if your network uses Dynamic Host Configuration Protocol (DHCP), then make sure that the settings are not provided automatically.

Using the Embedded Web Server

1. From the Embedded Web Server, click **Settings** > **Device** > **Preferences** > **Date and Time** > **Network Time Protocol**.
2. Select **Enable NTP**, and then type the IP address or host name of the NTP server.
3. If the NTP server requires authentication, then in the Enable Authentication menu, select **MD5 key**.

4 In the “Install MD5 key” field, browse to the file containing the NTP authentication credentials.

5 Click **Save**.

Using the control panel

1 From the home screen, touch **Settings** > **Device** > **Preferences** > **Date and Time** > **Network Time Protocol**.

2 Set Enable NTP to **On**.

3 Touch **NTP Server**, type the IP address or host name of the NTP server, and then touch **OK**.

4 If the NTP server requires authentication, then set Enable Authentication to **MD5 key**.

Configuring the system clock manually

Using the Embedded Web Server

1 From the Embedded Web Server, click **Settings** > **Device** > **Preferences** > **Date and Time** > **Configure**.

2 In the “Manually Set Date and Time” field, configure the date and time.

3 Set the date format, time format, and time zone.

4 Click **Save**.

Using the control panel

1 From the home screen, touch **Settings** > **Device** > **Preferences** > **Date and Time** > **Configure**.

2 Touch **Manually Set Date and Time**, configure the date and time, and then touch **Set**.

3 Set the date format, time format, and time zone.

Configuring security audit logging

Using the Embedded Web Server

1 From the Embedded Web Server, click **Settings** > **Security** > **Security Audit Log**.

2 Select **Enable Audit** and **Enable Remote Syslog**, and then configure the following:

- **Remote Syslog Server**—Type the IP address or host name of the remote syslog server.
- **Remote Syslog Port**—Enter the port number of the remote syslog server used on the destination server.
- **Remote Syslog Method**—Select **Normal UDP** or **Stunnel**, depending on the configuration on the destination server.
- **Severity of Events to Log**—Select **5 - Notice**. Events specified at this severity level and up are logged.
- **Remote Syslog Non-Logged Events**—Send all events to the remote server regardless of the specified severity level.
- **Admin's E-mail Address**—Type one or more e-mail addresses to which the notifications about certain log events are sent automatically. Use commas to separate multiple e-mail addresses.
- **E-mail Log Cleared Alert**—Send an e-mail when you clear the log.
- **E-mail Log Wrapped Alert**—Send an e-mail when the log is full and begins to overwrite the oldest entries.

- **Log Full Behavior**—Select whether to overwrite the oldest entries or to delete all entries and send a notification through e-mail when the log storage is full.
- **E-mail % Full Alert**— Send an e-mail when log storage space reaches a specified percentage of capacity.
- **% Full Alert Level**— Specify the percentage (1–99) of log storage space that must be used before an e-mail alert is triggered.
- **E-mail Log Exported Alert**—Send an e-mail when the log file is exported.
- **E-mail Log Settings Changed Alert**—Send an e-mail when log settings are changed.
- **Log Line Endings**—Specify how line endings are handled in the log file, depending on the operating system in which the file is parsed or viewed.
- **Digitally Sign Exports**—Add a digital signature to e-mail alerts.

Note: To use e-mail alerts, configure the SMTP settings. For more information, see "Configuring e-mail" on page 20.

3 Click **Save**.

Using the control panel

1 From the home screen, touch **Settings** > **Security** > **Security Audit Log**.

2 Set Enable Audit and Enable Remote Syslog to **On**, and then configure the following:

- **Remote Syslog Server**—Type the IP address or host name of the remote syslog server.
- **Remote Syslog Port**—Enter the port number of the remote syslog server used on the destination server.
- **Remote Syslog Method**—Select **Normal UDP** or **Stunnel**, depending on the configuration on the destination server.
- **Severity of Events to Log**—Select **5 - Notice**. Events specified at this severity level and up are logged.
- **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 to support sorting and filtering by network monitor or intrusion detection software.
- **Admin's E-mail Address**—Type one or more e-mail addresses to which the notifications about certain log events are sent automatically, and then touch **OK**. Use commas to separate multiple e-mail addresses.
- **Log Full Behavior**—Select whether to overwrite the oldest entries or to delete all entries and send a notification through e-mail when the log storage is full.
- **% Full Alert Level**— Specify the percentage (1–99) of log storage space that must be used before an e-mail alert is triggered.
- **Log Line Endings**—Specify how line endings are handled in the log file, depending on the operating system in which the file is parsed or viewed.

3 Set the following to **On**:

- **Remote Syslog Non-Logged Events**—Send all events to the remote server regardless of the specified severity level.
- **E-mail Log Cleared Alert**—Send an e-mail when you clear the log.
- **E-mail Log Wrapped Alert**—Send an e-mail when the log is full and begins to overwrite the oldest entries.
- **E-mail % Full Alert**— Send an e-mail when log storage space reaches a specified percentage of capacity.
- **E-mail Log Exported Alert**—Send an e-mail when the log file is exported.
- **E-mail Log Settings Changed Alert**—Send an e-mail when log settings are changed.
- **Digitally Sign Exports**—Add a digital signature to e-mail alerts.

Note: To use e-mail alerts, configure the SMTP settings. For more information, see “Configuring e-mail” on page 20.

Configuring e-mail

Note: Make sure that the printer is configured to send user data as an attachment to e-mail.

Using the Embedded Web Server

1. From the Embedded Web Server, click **Settings** > **Device** > **Notifications** > **E-mail Alerts Setup** > **E-mail Setup**.
2. Configure the SMTP settings, and then click **Save**.
   - **Primary SMTP Gateway**—Type the IP address or host name of the server used for sending e-mail.
   - **Primary SMTP Gateway Port**—Enter the port number of the primary SMTP server.
   - **Secondary SMTP Gateway**—Type the server IP address or host name of the secondary or backup SMTP server.
   - **Secondary SMTP Gateway Port**—Enter the port number of the secondary or backup SMTP server.
   - **SMTP Timeout**—Enter how long the printer waits for the server to respond before it times out.
   - **Reply Address**—Type the e-mail address where you want to receive responses.
   - **Use SSL/TLS**—Specify whether to send an e-mail using an encrypted link.
   - **SMTP Server Authentication**—Specify the type of authentication used to access the SMTP server.
   - **Device-Initiated E-mail**—Select **Use Device SMTP Credentials**.

   Note: If the printer requires user credentials to send e-mail, then specify the appropriate information for authentication credentials.
3. From the Embedded Web Server, click **E-mail** > **E-mail Defaults** > **Admin Controls**.

   Note: This setting is applicable only in some printer models.
4. In the E-mail Images Sent As menu, select **Attachment**, and then click **Save**.
5. Click **Web Link Setup**, and then make sure that all fields are cleared.
6. Click **Save**.

Using the control panel

1. From the home screen, touch **Settings** > **Device** > **Notifications** > **E-mail Alerts Setup** > **E-mail Setup**.
2. Configure the SMTP settings.
   - **Primary SMTP Gateway**—Type the IP address or host name of the server used for sending e-mail.
   - **Primary SMTP Gateway Port**—Enter the port number of the primary SMTP server.
   - **Secondary SMTP Gateway**—Type the server IP address or host name of the secondary or backup SMTP server.
   - **Secondary SMTP Gateway Port**—Enter the port number of the secondary or backup SMTP server.
   - **SMTP Timeout**—Enter how long the printer waits for the server to respond before it times out.
   - **Reply Address**—Type the e-mail address where you want to receive responses.
   - **Use SSL/TLS**—Specify whether to send an e-mail using an encrypted link.

- **SMTP Server Authentication**—Specify the type of authentication used to access the SMTP server.
- **Device-Initiated E-mail**—Select **Use Device SMTP Credentials**.

Note: If the printer requires user credentials to send e-mail, then specify the appropriate information for authentication credentials.

3 From the home screen, touch **Settings** > **E-mail** > **E-mail Defaults** > **Admin Controls**.

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

4 In the E-mail Images Sent As menu, select **Attachment**, and then return to the previous menu.

5 Touch **Web Link Setup**, and then make sure that all fields are cleared.

Setting the fax storage location

1 From the home screen, touch **Settings** > **Device** > **Maintenance** > **Configuration Menu** > **Fax Configuration**.

2 From the Fax Storage Location menu, select **Disk**.

Configuring fax

If your printer includes fax capabilities and is attached to a phone line, then enable held faxes and disable fax forwarding and the driver to fax. The printer provides Group 3 digital fax capability in conformance with ITU-T Recommendations T.4 and T.30. This interface can be used to receive faxes to be printed, or to send faxes of scanned images.

Using the Embedded Web Server

1 From the Embedded Web Server, click **Settings** > **Fax** > **Analog Fax Setup**.

2 Do the following:

Enable held faxes

a Click **Fax Receive Settings** > **Holding Faxes**.

b Set Held Fax Mode to **Always On**, and then click **Save**.

Disable fax forwarding

a Click **Fax Receive Settings** > **Admin Controls**.

b Set Fax Forwarding to **Print**, and then click **Save**.

Disable the driver to fax

a Click **Fax Send Settings** > **Admin Controls**.

b Clear **Driver to Fax**, and then click **Save**.

Using the control panel

1 From the home screen, touch **Settings** > **Fax**.

2 Do the following:

Enable held faxes

a Touch **Analog Fax Setup** > **Fax Receive Settings** > **Holding Faxes**.

b Set Held Fax Mode to **Always On**.

Disable fax forwarding

a Touch **Analog Fax Setup** > **Fax Receive Settings** > **Admin Controls**.

b Set Fax Forwarding to **Print**.

Disable the driver to fax

a Touch **Analog Fax Setup** > **Fax Send Settings** > **Admin Controls**.

b Turn off **Driver to Fax**.

Configuring security reset jumper behavior

The security reset jumper is a hardware jumper on the controller board that can be used to reset the security settings on the device.

Note: Using the security reset jumper can remove the printer from the evaluated configuration.

1 From the home screen, touch **Settings** > **Security** > **Miscellaneous**.

2 Touch **Security Reset Jumper**, and then select either of the following:

- **Enable "Guest" access**—Grants access to all aspects of the printer to a guest user account. All login methods that were previously on the device still exists, but the guest user can access and delete them at will.
- **No Effect**—Removes access to all security menus. Use this option with caution.

Warning—Potential Damage: If **No Effect** is selected and the password (or other applicable credentials) is lost, then you are not able to access the security menus. To regain access to the security menus, contact your system administrator.

Configuring the minimum password length

For conformance, the minimum password length is eight characters. Lexmark recommends at least 15 characters. The maximum password length is 32 characters.

Using the Embedded Web Server

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

2 Enter the minimum password length.

3 Click **Save**.

Using the control panel

1 From the home screen, touch **Settings** > **Security** > **Miscellaneous**.

2 Enter the minimum password length.

Configuring login restrictions

Using the Embedded Web Server

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Restrictions**.
2. Configure the login restrictions.
   - **Login failures**—The number of failed login attempts before the user gets locked out. Enter a value from 1 to 10. The default value is 3.
   - **Failure time frame**—The time frame between failed login attempts before the user gets locked out. Enter a value from 1 to 60. The default value is 5.
   - **Lockout time**—The lockout duration. Enter a value from 1 to 60. The default value is 5.
   - **Web Login Timeout**—The delay for a remote login to be inactive before the user is logged off automatically. Enter a value from 1 to 120. The default value is 10.
3. Click **Save**.
4. From the Embedded Web Server, click **Settings** > **Device** > **Preferences**.
5. In the Screen Timeout field, set the idle time in seconds before the display shows the home screen, or before the printer logs off a user account automatically. Enter a value from 5 to 300 seconds. The default value is 60 seconds.

Using the control panel

1. From the home screen, touch **Settings** > **Security** > **Login Restrictions**.
2. Configure the login restrictions. For more information, see step 2 of "Using the Embedded Web Server" on page 23.

Configuring print permissions

1. From the home screen, touch **Settings** > **Security** > **Miscellaneous**.
2. Set Print Permission to **On**.

Disabling the Intelligent Storage Drive

On devices with an Intelligent Storage Drive, you must not use the drive to store user data.

Using the Embedded Web Server

1. From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous**.
2. Set Use Intelligent Storage Drive for User Data to **Off**.
3. Click **Save**.

Using the control panel

1. From the home screen, touch **Settings** > **Security** > **Miscellaneous**.
2. Set Use Intelligent Storage Drive for User Data to **Off**.

Setting up local accounts

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

Creating local accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click **Add User**.
3. Select **User Name/Password**.
4. From the User Information section, type the user information and authentication credentials.

   Notes:

   - The password must contain at least one lowercase letter, one uppercase letter, and one nonalphabetic character.
   - The password must not contain dictionary words or variations of the user name.
5. From the Permission Groups section, select one or more groups.

   Note: To create a group for the user, click **Add New Group**. For more information, see "Creating local account groups" on page 24.
6. Click **Save**.

Editing and deleting local accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Local Accounts section, click the authentication method where the user account belongs to.
3. Click the user account that you want to edit or delete.
4. Do either of the following:
   - To edit the user account, update the user information, and then click **Save**.
   - To delete the user account, click **Delete User**.

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

Setting up local groups and permissions

Creating local account groups

Use groups to customize users' access to applications and printer functions.

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. Do either of the following:

Add a group when managing permissions

a From the Local Accounts section, click **Manage Groups/Permissions**.

b Click **Add Group**.

Add a group when creating or editing a user account

a Create or edit a user account.

b From the Permission Groups section, select **Add New Group**.

3 Type a unique group name.

4 From the Access Controls section, select the functions, menus, and applications that the group can access.

5 Click **Save**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- For more information on access controls, see "Understanding access controls" on page 30.

Editing or deleting local account groups

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

2 From the Local Accounts section, click **Manage Groups/Permissions**.

3 Click the group, and then do either of the following:

- Configure the access controls, and then click **Save**.
- Click **Delete Group**.

Notes:

- To import access controls from another group, click **Import Access Controls**, and then select a group.
- To delete multiple groups, select the groups, and then click **Delete**.
- For more information on access controls, see "Understanding access controls" on page 30.

Setting up network accounts

Creating an LDAP or LDAP+GSSAPI login method

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

2 From the Network Accounts section, click **Add Login Method** > **LDAP**.

3 Select the authentication type.

- LDAP
- LDAP+GSSAPI

4 Configure the settings.

General Information

- **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**—Enter the port where 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 used when logging 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 only Windows operating system authentication credentials.

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

Device Credentials

- **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 in the LDAP +GSSAPI setup.
  - **Device Password**—Type the password for the user.

Advanced Options

- **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 users' 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 more information, contact your system administrator.
- **Mail Attribute**—Type the LDAP attribute that contains the users' e-mail addresses. The default value is **`mail`**.
- **Fax number Attribute**—Type the LDAP attribute that contains the users' fax number. The default value is **`facsimiletelephonenumber`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Home Directory Attribute**—Type the LDAP attribute that contains the users' home directory. The default value is **`homeDirectory`**.

- **Group Membership Attribute**—Type the LDAP attribute required for group search. The default value is **memberOf**.
- **Search Base**—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.

Search Specific Object Classes

- **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.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail 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.

5 Click **Save and Verify**.

Editing or deleting LDAP or LDAP+GSSAPI login methods

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

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

3 Do either of the following:

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

Creating a Kerberos login method

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

2 From the Network Accounts section, click **Add Login Method** > **Kerberos**.

3 Do one of the following:

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. The realm must be typed in uppercase.

Import a Kerberos configuration file

In the Import Kerberos File field, browse to the krb5.conf file.

4. If necessary, from the Miscellaneous Settings section, configure the following settings:
   - **Character Encoding**—Select the character encoding used for the configuration file.
   - **Disable Reverse IP Lookups**
5. Click **Save and Verify**.

Creating an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From 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 the user belongs to.
4. Click **Join Domain**.

Editing or deleting an Active Directory login method

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the Network Accounts section, click the Active Directory login method.
3. Do either of the following:
   - To delete the login method, click **Unjoin Domain**.
   - Configure the following settings, and then click **Save and Verify**.

     General Information

     - **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.

Device Credentials

- **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.

Advanced Options

- **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 users' 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 users' e-mail addresses. The default value is **`mail`**.
- **Fax number Attribute**—Type the LDAP attribute that contains the users' fax number. The default value is **`facsimiletelephonenumber`**.
- **Full Name Attribute**—Type the LDAP attribute that contains the users' full names. The default value is **`cn`**.
- **Home Directory Attribute**—Type the LDAP attribute that contains the users' home directory. The default value is **`homeDirectory`**.
- **Group Membership Attribute**—Type the LDAP attribute required for group search. The default value is **`memberOf`**.
- **Search Base**—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.

Search Specific Object Classes

- **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.

Address Book Setup

The following settings are used to configure the address book used when scanning to an e-mail 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.

Understanding access controls

Access controls let you limit users' access to functions, applications, and printer management. Depending on the login method that you are using, access controls are assigned to a group where a user belongs to.

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

1. From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.
2. From the login method that you are using, click **Manage Permissions** or **Manage Groups/Permissions**.
3. Select a group, and then configure the access controls.
   - **Function Access**—Allow users to access printer functions.
   - **Administrative Menus**—Allow users to access the menus in the Embedded Web Server that are used to manage functions, applications, and security.
   - **Device Management**—Allow users to use printer management options.
   - **Apps**—Allow users to use the application when the application access control is selected.

Note the following access controls and their required level of protection.

- **No Access**—Disable access to a function for all users and administrators.
  Remote Management
  Create Profiles
  Held Jobs Access
  Internal Printing Protocol (IPP)
  Manage Bookmarks
  Use Profiles
  Manage Shortcuts
  FTP Function
- **Administrator access only**—Use an authentication method that provides administrator-only access.
  Security Menu
  Network/Ports Menu
  SE Menu
  Device Menu
  Release Held Faxes
  Access Address Book in Apps
  Modify Address Book
  Reports Menu
  Option Card Menu
  Import / Export Settings
  Apps Configuration
  Firmware Updates
  New Apps
  Out of Service Erase

- **Authenticated Users**—Use an authentication method that provides access to authenticated users.
  - Cancel Jobs At Device
  - Operator Panel Lock
- **Administrator discretion**—Use any valid setting acceptable at administrator discretion.
  - Copy Function
  - Color Dropout
  - E-mail Function
  - Fax Function
  - Change Language from Home Screen
  - Paper Menu
  - Screen Saver
- **Not applicable**—USB ports are disabled.
  - Flash Drive Print
  - Flash Drive Scan
  - Flash Drive Color Printing
- **Required**—Enable the following access controls so the printer can accept print jobs.
  - B/W Print
  - Color Print

Setting default login methods

1. From the Embedded Web Server, click **Security** > **Login Methods**.
2. Click **Change** beside Default Browser Login.
3. Select the login method that you want to use for Control Panel and Browser.

User access

Administrators and users are required to log in to the printer using a method that provides both authentication and authorization. Under the evaluated configuration, three options are available for allowing access to network-connected devices: Local Accounts, LDAP, LDAP+GSSAPI, and Smart Card Authentication.

Configuring Smart Card Authentication Client

Configuring login screen settings

Use the login screen settings to set how you want users to log in to the printer.

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Login Screen section, in the Login Type menu, select **Smart Card Only**.
3. Set User Validation Mode to **Active Directory**.
4. Click **Apply**.

Configuring advanced settings

1. From the Embedded Web Server, navigate to the configuration page for the application:

   Apps > **Smart Card Authentication Client** > **Configure**

2. From the Advanced Settings section, select a session user ID.

   Note: Some applications, such as Secure E-mail, require a value for the session user ID.

3. In the E-mail From Address menu, select where the printer retrieves the user email address.

4. If necessary, select **Use SSL for User Info** to retrieve user information from the domain controller using an SSL connection.

5. If necessary, in the Other User Attributes field, type other LDAP attributes that must be added to the session. Use commas to separate multiple values.

6. In the Group Authorization List, type the Active Directory groups that can access applications or functions. Use commas to separate multiple values.

   Note: The groups must be in the LDAP server.

7. If DNS is not enabled in your network, then upload a host file.

   Type the mappings in the text file in the format of ***xy***, where ***x*** is the IP address and ***y*** is the host name. You can assign multiple host names to an IP address. For example, **`255.255.255.255 HostName1 HostName2 HostName3`**.

   You cannot assign multiple IP addresses to a host name. To assign IP addresses to groups of host names, type each IP address and its associated host names on a separate line of the text file.

   For example:

   ```
   123.123.123.123 HostName1 HostName2
   456.456.456.456 HostName3
   ```

8. Click **Apply**.

Controlling access to device functions

Securing access to the printer

Securing access to the home screen

Users are required to authenticate before accessing the printer home screen.

Note: Before you begin, make sure that the Display Customization application is enabled in your printer. For more information, see the *Display Customization Administrator's Guide*.

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

2. From the Public section, click **Manage Permissions**.

3. Expand **Apps**, clear **Slideshow**, **Change Wallpaper**, and **Screen Saver**, and then click **Save**.

4. From the Additional Login Methods section, click **Manage Permissions** beside Smart Card.

5 Select a group whose permissions you want to manage.

Note: The All Users group is created by default. More group names appear when you specify existing Active Directory groups in the Group Authorization List field. For more information, see "Configuring advanced settings" on page 32.

6 Expand **Apps**, and then select **Slideshow**, **Change Wallpaper**, and **Screen Saver**.

7 Click **Save**.

Securing access to individual applications and functions

Users are required to authenticate before accessing an application or a built-in printer function.

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

2 From the Public section, click **Manage Permissions**.

3 Restrict public access to the applications or functions that you want to secure. Do any of the following:

- For Secure E-mail, expand **Function Access**, clear **E-mail Function**, and then click **Save**.
- For other applications or functions, expand one or more categories, clear the application or function, and then click **Save**.

4 From the Additional Login Methods section, click **Manage Permissions** beside Smart Card.

5 Select a group whose permissions you want to manage.

Note: The All Users group is created by default. More group names appear when you specify existing Active Directory groups in the Group Authorization List field. For more information, see "Configuring advanced settings" on page 32.

6 Select the applications or functions that you want authenticated users to access. Do any of the following:

- For Secure E-mail, expand **Function Access**, and then select **E-mail Function**.
- For other applications or functions, expand one or more categories, and then select the application or function.

7 Click **Save**.

Disabling unused applications

1 From the Embedded Web Server, click **Apps**.

2 Select an unused application.

3 Click **Stop**.

Troubleshooting

Login issues

Cannot detect the card reader or the smart card

Try one or more of the following:

Make sure that the card reader is connected properly to the printer

Make sure that the card reader and the smart card are compatible

Make sure that the card reader is supported

For a list of supported card readers, see the *Readme* file.

Make sure that the card reader driver is installed on the printer

Contact your Lexmark representative

Error reading the smart card

Try one or more of the following:

Make sure that the smart card is supported

For a list of supported smart cards, see the *Readme* file.

Make sure that the smart card driver is installed in the printer

User is locked out

Try one or more of the following:

Update the allowed number of login failures and lockout time

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

The user may have reached the allowed number of login failures.

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

   Note: Wait for the lockout time to pass before the new settings take effect.

Reset or replace the smart card

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

Printer home screen does not lock

Try one or more of the following:

Make sure that Display Customization is enabled

For more information, see the *Display Customization Administrator's Guide*.

Secure access to the home screen

For more information, see "Securing access to the home screen" on page 32.

Cannot generate or read certificate information from the smart card

Try one or more of the following:

Make sure that the certificate information on the smart card is correct

Contact your Lexmark representative

Domain controller certificate is not installed

Make sure that the correct certificate is installed on the printer

For information on installing, viewing, or modifying certificates, see "Creating and modifying digital certificates" on page 14.

Cannot find realm in the Kerberos configuration file

Add or change the realm

- If you are using simple Kerberos setup, then do the following:
  1. From the Embedded Web Server, navigate to the configuration page for the application:
     Apps > **Smart Card Authentication Client** > **Configure**
  2. From the Simple Kerberos Setup section, in the Realm field, add or change the realm. The realm must be typed in uppercase.

     Note: The simple Kerberos setup does not support multiple Kerberos realm entries. If multiple realms are needed, then install a Kerberos configuration file containing the necessary realms.
  3. Click **Apply**.
- If you are using the device Kerberos setup file, then add or change the realm in the file. The realm must be typed in uppercase. When you are finished, reinstall the file on the printer.

Cannot access individual applications and functions on the printer

Try one or more of the following:

Allow secure access to applications or functions

For more information, see “Securing access to individual applications and functions” on page 33.

If the user belongs to an Active Directory group, then make sure that the group is authorized to access the applications and functions

LDAP issues

LDAP lookups fail

Try one or more of the following:

Make sure 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 it in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Security**.
2. From the Network Accounts section, click **Kerberos**.
3. From the Miscellaneous Settings section, select **Disable Reverse IP Lookups**.
4. Click **Save and Verify**.

If the LDAP server requires SSL, then enable SSL for LDAP lookups

1. From the Embedded Web Server, navigate to the configuration page for the application:
   Apps > **Smart Card Authentication Client** > **Configure**
2. From the Advanced Settings section, select **Use SSL for User Info**.
3. Click **Apply**.

Narrow the LDAP search base to the lowest possible scope that includes all necessary users

Make sure that all LDAP attributes that are being searched for are correct

Audit log

The security audit log is a record of security-related events. The log is stored locally in the device, and can be exported through e-mail or browsed on request. Log records can be sent to an external Syslog server while they are generated.

The basic format of the log records is defined in RFC5424. The following is the generic log format:

<PRI>VERSION TIMESTAMP HOSTNAME APPNAME PROCID <MSGID> [SD-ELEMENT] MSG

Where:

PRI is a priority value that is a two- or three-digit number that is defined in RFC5424. The value must be enclosed in **<** and **>**. The severity of the event is part of the input to the calculation of this number.

VERSION is a value of 1 that is the version of the specification that is used for defining the log file.

TIMESTAMP is the ISO 8601 time in ([YYYY-MM-DD]T[hh:mm:ss]) format.

HOSTNAME is the host name or IP address of the device.

APPNAME is the application name indicating the process that triggered the event log message.

PROCID is the process ID that is generally specified as 0, but may be another valid process ID for some applications.

MSGID is a text string that is defined within each event. The string must be enclosed in **<** and **>**. It provides more information about the event.

[SD-ELEMENT] is a structured data element that consists of one EventNum value followed by zero or more name-value pairs that provide detailed log information.

MSG contains the Event Name and Event Message fields described in the individual event definitions.

Auditable event	Sample audit message
Job completed	**<53>1 2017-10-29T15:05:59Z CX725 jobmanager 0 <job> [event17375@641 JobId="105" Job_Type="InternalPrintWorkflow"] Job Completed:**
Job started	**<53>1 2017-10-21T18:12:27Z CX725 jobmanager 0 <job> [event17327@641 JobId="38" Job_Type="FaxSendWorkflow"] Job Started:**
Successful user identification and authentication	**<53>1 2017-10-21T16:17:30Z CS820 auth 0 <web login> [event11527@641 SessionId="Fak4tZcHTBH0L6Cs" Auth_Method="Username/Password" Username="admin" UniqueUserId="69901267-0520-460f-baf6-6bc56180e730" Fullname="Administrator"] Login successful: 'admin'**
Unsuccessful user authentication	**<52>1 2017-11-13T19:31:37Z CX922 auth 0 <web login> [event47@641 Auth_Method="Username/Password"] Login failed: 'admin'**
Unsuccessful user identification	**<52>1 2017-11-30T14:45:22Z CX820 auth 0 <web login> [event2744@641 Auth_Method="Username/Password"] Login failed: 'bogus'**

Auditable event	Sample audit message
Use of management functions	**<53>1 2017-11-14T19:07:52Z CX922 auth 0 <setting> [event75@641 SessionId="h.8oL7lB3ZcK6Rbv"] Permission 'fax' added for LDAP group: 'Users'**
Modification to the group of users that are part of a role	**<53>1 2017-10-21T16:07:20Z CX820 auth 0 <setting> [event13960@641 SessionId="YTLGJH3SYqpyKZDQ"] Permission 'email' added for group: 'Users'**
Changes to the time	**<53>1 2017-10-01T00:31:00Z CX820 timemgr 0 <time> [event14151@641] Time changed due to time source change**
Failure to establish session	**<52>1 2017-11-15T05:34:25Z CX922 IPSec 0 <ipsec> [event219@641] peer=10.197.46.31[4500] : msg[6]=Retransmit Timeout :IKE message retransmission timed out**
Audit log cleared by an authorized administrator	**<49>1 2017-11-22T21:10:02Z CX922 Audit 675 <audit> [event1@641 SessionId="AMewwauzzBfbdjHH"] Audit Log Cleared**
Unsuccessful login attempts limit met	**<53>1 2024-04-08T13:35:52Z MX632 auth 0 <web login> [event21840@641] User is locked out: 'user1'**

Erasing keys in flash memory

The following types of keys are stored in the flash memory:

- **RSA private keys**—These keys are associated with device certificates and are overwritten when the device certificate is deleted.
- **IPSec preshared keys (PSKs)**—These keys are overwritten when the PSK setting is modified or cleared.

When the flash component performs wear leveling or garbage collection, physical copies of these keys may continue to exist inside the flash component for some time.

When any of these keys are destroyed, they are first overwritten in the flash memory with zeroes. You can see the changes in the visible storage locations for these items in the flash component.

The flash component supports the TRIM command and implements garbage collection to destroy persistent copies of old storage locations when not actively engaged in other tasks. The file system that maps to the flash component and location of the keys also supports the TRIM command. The file system is configured to use the command.

Out of service erase

To wipe the flash storage:

1. From the home screen, touch **Settings** > **Device** > **Maintenance** > **Out of Service Erase**.
2. Select **Sanitize all information on nonvolatile memory**.
3. Touch **Erase**.
4. Select **Start initial setup wizard**, and then touch **Next**.
5. Touch **Start**.

   Note: This process overwrites all of flash storage with ones before reformatting.

To wipe the hard disk:

1. From the home screen, touch **Settings** > **Device** > **Maintenance** > **Out of Service Erase**.
2. Select **Sanitize all information on hard disk**.
3. Touch **Erase**.
4. Select **1 Pass Erase**, **3 Pass Erase**, or **7 Pass Erase**, and then touch **Next**.
5. Touch **Start**.

   Note: 1 Pass Erase overwrites the entire hard disk with zeroes. 3 Pass Erase overwrites the entire hard disk with 0xAA, 0x55, and then a random value (DoD 5220-22.M). 7 Pass Erase overwrites the entire hard disk with zeroes, 0xFF, random value, 0x96, 0xAA, 0x55, and then a random value (DoD 5220-22.M ECE).

User responsibilities

When a user releases a held print job, makes a copy, or sends a fax or email, it is the user's responsibility to make sure that the job is completely printed or sent before logging out from the panel and physically leaving the device. Failure to do so may result in the ability for another user to cancel the job or view printed output.

Notices

Edition notice

August 2024

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, go to **http://support.lexmark.com**.

For information on Lexmark's privacy policy governing the use of this product, go to **www.lexmark.com/privacy**.

For information on supplies and downloads, go to **www.lexmark.com**.

© **2016 Lexmark International, Inc.**

All rights reserved.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

Lexmark and the Lexmark logo are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Active Directory and Windows are trademarks of the Microsoft group of companies.

All other trademarks are the property of their respective owners.

Index

A

access controls 33
  understanding 30
accessing the Embedded Web Server 8
Active Directory
  creating login method 28
  deleting login method 28
  editing login method 28
advanced settings
  configuring 32
AirPrint
  disabling 13
applications
  securing 33
assumptions 6
attaching a lock 9
audit log 37
  overview 37
audit logging
  configuring 18
authentication and authorization options 31

C

cannot access applications or functions on the printer 36
cannot detect the card reader 34
cannot find realm in the Kerberos configuration file 35
cannot generate or read certificate information from card 35
cannot read the smart card 34
card is locked out 34
card reader not detected 34
certificate error 35
certificates
  creating and modifying 14
change history 4
checklist
  configuration 10
configuration
  checking firmware before 8
  checking physical interfaces before 8
configuration checklist 10
configuring login restrictions 23
configuring NTP settings 17
configuring print permissions 23
configuring the minimum password length 22
configuring the system clock manually 17
configuring time source settings 17
creating an Active Directory login method 28
creating groups
  local accounts 24
creating Kerberos login method 27
creating LDAP login method 25
creating LDAP+GSSAPI login method 25
creating local accounts 24
  password 24
  user name 24

D

data files
  erasing 13
date and time settings 17
default login methods
  setting 31
deleting an Active Directory login method 28
deleting LDAP login method 27
deleting LDAP+GSSAPI login method 27
deleting local account groups 25
deleting local accounts
  password 24
  PIN 24
  user name 24
  user name and password 24
digital certificates
  creating and modifying 14
disabling AirPrint 13
disabling flash drive access 13
disabling the host USB 12
disabling the Intelligent Storage Drive 23
disabling ThinPrint 12
disabling unused applications 33
Display Customization
  enabling 32
domain certificate error 35
domain controller certificate not installed 35

E

e-mail
  configuring 20
editing an Active Directory login method 28
editing local account groups 25
editing local accounts
  password 24
  PIN 24
  user name 24
  user name and password 24
Embedded Web Server
  accessing 8
encrypting network data 16
encryption
  enabling 11, 12
  IPsec 16
environment
  operating 6
erasing keys in flash memory 39
erasing temporary data files 13
error reading the smart card 34
error while reading card 34
e-mail function
  securing 33

F

fax forwarding 21
fax settings
  driver to fax 21
  fax forwarding 21
  held faxes 21
fax storage location
  setting 21
firmware
  checking 8
  updating 9
flash drive access
  disabling 13
functions
  securing 33

H

held faxes 21
held jobs
  securing 33
hiding protected home screen icons 13
holding all jobs 13
home screen 7
  securing access 32
home screen icons
  hiding 13
host USB
  disabling 12
hosts file
  installing 32

I

Intelligent Storage Drive
  disabling 23
interfaces
  checking during preconfiguration 8
IPsec
  setting up 16

J

jobs
  holding 13

K

Kerberos
  creating login method 27
keyboard on the display
  using 7
keys
  erasing in flash memory 39

L

LDAP
  creating login method 25
  deleting login method 27
LDAP lookups fail 36
LDAP+GSSAPI
  creating login method 25
  deleting login method 27
local accounts
  creating 24
  creating groups 24
  creating user name 24
  deleting groups 25
  deleting password 24
  deleting PIN 24
  deleting user name 24
  deleting user name and password 24
  editing groups 25
  editing password 24
  editing PIN 24
  editing user name and password 24
lock
  attaching 9
logging
  configuring the security audit log 18
login method
  creating Active Directory 28
  creating LDAP 25
  creating LDAP+GSAAPI 25
  deleting Active Directory 28
  deleting LDAP 27
  deleting LDAP+GSSAPI 27
  editing Active Directory 28
login restrictions
  configuring 23
login screen settings
  configuring 31

M

minimum password length
  configuring 22
mirror encryption
  enabling 11, 12
missing Kerberos realm 35
multifunction products 6

N

network adapter
  setting 12
NTP settings
  configuring 17

O

objectives 6
operating environment 6
Out of Service Erase 40
overview 6

P

physical configuration checklist 8
physical interfaces
  checking during preconfiguration 8
port access
  shutting down 17
preconfiguration tasks
  checking firmware 8
  checking physical interfaces 8
print permissions
  configuring 23
printer home screen does not lock 35
printers
  supported 6
protected home screen icons
  hiding 13

R

realm not found 35

S

securing
  applications 33
  e-mail function 33
  held jobs 33
  home screen 32
  printer functions 33
security
  reset jumper on the controller board 22
  security audit log 18
security audit log
  configuring 18
security certificates
  creating and modifying 14
security objectives 6
security reset jumper
  enabling 22
setting default login methods 31
setting the fax storage location 21
shutting down port access 17
single-function printers
  supported 6
SMTP settings
  configuring 20
supported printers 6
syslog
  configuring 18
system clock
  configuring 17

T

ThinPrint
  disabling 12
time source settings
  configuring 17
touch screen
  using 7
troubleshooting
  cannot access applications or functions on the printer 36
  cannot detect the card reader 34
  cannot find realm in the Kerberos configuration file 35
  cannot generate or read certificate information from card 35
  cannot read the smart card 34
  card reader not detected 34
  certificate error 35
  domain certificate error 35
  domain controller certificate not installed 35
  error reading the smart card 34
  LDAP lookups fail 36
  missing Kerberos realm 35
  printer home screen does not lock 35
  realm not found 35
  user is locked out 34

U

unauthorized user 36
understanding access controls 30
unused applications
  disabling 33
updating firmware 9
  flash file 9
user is locked out 34
user responsibility 41