Common Criteria

Installation Supplement and Administrator Guide

September 2015 **www.lexmark.com**

3077517-001

Contents

Overview and first steps

Overview

This guide describes how to configure a supported Lexmark™ printer to reach Common Criteria *Evaluation Assurance Level 2* (EAL 2). Carefully follow the instructions in this guide to make sure that the device meets the requirements of the evaluation.

Using this guide

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* (EWS) 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*. For information on using the printer control panel, see "Appendix A: Using the touch screen" on page 42.

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

Supported printers

MFPs with a hard disk

- Lexmark CX510h
- Lexmark MX511h
- Lexmark MX611h
- Lexmark MX710h
- Lexmark MX711h
- Lexmark MX810
- Lexmark MX811
- Lexmark MX812
- Lexmark MX910
- Lexmark MX911
- Lexmark MX912
- Lexmark XM7155
- Lexmark XM7163
- Lexmark XM7170
- Lexmark XM9145
- Lexmark XM9155
- Lexmark XM9165
- Lexmark XC2132

MFPs without a hard disk

- Lexmark CX410
- Lexmark CX510
- Lexmark MX410
- Lexmark MX510
- Lexmark MX511
- Lexmark MX610
- Lexmark MX611
- Lexmark MX710
- Lexmark MX711
- Lexmark XM1145
- Lexmark XM3150
- Lexmark XM5163
- Lexmark XM5170

SFPs

- Lexmark CS510
- Lexmark M3150
- Lexmark M5155
- Lexmark M5163
- Lexmark M5170
- Lexmark MS610E
- Lexmark MS810E
- Lexmark MS812E

Note: MFPs support copy, e-mail, fax, and printing features. SFPs support printing features only. Printers with a hard disk support hard disk features. This guide describes the configuration of features that are not available on 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 provides protection from unauthorized access to printer external interfaces.
- The administration platform and local area network are physically and logically secured.
- Authorized administrators are trained and are capable of performing tasks related to the installation, configuration, operation, and maintenance of the network environment including—but 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 provides the ability to identify and authenticate users whose accounts are defined externally (LDAP, Kerberos, etc.).

- When an administrator configures *Network Time Protocol* (NTP), the operating environment provides reliable time stamps.
- Printer 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.

Before configuring the printer (required)

Before beginning configuration tasks, you must:

- Verify that no optional interfaces are installed
- Verify the firmware version
- Attach a lock to the printer
- Set fax storage location
- Encrypt the hard disk

Verifying physical interfaces and installed firmware

1. Inspect the printer to verify that only one network interface is installed. There should be no optional network, parallel, or serial interfaces.

   Note: USB ports that perform document processing functions are disabled at the factory.

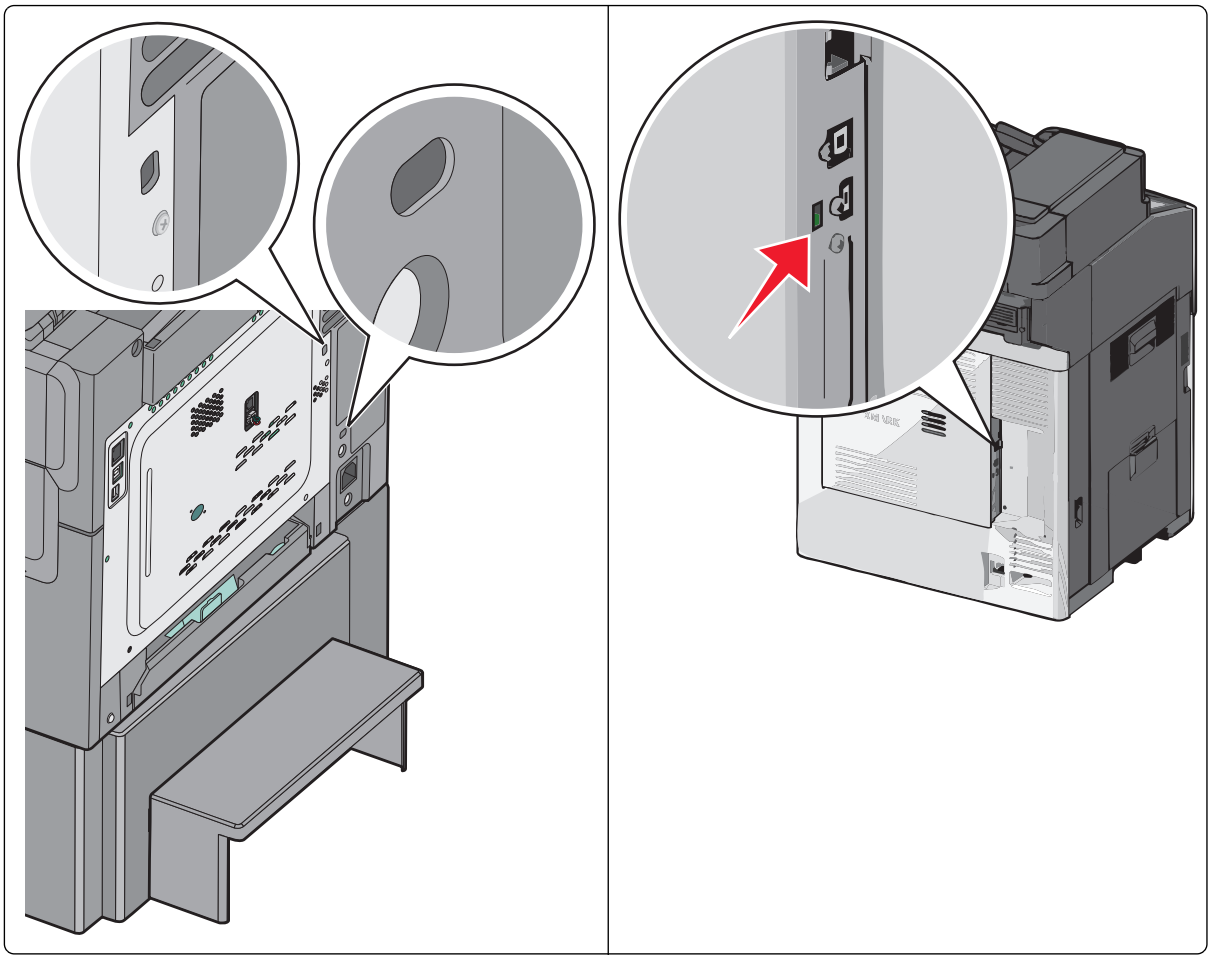
2. Turn the printer on using the power switch.
3. From the home screen, touch  > **Reports** > **Menu Settings Page**. Several pages of device information will print.
4. In the Installed Features section, verify that no Download Emulator (DLE) option cards have been installed.
5. If you find additional interfaces, or if a DLE card has been installed, then contact your Lexmark representative before proceeding.
6. To check the firmware version, under Device Information, locate **Base** = and **Network** =.
7. To verify that the Base and Network values are correct and up-to-date, contact your Lexmark representative.

Attaching a lock

Once a lock is attached, the metal plate and controller board cannot be removed, and the security jumper cannot be accessed without causing visible damage to the device.

1. Make sure that the printer case is closed.
2. Locate the security slot, and then attach a lock. It is the same type of security slot found on most laptop computers and can normally be found on the back of the printer near an outside edge.

   The following illustrations show the most common security slot locations:



Encrypting the hard disk

Hard disk encryption helps prevent the loss of sensitive data in the event your printer—or its hard disk—is stolen.

Note: Disk encryption can take several minutes to complete.

1. Turn off the printer using the power switch.
2. Simultaneously press and hold the **2** and **6** keys on the numeric keypad while turning the printer back on. It takes approximately a minute to boot into the Configuration menu.

   When the printer is ready, the touch screen displays a list of functions instead of standard home screen icons such as Copy and Fax.
3. Verify that the printer is in Configuration mode by locating the **Exit Config Menu** icon in the lower-right corner of the touch screen.
4. Scroll through the configuration menus to locate the Fax Storage Location menu.
   a. Touch **Fax Storage Location**.
   b. Set Fax Storage Location to **Disk**, and then touch **Submit**.
      The printer returns to the main Configuration menu.
5. Scroll through the configuration menus to locate the Disk Encryption menu.

   Warning: Enabling disk encryption will erase the contents of the hard disk.

6 Touch **Disk Encryption** > **Enable**.

The following message appears: **`Contents will be lost. Continue?`**

- Touch **Yes** to proceed with disk wiping and encryption. A status bar will indicate the progress of the encryption task. Disk encryption can take several hours to complete.

  After the disk is encrypted, the printer returns to the Enable/Disable screen.

  Warning: Do not turn off the printer during the encryption process. Doing so may result in loss of data.

7 Touch **Back**, and then touch **Exit Config Menu**.

The printer undergoes a power-on reset, and then returns to normal operating mode.

Disabling the USB buffer

Disabling the USB buffer disables the USB host port on the back of the device.

1 From the home screen, touch  > **Network/Ports** > **Standard USB**.

2 In the USB Buffer field, enter **0** or select **Disabled**.

3 Touch **Submit**.

Installing the minimum configuration

You can achieve an evaluated configuration on a non-network (standalone) printer in just a few steps. For this configuration, all tasks are performed at the printer, using the touch screen.

Configuring the printer

Configuration checklist

This checklist outlines the steps required to implement an evaluated configuration on a standalone printer. For information about additional configuration options, see “Administering the printer” on page 16.

After completing the preconfiguration tasks found in “Before configuring the printer (required)” on page 7, continue with this section to configure the settings needed to achieve the evaluated configuration for a standalone printer:

1. Set up disk wiping.
2. Create user accounts.
3. Create security templates.
4. Restrict access to device functions.
5. Disable home screen icons.

Configuring disk wiping

Disk wiping is used to remove residual confidential material from the printer. Disk wiping uses random data patterns to securely overwrite files stored on the hard drive that have been marked for deletion. Multi-pass wiping is compliant with the DoD 5220.22-M standard for securely erasing data from a hard disk.

1. From the home screen, touch  > **Security** > **Disk Wiping**.
2. Make sure Wiping Mode is set to **Auto**.

   Note: By default, Wiping Mode is set to Auto, and it cannot be modified.
3. Set Automatic Method to **Multi-pass**.
4. Touch **Submit**.

Enabling the backup password (optional)

Note: Using a backup password is strongly discouraged because it can degrade the overall security of your printer.

Make sure the backup password:

- Contains a minimum of eight characters
- Contains at least one lowercase letter, one uppercase letter, and one non-alphabetic character
- Is not a dictionary word or a variation of the user ID

1. From the home screen, touch  > **Security** > **Edit Security Setups** > **Edit Backup Password** > **Password**.
2. Type the password you want to use, and then touch **Done**.
3. Retype the password, and then touch **Done** to save the new password and return to the Edit Backup Password screen.
4. Set Use Backup Password to **On**.
5. Touch **Submit**.

Creating user accounts

To create accounts for use with the evaluated configuration, assign user IDs, passwords, and groups to users. When configuring security templates, select one or more of these groups, and then apply a security template to each device function. The printer supports up to 250 user accounts and 32 user groups.

Step 1: Defining groups

1. From the home screen, touch  > **Security** > **Edit Security Setups** > **Edit Building Blocks** > **Internal Accounts** > **General Settings** > **Groups for Internal Accounts** > **Add Entry**.
2. In the Name field, type **Administrator_Only**.
3. Touch **Done** to save this group and return to the Groups for Internal Accounts screen.
4. Touch **Add Entry**.
5. In the Name field, type **Authenticated_Users**.
6. Touch **Done** to save this group.

Note: To allow access to some administrative functions while restricting others, create more groups, such as “Administrator_Reports” and “Administrator_Security.”

Scenario 1: Using two groups

Select	For
Administrator_Only	Administrators allowed to access all device functions
Authenticated_Users	• Administrators • Non-administrators (all other users)

Scenario 2: Using multiple groups

Select	For
Administrator_Only	Administrators allowed to access all device functions
Administrator_Reports	• Administrators allowed to access all device functions • Administrators allowed to use device functions and access the Reports menu

Select	For
Administrator_Security	• Administrators allowed to access all device functions • Administrators allowed to use device functions and access the Security menu
Authenticated_Users	• Administrators allowed to access all device functions • Administrators allowed to use device functions and access the Reports menu • Administrators allowed to use device functions and access the Security menu • Non-administrators (all other users)

Step 2: Creating accounts

1. From the home screen, touch  > **Security** > **Edit Security Setups** > **Edit Building Blocks** > **Internal Accounts** > **General Settings**.
2. Set Required User Credentials to **User ID and password**, and then touch **Submit**. The printer returns to the Internal Accounts screen.
3. Select **Manage Internal Accounts** > **Add Entry**.
4. Type the user's account name (example: “Jack Smith”), and then touch **Done**.
5. Type a user ID for the account (example: “jsmith”), and then touch **Done**.
6. Type a password for the account, and then touch **Done**.

   Make sure the password:
   - Contains a minimum of eight characters.
   - Contains at least one lowercase letter, one uppercase letter, and one non-alphabetic character.
   - Is not a dictionary word or a variation of the user ID.
7. Retype the password, and then touch **Done**.
8. Type the user's e-mail address (example: “jsmith@company.com”), and then touch **Done**.
9. From the Set Groups screen, add one or more groups, as follows:
   - For users who should have administrator privileges, select the Authenticated_Users group and one or more Administrator groups if necessary. If you have created multiple groups to allow access to specific device functions, then select all groups in which the administrator should be included.
   - For all other users, add only the Authenticated_Users group.
10. Touch **Done**.
11. If necessary, repeat step 3 through step 8 to add more users.

Creating security templates

Assign a security template to each device function to restrict user access to that function. At a minimum, create two security templates: one for "Administrator_Only" and one for "Authenticated_Users." To allow access to some administrative functions while restricting others, create more security templates, such as “Administrator_Reports” or “Administrator_Security.” Each template is populated with groups containing users authorized to access the functions protected by that template.

1. From the home screen, touch > **Security** > **Edit Security Setups** > **Edit Security Templates** > **Add Entry**.
2. Type a unique name to identify the template. Use a descriptive name, such as ”Administrator_Only” or “Authenticated_Users,” and then touch **Done**.
3. On the Authentication Setup screen, select the internal accounts building block, and then touch **Done**.
4. On the Authorization Setup screen, select the internal accounts building block, and then touch **Done**.
5. Select one or more groups to be included in the template, and then touch **Done** .

Modifying or deleting an existing security template

Note: You can delete a security template only if it is not in use; however, security templates currently in use can be modified.

1. From the home screen, touch > **Security** > **Edit Security Setups** > **Edit Security Templates**.
2. Do one of the following:
   - To remove all security templates, touch **Delete List**.
   - To remove an individual security template, select it from the list, and then touch **Delete Entry**.
   - To modify an individual security template, select it from the list, and then touch **Open Entry**.

Controlling access to device functions

Access to device functions can be restricted by applying security templates to individual functions. For a list of access controls and what they do, see “Appendix D: Access controls” on page 46.

1. From the home screen, touch > **Security** > **Edit Security Setups** > **Edit Access Controls**.
2. Select the appropriate level of protection for each function, as specified in the following table. It may be necessary to scroll through several screens to set all access controls.
3. After assigning an appropriate security template to all functions, touch **Submit**.

Levels of protection include the following:

- **Administrator access only**—Use an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Authenticated users only**—Use an internal account or a security template, as long as it provides access to authenticated users only. These access controls must not be set to **No Security**.
- **Disabled**—Disable access to a function for all users and administrators.
- **Not applicable**—Another setting disables the function. No change is required, although we recommend setting these access controls to **Administrator access only** or **Disabled**.

Access controls and required levels of protection

Access control	Level of protection
Security Menu at the Device	Administrator access only
Security Menu Remotely	Administrator access only
Service Engineer Menus at the Device	Administrator access only
Service Engineer Menus Remotely	Administrator access only
Configuration Menu	Disabled
Paper Menu at the Device	Authenticated users only
Paper Menu Remotely	Authenticated users only
Reports Menu at the Device	Administrator access only
Reports Menu Remotely	Administrator access only
Settings Menu at the Device	Administrator access only
Settings Menu Remotely	Administrator access only
Network/Ports Menu at the Device	Administrator access only
Network/Ports Menu Remotely	Administrator access only
Manage Shortcuts at the Device	Authenticated users only
Manage Shortcuts Remotely	Authenticated users only
Supplies Menu at the Device	Authenticated users only
Supplies Menu Remotely	Authenticated users only
Option Card Configuration at the Device	Administrator access only
Option Card Configuration Remotely	Administrator access only
Web Import/Export Settings	Disabled
Apps Configuration	Administrator access only
Remote Management	Disabled
Firmware Updates	Disabled or Administrator access only
PJL Device Setting Changes	Disabled
Operator Panel Lock	Authenticated users only
Configuration File Import/Export	Disabled or Administrator access only
Internet Printing Protocol (IPP)	Disabled
Address Book	Authenticated users only
Create Profiles	Disabled
Create Bookmarks at the Device	Disabled
Create Bookmarks Remotely	Disabled
Flash Drive Print	Disabled
Flash Drive Color Printing	Disabled

Access control	Level of protection
Flash Drive Scan	Disabled
Copy Function	Authenticated users only
Copy Color Printing	Authenticated users only
Allow Flash Drive Access	Disabled
Color Dropout	Authenticated users only
E-mail Function	Authenticated users only
Fax Function	Authenticated users only
Release Held Faxes	Administrator access only
FTP Function	Disabled
Held Jobs Access	Disabled
Use Profiles	No Security
Change Language from Home Screen	Authenticated users only
Cancel Jobs at the Device	Authenticated users only
Apps 1	Authenticated users only
Apps 2–10	Administrator access only
New Apps	Administrator access only
Idle screen	Authenticated users only
Secure Held Print Jobs	Authenticated users only

Disabling home screen icons

The final step is to remove unnecessary icons from the printer home screen.

1. From the home screen, touch  > **Settings** > **General Settings** > **Home screen customization**.
2. Set the following to **Do not display**.
   - FTP
   - FTP shortcuts
   - Search Held Jobs
   - Held Jobs
   - USB Drive
   - Jobs by user

   Note: If other functions (such as Fax) are not available to users, then you can also disable the icons for those functions.
3. Touch **Submit**.

Administering the printer

This chapter describes how to configure additional settings and functions that may be available on your device.

Accessing the Embedded Web Server (EWS)

Many settings can be configured using either the EWS or the touch screen.

1. Obtain the printer IP address or host name:
   - From the printer home screen
   - From the TCP/IP section in the Network/Ports menu
   - By printing a network setup page or menu settings page, and then finding the TCP/IP section

   Notes:

   - An IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.
   - A host name must consist only of US-ASCII, alphanumeric characters, and a hyphen, such as **BOBS-PRINTER**.
2. Open a Web browser, and then type the printer IP address or host name in the address field using the secure version of the page (example: **https://*yyy.y.y.y***, where ***yyy.y.y.y*** is the IP address or host name of the printer).

   The Embedded Web Server appears.

Settings for network-connected printers

After attaching the printer to a network, you will need to configure additional settings. This section covers the basic settings required for a network-connected printer.

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

The values entered here will be present in all new certificates generated in the Certificate Management task.

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

   Note: For information about accessing the EWS, see “Accessing the Embedded Web Server (EWS)” on page 16.
2. Click **Set Certificate Defaults**.
3. Enter values in the appropriate fields:
   - **Common Name**—Type a name for the device.

     Note: Leave this field blank if you want to use the device 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 (2-character maximum).
- **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, enter an IP address using the format IP:123.123.123.123. Leave this field blank if you want to use the IPv4 address.

4 Click **Submit**.

Note: All fields accept a maximum of 128 characters, except where noted.

Creating a new certificate

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

Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 Click **Device Certificate Management** > **New**.

3 Enter values in the appropriate fields:

- **Friendly Name**—Type a name for the certificate (64-character maximum).
- **Common Name**—Type a name for the device.

  Note: Leave this field blank if you want to use the device 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 (2-character maximum).
- **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, enter an IP address using the format IP:123.123.123.123 or a DNS address using the format DNS:ldap.company.com. Leave this field blank if you want to use the IPv4 address.

4 Click **Generate New Certificate**.

Note: All fields accept a maximum of 128 characters, except where noted.

Viewing, downloading, and deleting a certificate

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

Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 Click **Device Certificate Management**.

3 Select a certificate from the list.

The details of the certificate are displayed in the Device Certificate Management window.

4 Do any of the following:

- **Delete**—Remove a previously stored certificate.
- **Download To File**—Download or save the certificate as a PEM (.cer) file.
  The contents of the file should be in the following format:

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

- **Download Signing Request**—Download or save the signing request as a .csr file.
- **Install Signed Certificate**—Upload a previously signed certificate.

Installing a CA certificate

A *Certificate Authority* (CA) certificate is required if you will be using the PKI Authentication application.

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

Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 Click **New**.

3 Click **Browse** to locate the Certificate Authority Source file, and then click **Submit**.

Note: The Certificate Authority Source file must be in PEM (.cer) format.

4 Reboot the printer by turning it off and back on using the power switch.

Setting up IPSec

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

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

Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 Select the **IPSec Enable** check box, and then click **Submit**. Your browser will return to the Security page.

3 Click **IPSec**.

4 In the Settings section, click **Certificate Validation**, and then select the **Validate Peer Certificate** check box.

5 In the Connections section, click either **Pre-Shared Key Authenticated Connections** or **Certificate Authenticated Connections**, and then click one of the numbered **Host** fields.

6 Type the IP address of the client device you want to connect to the printer.

Note: If you are using *Pre-Shared Key* (PSK) Authentication, then also type the key. Retain the key to use later when configuring client devices.

7 If necessary, configure IPSec on client devices that will connect to the printer.

8 Click **Submit**.

Disabling the AppleTalk protocol

IP is the only network protocol permitted under this evaluation. The AppleTalk protocol must be disabled.

Using the EWS

Note: For information about accessing the EWS, see “Accessing the Embedded Web Server (EWS)” on page 16.

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **AppleTalk**.
2. Verify that the Activate check box is cleared, and then click **Submit**.

Using the touch screen

1. From the home screen, touch  > **Network/Ports** > **Standard Network** > **STD NET SETUP** > **AppleTalk** > **Activate**.

   Note: It might be necessary to scroll down to find the AppleTalk selection.
2. Set Activate to **No**.
3. Touch **Submit**. The printer will return to the AppleTalk screen. From there you can touch **Back** to return to the Std Network Setup screen or the home icon to return to the home screen.

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** > **Security** > **TCP/IP Port Access**.
2. Clear the following check boxes:
   - TCP 21 (FTP)
   - UDP 69 (TFTP)
   - TCP 79 (FINGER)
   - UDP 161 (SNMP)
   - TCP 631 (IPP)
   - TCP 5000 (XML)
   - TCP 5001 (IPDS)
   - TCP 6110/UDP6100/TCP6100
   - TCP 9000 (Telnet)
   - UDP 9300/UDP 9301/UDP 9302 (NPAP)
   - TCP 9500/TCP 9501 (NPAP)
   - TCP 9600 (IPDS)
   - UDP 9700 (Plug-n-Print)
   - TCP 10000 (Telnet)
   - ThinPrint
   - TCP 65002 (WSD Print Service)
   - TCP 65004 (WSD Scan Service)
3. Click **Submit**.

Other settings and functions

Network Time Protocol

Use Network Time Protocol (NTP) to automatically sync printer date and time settings with a trusted clock so that Kerberos requests and audit log events will be accurately time-stamped.

Note: If your network uses DHCP, then verify that NTP settings are not automatically provided by the DHCP server before manually configuring NTP settings.

Using the EWS

1. From the Embedded Web Server, click **Settings** > **Security** > **Set Date and Time**.

   Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2. In the Network Time Protocol section, select the **Enable NTP** check box, and then type the IP address or host name of the NTP Server.
3. If the NTP server requires authentication, then select **MD5 key** or **Autokey IFF** from the Authentication menu.
   a. Click **Install MD5 key** or **Install Autokey IFF params**, and then browse to the file containing the NTP authentication credentials.
   b. Click **Submit**.
4. Click **Submit**.

Using the touch screen

1. From the home screen, touch  > **Security** > **Set Date and Time**.
2. Set Enable NTP to **On**.
3. Touch the **NTP Server** field, type the IP address or host name of the NTP server, and then touch **Submit**.
4. If the NTP server requires authentication, then set Enable Authentication to **On**.
5. Touch **Submit**.

Kerberos

If you are using LDAP+GSSAPI or Common Access Cards to control user access to the printer, then first configure Kerberos.

Using the EWS

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

   Note: For more information, see "Accessing the Embedded Web Server (EWS)" on page 16.

2. From the Advanced Security Setup section, click **Kerberos 5**.

3 From the Simple Kerberos Setup section, configure the following:
   - **KDC Address**—Type the IP address or host name of the KDC (Key Distribution Center) IP.
   - **KDC Port**—Type the number of the port used by the Kerberos server.
   - **Realm**—Type the realm used by the Kerberos server.

   Note: The Realm entry must be typed in all uppercase letters.

4 Click **Submit** to save the information as a krb5.conf file.

Note: Because only one krb5.conf file is used, uploading or submitting Simple Kerberos settings overwrites the configuration file.

Importing a Kerberos configuration file

Using the EWS, you can also import a krb5.conf file rather than configure the Simple Kerberos Setup.

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

   Note: For more information, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 From the Advanced Security Setup section, click **Kerberos 5**.

3 In the Import Kerberos File section, browse to your stored krb5.conf file.

4 Do one of the following:
   - Click **Submit** to upload the krb5.conf file.
   - Click **Delete File** to remove the Kerberos configuration file from the selected device.
   - Click **View File** to view the Kerberos configuration file for the selected device.
   - Click **Test Setup** to verify that the Kerberos configuration file for the selected device is functional.

   Note: After clicking **Submit**, the device automatically tests the krb5.conf file to verify that it is functional.

Using the touch screen

Simple Kerberos settings can be configured or adjusted using the touch screen.

1 From the home screen, touch  > **Security** > **Edit Security Setups** > **Edit Building Blocks** > **Simple Kerberos Setup**.

2 Type the KDC (Key Distribution Center) IP address or host name, and then touch **Done**.

3 Type the number of the port used by the Kerberos server, and then touch **Done**.

4 Type the realm used by the Kerberos server, and then touch **Done**.

   Note: The Realm entry must be typed in all uppercase letters.

Security audit logging

Using the EWS

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

   Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2 Select the **Enable Audit** check box.

3 Type the IP address or host name of the Remote Syslog Server, and then select the **Enable Remote Syslog** check box.

Note: The **Enable Remote Syslog** check box is unavailable until an IP address or host name is entered.

4 Type the Remote Syslog Port number used on the destination server.

5 For Remote Syslog Method, select **Normal UDP** or **Stunnel** (if implemented on the destination server).

6 For "Severity of events to log," select **5 - Notice**. The chosen severity level and anything higher (0–4) will be logged.

7 To send all events regardless of severity to the remote server, select the **Remote Syslog non-logged events** check box.

8 To automatically notify administrators about certain log events, type one or more e-mail addresses (separated by commas) in the "Admin's e-mail address" field, and then choose how events will be handled:

- Select **E-mail log cleared alert** if you want the printer to send an e-mail when the **Delete Log** button is clicked.
- Select **E-mail log wrapped alert** if you want the printer to send an e-mail when the log becomes full and begins to overwrite the oldest entries.
- For "Log full behavior," select **Wrap over oldest entries** or **E-mail log then delete all entries**.
- Select **E-mail % full alert** if you want the printer to send an e-mail when log storage space reaches a specified percentage of capacity.
- For "% full alert level" (1–99%), specify the percentage of log storage space that must be used before an e-mail alert is triggered.
- Select **E-mail log exported alert** if you want the printer to send an e-mail when the log file is exported.
- Select **E-mail log settings changed alert** if you want the printer to send an e-mail when log settings are changed.
- For "Log line endings," choose **LF (\n)**, **CR (\r)**, or **CRLF (\r\n)** to specify how line endings will be handled in the log file, depending on the operating system in which the file will be parsed or viewed.
- Select **Digitally sign exports** if you want the device to add a digital signature to e-mail alerts.

Note: To use e-mail alerts, click **Submit** to save changes, and then follow the **Setup E-mail Server** link to configure SMTP settings.

9 Click **Submit**.

Using the touch screen

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

2 Set Enable Audit to **Yes**.

3 Set Enable Remote Syslog to **Yes**.

4 Touch the **Remote Syslog Server** field, type the IP address or host name of the remote syslog server, and then touch **Submit**.

5 Touch the **Remote Syslog Port** field, type the remote syslog port number used on the destination server, and then touch **Submit**.

6 For Remote Syslog Method, select **Normal UDP** or **Stunnel** (if implemented on the destination server).

7 For "Log full behavior," select **Wrap over oldest entries** or **E-mail log then delete all entries**.

8 If you want the printer to automatically notify administrators of certain log events, then touch the **Admin's e-mail address** field, type one or more e-mail addresses (separated by commas), and then touch **Submit**.

9 If you want the printer to add a digital signature to e-mail alerts, then set “Digitally sign exports” to **On**.

10 For “Severity of events to log,” select **5 - Notice**. The chosen severity level and anything higher (0–4) will be logged.

11 If you want the printer to send all events regardless of severity to the remote server, then set “Remote Syslog non-logged events” to **Yes**.

12 If you want the printer to automatically notify administrators of certain log events, then adjust the following settings:

- To send an e-mail when the **Delete Log** button is clicked, set “E-mail log cleared alert” to **Yes**.
- To send an e-mail when the log becomes full and begins to overwrite the oldest entries, set “E-mail log wrapped alert” to **Yes**.
- To send an e-mail when log storage space reaches a specified percentage of capacity, set “E-mail % full alert” to **Yes**.
- For “% full alert level,” specify the percentage of log storage space that must be used before an e-mail alert is triggered.
- To send an e-mail when the log file is exported, set “E-mail log exported alert” to **Yes**.
- To send an e-mail when log settings are changed, set “E-mail log settings changed alert” to **Yes**.
- For ”Log line endings,” select **LF (\n)**, **CR (\r)**, or **CRLF (\r\n)** to specify how line endings will be handled in the log file, depending on the operating system in which the file will be parsed or viewed.

13 Touch **Submit**.

Note: To use e-mail alerts, you must also configure SMTP settings. For information about SMTP settings, see “E-mail” on page 23.

E-mail

User data sent by the printer using e-mail must be sent as an attachment.

Using the EWS

1 From the Embedded Web Server, click **Settings** > **E-mail/FTP Settings** > **E-mail Settings**.

Note: For information about accessing the EWS, see “Accessing the Embedded Web Server (EWS)” on page 16.

2 Under E-mail Settings, select **Attachment** for “E-mail images sent as.”

3 Under Web Link Setup, verify the following settings:

- **Server**—This must be blank.
- **Login**—This must be blank.
- **Password**—This must be blank.
- **Path**—This must be “/”.
- **File Name**—This must be “image” (default).
- **Web Link**—This must be blank.

SMTP settings

1. From the Embedded Web Server, click **Settings** > **E-mail/FTP Settings** > **SMTP Setup**.
2. Under SMTP Setup, type the IP address or host name of the Primary SMTP Gateway the printer will use for sending e-mail.
3. Type the Primary SMTP Gateway Port number of the destination server.
4. If you are using a secondary or backup SMTP server, then type the IP address or host name and SMTP port for that server.
5. For SMTP Timeout, type the number of seconds (5–30) the device will wait for a response from the SMTP server before timing out.
6. If you want to receive responses to messages sent from the printer (in case of failed or bounced messages), then type a Reply Address.
7. From the Use SSL/TLS list, select **Disabled**, **Negotiate** or **Required** to specify whether e-mail will be sent using an encrypted link.
8. If the SMTP server requires user credentials, then select an authentication method from the SMTP Server Authentication list.
9. From the Device-Initiated E-mail list, select **Use Device SMTP Credentials**.
10. From the User-Initiated E-mail list, select the option most appropriate for your network or server environment.
11. If the printer must provide credentials in order to send e-mail, then enter the information appropriate for your network under Device Credentials.

Using the touch screen

1. From the home screen, touch  > **Settings** > **E-mail Settings** > **E-mail Server Setup** > **Web Link Setup**.
2. Verify the following settings:
   - **Server**—This must be blank.
   - **Login**—This must be blank.
   - **Password**—This must be blank.
   - **Path**—This must be “/”.
   - **File Name**—This must be “image” (default).
   - **Web Link**—This must be blank.
3. Touch **Back**, and then touch **Back** again to return to the E-mail Settings screen.
4. Set **E-mail images sent as** to **Attachment**.
5. Touch **Submit**.

SMTP settings

1. From the home screen, touch  > **Network/Ports** > **SMTP Setup**.
2. Touch the **Primary SMTP Gateway** field, type the IP address or host name of the primary SMTP gateway the printer will use for sending e-mail, and then touch **Submit**.

3 Touch the **Primary SMTP Gateway Port** field, type the primary SMTP gateway port number of the destination server, and then touch **Submit**.

4 If you are using a secondary or backup SMTP server, then provide the IP address or host name and the SMTP port number for that server.

5 For SMTP Timeout, select the number of seconds (5–30) the printer will wait for a response from the SMTP server before timing out.

6 If you want to receive responses to messages sent from the printer (in case of failed or bounced messages), then provide a Reply Address.

7 Set Use SSL to **Disabled**, **Negotiate** or **Required** to specify whether e-mail will be sent using an encrypted link.

8 If the SMTP server requires user credentials, then select a method for SMTP Server Authentication.

9 Set Device-Initiated E-mail to **Use Device SMTP Credentials**.

10 For User-Initiated E-mail, select the option most appropriate for your network or server environment.

11 If the printer must provide credentials in order to send e-mail, then enter the information appropriate for your network in the “Device Userid,” “Device password,” and “Kerberos 5 Realm” or “NTLM Domain” fields.

12 Touch **Submit**.

Fax

If your printer includes fax capabilities and is attached to a phone line, then you must disable fax forwarding, enable held faxes, and disable driver to fax.

Using the EWS

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

Note: For information about accessing the EWS, see “Accessing the Embedded Web Server (EWS)” on page 16.

2 Under Fax Receive Settings, click **Holding Faxes**.

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

4 Click **Submit** to save your changes and return to the Settings page.

5 Under Fax Send Settings, clear the **Driver to fax** check box.

6 Under Fax Receive Settings, select **Print** from the Fax Forwarding list.

7 Click **Submit**.

Using the touch screen

1 From the home screen, touch  > **Settings** > **Fax Settings** > **Analog Fax Setup** > **Fax Receive Settings** > **Holding Faxes**.

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

3 Touch **Submit** to save your changes and return to the Fax Receive Settings screen.

4 Set Fax Forwarding to **Print**.

5 Touch **Submit** to save your changes and return to the Analog Fax Setup screen.

6 Touch **Fax Send Settings**.

7 Set “Driver to fax” to **No**.

8 Touch **Submit**.

Setting up a fax storage location (optional)

1 Turn off the printer using the power switch.

2 Simultaneously press and hold the **2** and **6** keys on the numeric keypad while turning the printer back on. It takes approximately a minute to boot into the Configuration menu.

When the printer is ready, the touch screen shows a list of functions instead of standard home screen icons such as Copy and Fax.

3 Verify that the printer is in Configuration mode by locating the **Exit Config Menu** icon in the lower right corner of the touch screen.

4 Touch **Fax Storage Location**.

5 Set Fax Storage Location to **Disk**, and then touch **Submit**.

The printer returns to the main Configuration menu.

6 Touch **Back**, and then touch **Exit Config Menu**.

The printer undergoes a power-on reset and then returns to normal operating mode.

Configuring security reset jumper behavior

The security reset jumper is a hardware jumper located on the motherboard 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  > **Security** > **Miscellaneous Security Settings**.

2 For Security Reset Jumper, select any of the following:

- **Access controls = “No security”**—This removes security only from function access controls.
- **Reset factory security defaults**—This restores all security settings to default values.
- **No Effect**—This removes access to *all* security menus (use with caution).

3 Touch **Submit** to save the changes.

Warning—Potential Damage: If **No Effect** is selected and the password (or other applicable credential) is lost, then you will not be able to access the security menus. To regain access to the security menus, a service call will be required to replace the device RIP card (motherboard).

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: Internal Accounts, LDAP+GSSAPI, and Smart Card Authentication.

Creating user accounts through the EWS

Creating internal (device) accounts for use with the evaluated configuration involves not only assigning a user ID and password to each user, but also segmenting users into groups. When configuring security templates, you will select one or more of these groups, and then you will apply a security template to each device function to control access to that function. The printer supports a maximum of 250 user accounts and 32 user groups.

Example: Employees in the warehouse will be given access to black-and-white printing only, administrative office staff will be able to print in black and white and send faxes, and employees in the marketing department will have access to black-and-white printing, color printing, and faxing.

Security template	Groups included in template	Template will be applied to
basic_user	• Warehouse • Office • Marketing	Copy Function
color_user	Marketing	Copy Color Printing
fax_user	• Office • Marketing	Fax Function

When creating internal accounts in Scenario 1, you would select the group that corresponds to the user's department.

Security template	Groups included in template	Template will be applied to
basic_user	black_and_white	Copy Function
color_user	color	Copy Color Function
fax_user	fax	Fax Function

When creating internal accounts in Scenario 2, you would select the following groups for each type of user:

- Warehouse employee—Black_and_white group only.
- Office employee—Black_and_white group, fax group.
- Marketing employee—Black_and_white group, color group, fax group.

Step 1: Defining groups

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

   Note: For information about accessing the EWS, see "Accessing the Embedded Web Server (EWS)" on page 16.

2. Under Advanced Security Setup, Step 1, click **Internal Accounts**.
3. Click **Setup groups for use with internal accounts**.
4. Type a Group Name.
5. Click **Add**.
6. If necessary, repeat the steps to add more groups.

Step 2: Creating accounts

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, Step 1, click **Internal Accounts**.

3 From the Required User Credentials list, select **User ID and password**.

4 Click **Submit**.

5 Click **Settings** > **Security** > **Security Setup** > **Internal Accounts**.

6 Click **Add an Internal Account**, and then provide the information needed for each account:

- **Account Name**—Type the user's account name (example: “Jack Smith”).
- **User ID**—Type an ID for the account (example: “jsmith”).
- **Password**—Passwords must:
  - Contain a minimum of eight characters.
  - Contain at least one lowercase letter, one uppercase letter, and one non-alphabetic character.
  - Not be dictionary words or a variation of the user ID.
- **Re-enter password**—Retype the password.
- **E-mail**—Type the user's e-mail address (example: “jsmith@company.com”).
- **Groups**—Select the group or groups to which the account should belong. Hold down the **Ctrl** key to select multiple groups for the account.

7 Click **Submit**.

Configuring LDAP+GSSAPI

On networks running Active Directory, you can use LDAP+GSSAPI to take advantage of authentication and authorization services already deployed on the network. User credentials and group designations can be pulled from your existing system, making access to the printer as seamless as other network services.

Supported devices can store a maximum of five LDAP+GSSAPI configurations. Each configuration must have a unique name.

Note: You must configure Kerberos before setting up LDAP+GSSAPI. For information about configuring Kerberos, see “Kerberos” on page 20.

Using the EWS

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

Note: For information on accessing the EWS, see “Accessing the Embedded Web Server (EWS)” on page 16.

2 Under Advanced Security Setup, Step 1, click **LDAP+GSSAPI**.

3 Click **Add an LDAP+GSSAPI Setup**.

4 Configure the following LDAP+GSSAPI Server Setup settings:

General Information

- **Setup Name**—Type a name that will be used to identify this particular LDAP+GSSAPI Server Setup when creating security templates.
- **Server Address**—Type the IP address or the host name of the LDAP server where authentication will be performed.

  Note: For LDAP+GSSAPI, the LDAP server can be the domain controller or a separate server.
- **Server Port**—Type the port number used to communicate with the LDAP server. The default LDAP port is 389.

- **Use SSL/TLS**—Select **None**, **SSL/TLS** (Secure Sockets Layer/Transport Layer Security), or **TLS**.
- **Userid Attribute**—Type **sAMAccountName** (default), **uid**, **userid**, **user-defined**, or **cn** (common name).
- **Mail Attribute**—Type the mail attribute.
- **Full Name Attribute**—Type the full name attribute.
- **Search Base**—Specify the node in the LDAP server where user accounts reside. Multiple search bases can be entered, separated by semicolons.

  Note: A search base consists of multiple attributes, such as cn (common name), ou (organizational unit), o (organization), c (country), or dc (domain), separated by semicolons.
- **Search Timeout**—Specify a value from 5 to 30 seconds.
- **Use Kerberos Service Ticket**—If selected, then a Kerberos ticket is presented to the LDAP server using the GSSAPI protocol to obtain access.

Device Credentials (optional)

- **Use Active Directory Device Credentials**—If selected, then user credentials and group designations can be pulled from the existing network comparable to other network services.
- **MFP's Kerberos Username**—Type the distinguished name of the print server or servers.
- **MFP's Password**—Type the Kerberos password for the print servers.

Search specific object classes (optional)

- **person**—If selected, then the "person" object class will also be searched.
- **Custom Object Class**—If selected, then this custom search object class will also be searched. The administrator can define up to three custom search object classes.

LDAP Group Names

- Administrators can associate as many as 32 named groups stored on the LDAP server by entering identifiers for those groups under the Group Search Base list. Both the **Short name for group** and **Group Identifier** must be provided.
- When creating security templates, the administrator can pick groups from this setup for controlling access to device functions.

5 Click **Submit**.

Using the touch screen

1 From the home screen, touch  > **Security** > **Edit Security Setups** > **Edit Building Blocks** > **LDAP+GSSAPI**.

2 Touch **Add Entry**.

3 Type a setup name, and then touch **Done**. This name will be used to identify this particular LDAP+GSSAPI Server Setup when creating security templates.

4 For Server Address, type the IP address or host name of the LDAP server where authentication will be performed, and then touch **Done**. The printer returns to the General Information screen.

5 Touch **General Information**, and then adjust the following settings:

- **Server Port**—Type the port number used to communicate with the LDAP server. The default LDAP port is 389.
- **Use SSL/TLS**—Select **None**, **SSL/TLS** (Secure Sockets Layer/Transport Layer Security), or **TLS**.

- **Userid Attribute**—Type **sAMAccountName** (default), **uid**, **userid**, **user-defined**, or **cn** (common name).
- **Mail Attribute**—Type the mail attribute.
- **Full Name Attribute**—Type the full name attribute.
- **Search Base**—Specify the node in the LDAP server where user accounts reside. Multiple search bases can be entered, separated by semicolons.

  Note: A search base consists of multiple attributes, such as cn (common name), ou (organizational unit), o (organization), c (country), or dc (domain), separated by semicolons.
- **Search Timeout**—Specify a value from 5 to 30 seconds.

Touch **Submit** to save the settings and return to the General Information screen.

6 Touch **Device Credentials**. If necessary, adjust the following settings:

- **Use Active Directory Device Credentials**—Touch to select or clear. When the printer authenticates to the LDAP server, it can provide Active Directory device credentials in addition to supporting anonymous binding or the specified credentials in the MFP's Kerberos Username and MFP's Password fields.
- **MFP's Kerberos Username**—Type the distinguished name of the print server or servers.
- **MFP's Password**—Type the Kerberos password for the print servers.

Touch **Done** to save the settings and return to the General Information screen.

7 Touch **Search Specific Object Classes**. If necessary, adjust the following settings:

- **person**—Select **On** or **Off** to specify whether the “person” object class will also be searched.
- **Custom Object Classes**—For each custom object class you want to define, select **On** or **Off** to specify whether that class will be searched, and then type a name for that class.

Touch **Submit** to save the settings and return to the General Information screen.

8 Select **LDAP Group Names**. If necessary, adjust the following settings:

- **Group Search Base**—Type the name of the group search base, and then touch **Submit**. Touch **Back** to return to the LDAP Group Names screen.
- **GSSAPI Group (1–32)**—For each group you want to define, select a numbered group, and then specify the “Short name for group” and “Group Identifier.” Touch **Done** to save your changes and return to the LDAP Group Names screen.

When creating security templates, the administrator can pick groups from this setup for controlling access to device functions.

Configuring Smart Card Authentication Client

Configuring login screen settings

You can use the login screen settings to choose how users will be allowed to log in to the printer and whether they will be prompted for a PIN or a password after inserting a Smart Card.

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Login Screen heading, from the Login Type menu, select **Smart Card Only**.

3 Set User Validation Mode to **Active Directory**.

4 Click **Apply**.

Controlling access to device functions

Configuring Secure Held Print Jobs

Configuring and securing the application

1. From the Embedded Web Server, access the configuration page for the Secure Held Print Jobs application.
2. Specify the text and image that you want to appear on your home screen.

   Note: Some applications require changing the settings from the profile page.
3. From the Release Options section, configure the following settings to specify how users are allowed to release print jobs:
   - **Release Method**—Select either of the following:
     - **User selects job(s) to print**—Let users choose the jobs they want to print.
     - **All jobs print automatically**—Print all pending jobs automatically when the user touches the application icon and authenticates.
   - **Display Print Jobs Sorted By**—Specify the order of jobs listed on the control panel.
4. From the Job Expiration section, set the expiration for Verify jobs and Repeat jobs.

   There are four types of held jobs:
   - **Confidential**—Store jobs on the printer until you log in and release or delete them.
   - **Verify**—Print one copy of a job to make sure that it is satisfactory before printing the remaining copies. The job is automatically deleted from the printer after all copies are printed.
   - **Reserve**—Store print on the printer and automatically delete them after printing.
   - **Repeat**—Print all copies of a job and store the job on the printer for later printing. You can print copies as long as the job is stored on the printer.

   To set the expiration of Confidential and Reserve jobs, use the printer Confidential Print Setup on the Embedded Web Server. (Click **Settings** or **Configuration**, and then click **Security** > **Confidential Print Setup**.) By default, only Confidential jobs can be set to expire. The Job Expiration settings let you set Verify and Repeat jobs to expire either at the same time as Confidential jobs or at another time.
5. From the Advanced Settings section, configure the following settings:
   - **Require All Jobs to be Held**—Let all jobs remain on the printer until released by an authorized user or until they expire.
   - **Clear Print Data**—Clear the memory associated with each job when the job is released.
6. Apply the changes.

Securing access to the printer

Securing access to the home screen

Use this method to require users to authenticate to view and use the printer home screen.

Note: The Background and Idle Screen application must be installed and running on the printer before you can secure access to the home screen.

1. From the Embedded Web Server, access the configuration page for Background and Idle Screen.
2. Under the Idle Screen Settings heading, make sure **Enable** is selected.
3. In the Start Time field, enter **0**. This prompts the printer to start the secure idle screen immediately (0 seconds) after a user's login session ends.
4. Under the Home Screen Background heading, clear **Enable**.
5. If you want to add custom idle screen images, then click **Add** under the Idle Screen Images heading.
6. Type an image name, and then upload the file you want to use.

   Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.
7. Apply the changes.
8. Repeat step 5 through step 7 to add more idle screen images. You can add up to ten images.
9. If you want to add a custom home screen background image, then under the Home Screen Background heading, select one of the default images, or upload a custom image in the Custom Image field.

   Note: For information about compatible image file types and recommended file sizes, see the mouse-over help.
10. If necessary, configure the other application settings. For more information about configuring the application, see the *Background and Idle Screen Administrator's Guide*.
11. Apply the changes.
12. Secure access to the idle screen using Smart Card Authentication Client.
    a. Create a security template for Smart Card Authentication Client to obtain user credentials. For more information, see "Creating security templates" on page 13.
    b. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup** > **Access Controls**.
    c. If necessary, expand the **Device Solutions** folder.
    d. From the Idle Screen drop-down menu, select your security template.
    e. Click **Submit**.

Controlling access to device functions using the EWS

Access to printer functions can be restricted by applying security templates to individual functions. A list of access controls and what they do can be found in "Appendix D: Access controls" on page 46.

1. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup**.
2. From the Advanced Security Setup section, click **Access Controls**.
3. Click **Expand All** to see all available access controls.
4. Select the appropriate level of protection for each function, as specified in the following table.
5. Click **Submit**.

Levels of protection include:

- **Administrator access only**—Use an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Authenticated users only**—Use an internal account or a security template, as long as it provides access to authenticated users only. These access controls must not be set to **No Security**.
- **Disabled**—Disable access to a function for all users and administrators.
- **Not applicable**—Another setting disables the function. No change is required, although we recommend setting these access controls to **Administrator access only** or **Disabled**.

Administrative Menus

Access control	Level of protection
Security Menu at the Device	Administrator access only
Security Menu Remotely	Administrator access only
Service Engineer Menus at the Device	Administrator access only
Service Engineer Menus Remotely	Administrator access only
Configuration Menu	Disabled
Paper Menu at the Device	Authenticated users only
Paper Menu Remotely	Authenticated users only
Reports Menu at the Device	Administrator access only
Reports Menu Remotely	Administrator access only
Settings Menu at the Device	Administrator access only
Settings Menu Remotely	Administrator access only
Network/Ports Menu at the Device	Administrator access only
Network/Ports Menu Remotely	Administrator access only
Manage Shortcuts at the Device	Authenticated users only
Manage Shortcuts Remotely	Authenticated users only
Supplies Menu at the Device	Authenticated users only
Supplies Menu Remotely	Authenticated users only
Option Card Configuration at the Device	Administrator access only
Option Card Configuration Remotely	Administrator access only

Management

Access control	Level of protection
Web Import/Export Settings	Disabled
Apps Configuration	Administrator access only
Remote Management	Disabled
Firmware Updates	Disabled or Administrator access only
PJL Device Setting Changes	Disabled

Access control	Level of protection
Operator Panel Lock	Authenticated users only
Configuration Files Import/Export	Disabled and Administrator access only
Internet Printing Protocol (IPP)	Disabled

Function Access

Access control	Level of protection
Address Book	Authenticated users only
Create Profiles	Disabled
Create Bookmarks at the Device	Disabled
Create Bookmarks Remotely	Disabled
Flash Drive Print	Disabled
Flash Drive Color Printing	Disabled
Flash Drive Scan	Disabled
Copy Function	Authenticated users only
Allow Flash Drive Access	Disabled
Copy Color Printing	Authenticated users only
Color Dropout	Authenticated users only
E-mail Function	Authenticated users only
Fax Function	Authenticated users only
Release Held Faxes	Administrator access only
FTP Function	Disabled
Held Jobs Access	Disabled
Use Profiles	No Security
Change Language from Home Screen	Authenticated users only
Cancel Jobs at the Device	Authenticated users only

Device Apps

Access control	Level of protection
Apps 1	Authenticated users only
Apps 2–10	Administrator access only
New Apps	Administrator access only
Idle screen	Authenticated users only
Secure Held Print Jobs	Authenticated users only

Troubleshooting

Login issues

USB device is not supported

Make sure that a supported smart card reader is attached

Remove the unsupported reader and attach a valid reader. For information on the supported readers, contact your Lexmark representative.

Printer home screen fails to return to a locked state when not in use

Try one or more of the following:

Make sure that the authentication token is installed and running

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management**.
2. Make sure that the authentication token appears in the list of installed solutions and that it is in a “Running” state.
   - If the authentication token is installed but is not running, then select the check box next to the application name, and then click **Start**.
   - If the authentication token does not appear in the list of installed solutions, then contact the Solutions Help Desk for assistance.

Make sure that Smart Card Authentication is installed and running

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management**.
2. Make sure that the Smart Card Authentication solution appears in the list of installed solutions and that it is in a

   "Running" state
   - If Smart Card Authentication is installed but is not running, then select the application name, and then click **Start**.
   - If the authentication token does not appear in the list of installed solutions, then contact the Solutions Help Desk for assistance.

Login screen does not appear when a smart card is inserted

Make sure that the smart card is recognized by the reader

Contact the Solutions Help Desk for assistance.

KDC and MFP clocks are out of sync

This error indicates that the printer clock is more than five minutes out of sync with the domain controller clock.

Make sure that the date and time settings on the printer are correct

1. From the Embedded Web Server, click **Settings** > **Security** > **Set Date and Time**.
2. If you have manually configured date and time settings, then adjust the settings if necessary. Make sure that the time zone and daylight saving time settings are correct.

   Note: If your network uses DHCP, then make sure that NTP settings are not automatically provided by the DHCP server before manually configuring NTP settings.
3. If the printer uses an NTP server, then make sure that those settings are correct and that the NTP server is functioning correctly.
4. Apply the changes.

Kerberos configuration file is not uploaded

This error occurs when Smart Card Authentication is configured to use the Device Kerberos Setup, but no Kerberos file has been uploaded.

Make sure that the Kerberos file has been uploaded

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. If you are using Simple Kerberos Setup, then clear the **Use Device Kerberos Setup** check box, and then apply the changes.
3. If you are using a Kerberos configuration file, then do the following:
   a. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup** > **Kerberos 5**.
   b. Under Import Kerberos File, browse to the krb5.conf file, and then click **Submit**.

Unable to authenticate users

Make sure that the Realm specified in the Kerberos settings is in uppercase

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. For Simple Kerberos Setup, make sure that the Realm is correct and typed in uppercase.
3. If you are using krb5.conf file, then make sure that the Realm entries in the configuration file are in uppercase.

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 16.

KDC did not respond within the required time

Try one or more of the following:

Make sure that the IP address or host name of the KDC is correct

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. For Simple Kerberos Setup, make sure that the IP address or host name specified for the Domain Controller is correct, and then apply the changes.
3. If you are using a krb5.conf file, then make sure that the IP address or host name specified for the Domain Controller is correct.

Make sure that the KDC is available

You can specify multiple KDCs in the Smart Card Authentication settings or in the krb5.conf file.

Make sure that Port 88 is not blocked by a firewall

Port 88 must be opened between the printer and the KDC for authentication to work.

User realm not found in the Kerberos configuration file

Make sure that the Windows Domain is specified in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. Under Simple Kerberos Setup, add the Windows Domain in lowercase to the Domain setting.

   For example, if the Domain setting is **`mil,.mil`** and the Windows Domain is **`x.y.z`**, then change the Domain setting to **`mil,.mil,x.y.z`**.
3. If you are using a krb5.conf file, then add an entry to the domain_realm section. Map the lowercase Windows Domain to the uppercase realm (similar to the existing mapping for the “mil” domain).

Cannot find realm on card in the Kerberos configuration file

This error occurs during smart card login.

Upload a Kerberos configuration file and make sure that the realm has been added to the file

The Smart Card Authentication settings do not support multiple Kerberos Realm entries. If multiple realms are needed, then create and upload a krbf5.conf file containing the needed realms. If you are already using a Kerberos configuration file, then make sure that the missing realm is added to the file correctly.

Client is unknown

This error indicates that the KDC being used to authenticate the user does not recognize the User Principal Name specified in the error message.

Make sure that the Domain Controller information is correct

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. For Simple Kerberos Setup, make sure that the IP address or host name of the Domain Controller is correct.
3. If you are using a Kerberos configuration file, then make sure that the Domain Controller entry is correct.

Login does not respond at “Getting User Info”

For information on LDAP-related issues, see“LDAP issues” on page 38.

User is logged out automatically

Increase the Panel Login Timeout interval

1. From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.
2. Increase the time (in seconds) of the Panel Login Timeout setting.
3. Apply the changes.

LDAP issues

LDAP lookups take a long time and then fail

This issue can occur during login (at “Getting User Info”) or during address book searches. Try one or more of the following:

Make sure that Port 389 (non-SSL) and Port 636 (SSL) are not blocked by a firewall

The printer uses these ports to communicate with the LDAP server. The ports must be open for LDAP lookups to work.

Make sure that the LDAP search base is not too broad in scope

Narrow the LDAP search base to the lowest possible scope that will include all necessary users.

LDAP lookups fail almost immediately

Try one or more of the following:

Make sure that the Address Book Setup contains the host name for the LDAP server

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **Address Book Setup**.
2. Make sure that the host name (not the IP address) of the LDAP server specified in the Server Address field is correct.
3. Apply the changes.

Make sure that the Address Book Setup settings are correct

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **Address Book Setup**.
2. If necessary, modify the following settings:
   - **Server Port**—Set this port to 636.
   - **Use SSL/TLS**—Select **SSL/TLS**.
   - **LDAP Certificate Verification**—Select **Never**.
3. Apply the changes.

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

Make sure that the LDAP attributes for the user e-mail address and home directory are correct

Held Jobs / Print Release Lite issues

Cannot use the Held Jobs feature

Add the user to the appropriate Active Directory group

If user authorization is enabled for Held Jobs, then add the user to an Active Directory group that is included in the authorization list for the Secure Held Print Jobs function.

Cannot determine Windows user ID

Make sure that Smart Card Authentication sets the user ID for the session

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. From the User Session and Access Control section, for the Session Userid setting, specify how to obtain the Windows user ID when logging in:
   - **None**—The user ID is not set. Select this option if the user ID is not needed by other applications.
   - **User Principal Name**—The smart card principal name or the credential provided by manual login is used to set the user ID (userid@domain).
   - **EDI-PI**—The user ID portion of the smart card principal name or the credential provided by manual login is used to set the user ID.
   - **LDAP Lookup**—The user ID is retrieved from Active Directory.
3. Apply the changes.

No jobs available for user

Try one or more of the following:

Make sure that the Smart Card Authentication sets the correct user ID

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Smart Card Authentication** > **Configure**.
2. From the User Session and Access Control section, select **LDAP Lookup** for the Session UserID setting.
3. Apply the changes.

Make sure that the jobs were sent to the correct printer and were printed

The jobs may have been sent to a different printer, or automatically deleted because they were not printed quickly enough.

Jobs are printing immediately

Try one or more of the following:

Make sure that Secure Held Print Jobs is installed and running

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management**.
2. Verify that the Secure Held Print Jobs solution appears in the list of installed solutions and that it is in a “Running” state.
   - If Secure Held Print Jobs is installed but is not running, then select the check box next to the application name, and then click **Start**.
   - If Secure Held Print Jobs does not appear in the list of installed solutions, then contact the Solutions Help Desk for assistance.

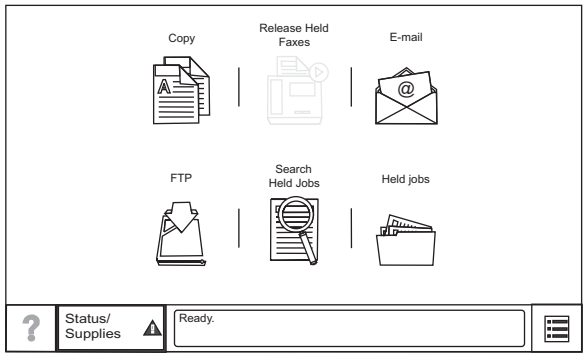
Make sure that all jobs are required to be held

1. From the Embedded Web Server, click **Settings** > **Apps** > **Apps Management** > **Secure Held Print Jobs** > **Configure**.
2. From the Advanced Settings section, enable **Require All Jobs to be Held** and **Clear Print Data** .
3. Apply the changes.

Appendix A: Using the touch screen

Understanding the home screen

The screen located on the front of the printer is touch-sensitive and can be used to access device functions and navigate settings and configuration menus. The home screen looks similar to this (yours may contain additional icons):

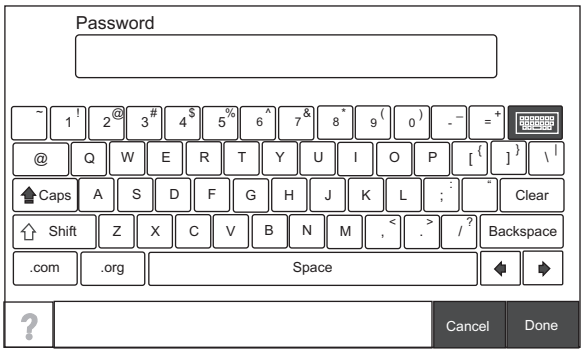


Touch  on the lower right to access settings and configuration menus for the device.

Note: Access to device menus may be restricted to administrators only.

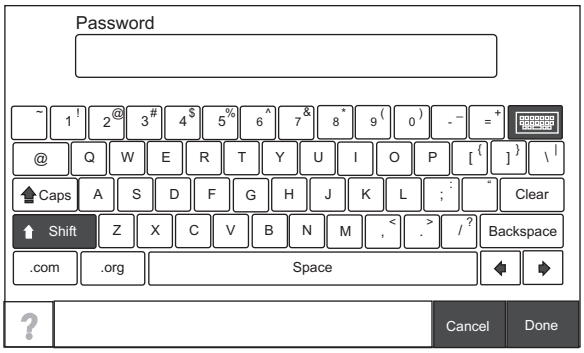
Using the on-screen keyboard

Some device 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 display may also contain other icons, such as Next, Submit, Cancel, and the home icon.

To type a single uppercase or shift character, touch **Shift**, and then touch the letter or number you need to uppercase. To turn on Caps Lock, touch **Caps**, and then continue typing. Caps Lock will remain engaged until you touch **Caps** again.



Touch **Backspace** to delete a single character or **Clear** to delete everything you have typed.

Appendix B: Acronyms

Acronyms used in this guide

CA	Certificate Authority
CAC	Common Access Card
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoD	Department of Defense
EAL	Evaluation Assurance Level
EWS	Embedded Web Server
GIF	Graphic Interchange Format
GSSAPI	Generic Security Service Applications Programming Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
KDC	Key Distribution Center
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction printer
NTLM	NT LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RFC	Request for Comment
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus

Appendix C: Checking the Embedded Solutions Framework version

Checking which version of the Embedded Solutions Framework is installed on a printer

1. Obtain the printer IP address:
   - From the printer home screen
   - From the TCP/IP section in the Network/Ports menu
   - By printing a network setup page or menu settings page, and then finding the TCP/IP section

   Note: An IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.
2. Open a Web browser, and then type the printer IP address in the address field.
3. From the Embedded Web Server, click **Reports** > **Device Settings**.
4. Scroll down until you see “Embedded Solutions” (usually found near the bottom).
5. In the Embedded Solutions section, note the value next to “Framework =”. This signifies the installed version.

Note: To view the complete list of supported printers for each version of the Embedded Web Server, see the *Readme* file.

Appendix D: Description of access controls

Appendix D: Access controls

Note: Depending on the device type and installed options, some access controls (referred to on some devices as Function Access Controls) may not be available for your printer.

Administrative Menus

Function access control	What it does
Configuration Menu	This protects access to the Configuration Menu.
Manage Shortcuts at the Device	This protects access to the Manage Shortcuts section of the Settings menu from the printer control panel.
Manage Shortcuts Remotely	This protects access to the Manage Shortcuts section of the Settings menu from the Embedded Web Server.
Network/Ports Menu at the Device	This protects access to the Network/Ports section of the Settings menu from the printer control panel.
Network/Ports Menu Remotely	This protects access to the Network/Ports section of the Settings menu from the Embedded Web Server.
Option Card Configuration at the Device	This controls access to the Option Card Configuration section of the Settings menu from the printer control panel. This applies only when an Option Card with configuration options is installed on the device.
Option Card Configuration Remotely	This controls access to the Option Card Configuration section of the Settings menu from the Embedded Web Server. This applies only when an Option Card with configuration options is installed on the device.
Paper Menu at the Device	This protects access to the Paper menu from the printer control panel.
Paper Menu Remotely	This protects access to the Paper menu from the Embedded Web Server.
Reports Menu at the Device	This protects access to the Reports menu from the printer control panel.
Reports Menu Remotely	This protects access to the Reports menu from the Embedded Web Server.
Security Menu at the Device	This protects access to the Security menu from the printer control panel.
Security Menu Remotely	This protects access to the Security menu from the Embedded Web Server.
Service Engineer Menus at the Device	This protects access to the Service Engineer menu from the printer control panel.
Service Engineer Menus Remotely	This protects access to the Service Engineer menu from the Embedded Web Server.
Settings Menu at the Device	This protects access to the General and Print Settings sections of the Settings menu from the printer control panel.
Settings Menu Remotely	This protects access to the General and Print Settings sections of the Settings menu from the Embedded Web Server.

Management

Function access control	What it does
Firmware Updates	This controls the ability to update firmware from any source other than a flash drive. Firmware files that are received through FTP, the Embedded Web Server, etc., will be ignored (flushed) when this function is protected.
Operator Panel Lock	This protects access to the locking function of the printer control panel. If this is enabled, then users with appropriate credentials can lock and unlock the printer touch screen. In a locked state, the touch screen displays only the "Unlock Device" icon, and no further operations can be performed at the device until appropriate credentials are entered. Once unlocked, the touch screen will remain in an unlocked state even if the user logs out of the device. To enable the control panel lock, the user must select the "Lock Device" icon, and then enter the appropriate credentials.
PJL Device Setting Changes	When disabled, all device settings changes requested by incoming print jobs are ignored.
Remote Management	This controls access to printer settings and functions by remote management tools such as MarkVision™. When protected, no printer configuration settings can be altered except through a secured communication channel (such as that provided by a properly configured installation of MarkVision).
Apps Configuration	This controls access to the configuration of any installed applications.
Web Import/Export Settings	This controls the ability to import and export printer settings files (UCF files) from the Embedded Web Server.
Configuration Files Import/Export	This controls the ability to import and export settings and security configuration files.
Internet Printing Protocol (IPP)	This controls the ability to use the IPP.

Function Access

Function access control	What it does
Address Book	This controls the ability to perform address book searches in the Scan to Fax and Scan to E-mail functions.
Cancel Jobs at the Device	This controls the ability to cancel jobs from the printer control panel.
Change Language from Home Screen	This controls access to the Change Language feature from the printer control panel.
Color Dropout	This controls the ability to use the Color Dropout feature for scan and copy functions.
Copy Color Printing	This controls the ability to perform color copy functions. Users who are denied will have their copy jobs printed in black and white.
Copy Function	This controls the ability to use the Copy function.
Create Bookmarks at the Device	This controls the ability to create new bookmarks from the printer control panel.
Create Bookmarks Remotely	This controls the ability to create new bookmarks from the Bookmark Setup section of the Settings menu on the Embedded Web Server.
Create Profiles	This controls the ability to create new profiles.
E-mail Function	This controls access to the Scan to E-mail function.

Function access control	What it does
Fax Function	This controls access to the Scan to Fax function.
Flash Drive Color Printing	This controls the ability to print color from a flash drive. Users who are denied will have their print jobs printed in black and white.
Allow Flash Drive Access	This controls the ability to access the flash drive.
Flash Drive Print	This controls the ability to print from a flash drive.
Flash Drive Scan	This controls the ability to scan documents to a flash drive.
FTP Function	This controls access to the Scan to FTP function.
Held Jobs Access	This protects access to the Held Jobs function.
PictBridge Printing	This controls the ability for some devices to print from an attached PictBridge-enabled digital camera. **Note:** Selected devices only.
Release Held Faxes	This controls the ability to release (print) held faxes.
Use Profiles	This controls access to profiles, such as scanning shortcuts, workflows, and eSF applications.

Device Applications

Function access control	What it does
New Apps	This controls the initial security profile of each application-specific access control installed on the printer.
App 1–10	The App 1 through App 10 access controls can be assigned to installed eSF applications and profiles created by LDSS. The access control for each application is assigned in the creation or configuration of the application or profile.

Notes:

- Depending on the applications you have installed, additional application-specific access controls may be listed below apps 1–10. Use these additional access controls if they are available for your installed applications. If no additional solution-specific access controls are available, then assign one of the ten numbered access controls to each application you want to protect.
- Some applications may be included with printers as default configurations and appear as function access control selections.

Notices

Edition notice

September 2015

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, visit **http://support.lexmark.com**.

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

Trademarks

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

All other trademarks are the property of their respective owners.

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.

Index