Common Criteria

Installation Supplement and Administrator Guide

November 2011 **www.lexmark.com**

3065326-001

740 West New Circle Road
Lexington, Kentucky 40550

Edition notice

November 2011

For Lexmark technical support, visit **support.lexmark.com**.

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

If you don't have access to the Internet, you can contact Lexmark by mail:

Lexmark International, Inc.
Bldg 004-2/CSC
740 New Circle Road NW
Lexington, KY 40550

Contents

Overview and first steps

Overview

This guide describes how to configure a supported Lexmark™ *multifunction printer* (MFP) to reach Common Criteria *Evaluation Assurance Level 2* (EAL 2). It is critical that you carefully follow the instructions in this guide, as failure to do so may result in a device that does not meet the requirements of the evaluation.

Using this guide

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

Some settings can be configured using either the *Embedded Web Server* (EWS), or the device touch screen. Where applicable, instructions for both methods are included.

For information about physically setting up the MFP or using device features, see the *User Guide* that came with your MFP. For information about using the MFP touch screen, see"Appendix A: Using the touch screen" on page 44.

Supported devices

This guide describes how to implement an evaluated configuration on the following models:

- Lexmark X548
- Lexmark XS548
- Lexmark X792
- Lexmark XS796
- Lexmark X925
- Lexmark XS925
- Lexmark X950
- Lexmark X952
- Lexmark X954
- Lexmark XS955
- Lexmark 6500e scanner with T650 printer
- Lexmark 6500e scanner with T652 printer
- Lexmark 6500e scanner with T654 printer
- Lexmark 6500e scanner with T656 printer

Note: If you are using a Lexmark 6500e scanner with a T650, T652, T654, or T656 printer, then you must complete the setup and configuration steps in the *Setup Guide* that came with the scanner before following the instructions in this guide.

Operating environment

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

- The MFP is installed in a cooperative, nonhostile environment that is physically secure or monitored and provides protection from unauthorized access to MFP external interfaces.
- The administration platform and local area network are physically and logically secure.
- 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 MFP 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.
- MFP users are aware of and are trained to follow the security policies and procedures of their organization. Users are authorized to use the MFP according to these policies and procedures.

Before configuring the device (required)

Before beginning configuration tasks, you must:

- Verify that no optional interfaces are installed
- Verify the firmware
- Attach a lock to the MFP
- Encrypt the hard disk

Verifying physical interfaces and installed firmware

1. Inspect the MFP 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 MFP 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 verify the firmware version, under Device Information, locate **Base =**, and **Network =**.
7. Contact your Lexmark representative to verify that the Base and Network values are correct and up-to-date.

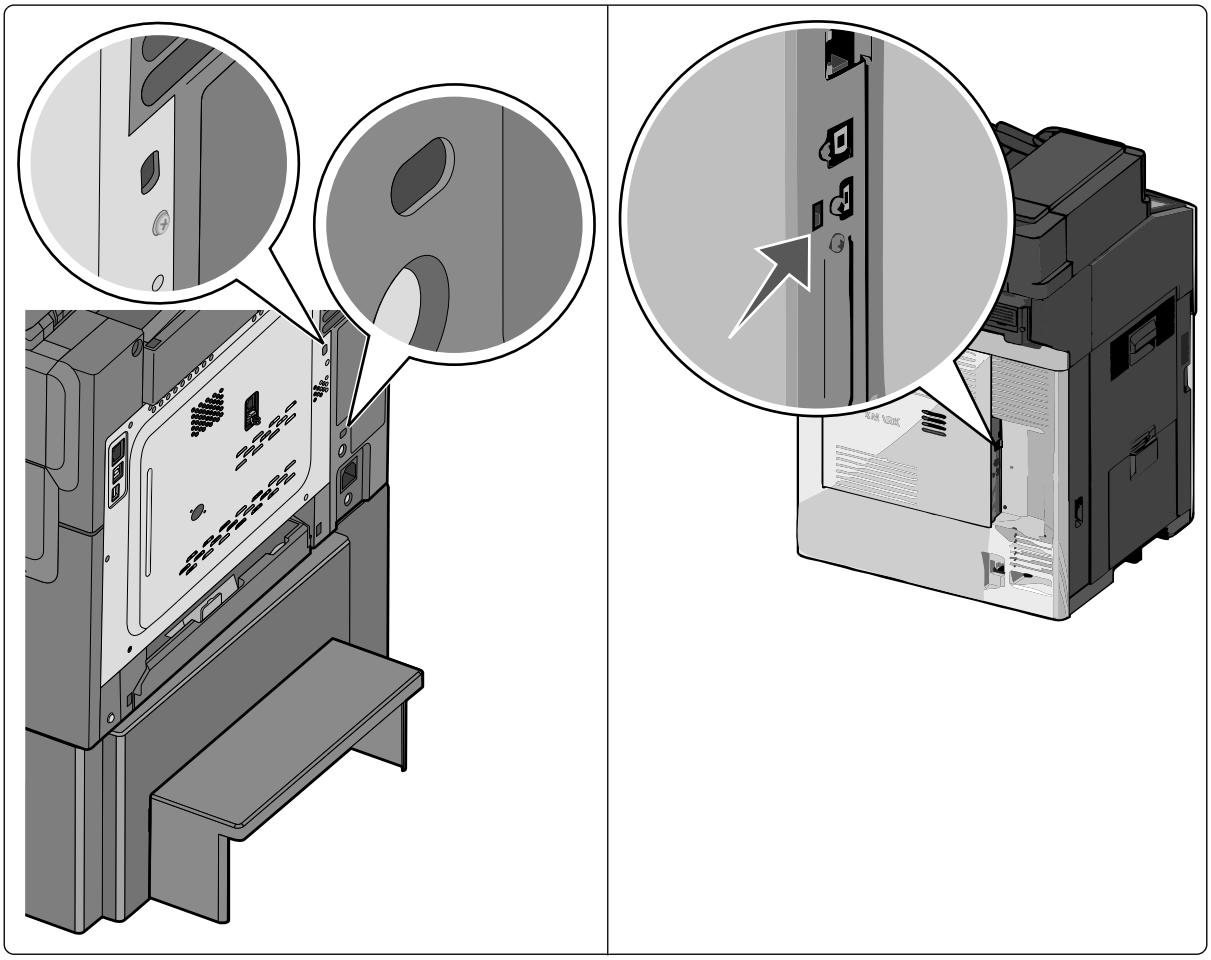
Attaching a lock

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

Note: If you are using a Lexmark 6500e scanner with a T650, T652, T654, or T656 printer, then you must attach a lock to both the scanner and the printer.

1. Verify that the MFP 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 MFP 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 MFP—or its hard disk—is stolen.

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

   Once the MFP 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 MFP 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 Disk Encryption menu selection.

5 Touch **Disk Encryption** > **Enable**.

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

6 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 has been encrypted, the MFP will return to the Enable/Disable screen.

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

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

The MFP will undergo a power-on reset, and then return 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 Set USB Buffer to **Disabled**.

3 Touch **Submit**.

Installing the minimum configuration

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

Configuring the device

Configuration checklist

This checklist outlines the steps required to implement an evaluated configuration on a standalone device. For information about additional configuration options, see “Administering the device” on page 15.

After completing the pre-configuration tasks found in “Before configuring the device (required)” on page 6, continue with this section to configure the settings needed to achieve the evaluated configuration for a standalone device:

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 device. 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. Set Wiping Mode to **Auto**.
3. Set Automatic Method to **Multi-pass**.
4. Touch **Submit**.

Enabling the backup password (optional)

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

Note: The backup password should:

- Contain a minimum of 8 characters.
- Contain at least one lowercase letter, one uppercase letter, and one non-alphabetic character.
- Not be 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

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 MFP supports a maximum of 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**.

2 On the Groups for Internal Accounts screen, touch **Add Entry**.

3 For the Name, type **Administrator_Only**.

4 Touch **Done** to save this group and return to the Groups for Internal Accounts screen.

5 Touch **Add Entry**.

6 For the Name, type **Authenticated_Users**.

7 Touch **Done** to save this group.

Note: If there is a need to grant access to some administrative functions while restricting others, then you can create additional groups, such as “Administrator_Reports” or “Administrator_Security.”

Scenario 1: Using two groups

Group name	Type of user group would be selected for
Administrator_Only	Administrators permitted to access all device functions
Authenticated_Users	• Administrators • Non-administrators (all other users)

Scenario 2: Using multiple groups

Group name	Type of user group would be selected for
Administrator_Only	Administrators permitted to access all device functions
Administrator_Reports	• Administrators permitted to access all device functions • Administrators permitted to use device functions and access the Reports menu
Administrator_Security	• Administrators permitted to access all device functions • Administrators permitted to use device functions and access the Security menu

Group name	Type of user group would be selected for
Authenticated_Users	• Administrators permitted to access all device functions • Administrators permitted to use device functions and access the Reports menu • Administrators permitted 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. On the General Settings screen, set Required User Credentials to **User ID and password**, and then touch **Submit**. The MFP will return 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**. Passwords must:
   - Contain a minimum of 8 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.
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 as needed. If you have created multiple groups to grant 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. After selecting the appropriate group or groups, touch **Done** to save the account and return to the Manage Internal Accounts screen, where the user should now be listed.
11. Repeat the steps as needed to add more users.

Creating security templates

A security template is assigned to each device function to control which users are permitted to access that function. At a minimum, you must create two security templates: one for "Administrator_Only" and one for "Authenticated_Users." If there is a need to grant access to some administrative functions while restricting others, then you can create additional security templates, such as “Administrator_Reports” or “Administrator_Security.” Each template will be 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**.
2. Touch **Add Entry**.

3 Type a unique name to identify the template. Use a descriptive name, such as ”Administrator_Only” or “Authenticated_Users,” and then touch **Done**.

4 On the Authentication Setup screen, select the internal accounts building block, and then touch **Done**.

5 On the Authorization Setup screen, select the internal accounts building block, and then touch **Done**.

6 Select one or more groups to be included in the template, and then touch **Done** to save your changes and return to the Edit Security Templates screen.

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.

From the home screen, touch > **Security** > **Edit Security Setups** > **Edit Security Templates**.

- 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 “Access controls” on page 47.

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:

- **Administrator access only**—This can be an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Authenticated users only**—This can be 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**—This disables access to a function for all users and administrators.
- **Not applicable**—The function has been disabled by another setting. No change is required, although it is recommended that you set 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

Access control	Level of protection
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
Solutions Configuration	Administrator access only
Remote Management	Administrator access only
Firmware Updates	Disabled
PJL Device Setting Changes	Disabled
Operator Panel Lock	Authenticated users only
Address Book	Authenticated users only
Create Profiles	Disabled
Create Bookmarks at the Device	Disabled
Create Bookmarks Remotely	Disabled
Flash Drive Print	Not applicable—USB port disabled
Flash Drive Color Printing	Not applicable—USB port disabled
Flash Drive Scan	Not applicable—USB port disabled
Copy Function	Authenticated users only
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

Access control	Level of protection
Held Jobs Access	Disabled
Use Profiles	Authenticated users only
Change Language from Home Screen	Authenticated users only
Cancel Jobs at the Device	Administrator access only
PictBridge Printing	Not applicable—USB port disabled
Solution 1	Authenticated users only **Note:** When eSF applications are configured, Solution 1 controls access to Held Jobs.
Solutions 2-10	Administrator access only
New Solutions	Administrator access only

Disabling home screen icons

The final step is to remove unneeded icons from the MFP home screen.

1. From the home screen, touch > **Settings** > **General Settings**.
2. Touch **Home screen customization**.
3. Set FTP, FTP shortcuts, and USB Drive to **Do not display**.

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

Administering the device

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

Using the Embedded Web Server

Many settings can be configured using either the Embedded Web Server (EWS) or the touch screen.

Accessing the EWS

1. Type the device IP address or host name in the address field of your Web browser using the secure version of the page (with the address beginning “https://”).
2. Use the navigation menu on the left to access configuration and report menus.

   Note: If the device IP address or host name is not readily apparent, then you can find it by printing a network setup page.

Printing a network setup page

From the home screen, touch > **Reports** > **Network Setup Page**.
After the network setup page prints, the MFP will return to the home screen.

Settings for network-connected devices

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

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 “Using the Embedded Web Server” on page 15.
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:255.255.255.255. 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 “Using the Embedded Web Server” on page 15.

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:255.255.255.255 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 “Using the Embedded Web Server” on page 15.

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 “Using the Embedded Web Server” on page 15.

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 MFP 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 “Using the Embedded Web Server” on page 15.

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 **Encryption**, and then select **3DES** from the Proposed Encryption Method drop-down menu.
5. In the Settings section, click **Certificate Validation**, and then select the **Validate Peer Certificate** check box.
6. In the Connections section, click either **Pre-Shared Key Authenticated Connections** or **Certificate Authenticated Connections**, and then click one of the numbered **Host** fields.
7. Type the IP address of the client device you want to connect to the MFP. If you are using *Pre-Shared Key* (PSK) Authentication, then also type the key.

   Note: If you are using PSK Authentication, then retain the key to use later when configuring client devices.

8. Configure IPSec as needed on client devices that will connect to the MFP.
9. 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 “Using the Embedded Web Server” on page 15.

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**.
2. From the Std Network Setup screen, touch **AppleTalk** > **Activate**.

   Note: It might be necessary to scroll down to find the AppleTalk selection.
3. Set Activate to **No**.
4. Touch **Submit**. The MFP 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 MFP using a network connection. For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

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 MFP 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 “Using the Embedded Web Server” on page 15.

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 drop-down 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 will be using LDAP+GSSAPI or Common Access Cards to control user access to the MFP, then you must first configure Kerberos.

Using the EWS

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

   Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

2 Under Advanced Security Setup, at Step 1, click **Kerberos 5**.

3 Under Simple Kerberos Setup, for KDC Address, type the IP address or host name of the KDC (Key Distribution Center) IP.

4 For KDC Port, type the number of the port used by the Kerberos server.

5 For Realm, type the realm used by the Kerberos server.

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

6 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 will overwrite 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 information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

2 Under Advanced Security Setup, at Step 1, click **Kerberos 5**.

3 Under Import Kerberos File, click **Browse** to navigate to your stored krb5.conf file.

4 Click **Submit** to upload the krb5.conf file.

Note: After you click **Submit**, the device will automatically test the krb5.conf file to verify that it is functional.

Notes:

- 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.

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 “Using the Embedded Web Server” on page 15.

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 MFP to send an e-mail when the **Delete Log** button is clicked.
- Select **E-mail log wrapped alert** if you want the MFP 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 MFP 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 MFP to send an e-mail when the log file is exported.
- Select **E-mail log settings changed alert** if you want the MFP 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 MFP to automatically notify administrators of certain log events, 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 MFP 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 MFP 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 MFP to automatically notify administrators of certain log events, then adjust the following settings as needed:
- 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 22.

E-mail

User data sent by the MFP 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 “Using the Embedded Web Server” on page 15.

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 MFP 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 MFP (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 MFP 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 MFP 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 MFP will wait for a response from the SMTP server before timing out.

6 If you want to receive responses to messages sent from the MFP (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 MFP 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 MFP 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 “Using the Embedded Web Server” on page 15.

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

   Once the MFP 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 MFP 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 MFP returns to the main Configuration menu.
6. Touch **Back**, and then touch **Exit Config Menu**.

   The MFP will undergo a power-on reset and then return 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 MFP 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 MFP using a method that provides both authentication and authorization. Under the evaluated configuration, three options are available for granting access to network-connected devices: internal accounts, LDAP+GSSAPI, and PKI Authentication (used with DoD Common Access Cards).

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 MFP 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.

Scenario 1: Creating groups based on department

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.

Scenario 2: Creating groups based on device function

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 “Using the Embedded Web Server” on page 15.

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. Repeat the steps as needed 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 8 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 MFP 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 19.

Using the EWS

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

Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

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.
- **Required User Input**—Select either **User ID and Password** or **User ID** to specify which credentials a user must provide when attempting to access a function protected by the LDAP building block.

Device Credentials (optional)

- **Use Active Directory Device Credentials**—Click 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.

Search specific object classes (optional)

- **person**—Click to select or clear. This specifies that the “person” object class will also be searched.
- **Custom Object Class**—Click to select or clear. 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.

- **Group Search Base**—Type the name of the group search base.
- For each LDAP+GSSAPI group you want to define, specify the “Short name for group” and the Group Identifier.
- When creating security templates, you will select groups from this setup to control 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 MFP returns to the General Information screen.

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

- **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**, and then adjust the following settings as needed (optional):

- **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**, and then adjust the following settings as needed (optional):

- **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**, and then adjust the following settings as needed:

- **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, you will select groups from this setup to control access to device functions.

Configuring Common Access Card access

A set of *Public Key Infrastructure* (PKI) embedded applications comes installed on the MFP. These applications provide for additional functionality, including the use of Smart Cards such as the Department of Defense Common Access Card (CAC). For more information on using a card reader with your MFP, see “Using a Common Access Card to access the printer” on page 50.

Note: You must configure Kerberos before setting up CAC access. For information about configuring Kerberos, see “Kerberos” on page 19.

Step 1: Start the authentication token application

The authentication token application comes in a “Stopped” state and must be started before you configure PKI Authentication.

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)**.

   Note: For information on accessing the EWS, see “Using the Embedded Web Server” on page 15.

2. On the Solutions tab, verify that the authentication token is not running. If it is not, then select the check box next to the application, and then click **Start**.

   After the Solutions tab reloads, the authentication token application should be listed as “Running.”

Step 2: Configure PKI Authentication

PKI Authentication provides the login screen and authentication mechanism and supports user authorization to the MFP and its functions.

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
2. Select the check box next to the PKI Authentication application, and then click **Start**. When the Solutions tab reloads, PKI Authentication should be in a “Running” state.
3. From the Solutions tab, click **PKI Authentication** > **Configure**.
4. For Logon Type, select **Card Only** so that users will be required to insert a Common Access Card to access the MFP.
5. Select whether the Card PIN can be numeric only or alphanumeric.
6. If you want to, provide a custom Logon Screen Text with special instructions for users or a custom Logon Screen Image. Custom screen images must be in GIF format and must not be larger than 800 x 320 pixels.
7. Clear the **Allow Copy without Card** and the **Allow Fax without Card** check boxes.
8. Set “User Validation Mode” to **Active Directory**.
9. Select the **Use Device Kerberos Setup** check box to use the Kerberos settings already configured on the MFP, or clear the check box to use Simple Kerberos Setup.
10. For Simple Kerberos Setup, you must provide:
    - **Realm**—This is the Kerberos realm as configured in Active Directory, typically the Windows Domain Name. The realm must be entered in uppercase.
    - **Domain Controller**—This is the IP address or host name of the domain controller used for validation. Multiple values can be entered, separated by commas. They will be tried in the order listed.

- **Domain**—This is the card domain that should be mapped to the specified realm. This is the principal name used on the card and should be listed by itself, followed by a comma, a period, and then the principal name again. This value is case-sensitive and usually appears in lowercase. Multiple values can be entered, separated by commas.

  Example: If a U.S. DoD Common Access Card uses "123456789@mil" to identify a user, then "mil" is the principal name. In this case, you would enter the domain as **`mil,.mil`**.
- **Timeout**—This is the amount of time the MFP should wait for a response from the domain controller before moving to the next one in the list.

11 If users are allowed to log in manually, then provide at least one Manual Login Domain (a Windows Domain Name) to choose from when logging in. Multiple domains can be entered, separated by commas.

12 Select a DC Validation Mode for validating the domain controller certificate when users log into the MFP:

- **Device Certificate Validation**—This is the most common method. The certificate of the CA that issued the domain controller certificate must also be installed on the MFP.
- **Device Chain Validation**—The entire certificate chain, from the domain controller to the root CA, must be installed on the MFP.
- **OCSP Validation**—The entire certificate chain, from the domain controller to the root CA, must be installed on the MFP, and *Online Certificate Status Protocol* (OCSP) settings must be configured.

13 If you selected OCSP Validation, then configure the following:

- **Responder URL**—This is the IP address or host name of an OCSP responder/repeater, along with the port being used (usually 80). The correct format is "http://ip_address:port_number" (http://255.255.255.0:80). Multiple values can be entered, separated by commas. They will be tried in the order listed.
- **Responder Certificate**—Browse to locate the X.509 certificate for the responder.
- **Responder Timeout**—This is the amount of time the MFP should wait for a response from the OCSP Responder before moving to the next one in the list.
- **Unknown Status is Valid**—Select this check box to allow a user to log in even if the OCSP response indicates that the certificate status is unknown.

14 In the User Session and Access Control section, verify that the **Share Session with LDD** check box is not selected.

15 If DNS is not enabled on the network, or if some servers are multi-homed, then under Advanced Settings, click **Browse** to locate a Hosts File with host name–IP address mappings.

16 Select the **Wait for Active Network** check box to display **`Waiting for network`** on the touch screen after the MFP is turned on. This message disappears when the network becomes available.

17 Click **Apply**.

Note: You must install at least one Certificate Authority (CA) certificate for PKI Authentication to work. For more information on uploading a CA certificate, see "Creating and modifying digital certificates" on page 15.

Creating security templates using the EWS

A security template is assigned to each device function to control which users are permitted to access that function. At a minimum, you must create two security templates: one for "Administrator_Only" and one for "Authenticated_Users." If there is a need to grant access to some functions while restricting others, then you can create additional security templates, such as “Administrator_Reports” or “Color_User.” Each template will be populated with groups containing users authorized to access the functions protected by that template. A “PKI Authentication” security template is created automatically when you configure PKI Authentication.

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

   Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

2 Under Advanced Security Setup, Step 2, click **Security Template**.

3 Under Manage Security Templates, click **Add a Security Template**.

4 In the Security Template Name field, type a unique name for the template. It can be helpful to use a descriptive name, such as “Administrator_Only” or “Authenticated_Users.”

5 From the Authentication Setup list, select a method for authenticating users. This list will be populated with the authentication building blocks that have been configured on the MFP (internal accounts, LDAP+GSSAPI, or PKI Authentication).

   Notes:

   - Because a PKI Authentication security template is created when you configure PKI Authentication, the PKI Authentication building block would be used only when modifying other security templates to add authorization.
   - Even if it has been configured, PKI Authentication will not be displayed in the list of available building blocks if the application is in a “Stopped” state. For information about starting PKI Authentication, see “Configuring Common Access Card access” on page 30.

6 Click **Add authorization**, and then select an option from the Authorization Setup list. This list will be populated with the authentication building blocks that have been configured on the MFP (internal accounts, LDAP+GSSAPI, or PKI Authentication).

7 Click **Modify Groups**, and then select one or more groups to include in the security template. Hold down the **Ctrl** key to select multiple groups.

8 Click **Save Template**.

Modifying or deleting an existing security template

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

2 Under Advanced Security Setup, Step 2, click **Security Template**.

3 Select a security template from the list.

4 Edit the fields as necessary.

5 Click **Modify** to save your changes, **Delete Entry** to delete the template, or **Cancel** to retain previously configured values.

Notes:

- Clicking **Delete List** from the Manage Security Templates screen will delete all security templates on the MFP, regardless of which one is selected. To delete an individual security template, select it from the list, and then click **Delete Entry**.
- You can delete a security template only if it is not in use; however, security templates currently in use can be modified.

Controlling access to device functions

Configuring PKI Held Jobs

PKI Held Jobs, also referred to as Release Print Jobs, is used to securely hold documents at the printer until released by an authorized user.

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Held Jobs** > **Configure**.

   Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

2. If you want to, specify custom icon text that will appear above the Held Jobs icon on the printer home screen.
3. To select an alternate image for the Up Icon (the image that appears when the Held Jobs icon has not been pressed), click **Browse** to locate the image you want to use. To view the default icon image, click **View Current Value**.
4. To select an alternate image for the Down Icon (the image that displays when the Held Jobs icon is pressed), click **Browse** to locate the image you want to use. To view the default icon image, click **View Current Value**.
5. For Access Control, select **Solution-specific access control 1**.
6. Select from the following Release Options to specify how users will be able to release print jobs:
   - **Release Method**—Select **User Selects job(s) to print** if you want to allow users to choose which jobs they want to print, or select **All jobs print automatically** to have all jobs pending for a user print automatically when the user selects the **Held jobs** icon.
   - Select the **Show Copies Screen** check box if you want to allow users to change the number of copies for each job from the printer.
   - Select the **Allow Users to Print All** check box if you want to allow users to select a **Print All** button rather than select each print job individually.
   - **Display Print Jobs Sorted By**—Select **Date Printed (Descending)**, **Date Printed (Ascending)**, or **Job Name** to specify the order in which print jobs are displayed.
7. Note that there are four types of held jobs: Confidential Print, Reserve Print, Verify Print, and Repeat Print. The expiration of Confidential and Reserve Print jobs is controlled by the Confidential Print Setup (**Settings** > **Security** > **Confidential Print Setup**).

   By default, only Confidential Print jobs can be set to expire. Using Job Expiration, you can also set Verify Print and Repeat Print jobs to expire, either at the same time Confidential jobs expire or at another time:

   Note: The interval chosen for Job Expiration represents the minimum time a job will be held before being removed. Depending on how often a specific device polls for state changes, jobs marked for removal may remain on the device for up to an hour after the time chosen for expiration. For example, if held jobs are set to expire after an hour, then it will actually be between one and two hours before an expiring job is removed.

- **Verify Job Expiration**—This can be set to **Off**, **Same as Confidential Print**, or one of four intervals ranging from one hour to one week.
- **Repeat Job Expiration**—This can be set to **Off**, **Same as Confidential Print**, or one of four intervals ranging from one hour to one week.

8 Under Advanced Settings, select the **Require All Jobs to be Held** and **Clear Print Data** check boxes.

9 Click **Apply**.

Controlling access to device functions using the EWS

Access to MFP functions can be restricted by applying security templates to individual functions. A list of access controls and what they do can be found in “Access controls” on page 47.

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

Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15.

2 Under Advanced Security Setup, Step 3, 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**—This can be an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Authenticated users only**—This can be 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**—This disables access to a function for all users and administrators.
- **Not applicable**—The function has been disabled by another setting. No change is required, although it is recommended that you set 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

Access control	Level of protection
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
Solutions Configuration	Administrator access only
Remote Management	Administrator access only
Firmware Updates	Disabled
PJL Device Setting Changes	Disabled
Operator Panel Lock	Authenticated users only

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	Not applicable–USB port disabled
Flash Drive Color Printing	Not applicable–USB port disabled
Flash Drive Scan	Not applicable–USB port disabled
Copy Function	Authenticated users only
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

Access control	Level of protection
Use Profiles	Authenticated users only
Change Language from Home Screen	Authenticated users only
Cancel Jobs at the Device	Administrator access only
PictBridge Printing	Not applicable–USB port disabled

Device Solutions

Access control	Level of protection
Solution 1	Authenticated users only **Note:** When eSF applications are configured, Solution 1 controls access to Held Jobs.
Solutions 2–10	Administrator access only
New Solutions	Administrator access only

Troubleshooting

Login issues

“Unsupported USB Device” error message

Make sure a supported Smart Card reader is attached

Only the OmniKey reader that came with the printer is supported. Remove the unsupported reader and attach the OmniKey reader.

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

Try one or more of the following:

Make sure the authentication token is installed and running

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)**.
2. Verify 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 Lexmark Solutions Help Desk for assistance.

Make sure PKI Authentication is installed and running

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

Login screen does not appear when a Smart Card is inserted

Make sure the Smart Card is recognized by the reader

Contact the Lexmark Solutions Help Desk for assistance.

“The KDC and MFP clocks are different beyond an acceptable range; check the MFP's date and time” error message

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

Verify the date and time on the printer

1. From the Embedded Web Server, click **Settings** > **Security** > **Set Date and Time**.
2. If you have manually configured date and time settings, then verify and correct them as needed. Make sure the time zone and daylight savings time settings are correct.

   Note: If your network uses DHCP, then verify that NTP settings are not automatically provided by the DHCP server before manually configuring NTP settings.
3. If you have configured the printer to use an NTP server, then verify that those settings are correct and that the NTP server is functioning correctly.
4. Click **Submit** to save any needed changes.

“Kerberos configuration file has not been uploaded” error message

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

Make sure the Kerberos file has been uploaded

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. If the Simple Kerberos Setup has been configured in PKI Authentication, then clear the **Use Device Kerberos Setup** check box, and then click **Apply**.
3. If a Kerberos configuration file is needed, then:
   a. From the Embedded Web Server, click **Settings** > **Security** > **Security Setup** > **Kerberos 5**.
   b. Under Import Kerberos File, click **Browse** to locate the appropriate krb5.conf file, and then click **Submit**.

Users are unable to authenticate

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

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. If the Simple Kerberos Setup has been used, then verify that the Realm is correct and has been typed in uppercase.
3. If a krb5.conf file has been uploaded, then verify that the Realm entries in the configuration file are in uppercase.

“The Domain Controller Issuing Certificate has not been installed” error message

Make sure that the correct certificate has been installed on the printer

For information on installing, viewing, or modifying certificates, see “Creating and modifying digital certificates” on page 15.

“The KDC did not respond within the required time” error message

Try one or more of the following:

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

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. If the Simple Kerberos Setup has been configured in PKI Authentication, then verify the IP address or host name specified for the Domain Controller, and then click **Apply** to save any needed changes.
3. If a krb5.conf file has been uploaded, then verify that the IP address or host name specified for the Domain Controller is correct.

Make sure the KDC is available

You can specify multiple KDCs in the PKI Authentication settings or in the krb5.conf file. This will typically resolve the issue.

Make sure Port 88 is not blocked by a firewall

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

“User's Realm was not found in the Kerberos Configuration file” error message

Make sure the Windows Domain is specified in the Kerberos settings

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. Under Simple Kerberos Setup, add the Windows Domain in lowercase to the Domain setting.

   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, mapping the lowercase Windows Domain to the uppercase realm (similar to the existing mapping for the “mil” domain).

“Realm on the card was not found in the Kerberos Configuration File” error message

This error occurs during Smart Card login.

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

The PKI Authentication settings do not support multiple Kerberos Realm entries. If multiple realms are needed, then you must create and upload a krbf5.conf file containing the needed realms. If you are already using a Kerberos configuration file, then verify that the missing realm has been added to the file correctly.

“Client [NAME] unknown” error message

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

Verify that the Domain Controller information is correct

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. If the Simple Kerberos Setup has been configured, then verify that the IP address or host name of the Domain Controller is correct.
3. If you are using a Kerberos configuration file, then verify that the Domain Controller entry is correct.

Login does not respond at “Getting User Info”

For information about LDAP-related issues, see“LDAP issues” on page 41.

User is logged out almost immediately after logging in

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, and then click **Submit** to save your 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 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 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

This issue can occur during address book searches, user e-mail address searches, or user home directory searches. Try one or more of the following:

Verify 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. Verify that the host name (not the IP address) of the LDAP server has been entered in the Server Address field.
3. Click **Submit** to save any needed changes.

Verify or adjust Address Book Setup settings

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **Address Book Setup**.
2. Verify or adjust the following settings:
   - **Server Port**—Set this to 636.
   - **Use SSL/TLS**—Select **SSL/TLS**.
   - **LDAP Certificate Verification**—Select **Never**.
3. Click **Submit** to save any needed changes.

Narrow the LDAP search base

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

Verify that the LDAP attributes being searched for are correct

Verify that the LDAP attributes for the user's e-mail address and home directory are correct.

Held Jobs/Print Release Lite issues

“You are not authorized to use this feature” Held Jobs error message

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 Held Jobs function.

“Unable to determine Windows User ID” error message

Make sure PKI Authentication is setting the user ID for the session

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. In the User Session and Access Control section, for the Session Userid setting, specify how the Windows user ID will be obtained when a user attempts to log in:
   - **None**—The user ID is not set. You can 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. Click **Apply** to save any needed changes.

“There are no jobs available for [USER]” error message

Try one or more of the following:

Make sure PKI Authentication is setting the correct user ID

Normally, LDAP lookup is used to set this value.

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Authentication** > **Configure**.
2. In the User Session and Access Control section, select **LDAP Lookup** for the Session Userid setting.
3. Click **Apply** to save any needed changes.

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

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

Jobs are printing out immediately

Try one or more of the following:

Make sure PKI Held Jobs is installed and running

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

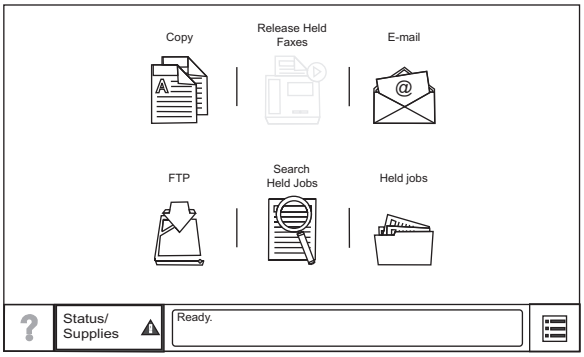
Make sure all jobs are required to be held

1. From the Embedded Web Server, click **Settings** > **Device Solutions** > **Solutions (eSF)** > **PKI Held Jobs** > **Configure**.
2. Under Advanced Settings, select the **Require All Jobs to be Held** and **Clear Print Data** check boxes.
3. Click **Apply**.

Appendix A: Using the touch screen

Understanding the home screen

The screen located on the front of the MFP 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):

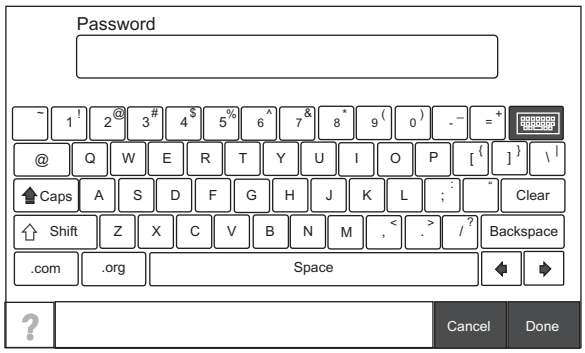


Touch  on the lower right to access settings and configuration menus for the device.

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

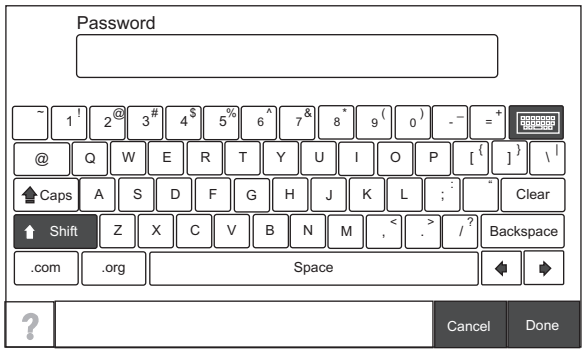
Using the on-screen keyboard

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: Description of access controls

Access controls

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.
NPA Network Adapter Setting Changes	When disabled, all network adapter NPA settings change commands are ignored.
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.
Remote Certificate Management	When disabled, it is no longer possible to manage certificates using remote management tools. Certificate Management is limited to the operations available from the printer control panel and 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.

Function access control	What it does
Settings Menu Remotely	This protects access to the General and Print Settings sections of the Settings menu from the Embedded Web Server.
Supplies Menu at the Device	This protects access to the Supplies menu from the printer control panel.
Supplies Menu Remotely	This protects access to the Supplies 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).
Solutions Configuration or eSF Configuration	This controls access to the configuration of any installed solutions.
Web Import/Export Settings	This controls the ability to import and export printer settings files (UCF files) from the Embedded Web Server.

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.

Function access control	What it does
Create Profiles	This controls the ability to create new profiles.
E-mail Function	This controls access to the Scan to E-mail function.
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.
Flash Drive Firmware Updates	This controls the ability to update firmware from a 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 to print from an attached PictBridge-enabled digital camera.
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 Solutions

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

Note: Depending on the solutions you have installed, additional solution-specific access controls may be listed below solutions 1–10. Use these additional access controls if they are available for your installed solutions. If no additional solution-specific access controls are available, then assign one of the ten numbered access controls to each solution you want to protect.

Appendix D: Using Common Access Cards

Using a Common Access Card to access the printer

1. Insert your Common Access Card into the card reader attached to the printer.
2. When prompted, enter your PIN using the keypad that appears on the touch screen, and then touch **Next**.

   It may take a moment for the printer to validate your credentials. After your credentials have been validated, the printer will return to the home screen.

Note: For more information about using the touch screen, see “Appendix A: Using the touch screen” on page 44.

Notices

LEXMARK SOFTWARE LICENSE AGREEMENT

PLEASE READ CAREFULLY BEFORE INSTALLING AND/OR USING THIS SOFTWARE: This Software License Agreement ("License Agreement") is a legal agreement between you (either an individual or a single entity) and Lexmark International, Inc. ("Lexmark") that, to the extent your Lexmark product or Software Program is not otherwise subject to a written software license agreement between you and Lexmark or its suppliers, governs your use of any Software Program installed on or provided by Lexmark for use in connection with your Lexmark product. The term "Software Program" includes machine-readable instructions, audio/visual content (such as images and recordings), and associated media, printed materials and electronic documentation.

BY USING AND/OR INSTALLING THIS SOFTWARE, YOU AGREE TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT SO AGREE, DO NOT INSTALL, COPY, DOWNLOAD, OR OTHERWISE USE THE SOFTWARE PROGRAM. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE AGREEMENT, PROMPTLY RETURN THE PRODUCT UNUSED AND REQUEST A REFUND OF THE AMOUNT YOU PAID. IF YOU ARE INSTALLING THIS SOFTWARE PROGRAM FOR USE BY OTHER PARTIES, YOU AGREE TO INFORM THE USERS THAT USE OF THE SOFTWARE PROGRAM INDICATES ACCEPTANCE OF THESE TERMS.

1. STATEMENT OF LIMITED WARRANTY. Lexmark warrants that the media (e.g., diskette or compact disk) on which the Software Program (if any) is furnished is free from defects in materials and workmanship under normal use during the warranty period. The warranty period is ninety (90) days and commences on the date the Software Program is delivered to the original end-user. This limited warranty applies only to Software Program media purchased new from Lexmark or an Authorized Lexmark Reseller or Distributor. Lexmark will replace the Software Program should it be determined that the media does not conform to this limited warranty.
2. DISCLAIMER AND LIMITATION OF WARRANTIES. EXCEPT AS PROVIDED IN THIS LICENSE AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LEXMARK AND ITS SUPPLIERS PROVIDE THE SOFTWARE PROGRAM "AS IS" AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ABSENCE OF VIRUSES, ALL WITH REGARD TO THE SOFTWARE PROGRAM. This Agreement is to be read in conjunction with certain statutory provisions, as that may be in force from time to time, that imply warranties or conditions or impose obligations on Lexmark that cannot be excluded or modified. If any such provisions apply, then to the extent Lexmark is able, Lexmark hereby limits its liability for breach of those provisions to one of the following: replacement of the Software Program or reimbursement of the price paid for the Software Program.
3. LICENSE GRANT. Lexmark grants you the following rights provided you comply with all terms and conditions of this License Agreement:
   - **a** Use. You may Use one copy of the Software Program. The term "Use" means storing, loading, installing, executing, or displaying the Software Program. If Lexmark has licensed the Software Program to you for concurrent use, you must limit the number of authorized users to the number specified in your agreement with Lexmark. You may not separate the components of the Software Program for use on more than one computer. You agree that you will not Use the Software Program, in whole or in part, in any manner that has the effect of overriding, modifying, eliminating, obscuring, altering or de-emphasizing the visual appearance of any trademark, trade name, trade dress or intellectual property notice that appears on any computer display screens normally generated by, or as a result of, the Software Program.
   - **b** Copying. You may make one (1) copy of the Software Program solely for purposes of backup, archiving, or installation, provided the copy contains all of the original Software Program's proprietary notices. You may not copy the Software Program to any public or distributed network.

c Reservation of Rights. The Software Program, including all fonts, is copyrighted and owned by Lexmark International, Inc. and/or its suppliers. Lexmark reserves all rights not expressly granted to you in this License Agreement.

d Freeware. Notwithstanding the terms and conditions of this License Agreement, all or any portion of the Software Program that constitutes software provided under public license by third parties ("Freeware") is licensed to you subject to the terms and conditions of the software license agreement accompanying such Freeware, whether in the form of a discrete agreement, shrink-wrap license, or electronic license terms at the time of download. Use of the Freeware by you shall be governed entirely by the terms and conditions of such license.

4 TRANSFER. You may transfer the Software Program to another end-user. Any transfer must include all software components, media, printed materials, and this License Agreement and you may not retain copies of the Software Program or components thereof. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end-user receiving the transferred Software Program must agree to all these License Agreement terms. Upon transfer of the Software Program, your license is automatically terminated. You may not rent, sublicense, or assign the Software Program except to the extent provided in this License Agreement.

5 UPGRADES. To Use a Software Program identified as an upgrade, you must first be licensed to the original Software Program identified by Lexmark as eligible for the upgrade. After upgrading, you may no longer use the original Software Program that formed the basis for your upgrade eligibility.

6 LIMITATION ON REVERSE ENGINEERING. You may not alter, reverse engineer, reverse assemble, reverse compile or otherwise translate the Software Program, except as and to the extent expressly permitted to do so by applicable law for the purposes of inter-operability, error correction, and security testing. If you have such statutory rights, you will notify Lexmark in writing of any intended reverse engineering, reverse assembly, or reverse compilation. You may not decrypt the Software Program unless necessary for the legitimate Use of the Software Program.

7 ADDITIONAL SOFTWARE. This License Agreement applies to updates or supplements to the original Software Program provided by Lexmark unless Lexmark provides other terms along with the update or supplement.

8 LIMITATION OF REMEDIES. To the maximum extent permitted by applicable law, the entire liability of Lexmark, its suppliers, affiliates, and resellers, and your exclusive remedy shall be as follows: Lexmark will provide the express limited warranty described above. If Lexmark does not remedy defective media as warranted, you may terminate your license and your money will be refunded upon the return of all of your copies of the Software Program.

9 LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, for any claim arising out of Lexmark's limited warranty, or for any other claim whatsoever related to the subject matter of this Agreement, Lexmark's liability for all types of damages, regardless of the form of action or basis (including contract, breach, estoppel, negligence, misrepresentation, or tort), shall be limited to the greater of $5,000 or the money paid to Lexmark or its authorized remarketers for the license hereunder for the Software Program that caused the damages or that is the subject matter of, or is directly related to, the cause of action.

IN NO EVENT WILL LEXMARK, ITS SUPPLIERS, SUBSIDIARIES, OR RESELLERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS OR REVENUES, LOST SAVINGS, INTERRUPTION OF USE OR ANY LOSS OF, INACCURACY IN, OR DAMAGE TO, DATA OR RECORDS, FOR CLAIMS OF THIRD PARTIES, OR DAMAGE TO REAL OR TANGIBLE PROPERTY, FOR LOSS OF PRIVACY ARISING OUT OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PROGRAM, OR OTHERWISE IN CONNECTION WITH ANY PROVISION OF THIS LICENCE AGREEMENT), REGARDLESS OF THE NATURE OF THE CLAIM, INCLUDING BUT NOT LIMITED TO BREACH OF WARRANTY OR CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), AND EVEN IF LEXMARK, OR ITS SUPPLIERS, AFFILIATES, OR REMARKETERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY YOU BASED ON A THIRD-PARTY CLAIM, EXCEPT TO THE EXTENT THIS EXCLUSION OF DAMAGES IS DETERMINED LEGALLY INVALID. THE FOREGOING LIMITATIONS APPLY EVEN IF THE ABOVE-STATED REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE.

10 TERM. This License Agreement is effective unless terminated or rejected. You may reject or terminate this license at any time by destroying all copies of the Software Program, together with all modifications, documentation, and merged portions in any form, or as otherwise described herein. Lexmark may terminate your license upon notice if you fail to comply with any of the terms of this License Agreement. Upon such termination, you agree to destroy

all copies of the Software Program together with all modifications, documentation, and merged portions in any form.

11 TAXES. You agree that you are responsible for payment of any taxes including, without limitation, any goods and services and personal property taxes, resulting from this Agreement or your Use of the Software Program.

12 LIMITATION ON ACTIONS. No action, regardless of form, arising out of this Agreement may be brought by either party more than two years after the cause of action has arisen, except as provided under applicable law.

13 APPLICABLE LAW. This Agreement is governed non-exclusively by the laws of the country in which you acquired the Software Program (or, if that country has a federal system of government, then this Agreement will be governed by the laws of the political subdivision in which you acquired the Software). If you acquired the Software in the United States, the laws of the Commonwealth of Kentucky shall govern. No choice of law rules in any jurisdiction will apply.

14 UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Software has been developed entirely at private expense and is provided with RESTRICTED RIGHTS. Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar FAR provisions (or any equivalent agency regulation or contract clause).

15 CONSENT TO USE OF DATA. You agree that Lexmark, its affiliates, and agents may collect and use information you provide in relation to support services performed with respect to the Software Program and requested by you. Lexmark agrees not to use this information in a form that personally identifies you except to the extent necessary to provide such services.

16 EXPORT RESTRICTIONS. You may not (a) acquire, ship, transfer, or reexport, directly or indirectly, the Software Program or any direct product therefrom, in violation of any applicable export laws or (b) permit the Software Program to be used for any purpose prohibited by such export laws, including, without limitation, nuclear, chemical, or biological weapons proliferation.

17 CAPACITY AND AUTHORITY TO CONTRACT. You represent that you are of the legal age of majority in the place you sign this License Agreement and, if applicable, you are duly authorized by your employer or principal to enter into this contract.

18 ENTIRE AGREEMENT. This License Agreement (including any addendum or amendment to this License Agreement that is included with the Software Program) is the entire agreement between you and Lexmark relating to the Software Program. Except as otherwise provided for herein, these terms and conditions supersede all prior or contemporaneous oral or written communications, proposals, and representations with respect to the Software Program or any other subject matter covered by this License Agreement (except to the extent such extraneous terms do not conflict with the terms of this License Agreement, any other written agreement signed by you and Lexmark relating to your Use of the Software Program). To the extent any Lexmark policies or programs for support services conflict with the terms of this License Agreement, the terms of this License Agreement shall control.

Index

T

U

www.lexmark.com

PN 3065326 Rev. 001