LEXMARK™

Common Criteria

Installation supplement and administrator guide

April 2010 **www.lexmark.com**

3060008-002

740 West New Circle Road
Lexington, Kentucky 40550

Edition notice

April 2010

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

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

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

UNITED STATES GOVERNMENT RIGHTS

This software and any accompanying documentation provided under this agreement are commercial computer software and documentation developed exclusively at private expense.

Trademarks

Lexmark, Lexmark with diamond design, and MarkVision are trademarks of Lexmark International, Inc., registered in the United States and/or other countries.

All other trademarks are the property of their respective owners.

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 3* (EAL 3). 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 45.

Supported devices

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

- Lexmark X463
- Lexmark X464
- Lexmark X466
- Lexmark X651
- Lexmark X652
- Lexmark X654
- Lexmark X656
- Lexmark X658
- Lexmark X734
- Lexmark X736
- Lexmark X738
- Lexmark X860
- Lexmark X862
- Lexmark X864

Operating environment

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

- The MFP will be installed in a cooperative, non-hostile environment that is physically secure.
- The administration platform and local area network are physically and logically secure.

- Authorized administrators are knowledgeable about, and capable of performing tasks related to the installation, configuration, and maintenance of the network environment including—but not limited to—operating systems, network protocols, and security 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 (if installed)

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.

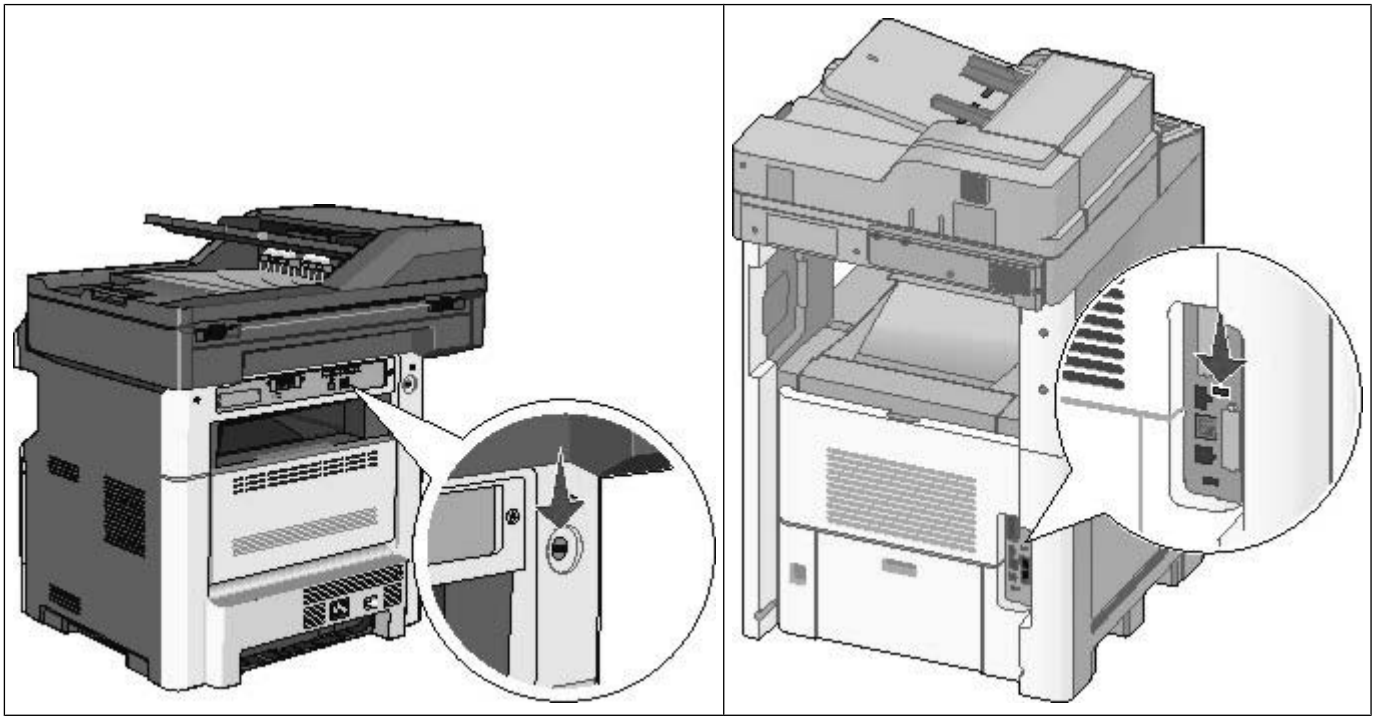
2. Turn the MFP on using the power switch.
3. From the home screen touch **Menus** > **Reports** > **Menu Settings Page**. Several pages of device information will print.
4. Under Installed Features, verify that no Download Emulator (DLE) option cards have been installed.
5. If you find additional interfaces, or if a DLE card has been installed, 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.

1. Verify that the MFP case is closed.
2. Locate the security lock port and attach a lock. It is the same type of lock port 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 lock port locations:



Encrypting the hard disk

Note: Not all devices have a hard disk installed. This section applies only to devices containing a hard disk.

If your MFP came with a hard disk installed, you must encrypt 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 fully powered up, the touch screen should display a list of functions, instead of standard home screen icons such as Copy or 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. Select **Disk Encryption**.
6. From the Disk Encryption menu, select **Enable**.

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

7 A message will be displayed asking you to confirm the action: **Contents will be lost. Continue?**

- Select **Yes** to proceed with disk wiping and encryption. A status bar will indicate the progress of the encryption task.

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

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

  Note: Disk encryption can take several hours to complete.

8 To finish, press **Back**, and then **Exit Config Menu**.

The MFP will 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 **Menus** > **Network/Ports** > **Standard USB**.

2 Scroll to the left to set the 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

Note: Not all devices have a hard disk installed. This section applies only to devices containing a hard disk.

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 **Menus** > **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: If used, the backup password should:

- Contain a minimum of 8 characters.
- Contain at least one lower case letter, one upper case letter, and one non-alphabetic character.
- Not be dictionary words or a variation of the User ID.

1. From the home screen, touch **Menus** > **Security** > **Edit Security Setups** > **Edit Backup Password** > **Password**.
2. Type the password you want to use, and then touch **Next**.
3. Re-enter the password, and then touch **Next** to save the new password and return to the Edit Backup Password screen.
4. From Edit Backup Password, 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. You will select one or more of these groups when configuring security templates, and then 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 **Menus** > **Security** > **Edit Security Setups** > **Edit Building Blocks** > **Internal Accounts** > **General Settings** > **Groups for Internal Accounts**.
2. On the Groups for Internal Accounts screen, select **Add Entry**.
3. For the Name, type **Administrator_Only**.
4. Touch **Next**, to save this group and return to the Groups for Internal Accounts screen.
5. On the Groups for Internal Accounts screen, select **Add Entry**.
6. For the Name, type **Authenticated_Users**.
7. Touch **Next**, to save this group.

Note: If there is a need to grant access to some administrative functions while restricting others, 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

Group name	Type of user group would be selected for
Administrator_Security	• Administrators permitted to access all device functions • Administrators permitted to use device functions, and access the Security menu
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 **Menus** > **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. From the Internal Accounts screen, select **Add Entry**.
4. Type the user's account name (example: "Jack Smith"), and then touch **Next**.
5. Type a user ID for the account (example: "jsmith"), and then touch **Next**.
6. Type a password for the account, and then touch **Next**. Passwords must:
   - Contain a minimum of 8 characters.
   - Contain at least one lower case letter, one upper case letter, and one non-alphabetic character.
   - Not be dictionary words or a variation of the User ID.
7. Re-type the password, and then touch **Next**.
8. Type the user's E-mail address (example: "jsmith@company.com"), and then touch **Next**.
9. 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, select all groups in which the administrator should be included.
   - For all other users, add only the Authenticated_Users group.
10. Touch **Next** to save the account and return to the Manage Internal Accounts screen, where the user should now be listed.
11. Repeat steps as needed to add additional 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, 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 **Menus** > **Security** > **Edit Security Setups** > **Edit Security Templates**.
2. Select **Add Entry**.
3. Type a unique name to identify the template. Use a descriptive name, such as ”Administrator _ Only”, or “Authenticated_Users”. Touch **Next**.
4. For **Authentication Setup**, select the internal accounts building block. Touch **Next**.
5. For **Authorization Setup**, select the internal accounts building block. Touch **Next**.
6. Select one or more groups to be included in the template, and then touch **Next** to save changes and return to Edit Security Templates.

Modifying or deleting an existing security template

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

1. From the home screen, touch **Menus** > **Security** > **Edit Security Setups** > **Edit Security Templates**.
2. To remove all security templates, select **Delete List**.
3. To remove an individual security template, select it from the list, and then touch **Delete Entry**
4. 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 48.

1. From the home screen, touch **Menus** > **Security** > **Edit Security Setups** > **Edit Access Controls**.
2. Select the appropriate level of protection for each function, as specified in the table below. 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**— Can be an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Any valid setting**— Can be any valid setting available for a function, at the discretion of the administrator.
- **Disabled**— Disables access to a function for all users and administrators.
- **Not applicable**—The function has been disabled by another setting. No change required, though it is recommended that you set these access controls to Administrator access only or Disabled.

Access Control	Level of protection
Address Book	Any valid setting
Cancel Jobs at the Device	Administrator access only
Change Language from Home Screen	Any valid setting
Color Dropout	Any valid setting
Configuration Menu	Disabled
Copy Color Printing	Any valid setting
Copy Function	Any valid setting
Create Bookmarks at the Device	Any valid setting
Create Bookmarks Remotely	Not applicable - all remote access disabled
Create Profiles	Disabled
E-mail Function	Any valid setting
eSF Configuration	Not applicable - all remote access disabled
Fax Function	Any valid setting
Firmware Updates	Disabled
Flash Drive Color Printing	Not applicable - USB port disabled
Flash Drive Firmware Updates	Not applicable - USB port disabled
Flash Drive Print	Not applicable - USB port disabled
Flash Drive Scan	Not applicable - USB port disabled
FTP Function	Any valid setting
Held Jobs Access	Disabled
Manage Shortcuts at the Device	Any valid setting
Manage Shortcuts Remotely	Not applicable - all remote access disabled
Network Ports/Menu at the Device	Administrator access only
Network Ports/Menu Remotely	Not applicable - all remote access disabled
NPA Network Adapter Setting Changes	Disabled
Operator Panel Lock	Any valid setting
Option Card Configuration at the Device	Any valid setting
Option Card Configuration Remotely	Not applicable - all remote access disabled
Paper Menu at the Device	Any valid setting
Paper Menu Remotely	Not applicable - all remote access disabled
PictBridge Printing	Not applicable - USB port disabled
PJL Device Setting Changes	Disabled

Access Control	Level of protection
Release Held Faxes	Administrator access only
Remote Certificate Management	Not applicable - all remote access disabled
Remote Management	Disabled
Reports Menu at the Device	Any valid setting
Reports Menu Remotely	Not applicable - all remote access disabled
Security Menu at the Device	Administrator access only
Security Menu Remotely	Not applicable - all remote access disabled
Service Engineer Menus at the Device	Administrator access only
Service Engineer Menus Remotely	Not applicable - all remote access disabled
Settings Menu at the Device	Administrator access only
Settings Menu Remotely	Not applicable - all remote access disabled
Solution 1	Authenticated users **Note:** When eSF applications are configured, Solution 1 controls access to Held Jobs.
Solutions 2–10	Administrator access only
Supplies Menu at the Device	Any valid setting
Supplies Menu Remotely	Not applicable - all remote access disabled
Use Profiles	Authenticated users
Web Import/Export Settings	Not applicable - all remote access disabled

Disabling home screen icons

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

1. From the home screen, touch **Menus** > **Settings** > **General Settings**.
2. Scroll to locate 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, 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

Access to the Embedded Web Server is disabled as part of the evaluated configuration on network-attached devices. Once a device is in the evaluated configuration, administrators can still adjust many settings using the touch screen. Restoring HTTP or HTTPS access to the Embedded Web Server is not recommended, because it removes your device from the evaluated configuration.

Note: If you enable HTTP or HTTPS access, be sure to disable it again after making any needed changes, to return your device to the evaluated configuration.

Enabling HTTP/HTTPS access to the Embedded Web Server

1. From the home screen, touch **Menus** > **Network/Ports** > **Standard Network** > **STD NET SETUP** > **TCP/IP**.
2. From TCP/IP, scroll to locate Enable HTTP Server.
3. Set Enable HTTP Server to **Yes**, and then touch **Submit**.
4. Again from the TCP/IP screen, scroll to locate Enable HTTPS.
5. Set Enable HTTPS to **Yes**, and then touch **Submit**.
6. Touch the home icon to return to the home screen.
7. Reboot the MFP by turning it off and back on using the power switch.

Disabling HTTP/HTTPS access using the EWS

1. From the EWS, click **Settings** > **Security** > **TCP/IP Port Access**.
2. Clear the following check boxes:
   - TCP 80 (HTTP)
   - TCP 443 (HTTPS)
3. Click **Submit**.

Disabling HTTP/HTTPS access using the touch screen

1. From the home screen, touch **Menus** > **Network/Ports** > **Standard Network** > **STD NET SETUP** > **TCP/IP**.
2. From TCP/IP, scroll to locate Enable HTTP Server.
3. Set Enable HTTP Server to **No**, and then touch **Submit**.
4. Again from the TCP/IP screen, scroll to locate Enable HTTPS.
5. Set Enable HTTPS to **No**.
6. Touch **Submit**.

Using the EWS

1. Type the device IP address or hostname 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 hostname is not readily apparent, you can find it by printing a network setup page.

Printing a network setup page

1. From the home screen, touch **Menus**.
2. Touch **Reports**.
3. Touch **Network Setup Page**.

   After the network setup page prints, the MFP will return to the home screen.

Settings for network-attached 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-attached 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 EWS, click **Settings** > **Security** > **Certificate Management**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.
2. Select **Set Certificate Defaults**.
3. Enter values in the appropriate fields:
   - **Common Name**—Type a name for the device.

     Note: Leave this field blank to use the device hostname 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 Name**—Type the country location for the company or organization issuing the certificate (2-character maximum).
   - **Province Name**—Type the name of the province where the company or organization issuing the certificate is located.

- **City Name**—Type the name of 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 to use the IPv4 address.

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

4 Click **Submit**.

Creating a new certificate

1 From the EWS, click **Settings** > **Security** > **Certificate Management**.

  Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2 Select **Device Certificate Management**.

3 Click **New**.

4 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 to use the hostname for the device.
- **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 Name**—Type the country location for the company or organization issuing the certificate (2-character maximum).
- **Province Name**—Type the name of the province where the company or organization issuing the certificate is located.
- **City Name**—Type the name of 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 to use the IPv4 address.

5 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 EWS, click **Settings** > **Security** > **Certificate Management**.

  Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2 Select **Device Certificate Management**.

3 Select a certificate from the list.

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

4 From here, you can:
- **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 EWS, click **Settings** > **Security** > **Certificate Management** > **Certificate Authority Management**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Click **New**.
3. **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 EWS, click **Settings** >**Security** > **IPSec**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Select the **IPSec Enable** check box, and then click **Submit**. Your browser will return to the EWS main page.
3. From the EWS, click **Settings** > **Security** > **IPSec**.
4. Under Settings, click **Encryption**, and select a Proposed Encryption Method of **3DES**.
5. Under Settings, click **Certificate Validation**, and select the **Validate Peer Certificate** check box.
6. Click **Submit**.
7. Under Connections, click either **Pre-Shared Key Authenticated Connections** or **Certificate Authenticated Connections**, and then one of the numbered **Host** fields.
8. Type the IP address of the client device you want to connect to the MFP. If using *Pre-Shared Key* (PSK) Authentication, also type the key.

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

9. Configure IPSec, as needed, on client devices that will connect to the MFP.

Disabling non-IP network protocols

IP is the only network protocol permitted under this evaluation. The NetWare, AppleTalk, and LexLink protocols must be disabled.

Using the EWS

Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

1. To disable NetWare:
   a. From the EWS, click **Settings** > **Network/Ports** > **NetWare**.
   b. Verify that the Activate and Port Enable check boxes are empty. If they are not, clear both boxes and then click **Submit**.
2. To disable AppleTalk:
   a. From the EWS, click **Settings** > **Network/Ports** > **AppleTalk**.
   b. Verify that the Activate check box is empty. If it is not, clear the check box and then click **Submit**.
3. To disable LexLink:
   a. From the EWS, click **Settings** > **Network/Ports** > **LexLink**.
   b. Verify that the Activate check box is empty. If it is not, clear the check box and then click **Submit**.

Using the touch screen

1. To disable AppleTalk:
   a. From the home screen, touch **Menus** > **Network/Ports** > **Standard Network** > **STD NET SETUP**.
   b. From the Std Network Setup screen, select **AppleTalk** > **Activate**.

      Note: It might be necessary to scroll down to find the AppleTalk selection.
   c. Set Activate to **No**.
   d. Touch **Submit**. The MFP will return to the AppleTalk screen. From there you can select **Back** to return to Std Network Setup, or the home icon to return to the home screen.
2. To disable NetWare:
   a. If not starting from Std Network Setup, from the home screen, touch **Menus** > **Network/Ports** > **Standard Network** > **STD NET SETUP**.
   b. From the Std Network Setup screen, select **NetWare** > **Activate**.

      Note: It might be necessary to scroll down to find the Netware selection.
   c. Set Activate to **No**.
   d. Touch **Submit**. The MFP will return to the NetWare screen. From there you can select **Back** to return to Std Network Setup, or the home icon to return to the home screen.
3. To disable LexLink:
   a. If not starting from Std Network Setup, from the home screen, touch **Menus** > **Network/Ports** > **Standard Network** > **STD NET SETUP**.
   b. From the Std Network Setup screen, select **LexLink** > **Activate**.

      Note: It might be necessary to scroll down to find the LexLink selection.

c Set Activate to **No**.

d Touch **Submit**. The MFP will return to the LexLink screen. From there you can select **Back** to return to Std Network Setup, 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. Once the HTTP and HTTPS ports have been disabled, you will no longer be able to access the EWS for remote management. For information about accessing the EWS, see "Using the Embedded Web Server" on page 15.

1 From the EWS, click **Settings** > **Security** > **TCP/IP Port Access**.

2 Clear the following check boxes:

- TCP 21 (FTP)
- UDP 69 (TFTP)
- TCP 79 (FINGER)
- TCP 80 (HTTP)
- UDP 161 (SNMP)
- TCP 443 (HTTPS)
- TCP 631 (IPP)
- TCP 5000 (XML)
- TCP 5001 (IPDS)
- TCP 6110/UDP6110/TCP6100
- TCP 8000 (HTTP)
- 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)
- Web Services

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, verify that NTP settings are not automatically provided by the DHCP server before manually configuring NTP settings.

Using the EWS

1. From the EWS, click **Settings** > **Security** > **Set Date and Time**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Select the **Enable NTP** check box, and then type the IP address or hostname of the NTP Server.
3. If the NTP server requires authentication, select the **Enable Authentication** check box, and then click "Install auth keys" to browse to the file containing the NTP authentication credentials.
4. Click **Submit**.

Using the touch screen

1. From the home screen touch **Menus** > **Security** > **Set Date and Time**.
2. Set Enable NTP to **On**.
3. Type the IP address or hostname of the NTP server.
4. If the NTP server requires authentication, 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, you must first configure Kerberos.

Using the EWS

1. From the EWS, click **Settings** > **Security** > **Security Setup**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Under Advanced Security Setup, Step 1, select **Kerberos 5**.
3. Under Simple Kerberos Setup, for KDC Address, type the IP address or hostname 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 EWS, click **Settings** > **Security** > **Security Setup**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Under Advanced Security Setup, Step 1, select **Kerberos 5**.
3. Under Import Kerberos File, click **Browse** to find and select 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 **Menus** > **Security** > **Edit Security Setups** > **Edit Building Blocks** >**Simple Kerberos Setup**.
2. From the Simple Kerberos Setup screen, select **KDC Address**, type the KDC (Key Distribution Center) IP address or hostname, and then touch **Submit**.
3. Select **KDC Port**, type the number of the port used by the Kerberos server, and then touch **Submit**.
4. Select **Realm**, and then type the realm used by the Kerberos server.

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

5. Touch **Submit**.

Security audit logging

Using the EWS

1. From the EWS, click **Settings** > **Security** > **Security Audit Log**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Select **Enable Audit**.
3. Type the IP address or hostname of the Remote Syslog Server, and then select **Enable Remote Syslog** .

   Note: The Enable Remote Syslog check box will be grayed out until an IP address or hostname 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 **Remote Syslog non-logged events**.

8 To have administrators automatically notified of 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, choose whether to have the log file **Wrap over oldest entries**, or **E-mail log then delete**.
- 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: In order to use E-mail alerts, you must 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 **Menus** > **Security** > **Security Audit Log** > **Configure Log**.

2 Set Enable Audit to **On**.

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

4 Type the IP address or hostname of the Remote Syslog Server.

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

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

7 For Log full behavior, choose whether to have the log file **Wrap over oldest entries**, or **E-mail log then delete**.

8 If you want the MFP to automatically notify administrators of certain log events, type one or more E-mail addresses (separated by commas) in the Admin's e-mail address field.

9 If you want the MFP to add a digital signature to E-mail alerts, 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, set “Remote Syslog non-logged events” to **On**.

12 If you want the MFP to automatically notify administrators of certain log events, 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 **On**.
   - To send an E-mail when the log becomes full and begins to overwrite the oldest entries, set "E-mail log wrapped alert" to **On**.
   - To send an E-mail when log storage space reaches a specified percentage of capacity, set "E-mail % full alert" to **On**.
   - 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 **On**.
   - To send an E-mail when log settings are changed, set "E-mail log settings changed alert" to **On**.
   - 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.
   - Select **Digitally sign exports** if you want the MFP to add a digital signature to E-mail alerts.

13 Touch **Submit**.

Note: In order to use E-mail alerts, you must also configure SMTP settings. For information about SMTP settings, see "E-mail" on page 24.

E-mail

User data sent by the MFP using E-mail must be sent as an attachment.

Using the EWS

1 From the EWS, 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. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

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

3 Under Web Link Setup, verify the following settings:
   - **Server**—must be blank.
   - **Login**—must be blank.
   - **Password**—must be blank.
   - **Path**—must be "/".
   - **Base file name image**—must be blank.
   - **Web Link**—must be blank.

SMTP settings

1 From the EWS, click **Settings** > **E-mail/FTP Settings** > **SMTP Setup**.

2 Under SMTP Setup, type the IP address or hostname 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 using a secondary or backup SMTP server, type the IP address/hostname 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), type a Reply Address.

7 From the Use SSL 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, 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/server environment.

11 If the MFP must provide credentials in order to send E-mail, enter the information appropriate for your network under Device Credentials.

Using the touch screen

1 From the home screen, touch **Menus** > **Settings** > **E-mail Settings** > **E-mail Server Setup**.

2 Scroll to locate Web Link Setup. Select **Web Link Setup**, and then verify the following settings:
- **Server**—must be blank.
- **Login**—must be blank.
- **Password**—must be blank.
- **Path**—must be "/".
- **Base file name image**—must be blank.
- **Web Link**—must be blank.

3 Touch **Back**, and then touch **Back** again to return to the E-mail Settings screen.

4 Scroll to locate "E-mail images sent as". Set "E-mail images sent as" to **Attachment**.

5 Touch **Submit**.

SMTP settings

1 From the home screen, touch **Menus** > **Network/Ports** > **SMTP Setup**.

2 Type the IP address or hostname of the Primary SMTP Gateway the MFP will use for sending E-mail.

3 Select the Primary SMTP Gateway Port number of the destination server.

4 If using a secondary or backup SMTP server, type the IP address/hostname, and select an SMTP port for that server.

5 Set the SMTP Timeout; 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), type 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, 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/server environment.

11 If the MFP must provide credentials in order to send E-mail, 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, you must disable fax forwarding, enable held faxes, and disable driver to fax.

Using the EWS

1 From the EWS, click **Settings** > **Fax Settings** > **Analog Fax Setup**.

Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

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

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

4 Click **Submit**, to save changes and return to Settings.

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 **Menus** > **Settings** > **Fax Settings** > **Analog Fax Setup** > **Fax Receive Settings**.

2 Scroll to locate Holding Faxes. Select **Holding Faxes**.

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

4 Touch **Submit**, to save changes and return to Fax Receive Settings.

5 From the Fax Receive Settings screen, scroll to locate Fax Forwarding. Set Fax Forwarding to **Print**.

6 Touch **Submit**, to save changes and return to Analog Fax Setup.

7 From the Analog Fax Setup screen, select **Fax Send Settings**.

8 Scroll to locate "Driver to fax". Set "Driver to fax" to **No**.

9 Touch **Submit**.

Setting up a fax storage location (optional)

If your device came with a hard disk installed, you have the option of setting up a fax storage location on the disk, if needed.

Note: Not all devices have a hard disk installed. This section applies only to devices containing a hard disk.

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 fully powered up, the touch screen should display a list of functions, instead of standard home screen icons such as Copy or 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. To set up a fax storage location, press the down arrow to scroll through the configuration menus until you locate the Fax Storage Location menu selection.
5. Select **Disk** as the Fax Storage Location, and then touch **Submit**.

   The MFP will return to the main Configuration menu.
6. To finish, press **Back**, and then **Exit Config Menu**. The MFP will 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 **Menus** > **Security** > **Miscellaneous Security Settings**.
2. For Security Reset Jumper, scroll to select **No Security** (to remove security only from function access controls), **Reset to Defaults** (to return all security settings to default values), or **No Effect** (to remove access to *all* security menus—use with caution).
3. Touch **Submit** to save the changes.

Warning—Potential Damage: If "No Effect" is chosen and the password (or other applicable credential) is lost, 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 login 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-attached devices: internal accounts, LDAP+GSSAPI, or 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. You will select one or more of these groups when configuring security templates, and then 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 EWS, click **Settings** > **Security** > **Security Setup**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Under Advanced Security Setup, Step 1, select **Internal Accounts**.
3. Select **Setup groups for use with internal accounts**.
4. Type a Group Name.
5. Click **Add**.
6. Repeat steps as needed to add more groups.

Step 2: Creating accounts

1. From the EWS, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, Step 1, select **Internal Accounts**.
3. From the Required User Credentials list, select **User ID and Password**.
4. Click **Submit**.
5. Return to **Settings** > **Security** > **Security Setup** > **Internal Accounts**.
6. Select **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 lower case letter, one upper case letter, and one non-alphabetic character.
     - Not be dictionary words or a variation of the User ID.
   - **Re-enter Password**—Type the password entered in the field above.
   - **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+GSAPPI. For information about configuring Kerberos, see "Kerberos" on page 21.

Using the EWS

1. From the EWS, click **Settings** > **Security** > **Security Setup**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.
2. Under Advanced Security Setup, Step 1, select **LDAP+GSSAPI**.
3. Click **Add an LDAP+GSSAPI Setup**.
4. The LDAP+GSSAPI Server Setup dialog is divided into four parts:

General Information

- **Setup Name**—Used to identify each particular LDAP+GSSAPI Server Setup when creating security templates.
- **Server Address**—The IP address or the hostname 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**—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**—Specify either **`sAMAccountName`** (the default), **`uid`**, **`userid`**, **`user-defined`**, or **`cn`** (common name).
- **Search Base**—The node in the LDAP server where user accounts reside. Multiple search bases can be entered, separated by semi-colons.

  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 semi-colons.
- **Search Timeout**—Specify a value of from 5-30 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)

- **MFP Kerberos Username**— Type the distinguished name of the print server(s).
- **MFP Password**—Type the Kerberos password for the print server(s).

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 (optional).

LDAP Group Names

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

5 Click **Submit**.

Using the touch screen

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

2 Select **Add Entry**.

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

4 For Server Address, type the IP address or hostname of the LDAP server where authentication will be performed, and then touch **Next**. The MFP will return to General Information.

5 From the General Information screen, select **General Information**, and then adjust the following settings as needed:

- **Setup Name**—Used to identify each particular LDAP+GSSAPI Server Setup when creating security templates.
- **Server Address**—The IP address or the hostname of the LDAP server where authentication will be performed.
- **Server Port**—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**—Specify either **`sAMAccountName`** (the default), **`uid`**, **`userid`**, **`user-defined`**, or **`cn`** (common name).
- **Search Base**—The node in the LDAP server where user accounts reside. Multiple search bases can be entered, separated by semi-colons.

  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 semi-colons.
- **Search Timeout**—Specify a value of from 5-30 seconds.

Touch **Submit**, to save settings and return to General Information.

6 From the General Information screen, select **Device Credentials**, and then adjust the following settings as needed (optional):

- **MFP Kerberos Username**— The distinguished name of the print server(s).
- **MFP Password**—The Kerberos password for the print server(s).

Touch **Submit**, to save settings and return to General Information.

7 From the General Information Screen, select **Search Specific Object Classes**, and then adjust the following settings as needed (optional):

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

Touch **Submit**, to save settings and return to General Information.

8 From the General Information Screen, select **LDAP Group Names**, and then adjust the following settings as needed:

- **Group Search Base**—Administrators can associate as many as 32 named groups stored on the LDAP server, by entering identifiers for those groups under the **Group Search Base** list. Both the Short name for group, and Group Identifier must be provided.
- **LDAPGSSAPI Groups 1-32**—For each LDAPGSSAPI Group you want to define, select a numbered group, and then specify the **Short name for the group**, and the **Group Identifier**. Touch **Submit** to save changes and return to the LDAP Group Names screen.

When creating Security Templates, you will pick groups from this setup for controlling 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 SmartCards 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 MFP" on page 51.

Note: You must configure Kerberos before setting up CAC access. For information about configuring Kerberos, see "Kerberos" on page 21.

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 EWS, click **Settings** > **Embedded Solutions**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. On the Solutions tab, verify that the authentication token is not running. If it is not, select the check box next to the application, and then click **Start**.
3. After the Solutions tab reloads, the authentication token application should now 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 EWS, click **Settings** > **Embedded Solutions**.
2. Under Installed Solutions, select the check box next to PKI Authentication, and 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 desired, provide custom Logon Screen Text, with special instruction for users, or a custom Logon Screen Image. Custom screen images must be in GIF format, and no larger than 800 x 320 pixels.
7. Clear the **Allow Copy without Card** check box.
8. Clear the **Allow Fax without Card** check box.
9. Set User Validation Mode to **Active Directory**.
10. Select **Use MFP Kerberos Setup** to use the Kerberos settings already configured on the MFP, or clear the check box to use Simple Kerberos Setup.
11. For Simple Kerberos Setup you must provide:
    - **Realm**—The Kerberos realm as configured in Active Directory; typically the Windows Domain Name. The Realm must be entered in UPPERCASE.
    - **Domain Controller**—IP address or hostname of the domain controller used for validation. Multiple values can be entered, separated by commas; they will be tried in the order listed.

- **Domain**—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, "mil" is the principal name. In this case, you would enter the Domain as "mil,.mil".
- **Timeout**—The amount of time the MFP should wait for a response from the domain controller before moving to the next one in the list.

12 If users are allowed to login manually, 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.

13 Select a DC Validation Mode for validating the domain controller certificate when users login to the MFP:
- **Device Certificate Validation**—The most common method. The certificate of the CA that issued the domain controller certificate must also be installed on the MFP.
- **MFP 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.

14 If you selected OCSP Validation, configure the following:
- **Responder URL**—The IP address or hostname 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**—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 login even if the OCSP response indicates the certificate status is unknown.

15 Under User Session and Access Control, verify that **Share Session with LDD** is not selected.

16 Under Advanced Settings, select **Disable Reverse DNS Lookups** if reverse lookups are not supported on your network.

17 To use only the information provided by the specified domain controller, select **Disable LDAP Referrals**.

Note: Leaving LDAP referrals enabled can increase LDAP search times.

18 If DNS is not enabled on the network, or if some servers are multi-homed, click **Browse** to locate a **Hosts File** with hostname-IP address mappings.

19 Select **Wait for Active Network**, to display **`Waiting for network...`** on the touch screen after the MFP is powered on. This message disappears when the network becomes available.

20 Click **Apply**.

Note: You must install at least one Certificate Authority (CA) certificate in order for PKI Authentication to work. For more information on uploading a CA certificate, see "Creating and modifying digital certificates" on page 16.

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, 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 EWS, click **Settings** > **Security** > **Security Setup**.

   Note: For information about accessing the EWS, see “Using the Embedded Web Server” on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. Under Advanced Security Setup, Step 2, select **Security Template**.
3. Under Manage Security Templates, select **Add a Security Template**.
4. In the Security Templates 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 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, and/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 32.

6. Click **Add authorization**, and then select 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, and/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 EWS, click **Settings** > **Security** > **Security Setup**.
2. Under Advanced Security Setup, Step 2, select **Security Template**.
3. Select a security template from the list.
4. Edit the fields as necessary.
5. Click **Modify** to save changes, or **Cancel** to retain previously configured values.

Notes:

- Clicking **Delete List** 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** in the Settings screen for that template.
- You can only delete a security template 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 MFP until released by an authorized user.

1. From the EWS, click **Settings** > **Embedded Solutions** > **PKI Held Jobs** > **Configure**.

   Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2. You can specify custom Icon Text to be displayed above the Held Jobs icon on the MFP home screen.
3. To select an alternate image for the Up Icon (the image that displays 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 determine 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 **All jobs print automatically**, to have all jobs pending for a user print automatically when they select the Held Jobs icon.
   - Select **Show Copies Screen** if you want to enable users to change the number of copies for each job from the printer.
   - Select **Allow Users to Print All** if you want to enable 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 determine the order in which print jobs are displayed.
7. 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, Verify and Repeat Print jobs can also be set to expire, either at the same time Confidential jobs expire, or at another time:
   - **Verify Job Expiration**—Can be set to **Off**, **Same as Confidential Print**, or one of four intervals ranging from one hour to one week.
   - **Repeat Job Expiration**—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 **Require All Jobs to be Held** and **Clear Print Data**.

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 the "Access Controls" on page 48.

1 From the EWS, click **Settings** > **Security** > **Security Setup**.

Note: For information about accessing the EWS, see "Using the Embedded Web Server" on page 15. Be sure to disable HTTP and HTTPS access after you have finished using the EWS.

2 Under Advanced Security Setup, Step 3, select **Access Controls**.

3 Select the appropriate level of protection for each function, as specified in the table below.

4 Click **Submit**.

Levels of protection include:

- **Administrator access only**— Can be an internal account or a security template, as long as it provides administrator-only authentication and authorization.
- **Any valid setting**— Can be any valid setting available for a function, at the discretion of the administrator.
- **Disabled**— Disables access to a function for all users and administrators.
- **Not applicable**—The function has been disabled by another setting. No change required, though it is recommended that you set these access controls to Administrator access only or Disabled.

Access Control	Level of protection
Address Book	Any valid setting
Cancel Jobs at the Device	Administrator access only
Change Language from Home Screen	Any valid setting
Color Dropout	Any valid setting
Configuration Menu	Disabled
Copy Color Printing	Any valid setting
Copy Function	Any valid setting
Create Bookmarks at the Device	Any valid setting
Create Bookmarks Remotely	Not applicable - all remote access disabled
Create Profiles	Disabled
E-mail Function	Any valid setting
eSF Configuration	Not applicable - all remote access disabled
Fax Function	Any valid setting
Firmware Updates	Disabled
Flash Drive Color Printing	Not applicable - USB port disabled
Flash Drive Firmware Updates	Not applicable - USB port disabled

Access Control	Level of protection
Flash Drive Print	Not applicable - USB port disabled
Flash Drive Scan	Not applicable - USB port disabled
FTP Function	Any valid setting
Held Jobs Access	Disabled
Manage Shortcuts at the Device	Any valid setting
Manage Shortcuts Remotely	Not applicable - all remote access disabled
Network Ports/Menu at the Device	Administrator access only
Network Ports/Menu Remotely	Not applicable - all remote access disabled
NPA Network Adapter Setting Changes	Disabled
Operator Panel Lock	Any valid setting
Option Card Configuration at the Device	Any valid setting
Option Card Configuration Remotely	Not applicable - all remote access disabled
Paper Menu at the Device	Any valid setting
Paper Menu Remotely	Not applicable - all remote access disabled
PictBridge Printing	Not applicable - USB port disabled
PJL Device Setting Changes	Disabled
Release Held Faxes	Administrator access only
Remote Certificate Management	Not applicable - all remote access disabled
Remote Management	Disabled
Reports Menu at the Device	Any valid setting
Reports Menu Remotely	Not applicable - all remote access disabled
Security Menu at the Device	Administrator access only
Security Menu Remotely	Not applicable - all remote access disabled
Service Engineer Menus at the Device	Administrator access only
Service Engineer Menus Remotely	Not applicable - all remote access disabled
Settings Menu at the Device	Administrator access only
Settings Menu Remotely	Not applicable - all remote access disabled
Solution 1	Authenticated users **Note:** When eSF applications are configured, Solution 1 controls access to Held Jobs.
Solutions 2–10	Administrator access only
Supplies Menu at the Device	Any valid setting

Access Control	Level of protection
Supplies Menu Remotely	Not applicable - all remote access disabled
Use Profiles	Authenticated users
Web Import/Export Settings	Not applicable - all remote access disabled

Troubleshooting

Login Issues

"Unsupported USB Device" error message

A non-supported SmartCard reader is attached

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

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

If the printer home screen does not return to a locked state when not in use, check the following:

The authentication token is not installed or running.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions**.
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 not running, 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, contact the Lexmark Solutions Help Desk for assistance.

PKI Authentication is not installed or running.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions**.
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 not running, 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, contact the Lexmark Solutions Help Desk for assistance.

Login screen does not appear when a SmartCard is inserted

The SmartCard is not 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 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, verify and correct as needed. Make sure the time zone and daylight savings time settings are correct.

   Note: If your network uses DHCP, 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, verify that those settings are correct, and that the NTP server is functioning correctly.

"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

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

Users are unable to authenticate

The Realm specified in the Kerberos settings is in lowercase

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

"The Domain Controller Issuing Certificate has not been installed" error message

If a certificate has been installed but it is not the correct certificate, the error message displayed will be "The Domain Controller Issuing Certificate [NAME OF CERTIFICATE] has not been installed.

No certificate, or an incorrect certificate has been installed on the printer

For information on installing, viewing, or modifying certificates, see "Creating and modifying digital certificates" on page 16.

"The KDC did not respond within the required time" error message

The IP address or hostname of the KDC is not correct

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

The KDC is not currently available

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

Port 88 is blocked by a firewall

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

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

This error occurs during manual login, and indicates the Windows Domain is not specified in the Kerberos settings.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **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", change the Domain setting to "mil,.mil,x.y.z".
3. If using a krb5.conf file, add an entry to the domain_realm section, mapping the lower case 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 SmartCard login.

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

"Client [NAME] unknown" error message

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

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

Login hangs for a long time at "Getting User Info..."

For information about LDAP-related issues, see"LDAP Issues" on page 42.

User is logged out almost immediately after logging in

Try increasing 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.

LDAP Issues

LDAP lookups take a long time, and then may or may not work

This normally occurs either during login (at "Getting User Info"), or during address book searches.

Port 389 (non-SSL) or port 636 (SSL) is blocked by a firewall

These ports are used by the printer to communicate with the LDAP server, and must be open in order for LDAP lookups to work.

Reverse DNS lookups are disabled on the network

The printer uses reverse DNS lookups to verify IP addresses. If reverse lookup is disabled on the network:

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.
2. Select **Disable Reverse DNS Lookups**.
3. Click **Apply**.

LDAP Referrals are enabled

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.
2. Select **Disable LDAP Referrals**.

Note: Leaving LDAP referrals enabled can increase LDAP search times.

3 Click **Apply**.

The LDAP search base is 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 normally occurs during address book searches, user E-mail address searches, or user home directory searches.

The Address Book Setup contains an IP address for the LDAP server

1 From the Embedded Web Server, click **Settings** > **Network/Ports** > **Address Book Setup**.

2 Verify that the Server Address has been entered as the hostname (not the IP address), of the LDAP server.

3 Click **Submit** to save any needed changes.

Port 389 is being used, but the LDAP server requires SSL

1 From the Embedded Web Server, click **Settings** > **Network/Ports** > **Address Book Setup**.

2 Verify or adjust the following settings:

- **Server Port**—Should be 636.
- **Use SSL/TLS**—Select **SSL/TLS**.
- **LDAP Certificate Verification**—Select **Never**.

3 Click **Submit** to save any needed changes.

The LDAP search base is incorrect

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

The LDAP attribute being searched for is not correct

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

Held Jobs/Print Release Lite Issues

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

This error usually indicates the user in not in an Active Directory group that is authorized to use the function. If user authorization is enabled for Held Jobs, add the user to an Active Directory group that is included in the authorization list for this function.

“Unable to determine Windows User ID” error message

This error indicates that PKI Authentication is not setting the userid for the session.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.
2. Under User Session and Access Control, select a **Session Userid** to determine how the Windows Userid will be obtained when a user attempts to log in:
   - **None**—The userid is not set. You can select this option if the userid is not needed by other applications.
   - **User Principal Name**—The SmartCard principal name, or the credential provided by manual login is used to set the userid (userid@domain).
   - **EDI-PI**—The userid portion of the SmartCard principal name, or the credential provided by manual login is used to set the userid (userid).
   - **LDAP Lookup**—The userid is retrieved from Active Directory.
3. Click **Apply** to save any needed changes.

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

PKI Authentication is not setting the correct userid

Normally, LDAP lookup is used to set this value.

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

The userid displayed is correct, but no jobs are listed

The user may have sent the job (or jobs) to a different printer, or the jobs were automatically deleted because they were not printed in time.

Jobs are printing out immediately

Most likely, the user is not selecting the print and hold feature when printing the job. Show the user how to select the print and hold feature in the print driver.

Appendix A: Using the touch screen

The home screen

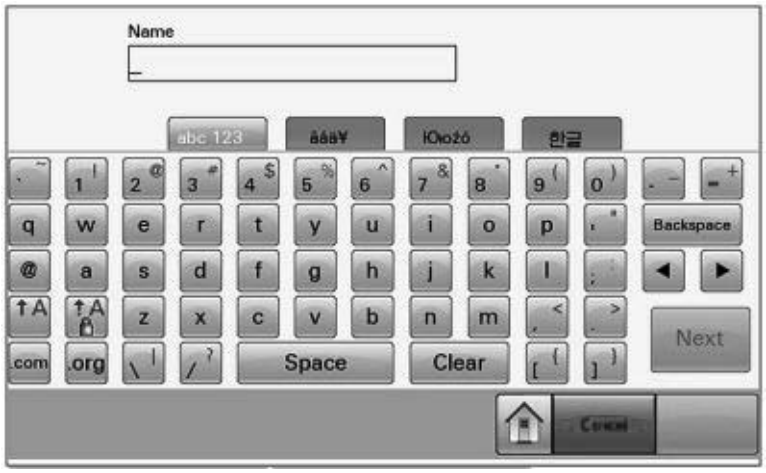
The screen located on the front of the MFP is touch-sensitive, and can be used to access device functions, and navigate settings and configuration menus. The “home screen” looks similar to this (yours may contain additional icons):

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

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

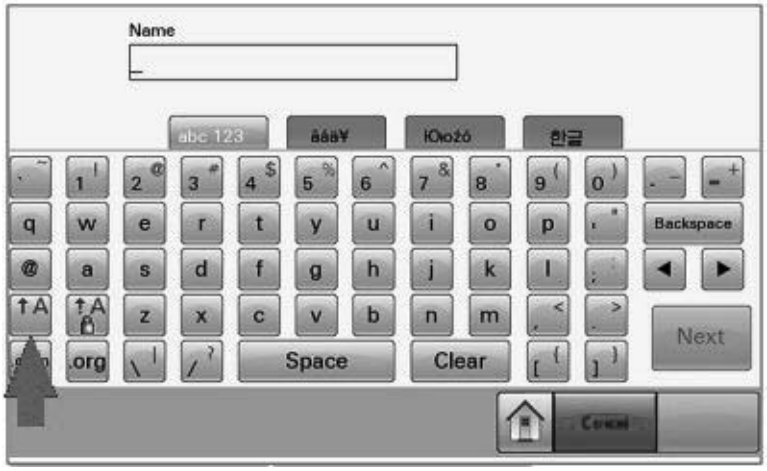
Using the on-screen keyboard

Some device settings require one or more alphanumeric entries, such as server addresses, user names, or passwords. When an alphanumeric entry is needed, a keyboard will be displayed:



As you touch the letters and numbers, your selections will be displayed in a corresponding field at the top of the screen. The keyboard display may also contain other icons, such as Next, Submit, Cancel, or the home screen graphic.

To type a single upper case or Shift character, touch the **up-arrow A**, and then touch the letter or number you need to capitalize or shift-select. To turn on caps-lock, touch the **up-arrow A with the lock symbol**, and then continue typing. Uppercase/Shift will remain engaged until you touch the lock key 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 device type and installed options, some Access Controls (referred to on some devices as Function Access Controls) may not be available for your printer.

Function Access Control	What it does
Address Book	Controls the ability to perform address book searches in the Scan to Fax and Scan to Email functions
Change Language from Home Screen	Controls access to the Change Language feature from the printer control panel
Color Dropout	Controls the ability to use the Color Dropout feature for scan and copy functions
Configuration Menu	Protects access to the Configuration Menu
Copy Color Printing	Controls the ability to perform color copy functions. Users who are denied will have their copy jobs output in black and white
Copy Function	Controls the ability to use the Copy function
Create Bookmarks at the Device	Controls the ability to create new bookmarks from the printer control panel
Create Bookmarks Remotely	Controls the ability to create new bookmarks from the Bookmark Setup section of the Settings menu in the Embedded Web Server
Create Profiles	Controls the ability to create new profiles
E-mail Function	Controls access to the Scan to Email function
eSF Configuration	Controls access to the configuration of any installed eSF applications
Fax Function	Controls access to the Scan to Fax function
Firmware Updates	Controls the ability to update firmware from any source other than a flash drive. Firmware files which are received via FTP, the Embedded Web Server, etc., will be ignored (flushed) when this function is protected.
Flash Drive Color Printing	Controls the ability to print color from a flash drive. Users who are denied will have their print jobs output in black and white.
Flash Drive Firmware Updates	Controls the ability to update firmware from a flash drive
Flash Drive Print	Controls the ability to print from a flash drive
Flash Drive Scan	Controls the ability to scan documents to a flash drive
FTP Function	Controls access to the Scan to FTP function
Held Jobs Access	Protects access to the Held Jobs function
Manage Shortcuts at the Device	Protects access to the Manage Shortcuts section of the Settings menu on the printer control panel
Manage Shortcuts Remotely	Protects access to the Manage Shortcuts item of the Settings menu from the Embedded Web Server

Function Access Control	What it does
Network Ports/Menu at the Device	Protects access to the Network/Ports section of the Settings menu from the printer control panel
Network Ports/Menu Remotely	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 adaptor NPA settings change commands are ignored
Operator Panel Lock	Protects access to the Operator Panel Lock. Users who are denied access cannot enable or disable the printer control panel lock.
Option Card Configuration at the Device	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 in the device.
Option Card Configuration Remotely	Controls access to the Option Card Configuration item of the Settings menu from the Embedded Web Server. This applies only when an Option Card with configuration options is installed in the device.
Paper Menu at the Device	Protects access to the Paper menu from the printer control panel.
Paper Menu Remotely	Protects access to the Paper menu from the Embedded Web Server.
PictBridge Printing	Controls ability to print from an attached PictBridge capable digital camera.
PJL Device Setting Changes	When disabled, all device settings changes requested by incoming print jobs are ignored.
Release Held Faxes	Controls the ability to release (print) Held Faxes.
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.
Remote Management	Controls access to printer settings and functions by remote management tools such as MarkVision™ Professional. When protected, no printer configuration setting can be altered except through a secured communication channel (such as that provided by a properly configured installation of MarkVision Professional).
Reports Menu at the Device	Protects access to the Reports menu from the printer control panel
Reports Menu Remotely	Protects access to the Reports menu from the Embedded Web Server
Security Menu at the Device	Protects access to the Security menu from the printer control panel
Security Menu Remotely	Protects access to the Security menu from the Embedded Web Server
Service Engineer Menus at the Device	Protects access to the Sevice Engineer menu from the printer control panel
Service Engineer Menus Remotely	Protects access to the Service Engineer menu from the Embedded Web Server
Settings Menu at the Device	Protects access to the General and Print Settings sections of the Settings menu from the printer control panel
Settings Menu Remotely	Protects access to the General and Print Settings items of the Settings menu from the Embedded Web Server
Solution 1–10	The Solution 1 through Solution 10 Access Controls can be assigned to installed eSF applications and/or profiles created by LDSS. The Access Control for each Solution is assigned in the creation or configuration of the application or profile.

Function Access Control	What it does
Supplies Menu at the Device	Protects access to the Supplies menu from the printer control panel
Supplies Menu Remotely	Protects access to the Supplies menu from the Embedded Web Server
User Profiles	Controls access to Profiles, such as scanning shortcuts, workflows, or eSF applications
Web Import/Export Settings	Controls the ability to import and export printer settings files (UCF files) from the Embedded Web Server

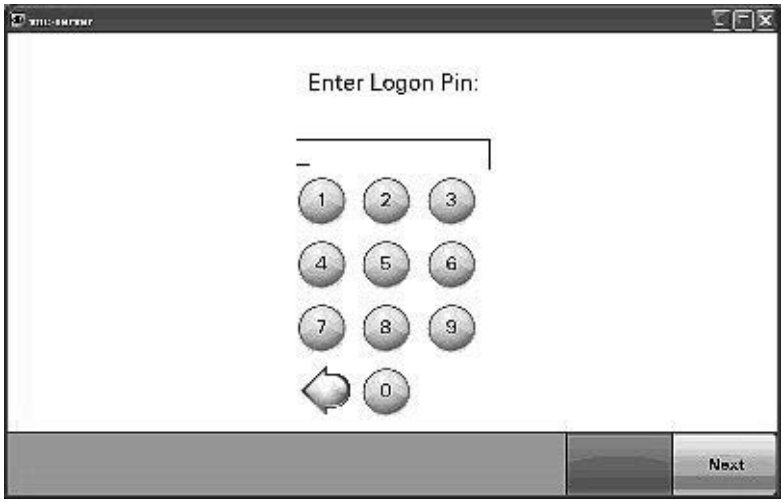
Appendix D: Using Common Access Cards

Using a Common Access Card to access the MFP

1 Insert your Common Access Card into the card reader attached to the MFP:

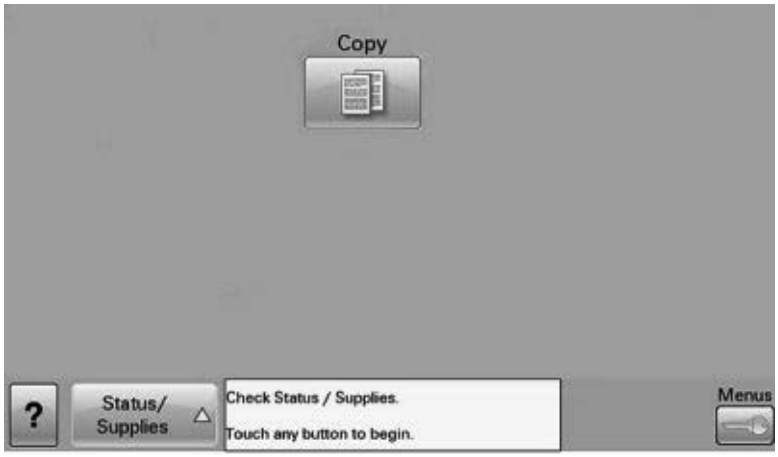
Note: The appearance of your MFP, including the location of the card reader, may vary.

2 When prompted, use the number pad located on the touch screen to enter your logon PIN, and then touch **Next**:



It may take a moment for the MFP to validate your credentials:

3 After your logon credentials have been validated, the MFP will return to the home screen:



Note: The MFP home screen may contain different icons than the one shown here. For more information about using the touch screen, see “Appendix A: Using the touch screen” on page 45.

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

S

T

U