PKI-Enabled Device

Installation and Configuration Guide

February 2010 **www.lexmark.com**

740 West New Circle Road
Lexington, Kentucky 40550

Edition notice

February 2010

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

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

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

Configuring PKI-enabled devices

Overview

This guide describes how to install Lexmark PKI applications, and configure supported Lexmark devices to take advantage of the enhanced security features of the *Public Key Infrastructure* (PKI) capabilities of your network. The applications include:

PKI Authentication—Provides the mechanism for authenticating and authorizing printer users.

PKI S/MIME Email—Enables users to sign and encrypt E-mail messages.

PKI Scan to Network—Enables users to scan documents to a network file share.

PKI Held Jobs—Holds print jobs securely at the printer until released by an authorized user. Also referred to as Print Release Lite.

PKI Authentication is the only required application, and must be installed and configured if you plan to attach a SmartCard reader to the printer.

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.

For information about physically setting up the printer or using printer features, see the *User Guide* or *Software and Documentation CD* that came with the printer.

Supported devices

This guide covers the following models:

Single-function devices

- Lexmark C736
- Lexmark T654
- Lexmark T656
- Lexmark W85x

Multi-function devices

- Lexmark X46x
- Lexmark X65x
- Lexmark X73x
- Lexmark X86x

Before configuring the printer

After initial setup tasks have been completed according to the *User's Guide*, connect the printer to your network. For information on how to connect your printer to a network, see the *Networking Guide* that came with the printer.

Accessing the Embedded Web Server

Most configuration tasks will be performed through the printer Embedded Web Server, so make sure you are able to connect:

1. Type the printer IP address or hostname in the address field of your Web browser. If the IP address is not readily apparent, you can print a network setup page to find it.
2. After you have connected to the Embedded Web Server, use the navigation menu on the left to access configuration and report menus.

Note: You can find additional information about many application settings using the mouseover help found in the Embedded Web Server. To access this information, position your cursor over the question mark symbol next to a setting.

Printing a network setup page

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

   The network setup page prints, and the printer returns to the home screen.

Installing the firmware and applications

Verifying and updating the firmware

Enabling PKI support for your printer involves three main components:

- The printer firmware
- The authentication token
- The Lexmark PKI applications

All three must be installed and configured before you install a SmartCard reader on your printer.

Verifying the firmware

1. From the Embedded Web Server, click **Reports** > **Device Information**.
2. Under Device Information, scroll down until you see Base =. See the table below to verify that your printer has the minimum required firmware version.

Printer model	Minimum firmware version
C736	LR.SK.P224cLDc
T654	LR.JP.P224cLDc
T656	LR.SJ.019
W85x	LR.JB.P108LDc
X46x	LR.BS.P224cLDc
X65x	LR.MN.P224cLDc

Printer model	Minimum firmware version
X73x	LR.FL.P224cLDc
X86x	LR.SP.P108LDc

Note: If your printer does not have the minimum firmware version or a later version installed, you will need to install a firmware update before proceeding to other configuration tasks. Contact the Lexmark Solutions Help Desk for help in obtaining the correct firmware.

Updating the firmware

If you have obtained a newer version of the firmware:

1 From the Embedded Web Server, click **Settings** > **Update Firmware**.

2 From the Update Firmware page, **Browse** to locate the new flash file, and then click **Submit**. It may take several minutes for the update to complete.

Note: Do not power off the printer while the update is in progress.

Installing the authentication token application

The authentication token application enables the printer to communicate with the type of authentication token being used (CAC/DOD or PKCS15-compatible card). You must install the correct application file for your card type:

Card type	Authentication token solution file
CAC/DOD	authtokencaccard-x.x.x.fls
PKCS15	authtokenpkcs15-x.x.x.fls
The file names shown are not version-specific. Use the latest version available for each file. For information about available versions, contact the Lexmark Solutions Help Desk.	

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

2 On the Solutions tab, click **Install**.

3 **Browse** to locate the correct application file, and then click **Start Install**.

4 After the installation has finished, click **Return**. On the Solutions tab, you should now see an authentication token listed under Installed Solutions.

Installing PKI applications

The PKI applications enable users to sign and encrypt E-mail messages sent from the printer, securely scan documents and images to a network file share, and hold documents at the printer until released by an authorized user. The authentication application is required, but all other applications are optional and can be installed as needed.

The installation files include:

Application	Installation file
PKI Authentication	pkiadauth-x.x.x.fls
PKI S/MIME Email	pkiademail-x.x.x.fls
PKI Scan to Network	pkiadnetworkscan.x.x.x-fls
PKI Held Jobs (Print Release Lite)	pkiadheldjobs.x.x.x.fls
The file names shown are not version-specific. Use the latest version available for each file. For information about available versions, contact the Lexmark Solutions Help Desk.	

PKI Authentication must be installed first. For each application you want to install:

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions**.
2. On the Solutions tab, click **Install**.
3. **Browse** to locate the correct application file, and then click **Start Install**.
4. After the installation has finished, click **Return**. The application should now be listed under Installed Solutions.

Configuring printer settings for use with PKI applications

Even if the printer has been set up previously, make sure all settings necessary for the PKI capability to function correctly have been configured.

TCP/IP settings

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP**.
2. Under TCP/IP:
   - Verify the Domain Name. Normally, the domain will be the same one assigned to user workstations.
   - If using a static IP address, verify the WINS Server Address, and the DNS Server Address.
   - If the printer is located in a different domain than the domain controller, the E-mail server, or any file share users may need to scan to from the device, list the additional domains in the Domain Search Order field, separated by commas.
3. Click **Submit**.

Date and time

In order for users to login to the printer, the printer clock must be set to within five minutes of the domain controller system clock. Printer clock settings can be updated manually, or configured to use *Network Time Protocol* (NTP), to automatically sync with a trusted clock—typically the same one used by the domain controller.

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

Configuring date and time manually

1. From the Embedded Web Server, click **Settings** > **Security** > **Set Date and Time**.
2. To manage the settings manually, type the correct date and time in `YYYY-MM-DD HH:MM` format, and then choose from the Time Zone drop-down list.

   Notes:

   - Entering manual settings automatically disables use of NTP.
   - Choosing "(UTC+user) Custom" from the Time Zone list will require configuration of additional settings under Custom Time Zone Setup.
3. If *Daylight Saving Time* (DST) is observed in your area, select **Automatically Observe DST**.
4. If you are located in a non-standard time zone or an area that observes an alternate DST calendar, adjust the Custom Time Zone Setup settings as needed.
5. Click **Submit**.

Using NTP

1. To sync to an NTP server rather than manage date and time settings manually, select **Enable NTP**, and then type the IP address or hostname of the NTP Server.
2. If the NTP server requires authentication, select **Enable Authentication** , and then use the "Install auth keys" link to browse to the file containing the NTP authentication credentials.
3. Click **Submit**.

Panel login timeout

To help prevent unauthorized access in the event a user leaves the printer unattended with a SmartCard inserted or without logging out, you can limit the amount of time a user stays logged in without activity. If the user does not touch the screen within the specified time—even if a SmartCard is still inserted—the session ends and the printer touch screen returns to the PIN entry or login screen.

1. From the Embedded Web Server, click **Settings** > **Security** > **Miscellaneous Security Settings**.
2. Under Miscellaneous Security Settings, click **Login Restrictions**.
3. Set the Panel Login Timeout value (in seconds). The recommended interval is 30 seconds.
4. Click **Submit**.

Certificate management

Certificates are needed for domain controller verification, and for SSL support in LDAP. In order to use PKI Authentication, you must install the certificate of the *Certificate Authority* (CA) that issued the certificate used by the domain controller. Additional certificates may be installed if needed. Each certificate must be in a separate PEM (.cer) file.

1. From the Embedded Web Server, click **Settings** > **Security** > **Certificate Management** > **Certificate Authority Management**.
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. The contents of the file should resemble the following:

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

Configuring Scan to Email

If users will have access to Scan to Email (with or without S/MIME capability), you must configure E-mail and address book settings on the printer. If users will not be allowed to access Scan to Email, you can skip this section.

SMTP settings

1. From the Embedded Web Server, click **Settings** > **E-mail/FTP Settings** > **SMTP Setup**.
2. Under SMTP Setup, type the IP address or hostname of the Primary SMTP Gateway the printer will use for sending E-mail.

   Note: If Kerberos will be used to authenticate users to the SMTP server, you must use the hostname.
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 the printer will wait for a response from the SMTP server before timing out.
6. Verify that the Reply Address field is empty.
7. For Use SSL, 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 **Kerberos 5** for SMTP Server Authentication. If Kerberos is not supported, select **No Authentication Required**.

   Note: If the SMTP server requires user authentication to send E-mail but does not support Kerberos, the IP address or hostname of the printer must be added to the SMTP server as a relay.

9 For Device-Initiated E-mail, select **None** or **Use Device SMTP Credentials**.

Note: If the printer must provide credentials in order to send E-mail, enter the appropriate information under Device Credentials.

10 For User-Initiated E-mail, select **Use Session User ID and Password** if using Kerberos, or **None** if not using Kerberos.

11 Click **Submit**.

E-mail settings

E-mail Server Settings

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

2 Under E-mail Server Settings, type a Subject line for E-mail messages sent from the printer. Suggestion: "Scanned Document".

3 Type a default Message to be displayed in the body of E-mail messages sent from the printer. Suggestion: "Please see the attached document."

4 From Send me a copy, select whether users can choose to send themselves a copy of E-mail messages they send from the printer:

- **Never appears**—The "Send me a copy" option never appears.
- **On by default**—The option is on, but can be turned off by users.
- **Off by default**—The option is off, but can be turned on by users.
- **Always on**—Users will always receive a copy of E-mail messages they send from the printer.

5 Continue to E-mail Settings to set scan defaults, or click **Submit** to save changes before continuing

Scan settings

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

2 Under E-mail Settings, the most commonly changed settings are:

- **Color**—Select **Gray** as the default setting, to reduce the file size of scanned documents and images.
- **Resolution**—The recommended range for resolution is 150 dpi-300 dpi. A higher resolution can be chosen to improve image quality, but it will also increase the file size of scanned documents.
- **Transmission Log**—The recommended setting is **Print only for error**.
- **E-mail Bit Depth**—Set to **8-bit** for grayscale imaging, or **1-bit** for black and white.

3 Adjust other scan settings as needed.

4 Click **Submit**.

Address Book setup

Configuring the printer Address Book enables users to search your network Global Address Book for E-mail addresses.

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

2 For Server Address, type the hostname (not the IP address), of the LDAP server.

3 Type the Server Port that will be used for address book lookups. The most commonly-used values are:

   Non-SSL connections—Port 389 (the default setting on the printer)

   SSL connections—Port 636

   Non-SSL Global Catalog—Port 3268

   SSL Global Catalog—Port 3269

4 Select whether or not **LDAP Certificate Validation** will be required.

5 Select **Use GSSAPI**.

6 Type a name for the Mail Attribute (usually "mail").

7 Leave the Fax Number Attribute at the default value.

8 Type one or more Search Base values to be used when querying the LDAP directory. Use commas to separate multiple entries. Example: "ou=installation,dc=branch,dc=mil".

9 Set the Search Timeout, to specify the maximum time allowed for each LDAP query.

10 Select the combination of LDAP attributes used to find the Displayed Name for an E-mail address (also referred to as the "friendly" name). If in doubt, leave the default value.

11 Type a number for the Max Search Results to be returned from an LDAP query.

12 Select **Use user credentials**.

13 Click **Submit**.

Configuring PKI Authentication

PKI Authentication must be configured and running for other PKI applications to work. It provides the login screen and authentication mechanism, and supports user authorization to the device and device functions.

Logon screen

The logon screen contains text and a graphic prompting the user to insert a SmartCard to access the printer. This screen can be configured to display custom text or a custom image, or icons for options such as Copy and Fax.

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.

2 For Logon Type, select whether users can access the printer using **Card Only** (SmartCard), **Card or Manual Login**, or **Manual Login Only** (userid/password).

3 Select whether Card Pin must be **Numeric Only**, or can be **Alphanumeric**.

4 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.

5 Select **Allow Copy without Card** if you want to enable users to make copies without authenticating to the printer.

6 Select **Allow Fax without Card** if you want to enable users to send faxes without authenticating to the printer.

7 Continue to Active Directory Configuration, or click **Apply** at the bottom of the screen to save changes.

Active Directory Configuration

Note: As with any form of authentication that relies on an external server, users will not be able to access protected device functions in the event a network issue prevents the printer from communicating with the authenticating server.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.
2. Under Active Directory Configuration, select a User Validation Mode:
   - **PIN Only**—Users are validated locally with SmartCard and PIN. Network functions that require authentication will not be available to users.
   - **Active Directory**—Users are validated against Active Directory with SmartCard and PIN.
3. Select **Use MFP Kerberos Setup** to use the Kerberos settings already configured on the printer, or clear the check box to use Simple Kerberos Setup.
4. 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 SmartCard domain that should be mapped to the specified Realm. This is the principal name used on the SmartCard, 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 principle name. In this case, you would enter the Domain as “mil,.mil”.
   - **Timeout**—The amount of time the printer should wait for a response from the domain controller before moving to the next one in the list.
5. 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.
6. Select a DC Validation Mode for validating the domain controller certificate when users login to the printer:
   - **Device Certificate Validation**—The most common method. The certificate of the CA that issued the domain controller certificate must also be installed on the printer.
   - **MFP Chain Validation**—The entire certificate chain, from the domain controller to the root CA, must be installed on the printer.
   - **OCSP Validation**—The entire certificate chain, from the domain controller to the root CA, must be installed on the printer, and *Online Certificate Status Protocol* (OCSP) settings must be configured.
7. 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 printer 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 if you want to allow users to login even if the OCSP response indicates the certificate status is unknown.
8. Continue to User Session and Access Control, or click **Apply** at the bottom of the screen to save changes.

User Session and Access Control

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 User ID 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. Select **Use SSL for User Info** if you want to use an SSL connection when performing an LDAP lookup to retrieve additional user information from the domain controller.
4. Select **Share Session with LDD** if you want to allow user information to be shared with *Lexmark Document Distributor* (LDD).

   Note: This may be required for LDD solutions to function properly.
5. Use Other User Attributes to list LDAP attributes that should be added to a user's session. This information would normally be used by other applications (such as LDD). Multiple values can be entered, separated by commas.
6. Use the Group Authorization List to allow only users in certain Active Directory groups access to specific printer functions, such as color printing. Multiple groups can be entered, separated by commas. Leave blank if not using group authorization.
7. From Device Access Control, select which Access Control should be used to authenticate and authorize users. Solution-specific access control 1 is the default and recommended setting.
8. Continue to Advanced Settings, or click **Apply** at the bottom of the screen to save changes.

Advanced Settings

Not all networks will require the advanced settings. Adjust them as needed to allow the printer to communicate on your network.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Authentication** > **Configure**.
2. Select **Disable Reverse DNS Lookups** if they are not supported on your network.
3. To use only the information provided by the specified LDAP server, select **Disable LDAP Referrals**.

   Note: Leaving LDAP referrals enabled can increase LDAP search times.
4. 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.
5. Click **Apply**.

Configuring PKI S/MIME Email

PKI S/MIME settings

This application is only used if Scan to Email is enabled. If you are not using Scan to Email, you can skip this section.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI S/MIME Email** > **Configure**.
2. For From Address, select either **Card Email Address** (SmartCard) or **LDAP Lookup**, to specify how the printer should retrieve the user's address when sending E-mail.

   Note: If manual login is allowed, you must select **LDAP Lookup**.
3. Under S/MIME Options, adjust the following settings:
   - Sign Email— Select **Disabled**, **Prompt User**, or **Always Sign** to determine whether outgoing E-mail messages will be signed using a digital certificate.
   - Encrypt Email—Select **Disabled**, **Prompt User**, or **Always Encrypt** to determine whether outgoing E-mail messages will be encrypted.

     Note: In order to send encrypted E-mail, each recipient's encryption certificate must be available in the Global Address Book.

   Possible signing and encryption combinations include:

Sign Email Setting	Encrypt Email Setting	Result
Disabled	Disabled	E-mail messages are sent without being signed or encrypted.
Disabled	Prompt User	User is prompted to choose: Do Not Encrypt the Email Encrypt the Email
Disabled	Always Encrypt	E-mail messages are always encrypted, but not signed.
Prompt User	Disabled	User is prompted to choose: Do Not Sign the Email Sign the Email
Prompt User	Prompt User	User is prompted to choose: Do Not Sign or Encrypt the Email Sign the Email Encrypt the Email Sign and Encrypt the Email
Prompt User	Always Encrypt	User is prompted to choose: Encrypt the Email Sign and Encrypt the Email
Always Sign	Disabled	E-mail messages are always signed, but not encrypted.
Always Sign	Prompt User	User is prompted to choose: Sign the Email Sign and Encrypt the Email

Sign Email Setting	Encrypt Email Setting	Result
Always Sign	Always Encrypt	E-mail messages are always signed and encrypted.

- Select **Require Email to be Signed or Encrypted** if you want to require users to choose at least one of the two options when sending E-mail.
- **Non-Repudiation Required for Signing**—If selected, the certificate used for signing E-mail messages must have the non-repudiation bit set.
- **Encryption Algorithm**—Select one of the available encryption sets; **Triple DES** is the most common setting.
- **LDAP-Primary Certificate**—The LDAP attribute searched first for a recipient's encryption certificate; "userSMIMECertificate" is the most common setting.
- **LDAP-Alternate Certificate**—The second LDAP attribute searched, if a recipient's certificate is not found in the primary attribute; "userCertificate" is the most common setting.

4 Under User Options, select one or more settings to determine which options will be available to users from the printer touch screen:

- **User Can Only Send to Self** (no other recipients can be added)
- **User Can Change Options** (scan settings)
- **User Can Change Subject**
- **User Can Change Message**
- **User Can Change Attachment Name**
- **Return to Email Screen**—By default, users are returned to the home screen after sending E-mail. This option returns the user to the E-maill screen, preserving previously selected recipients, subject, message, and scan options.

5 Click **Apply**.

Configuring PKI Scan to Network

If users will have access to Scan to Network, you must also configure PKI Scan to Network. If users will not be allowed to access Scan to Network, you can skip this section.

General Settings

General Settings control how text and icons are displayed on the printer home screen for Scan to Network, as well as which users are allowed to access the application.

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.

2 Under General Settings, you can specify custom Button Text to be displayed above the Scan to Network icon on the printer home screen.

3 To select an alternate image for the Up Icon (the image that displays when the Scan to Network 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 Scan to Network icon is pressed), click **Browse** to locate the image you want to use. To view the default icon image, click **View Current Value**.

5 From Scan to Network Authorization, select which Access Control should be used to authorize user groups. If groups are not being used, select the same setting used for Device Access Control in PKI Authentication (usually Solution-specific access control 1).

Note: Authorization can be further restricted when configuring specific Scan to Network file shares.

6 Continue to Default Scan Settings, or click **Apply** at the bottom of the screen to save changes.

Default Scan Settings

The default scan settings are passed to all new file shares. You can keep these defaults for individual file shares, or select new settings for each.

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.

2 Under Default Scan Settings, adjust the following settings as needed:

- **Format**—The default file format for scanned documents.
- **Content**—The default for the type of content in scanned documents.
- **Color**—Determines whether scanned documents will be in color, black and white, or grayscale.
- **Resolution**—The default resolution for scanned documents.

  Note: Higher resolutions produce better quality images, but also increase the file size of scanned documents.
- **Darkness**—The default darkness level for scanned documents.
- **Original Size**—The default paper size for scanned documents.
- **Sides (Duplex)**—Specifies whether the document being scanned is 1-sided or 2-sided.
- Select **Scan Edge to Edge** to scan documents all the way to the edge of the paper.

  Note: Leaving a small space around the edges that is not scanned usually results in better image quality.
- Select **Scan Preview** to allow users preview and verify the first page of a document before the rest is scanned.

3 Click **Apply** at the bottom of the screen to save changes, before continuing to File Shares.

Creating file shares

To create a new file share:

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.

2 Under File Shares, click **Add** to create a new share. The Add File Shares page will be displayed.

3 Under General Settings, configure the following attributes for the new share:

- **File Share Authorization**—Select the solution access control that determines which groups can access this file share. If a user is not allowed to access this share, it will not appear in the list of shares available to the user.

  Note: If groups are not being used, select the same setting used for Device Access Control in PKI Authentication (usually Solution-specific access control 1).
- **Display Name**—The name used to represent this file share in the list of shares available to a user.

- **UNC Path**—The path that corresponds to the network location of this share. The format will depend on whether it is a static or dynamic path. Possible options include:
  - **Static**—Use the fully-qualified UNC Path. Example: \\fileserver\CACNetworkShare
  - **Dynamic**—Use %u in the path to represent the data that will be used to create the path. Example: \\fileserver\shares\%u
- **Replacement Value**—Used to provide the data (%u) needed to create a dynamic UNC path. Select one of the following:
  - **User Prinicpal Name**—Obtains the principal name from a user's SmartCard.
  - **EDI-PI**—Obtains the 10-digit identifier from a user's DoD Common Access Card.
  - **LDAP Lookup**—Uses Active Directory to look up a specified LDAP attribute.
- **LDAP - Replacement Attribute**—The LDAP attribute used if "LDAP Lookup" is selected to obtain the Replacement Value.

  Examples of three common file share configurations:

Using Active Directory to obtain the user's home directory:

- **Display Name**—Home Directory
- **UNC Path**—%u
- **Replacement Value**—LDAP Lookup
- **LDAP - Replacement Attribute**—homeDirectory

Using a static file share:

- **Display Name**—Network Share
- **UNC Path**—\\fileserver\CACNetworkShare
- **Replacement Value**—User Principal Name
- **LDAP - Replacement Attribute**—Leave blank

Using a dynamic file share with the Windows User ID:

- **Display Name**—User Share
- **UNC Path**—\\dfs\shares\%u
- **Replacement Value**—LDAP Lookup
- **LDAP - Replacement Attribute**—samaccountname

- **Default Filename**—The default filename for scanned documents. If users are not allowed to change the default, a timestamp is automatically added to the default filename, to give each scanned document a unique name. The file extension is added automatically based on the file type selected.
- Select **User Can Rename File** if you want to allow users to change the default filename.
- Select **User Can Change Scan Settings** if you want to allow users to change scan settings.
- If users are allowed to rename files, select **Append Timestamp to Filename** to automatically add a timestamp to files that do not use the default filename.
- Select **Remove "$" from Fileshare Name** to remove the last dollar sign in the UNC path, so that users will be able to write to this share (necessary on some networks).
- Select **Create Directory** to create the specified directory if it does not already exist when a user attempts to scan a document to this share.

4 Under Default Scan Settings, select **Use Global Default Scan Settings** if you want to use the previously-defined default scan settings for this share, or adjust the individual settings as needed. For information about the settings, see "Default Scan Settings" on page 17.

5 Click **Apply**.

Editing or deleting a file share

To edit an existing file share:

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.

2 Under File Shares, highlight the name of the share you want to modify, and then click **Edit**. The configuration page for that share will be displayed.

3 Adjust the settings for the selected share as needed, and then click **Apply** to save your changes.

To delete a file share:

1 From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.

2 Under File Shares, highlight the name of the share you want to remove, and then click **Delete**. A confirmation page will be displayed.

3 Click **Remove** to finish deleting the share and return to the list of available file shares.

Configuring PKI Held Jobs

PKI Held Jobs settings

This application is only used if Print Release Lite is being implemented. If you are not using Print Release Lite, you can skip this section.

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

2 You can specify custom Icon Text to be displayed above the Held Jobs icon on the printer 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 From **Access Control**, select which Access Control should be used to authorize user groups. If groups are not being used, select the same setting used for Device Access Control in PKI Authentication (usually 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,** 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 allow users to change the number of copies for each job from the printer.
- Select **Allow Users to Print All** if you want to allow users to select a **Print All** (jobs) button, rather than select each print job individually.
- 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 printer 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 Select Advanced Settings as needed:

- Select **Require All Jobs to be Held** if you want to require all jobs to remain on the printer until released by an authorized user, or until they expire.
- Select **Clear Print Data** to clear the memory associated with each print job once the job is released.

9 Click **Apply**.

Troubleshooting

Login Issues

"Unsupported USB Device" error message

A supported SmartCard reader has been installed before the PKI firmware and applications

The reader can not be installed until the firmware and applications have been installed. Remove the card reader, and see "Installing the firmware and applications" on page 6.

A non-supported SmartCard reader is attached

Only the OmniKey reader shipped with the MFP 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

This error indicates that no certificate, or an incorrect certificate, has been installed on the printer. 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.

For information on installing, viewing, or modifying certificates, see “Certificate management” on page 10.

“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 24.

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.

Scan to Email issues

“Email cannot be sent because an error occurred trying to get your email address” error message

There is a conflict between the login type, and how the From Address is being retrieved

This error occurs when a user is logged in manually, but PKI S/MIME Email is configured to retrieve the From Address from a SmartCard.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI S/MIME Email** > **Configure**.
2. For From Address, select **LDAP Lookup**.
3. Click **Apply**.

The LDAP lookup failed

For help resolving LDAP-related problems, see “LDAP issues” on page 24.

“Email cannot be sent because you are not authorized to perform this function” 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 Scan to Email, add the user to an Active Directory group that is included in the authorization list for this function.

“The email cannot be sent because a valid digital signature could not be found on your card” error message

If users are required (or choose), to digitally sign E-mail messages, the Smart Card must contain a valid signing certificate. By default, the non-repudiation option is enabled for E-mail signing. If your certificate does not have the non-repudiation bit set, this option can be disabled:

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI S/MIME Email** > **Configure**.
2. Clear the **Non-Repudiation Required for Signing** check box.
3. Click **Apply**.

“The email cannot be sent because it cannot be digitally signed when a manual login is performed” error message

E-mail can only be digitally signed if the user logs in with a SmartCard. Verify that PKI S/MIME Email is not configured to require that E-mail be signed.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI S/MIME Email** > **Configure**.
2. Under S/Mime Options, select either **Disabled** or **Prompt User** for Sign Email.

3 Click **Apply**.

"Email cannot be sent. Unable to find valid encryption certificate for [E-mail address]" error message

This error indicates the LDAP Directory found in the Address Book Setup did not contain an encryption certificate for the specified E-mail address. Encrypted E-mail can only be sent to recipients found in the global address book, and each recipient must have an encryption certificate. Verify that the intended recipient is in your global address book.

Unable to send E-mail (SMTP-related issues)

When users are unable to send E-mail, there can be several possible causes:

"Invalid Message ID" error from the SMTP server

This problem occurs in earlier versions of the firmware, so verify that you have the correct firmware version installed. For information about finding the correct version for your printer, see "Verifying and updating the firmware" on page 6. If you have verified or updated your firmware and still experience this problem, contact the Lexmark Solutions Help Desk.

"501 5.5.4 Invalid Address" error from the SMTP server

The domain name on the device has not been configured correctly:

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

2 Under TCP/IP, verify or correct the Domain Name entry.

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

Note: For more information about TCP/IP settings, see "TCP/IP settings" on page 8.

The SMTP server allows only authenticated users to send E-mail

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

2 For SMTP Server Authentication, select **Kerberos 5**. If Kerberos is not supported, select **No Authentication Required**.

Note: If the SMTP server requires user authentication to send E-mail but does not support Kerberos, the IP address or hostname of the printer must be added to the SMTP server as a relay.

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

SMTP Server Authentication is set to Kerberos 5, but the printer settings point to an IP address for the SMTP server

If the SMTP server uses Kerberos for authentication, then you must point to the server by hostname, not IP address.

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

2 Under SMTP Setup, type the hostname of the Primary SMTP Gateway the device will use for sending E-mail.

3 If using a secondary or backup SMTP server, type the hostname for that server.

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

SMTP Server Authentication is set to Kerberos 5, but the SMTP server reports GSSAPI is not supported

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

2 For SMTP Server Authentication, select **No Authentication Required**.

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

The printer is unable to connect to the SMTP server because port 25 is blocked

You must adjust server and/or firewall settings to allow communication between the printer and SMTP server on port 25.

Scan to Network issues

"You are not authorized to use this feature" Scan to Network 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 Scan to Network, add the user to an Active Directory group that is included in the authorization list for this function.

"This feature is not available because no file shares have been configured by the system administrator" error message

You need to add at least one file share for users to scan to. For information on adding file shares, see "Configuring PKI Scan to Network" on page 16.

"This feature is not available because you are not authorized to scan to any of the available file shares" 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 all file shares, add the user to an Active Directory group that is included in the authorization list for the needed share (or shares).

"An LDAP error occurred trying to retrieve the selected file share destination" error message

The LDAP lookup failed

For information about LDAP-related issues, see "LDAP issues" on page 24.

The LDAP lookup succeeded, but the replacement value attribute does not exist or has no value

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.
2. Under File Shares, highlight the name of the share you want to modify, and then click **Edit**. The configuration page for that share will be displayed.
3. Under General Settings, verify or adjust the following settings:
   - **UNC Path**—The path that corresponds to the network location of this share. The format will depend on whether it is a static or dynamic path. Possible options include:
     - **Static**—Use the fully-qualified UNC Path. Example: \\fileserver\CACNetworkShare
     - **Dynamic**—Use %u in the path to represent the data that will be used to create the path.
Example: \\fileserver\shares\%u
   - **Replacement Value**—Used to provide the data (%u) needed to create a dynamic UNC path. Select one of the following:
     - **User Prinicpal Name**—Obtains the principal name from a user's SmartCard.
     - **EDI-PI**—Obtains the 10-digit identifier from a user's DoD Common Access Card.
     - **LDAP Lookup**—Uses Active Directory to look up a specified LDAP attribute.
   - **LDAP - Replacement Attribute**—The LDAP attribute used if “LDAP Lookup” is selected to obtain the Replacement Value.
4. Click **Apply** to save any needed changes.

“No UNC Path has been defined for this destination” error message

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.
2. Under File Shares, highlight the name of the share you want to modify, and then click **Edit**. The configuration page for that share will be displayed.
3. Under General Settings, verify or adjust the UNC Path setting.
4. Click **Apply** to save any needed changes.

“The scanned file size and saved file size do not match” error message

After scanning, the number of bytes scanned is compared to the number written to the saved file. If the numbers do not match, it typically means the file share is full, or the disk quota for the user has been reached. Check the free space available on the file share, and the disk quota for the user.

“User does not have read access to the file share; unable to verify the file size” error message

After scanning, the number of bytes scanned is compared to the number written to the saved file. If the user does not have read access to the file share, the file size cannot be determined. To correct this problem, grant the user read access to the file share.

“Invalid filename specified” error message

The user included an invalid character as part of the filename. The following characters cannot be used for filenames:
| < > \ / * ? ; : ^

“An error occurred connecting or writing to the File Share” error message

THE UNC PATH USED THE IP ADDRESS OF THE FILE SERVER

In order to connect to the file share with user credentials, the hostname of the file server must be used.

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.
2. Under File Shares, highlight the name of the share you want to modify, and then click **Edit**. The configuration page for that share will be displayed.
3. Under General Settings, verify or adjust the UNC Path setting to use the server hostname.
4. Click **Apply** to save any needed changes.

THE HOSTNAME OF THE FILE SERVER COULD NOT BE RESOLVED TO AN IP ADDRESS

If the hostname is not a fully-qualified domain name, the domain search order specified in the printer settings will be used to determine the appropriate domain name to append to the hostname. To verify domain search order settings:

1. From the Embedded Web Server, click **Settings** > **Network/Ports** > **TCP/IP**.
2. Under TCP/IP:
   - Verify the **Domain Name**. Normally, the domain will be the same one assigned to user workstations.
   - If the printer is located in a different domain than the domain controller, the E-mail server, or any file share users may need to scan to from the device, list the additional domains in the **Domain Search Order** field, separated by commas.
3. Click **Submit** to save any needed changes.

PORT 445 IS BLOCKED BY A FIREWALL

You must adjust server and/or firewall settings to allow communication between the printer and file server (or servers) on port 445.

“The network share name does not exist on the specified file server” error message

THE PRINTER CONNECTED TO THE FILE SERVER, BUT THE SHARE NAME DOES NOT EXIST

Verify that the share name is correct, and that the user has read/write access to that share.

The share name is correct, but ends in "$"

1. From the Embedded Web Server, click **Settings** > **Embedded Solutions** > **PKI Scan to Network** > **Configure**.
2. Under File Shares, highlight the name of the share you want to modify, and then click **Edit**. The configuration page for that share will be displayed.
3. Under General Settings, select **Remove "$" from Fileshare Name** to remove the last dollar sign in the UNC path.
4. Click **Apply** to save any needed changes.

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.

Notices

GNU Lesser General Public License

View the GNU Lesser General Public License online at **http://www.gnu.org/licenses/lgpl.html**.

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.

Additional copyrights

This product includes software developed by:

Copyright (c) 2002 Olaf Kirch

Copyright (c) 2003 Kevin Stefanik

Redistribution and use in source an binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution:

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index