Card Authentication

Administrator's Guide

December 2020

www.lexmark.com

Contents

Overview

Use the application to secure access to a printer using a card reader. When users tap in, their credentials are authenticated using either of the following:

- A master printer. If the master printer is offline, then a backup printer functions as the master printer until the master becomes online.

  Note: When setting up the printers, make sure that they are on the same network.

- Lightweight Directory Access Protocol (LDAP), Lexmark™ Document Distributor (LDD) servers, or Identity Service Providers, depending on the authentication set by the organization.

This document provides instructions on how to configure, use, and troubleshoot the application.

Setting up prerequisites

You may need administrative rights to configure the application.

Accessing the Embedded Web Server

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the printer home screen.
   - View the IP address in the TCP/IP section of the Network/Ports menu.
2. Open a web browser, and then type the printer IP address.

Adding an internal user account

An internal user account is required when using printer-based authentication.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do either of the following:
   - Click **Security** > **Security Setup** > **Internal Accounts** > **Add an Internal Account**.
   - Click **Security** > **Edit Security Setups** > **Internal Accounts** > **Add an Internal Account**.
3. Enter the account information, and then click **Submit**.
4. If necessary, from the Manage Internal Accounts section, type a custom building block name, and then specify the required user credentials.
5. Click **Submit**.

Setting up groups for internal user accounts

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do either of the following:
   - Click **Security** > **Security Setup** > **Internal Accounts** > **Setup groups for use with internal accounts**.
   - Click **Security** > **Edit Security Setups** > **Internal Accounts** > **Setup groups for use with internal accounts**.
3. Enter a group name, and then click **Add**.
4. Add internal accounts to the group.
5. Click **Submit**.

Creating a security template

A security template is composed of security building blocks, such as Internal Accounts, Kerberos, LDAP, LDAP +GSSAPI, and Active Directory. These templates are applied to the access control to secure printer functions and applications.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do either of the following:
   - Click **Security** > **Security Setup** > **Security Template** > **Add a Security Template**.
   - Click **Security** > **Edit Security Setups** > **Security Templates** > **Add a Security Template**.
3. Type a security template name, and then select one of the following authentication setups:
   - For printer-based authentication on a standalone setup, select an internal account building block.
   - For printer-based authentication with Lexmark Print Management (LPM) Serverless Print Release on an Active Directory setup, select an LDAP+GSSAPI building block.
   - For LDAP authentication, select an LDAP building block.
4. Click **Save Template**.

Note: To modify an existing security template, click the security template and then add or modify an authorization for the template.

Configuring access controls

Note: When using the **Admin Login** feature, make sure that you have configured the security template for internal accounts. For more information, see “Creating a security template” on page 6.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do either of the following:
   - Click **Security** > **Security Setup** > **Access Controls**.
   - Click **Security** > **Edit Security Setups** > **Access Controls**.
3. Click **Device Apps** or **Device Solutions**, and then do the following:
   - Set App 1 or Solution 1 to an internal account or LDAP+GSSAPI or Active Directory security template.
   - Set App 2 or Solution 2 to the application security template.

     Note: The application security template is the template with CardAuth as the authentication setup. For more information, see “Creating a security template” on page 6.
   - Set App 3 or Solution 3 to an LDAP security template.

   Notes:

   - If LPM Print Release is installed, then set the Print Release access control to the application security template.
   - Embedded Solutions Framework (eSF) version 2.x printers need the eSF Security Manager application to configure access control. For a list of these printers, see the *Readme* file.
4. Click **Submit**.

Configuring the application

Before you begin, do the following:

- Disable Background and Idle Screen and any existing authentication application.
- Install the following:
  - Card Authentication installer
  - Card reader driver
  - Card reader
  - eSF Security Manager

    Note: eSF version 2.x printers need the eSF Security Manager application to configure access control. For a list of these printers, see the *Readme* file.

Accessing the configuration page for the application

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do one of the following:
   - Click **Apps** > **Apps Management**.
   - Click **Device Solutions** > **Solutions (eSF)**.
   - Click **Embedded Solutions**.
3. Click **Card Authentication** > **Configure**.

Configuring administrator authentication

Note: When using the **Admin Login** feature, make sure that you have configured the security template for Internal accounts, PIN, and Password. For more information, see “Creating a security template” on page 6.

1. From the Embedded Web Server, access the configuration page for the application.
2. From the User Authentication section, set **Admin Login Access Control** to your preferred login method.

   Notes:

   - Make sure that the selected access control is configured with a security template. For more information, see “Creating a security template” on page 6.
   - Selecting **Disabled** hides the **Admin Login** option from the printer panel.
3. Click **Apply**.

Configuring the login screen

The login screen can be configured to do the following:

- Let users use the copy and fax functions without logging in.
- Let users select the login method to use.

- Add a login screen background and customize the login message.
- Disable the warning when no card reader is attached.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Login Screen section, configure the settings.

Note: For more information on each setting, see the mouse-over help.

3 Click **Apply**.

Enabling copy or fax without logging in

If "Allow Copy without Login" or "Allow Fax without Login" is enabled, then do the following:

1 From the Embedded Web Server, click **Settings** or **Configuration**.

2 Depending on your printer model, do either of the following:
- Click **Security** > **Security Setup** > **Access Controls** > **Function Access**.
- Click **Security** > **Edit Security Setups** > **Access Controls**.

3 Set the copy or the fax function to **No Security**.

4 Click **Submit**.

Printer-based authentication

Use printer-based authentication when validating users through a master printer.

Configuring printer-based user authentication

Before you begin, make sure that:

- The App 1 or Solution 1 access control is set to an internal account or LDAP+GSSAPI or Active Directory security template.
- The App 2 or Solution 2 access control is set to the application security template.

Note: For more information, see “Configuring access controls” on page 6.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Login Screen section, set Login Method to **Card or Manual Login**.

3 From the User Authentication section, do the following:
- Set Card Validation to **Printer-based**.
- Set Card Registration Access Control to **App 1** or **Solution 1**.
- Set Manual Login Access Control to **App 1** or **Solution 1**.
- Set Session Access Control to **App 2** or **Solution 2**.

Notes:

- If Card Registration Access Control is set to **None**, then you cannot register your card on the printer.
- Setting Manual Login Access Control to **None** requires only a card to log in even if Login Method is set to **Card or Manual Login**.

- For more information on each setting, see the mouse-over help.

4 Click **Apply**.

Setting up the role for the printer

Note: A client printer requires a master printer and a backup printer.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Printer-based Card Validation section, select a role for the printer.

- **Master**—The printer maintains the list of registered users.
- **Backup**—If the master printer is offline, then the backup printer assumes the role of the master until the master printer becomes online.
- **Client**—The printer does not store user information. A master or backup printer is required to validate user credentials.

Notes:

- If you have one printer, then set it as a master printer.
- If you have two printers, then set one as a master printer and the other as a backup printer.
- If you have three or more printers, then set one as master printer, one as backup printer, and the rest as client printers.

3 Type the host names or IP addresses of the master printer and the backup printer.

Notes:

- When setting up a backup printer, the host name or IP address of the master printer is required.
- When setting up client printers, the host names or IP addresses of the master and the backup printers are required.
- Before assigning a client printer to a new master printer, delete it from the old master printer.

4 Click **Apply**.

Web service authentication

Use web service authentication when validating users through an LDD server.

Configuring web service user authentication

Before you begin, make sure that the App 2 or Solution 2 access control is set to the application security template. For more information, see “Configuring access controls” on page 6.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Login Screen section, set Login Method to **Card or Manual Login**.

3 From the User Authentication section, do the following:

- Set Card Validation to **Web Service**.
- Set Card Registration Access Control and Manual Login Access Control to your preferred access control.
- Set Session Access Control to **App 2** or **Solution 2**.

Notes:

- If Card Registration Access Control is set to **None**, then you cannot register your card on the printer.
- Setting Manual Login Access Control to **None** requires only a card to log in even if Login Method is set to **Card or Manual Login**.
- For more information on each setting, see the mouse-over help.

4 Select **Verify Certificate** to validate all connections to the server. If Verify Certificate is not selected, then CA will not be validated.

Note: The Verify Certificate setting is applicable only to Identity Service and Web Service validation.

5 In the Verification Mode menu, select either **chain** or **peer**.

Note: The default value is chain.

6 Upload the server SSL certificate to connect securely to the server.

7 In the CheckHosts field, type the additional host names (other than the default server URL) to verify the entries in the certificate. Use commas to separate multiple host names.

Note: By default, that white list contains just the server URL. Type additional host names in the CheckHosts field to include them in the white list.

8 Click **Apply**.

Configuring web service settings

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Web Service Settings section, configure the settings.

Note: For more information on each setting, see the mouse-over help.

3 Click **Apply**.

Identity Service authentication

Use Identity Service authentication when validating users through an Identity Service server, such as the LPM Software as a Service (SaaS) server.

Configuring Identity Service user authentication

Before you begin, make sure that the App 2 or Solution 2 access control is set to the application security template. For more information, see “Configuring access controls” on page 6.

1 From the Embedded Web Server, access the configuration page for the application.

2 From the Login Screen section, set Login Method to **Card or Manual Login**.

3 From the User Authentication section, do the following:

- Set Card Validation to **Identity Service**.
- Set Card Registration Access Control to **Identity Service**.
- Set Manual Login Access Control to **Identity Service**.
- Set Session Access Control to **App 2** or **Solution 2**.

Notes:

- If Card Registration Access Control is set to **None**, then you cannot register your card on the printer.
- Setting Manual Login Access Control to **None** requires only a card to log in even if Login Method is set to **Card or Manual Login**.
- For more information on each setting, see the mouse-over help.

4 Select **Verify Certificate** to validate all connections to the server. If Verify Certificate is not selected, then CA will not be validated.

Note: The Verify Certificate setting is applicable only to Identity Service and Web Service validation.

5 In the Verification Mode menu, select either **chain** or **peer**.

Note: The default value is chain.

6 Upload the server SSL certificate to connect securely to the server.

7 In the CheckHosts field, type the additional host names (other than the default server URL) to verify the entries in the certificate. Use commas to separate multiple host names.

Note: By default, that white list contains just the server URL. Type additional host names in the CheckHosts field to include them in the white list.

8 Click **Apply**.

Configuring Identity Service settings

1 From the Embedded Web Server, access the configuration page for the application.

2 If necessary, from the Identity Service Settings section, select **Enable Idle Screen**.

Note: eSF version 2.x printers need the eSF Security Manager application when **Enable Idle Screen** is disabled. For a list of these printers, see the *Readme* file.

3 Type the host name or IP address of the Identity Service Provider.

4 If necessary, type the host name or IP address of the Badge Service Provider.

5 Upload the server SSL certificate to connect securely to the server.

6 If you have a Client ID and Client Secret from the Identity Service Provider, then type the information in their corresponding fields.

7 Set the application access policy.

- **Continue**—Continue using the printer even if connecting to the Identity Service server fails.
- **Fail**—Go back to the login screen if connecting to the Identity Service server fails.

8 To allow users to log in to the printer using a separate service account, select **Use Service Account**, and then enter the service account credentials.

9 Click **Apply**.

PIN authentication

Configuring PIN user authentication

Before you begin, make sure that the App 2 or Solution 2 access control is set to the application security template. For more information, see “Configuring access controls” on page 6.

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Login Screen section, set Login Method to an option that supports PIN authentication.
3. From the User Authentication section, do the following:
   - Set Card Validation to your preferred authentication method.
   - Set Card Registration Access Control to your preferred access control.
   - Set PIN Access Control to **App 1** or **Solution 1**.
   - Set Manual Login Access Control to your preferred access control.
   - Set Session Access Control to **App 2** or **Solution 2**.

   Notes:
   - If PIN Access Control is set to **None**, then you cannot register your PIN on the printer.
   - For more information on each setting, see the mouse-over help.
4. Click **Apply**.

Configuring PIN settings

1. From the Embedded Web Server, access the configuration page for the application.
2. From the PIN Settings section, in the Required Credentials menu, select a login method.
   - Userid and PIN—Requires a user name and PIN for authentication.
   - PIN only—Requires a PIN for authentication.
3. Type the web server address, and then select the minimum PIN length.
4. Type the invalid PIN error messages.
5. Click **Apply**.

LDAP authentication

Use LDAP authentication when validating users through an LDAP server.

Configuring LDAP user authentication

Before you begin, make sure that:

- The App 2 or Solution 2 access control is set to the application security template.
- The App 3 or Solution 3 access control is set to an LDAP security template.

  Note: For more information, see “Configuring access controls” on page 6.

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Login Screen section, set Login Method to **Card or Manual Login**.
3. From the User Authentication section, do the following:
   - Set Card Validation to **LDAP**.
   - Set the Card Registration Access Control to **App 3** or **Solution 3**.
   - Set Manual Login Access Control to **App 3** or **Solution 3**.
   - Set Session Access Control to **App 2** or **Solution 2**.

   Notes:

   - If Card Registration Access Control is set to **None**, then you cannot register your card on the printer.
   - Setting Manual Login Access Control to **None** requires only a card to log in even if Login Method is set to **Card or Manual Login**.
   - For more information on each setting, see the mouse-over help.
4. Click **Apply**.

Configuring LDAP settings

1. From the Embedded Web Server, access the configuration page for the application.
2. From the LDAP Settings section, configure the settings.

   Notes:

   - If **Use Address Book** is selected, then the application uses the LDAP settings that are already configured in the printer network accounts.
   - For more information on each setting, see the mouse-over help.
3. Click **Apply**.

Setting application preferences

1. From the Embedded Web Server, access the configuration page for the application.
2. Do one or more of the following:
   - To customize the printer home screen, configure the home screen settings.
   - To show registration messages, from the Advanced Settings section, select **Show Registration Intro Message** and **Show Registration Finished Message**.
   - To hear a *beep* after a successful login, from the Advanced Settings section, select **Enable Beep for Successful Login**, and then adjust the beep frequency.
   - To use a profile after a successful login, from the Advanced Settings section, in the Login Profile field, type a profile name.

   Note: For more information on each setting, see the mouse-over help.
3. Click **Apply**.

Viewing available profiles

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Manage Shortcuts** > **Manage Profile Shortcuts**.

Showing realms for user accounts

The Use Selected Realm feature is applicable only if the login methods for card registration and manual login are Kerberos, Active Directory, or LDAP+GSSAPI. This feature is also applicable only if card validation is set to Web Service or Printer-based.

For card registration, if this feature is enabled, then the badge ID that is registered is in username@realm format.

For manual login, if this feature is enabled, then the user name shown in the printer control panel is in username@realm format.

These settings do not apply to PIN login and PIN registration.

To enable this feature, do the following:

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Advanced Settings section, select **Use Selected Realm**.
3. Click **Apply**.

Exporting or importing a configuration file

1. From the Embedded Web Server, access the configuration page for the application.
2. Export or import the configuration file.

Notes:

- If a **`JVM Out of Memory`** error occurs, then repeat the export process until the configuration file is saved.
- If a timeout occurs and a blank screen appears, then refresh the web browser, and then click **Apply**.

Managing the application

Note: The status page for the application is available only when using printer-based authentication.

Accessing the status page for the application

Use the status page to monitor printer activity.

1. From the Embedded Web Server, click **Applications** > **Card Authentication**.
2. Note the following information:
   - **Status**—Shows the activity status of the printer.
     - **Not Configured**—The printer has not been configured.
     - **Offline**—No printer activity or communication is performed.
     - **Online**—The printer is active.
   - **Uptime**—Indicates how long the application has been running.
   - **(this printer)**—The current printer.
   - **Last Activity**—The last activity of the master printer.
   - **Number of Users**—The total number of registered users.
   - **Registration Status**—Indicates whether the printer is offline or online.
   - **Last Sync with Master**—The last time that the backup printer updated with the master printer.
   - **Last Contact with Master**—The last time that the backup printer communicated with the master printer.
   - **Last Sync as Master**—The last time that the backup printer functioned as the master printer.
   - **Last Activity as Master**—The last activity of the backup printer functioning as master printer.
   - **Duration as Master**—Indicates how long the backup printer has functioned as the master printer.
   - **Currently Serviced By**—The client printer recently in contact with the master or backup printer.
   - **Last Activity with Backup**—The last time that the client printer was in contact with the backup printer.

Managing user accounts and client printers

Note: This feature appears only when a printer functions as a master printer.

1. From the Embedded Web Server, access the status page for the application.
2. Do any of the following:

Delete user accounts

a. From the Master section, click **Delete Users**.

b. Type one or more user IDs, and then delete them.

Add client printers

a. From the Clients section, click **Add Clients**.

b. Type one or more printer IP addresses, and then add them.

Delete client printers

Note: You cannot delete client printers when the master printer is offline or when the application is uninstalled.

a From the Clients section, select one or more client printers.

b Click **Delete Clients**.

Reassigning printer roles

1 Configure a new master printer.

a From the Embedded Web Server of the new master printer, access the configuration page for the application.

b From the Printer-based Card Validation section, set Role to **Master**.

c Type the host name or IP address of the backup printer.

d Click **Apply**.

2 Assign the backup printer to the new master printer.

a From the Embedded Web Server of the backup printer, access the configuration page for the application.

b From the Printer-based Card Validation section, type the host name or IP address of the new master printer.

c Click **Apply**.

3 Delete the client printer from the current master printer.

a From the Embedded Web Server of the current master printer, access the status page for the application.

b From the Clients section, delete the client printer.

4 Reassign the client printer to the new master printer. Do either of the following:

Using the configuration page for the application

a From the Embedded Web Server of the client printer, access the configuration page for the application.

b From the Printer-based Card Validation section, set Role to **Client**.

c Type the host name or IP address of the new master printer.

Note: Make sure that the host name or IP address of the backup printer is correct.

d Click **Apply**.

Using the master printer status page

a From the Embedded Web Server of the new master printer, access the status page for the application.

b From the Clients section, click **Add Clients**.

c Type the IP address of the client printer, and then add it.

Using the application

Registering users

1. Tap your card on the card reader.
2. On the printer control panel, enter your credentials.

   Note: If you are using Kerberos or Active Directory or LDAP+GSSAPI for card registration, then select a realm.
3. Follow the instructions on the display.

Registering a PIN

Before you begin, make sure that the login method is set to support PIN authentication.

1. From the printer control panel, touch **PIN Login**.
2. Follow the instructions on the display.

Logging in to the printer manually

1. From the printer control panel, touch one of the following:
   - **PIN Login**
   - **Manual Login**
   - **Admin Login**

   Note: When selecting **Admin Login**, retrieving other user information from the LDAP server is not applicable.
2. Enter your login credentials.

   Note: If you are using Kerberos, Active Directory®, or LDAP+GSSAPI for manual login, then select a realm.
3. Follow the instructions on the display.

Troubleshooting

Application error

Try one or more of the following:

Check the system log

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Depending on your printer model, do one of the following:
   - Click **Apps** > **Apps Management**.
   - Click **Device Solutions** > **Solutions (eSF)**.
   - Click **Embedded Solutions**.
3. Click **System** > **Log**.
4. Select and submit the appropriate filters.
5. Analyze the log, and then resolve the problem.

Contact your Lexmark representative

Application does not run with the updated version of SaaS Print Release

Try one or more of the following:

Make sure that Print Release is configured properly

If you have upgraded your Print Management SaaS application to Print Release v2.0 or later, then make sure to disable Background and Idle Screen. Assign the Card Authentication access control to Print Release, and then make sure that Print Release is configured properly. For more information, see the *Print Release Administrator's Guide*.

Contact your Lexmark representative

Authentication error

Try one or more of the following:

Increase the printer timeout

If you are using Identity Service as a card validation method, then the printer may need more time to communicate to the Identity Service Provider.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **General Settings** > **Timeouts**.
3. Increase the screen timeout and the sleep mode.
4. Click **Submit**.

Make sure that the printer is connected to the network

For more information, see the printer *User's Guide*.

Make sure that the security server is online and is not busy

For more information, contact your system administrator.

User is locked out

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

Increase the lockout time and the allowed number of login failures

1. Depending on your printer model, from the Embedded Web Server, do one of the following:
   - Click **Settings** > **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.
   - Click **Configuration** > **Security**.
2. Increase the lockout time and the allowed number of login failures, or the auto logout delay.
3. Click **Submit**.

Cannot register a client printer

Try one or more of the following:

Make sure that the master printer or the backup printer is online

For more information, see "Accessing the status page for the application" on page 15.

Make sure that the master printer and the backup printer are configured properly

For more information, see "Configuring printer-based user authentication" on page 8.

Make sure that you do not exceed 23 registered client printers

For more information, see “Managing user accounts and client printers” on page 15.

Contact your Lexmark representative

Cannot validate the card

Try one or more of the following:

Set Login Method to Card or Manual Login

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Login Screen section, set Login Method to **Card or Manual Login**.
3. Click **Apply**.

Contact your Lexmark representative

Cannot find realm information

Try one or more of the following:

Some login methods for manual login or card registration, such as local accounts or LDAP, do not require realm selection. The login methods that require realm selection are Kerberos, Active Directory, and LDAP+GSSAPI.

Disable realm selection

1. From the Embedded Web Server, access the configuration page for the application.
2. From the Advanced Settings section, clear **Use Selected Realm**.
3. Click **Apply**.

Change the login method

1. From the Embedded Web Server, access the configuration page for the application.
2. From the User Authentication section, set Card Registration Access Control and Manual Login Access Control to **App 1** or **Solution 1**.
3. Click **Apply**.

Contact your Lexmark representative

Cannot connect to the LDAP server

Try one or more of the following:

Make sure that the LDAP settings are configured properly

For more information, see “Configuring LDAP settings” on page 13.

Contact your Lexmark representative

Frequently asked questions

Why can’t I add or delete a client printer when a backup printer acts as a master printer?

You can delete or add a client printer only when the master printer is online.

Can I remove a client printer and reassign it to its new master printer even if the current master printer is offline?

Yes, do the following:

1. From the Embedded Web Server of the client printer, install the application.
2. Set the role as a client printer, and then configure it to its new master and backup printers. For more information, see “Setting up the role for the printer” on page 9.

What if I accidentally uninstalled the application from the printer?

1. From the Embedded Web Server, install the application.
2. Set a role for the printer. For more information, see “Setting up the role for the printer” on page 9.

   Note: Make sure to set up the master printer, the backup printer, and then the client printers consecutively.
3. Depending on the role, configure the printer.

   Notes:

   - If the application is reinstalled on a master printer, then assign it to its backup printer.
   - If the application is reinstalled on a backup printer, then assign it to its master printer.
   - If the application is reinstalled on a client printer, then assign it to its master printer and backup printer.
   - For more information, see “Reassigning printer roles” on page 16.

Why can’t I see the copy or fax button on the lock screen even if I enabled it without logging in?

Set the copy or fax function access control to **No Security**. For more information, see “Configuring the login screen” on page 7.

What happens if I have the same access controls for Manual Login Access Control and Session Access Control?

To access printer functions from the home screen, you are required to enter your credentials when you log in manually.

Can I have different access controls for Manual Login Access Control and Card Validation?

Yes, except when you are using Identity Service authentication, then set Manual Login Access Control and Card Validation to **Identity Service**.

Why does the Admin Login feature not work with network accounts?

The **Admin Login** feature is applicable only to Internal Accounts, PIN, and Password security templates.

Notices

Edition notice

December 2020

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

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

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

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

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

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

GOVERNMENT END USERS

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

Trademarks

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

All other trademarks are the property of their respective owners.

Index

R

S

T

U

W