Secure E-mail

Administrator's Guide

January 2012

www.lexmark.com

Contents

Overview

Secure E-mail is an application that runs in place of the standard printer e-mail function and lets you digitally sign and encrypt e-mail sent from the printer.

Additional required applications

For the security features of the application to work correctly, the following must be installed and running on the printer:

- **An authentication module application**. This is needed to secure access to the e-mail function by requiring users to log in to the printer when they attempt to use the function. The authentication module is also needed to retrieve:
  - The authenticated user's e-mail address so that the user can send e-mail from the printer
  - The user certificates needed for digital signing and encryption
- **The eSF Security Manager application**. This application lets you secure access to the printer e-mail function by associating the function with the authentication module. For more information about eSF Security Manager, see the *eSF Security Manager Administrator's Guide*.

For a list of application requirements, including supported printers and required firmware versions, see the *Readme* file.

For information about physically setting up the printer or using the printer features, see the *User's Guide* on the *Software and Documentation* CD that came with the printer. After completing initial setup tasks according to the printer *User's Guide*, see the *Networking Guide* that came with the printer for information about how to connect the printer to your network.

Configuring Secure E-mail

Configuring printer settings for use with the application

Even if the printer has been set up previously, make sure all settings have been configured to enable the security features of the application to work correctly.

Configuring TCP/IP settings

Make sure all necessary TCP/IP settings have been configured.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Network/Ports** > **TCP/IP**.
3. Under the TCP/IP heading, do the following:
   - Verify the domain name. Normally, the domain will be the same one assigned to user workstations.
   - If you are using a static IP address, then verify the WINS server address and the DNS server address. If a backup DNS server is available, then type the backup DNS server address.
   - If the printer is located in a different domain than the domain controller, any e-mail servers you are using, or any file shares to which printer users may need to scan, then list the additional domains in the Domain Search Order field. Separate each domain name with a comma. If everything is in the same domain, then you can leave the Domain Search Order field blank.
4. Click **Submit**.

Configuring printer e-mail settings

For the application to work correctly, the SMTP, e-mail, and address book settings on the printer must be configured.

Configuring SMTP settings

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **E-mail/FTP Settings** > **SMTP Setup**.
3. Under the SMTP Setup heading, configure the following settings:
   - **Primary SMTP Gateway**—Type the IP address or host name of the primary SMTP server the printer will use for sending e-mail.

     Note: If you are using Kerberos to authenticate users to the SMTP server, then you must use the host name.
   - **Primary SMTP Gateway Port**—Enter the port number of the primary SMTP server.
   - **Secondary SMTP Gateway**—If you are using a secondary or backup SMTP server, then type the server IP address or host name.
   - **Secondary SMTP Gateway Port**—If you are using a secondary or backup SMTP server, then enter the server port number.
   - **SMTP Timeout**—Specify the number of seconds the printer will wait for a response from the SMTP server before timing out.

- **Reply Address**—Make sure this field is cleared.
- **Use SSL/TLS**—Select **Disabled**, **Negotiate**, or **Required** to specify whether e-mail will be sent using an encrypted link.

4 Under the Authentication heading, configure the following settings:

- **SMTP Server Authentication**—If the SMTP server requires user credentials, then select **Kerberos 5**. If Kerberos is not supported, then select **No authentication required**.

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

- **Device-Initiated E-mail**—Select **None** or **Use Device SMTP Credentials**.

  Note: If the printer must provide credentials to send an e-mail, then enter the appropriate information under the Device Credentials heading.

- **User-Initiated E-mail**—Select **Use Session User ID and Password** if you are using Kerberos authentication. Select **None** if you are not using Kerberos authentication.

5 Click **Submit**.

Configuring e-mail server settings

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

2 Click **E-mail/FTP Settings** > **E-mail Settings**.

3 Under the E-mail Server Settings heading, configure the following settings:

- **Subject**—Type a default subject line for each e-mail sent from the printer. For example, `Scanned Document`.
- **Message**—Type a default message for the body of each e-mail sent from the printer. For example, `Please see the attached document`.
- **Send me a copy**—You do not need to configure this setting. When the Secure E-mail application is installed and running, the “Send me a copy” option is always available to users when they send e-mail from the printer, regardless of how this setting is configured.

4 Click **Submit**.

Configuring scan settings

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

2 Click **E-mail/FTP Settings** > **E-mail Settings**.

3 Under the E-mail Settings heading, configure the following settings if necessary:

- **Color**—To reduce the file size of scanned documents and images, select **Off** or **Gray**.
- **Resolution**—The recommended range is between 150 dpi and 300 dpi. You can choose a higher resolution to improve image quality, but higher resolutions increase the file size of scanned documents and images.
- **Transmission Log**—The recommended setting is **Print only for error**.
- **E-mail Bit Depth**—Select **8 bit** for grayscale imaging or **1 bit** for black and white.

4 Adjust the other scan settings if necessary.

5 Click **Submit**.

Configuring the address book

Configuring these settings enables users to search your network global address book for e-mail addresses.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Network/Ports** > **Address Book Setup**.
3. Configure the following settings:
   - **Server Address**—Type the host name (not the IP address) of the LDAP server.
   - **Server Port**—Enter the server port number 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
   - **LDAP Certificate Verification**—Select **Never**, **Allow**, **Try**, or **Demand**.
   - **Use GSSAPI**—Select this check box.
   - **Mail Attribute**—Type a name for the mail attribute (usually “mail”).
   - **Fax Number Attribute**—Leave this set to the default value.
   - **Search Base**—Type one or more values to be used when querying the LDAP directory. Separate multiple values with a comma.
   - **Search Timeout**—Specify the maximum number of seconds allowed for each LDAP query.
   - **Displayed Name**—Select the combination of LDAP attributes to use to find the displayed name for an e-mail address (also referred to as the “friendly” name). If you are not sure which option to select, then leave this set to the default value.
   - **Max Search Results**—Specify the maximum number of search results to be returned from an LDAP query.
   - **Use user credentials**—Select this check box. This ensures that the address book is protected by the credentials that are provided when you secure access to the address book function. See “Securing access to the address book” on page 8.
4. Click **Submit**.

Configuring the application settings

Configuring digital signing

1. Access the application configuration settings from the Embedded Web Server.
2. Configure the following setting:
   - **Sign E-mail**—Do one of the following:
     - Select **Prompt User** to let users choose to digitally sign their e-mail.
     - Select **Disabled** to disable digital signing.
     - Select **Always Sign** to require all e-mail to be digitally signed.

     Note: For users to digitally sign e-mail, they must have a valid digital signing certificate.
3. Click **Apply**.

Configuring e-mail encryption

1. Access the application configuration settings from the Embedded Web Server.
2. Configure the following settings:
   - **Encrypt E-mail**—Do one of the following:
     - Select **Prompt User** to let users choose to encrypt their e-mail.
     - Select **Disabled** to disable encryption.
     - Select **Always Encrypt** to require all e-mail to be encrypted.

     Note: For users to send encrypted e-mail to a recipient, the recipient must be in the global address book and must have a valid encryption certificate.
   - **Encryption Algorithm**—Select an algorithm to use for encrypting e-mail. The most common setting is "Triple DES."
   - **LDAP-Primary Certificate**—Specify the LDAP attribute to search for a recipient's encryption certificate. The most common setting is "userSMIMECertificate."
   - **LDAP-Alternate Certificate**—Specify the LDAP attribute to search if a recipient's encryption certificate is not found in the primary attribute. The most common setting is "userCertificate."
3. Click **Apply**.

Securing access to the application

Note: Before securing access to the application, make sure an authentication module application and the eSF Security Manager application are installed and running on the printer. For more information about eSF Security Manager, see the *eSF Security Manager Administrator's Guide*.

This application runs in place of the standard e-mail function on the printer. For the security features of the application to work correctly, you must use an authentication module to secure access to the printer e-mail function. When users attempt to access the secured e-mail function, they will be prompted to authenticate.

After the authentication module has been associated with the e-mail function, it must be configured to specify where the printer should retrieve an authenticated user's e-mail address when the user sends an e-mail. The user's e-mail address will be placed in the "From" field of the sent e-mail.

To secure access to the e-mail function and specify where to get the user's e-mail address:

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security** > **Security Setup**.
3. From Step 2 under the Advanced Security Setup heading, click **Security Template**, and then click **Add a Security Template**.
4. Type a name for the security template (for example, **`Secure E-mail`**).
5. From the Authentication Setup drop-down menu, select the authentication module you want to use to secure access to the e-mail function, and then click **Save Template**.
6. From the Embedded Web Server, click **Settings** or **Configuration**, and then click **Security** > **Security Setup**.
7. From Step 3 under the Advanced Security Setup heading, click **Access Controls**.
8. If necessary, expand the **Function Access** folder.
9. From the E-mail Function drop-down menu, select your security template.

10 Click **Submit**.

11 Access the authentication module application configuration settings from the Embedded Web Server.

12 Configure the setting that specifies where to retrieve user e-mail addresses when sending e-mail.

13 If necessary, configure the other authentication module settings.

14 Click **Apply**.

Securing access to the address book

For users to search the global address book for e-mail addresses, you must use the authentication module to secure access to the address book function.

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

2 Click **Security** > **Security Setup**.

3 From Step 2 under the Advanced Security Setup heading, click **Security Template**, and then click **Add a Security Template**. If you have already created a security template for the authentication module you want to use, then skip to step 6.

4 Type a name for the security template (for example, **`Secure E-mail`**).

5 From the Authentication Setup drop-down menu, select the authentication module you want to use to secure access to the address book function, and then click **Save Template**.

6 From the Embedded Web Server, click **Settings** or **Configuration**, and then click **Security** > **Security Setup**.

7 From Step 3 under the Advanced Security Setup heading, click **Access Controls**.

8 If necessary, expand the **Function Access** folder.

9 From the Address Book drop-down menu, select your security template.

10 Click **Submit**.

For more information about configuring security templates and using access controls, see the *Embedded Web Server Administrator's Guide* for your printer.

Using Secure E-mail

Note: If users log in to the application manually (using a user name and password), then you must enable the authentication module application setting that tells the printer to retrieve all user information before allowing users to access secured applications. This ensures that a manual login user's e-mail address is stored in the login session and is available for use with Secure E-mail. If this setting is not enabled, then manual login users cannot send e-mail to themselves automatically. The "Send me a copy" option will not be available.

Sending secure e-mail

Note: You can return to the printer home screen if you want to cancel the sending of the e-mail.

1. Load the document into the printer.

   Note: Documents may be loaded into the Automatic Document Feeder (ADF) or on the scanner glass. For information on the different methods of loading documents, see the *User's Guide* that came with the printer.

2. From the printer home screen, touch the application icon.
3. If prompted, enter your authentication credentials.
4. Use the keyboard to type an e-mail address, or search the address book. Select **Send me a copy** if you want to automatically send a copy of the e-mail to yourself.
5. Touch **Next Address** to add additional recipients.
6. When you are done adding recipients, touch **E-mail It**.
7. If prompted, select whether to digitally sign the e-mail, encrypt the e-mail, or do both. Leave both options cleared to send an unsigned, unencrypted e-mail.

   Note: Depending on how the application is configured, you may see only one option, or you may not see this prompt at all.

8. If prompted, enter your PIN or password for sending digitally signed e-mail.
9. To digitally sign e-mail, you must have a valid digital signing certificate. If a signing certificate error message appears, then follow the instructions on the screen:
   - If the message "No signing certificate is available to sign your e-mail" appears, then touch **Next** to send the e-mail without a digital signature, or return to the home screen to cancel the sending of the e-mail.
   - If the message "The e-mail cannot be sent because your signing certificate could not be found" appears, then you will need to obtain a signing certificate, or the application will need to be configured to allow you to send unsigned e-mail.
10. For encrypted e-mail to be sent to a recipient, the recipient must be in the global address book and must have a valid encryption certificate. If an encryption certificate error message appears, then follow the instructions on the screen:
    - If the message "Cannot encrypt e-mail for one or more recipients" appears, then do one of the following:
      - Select **Send encrypted e-mail only** to send encrypted e-mail only to recipients who have encryption certificates. Recipients who do not have encryption certificates will not receive the e-mail.
      - Select **Send all e-mails unencrypted** to send unencrypted e-mail to all recipients.
      - Return to the home screen to cancel the sending of the e-mail.

- If the message “Encryption certificate not found for one or more recipients” appears, then touch **Next** to send encrypted e-mail only to recipients who have encryption certificates (recipients who do not have encryption certificates will not receive the e-mail), or return to the home screen to cancel the sending of the e-mail.
- If the message “No encryption certificates could be found for any of the addresses you entered” appears, then touch **Next** to send unencrypted e-mail to all recipients, or return to the home screen to cancel the sending of the e-mail.
- If the message “The e-mail cannot be sent because encryption certificates could not be found for any recipients” appears, then each recipient will need to obtain an encryption certificate, or the application will need to be configured to allow you to send unencrypted e-mail.

The printer performs a connection test with the e-mail server, and then scans the first page of your document.

11 To scan additional pages, load the next page, and then touch **Scan the Next Page**. If you have no more pages to scan, then touch **Finish the Job**.

Troubleshooting

Secure E-mail issues

“The e-mail cannot be sent because your e-mail address could not be retrieved” error message

This error occurs when the authentication module could not retrieve the user’s e-mail address. Try one or more of the following:

Make sure the printer e-mail function is secured

For the authentication module to retrieve user e-mail addresses, the printer e-mail function must be secured correctly. See “Securing access to the application” on page 7.

Make sure user e-mail addresses are retrieved correctly

1. Access the authentication module application configuration settings from the Embedded Web Server.
2. Make sure the setting that specifies where the printer should retrieve user e-mail addresses is configured correctly.
3. Click **Apply**.

Check the LDAP settings

For information about resolving LDAP issues, see “Secure E-mail LDAP issues” on page 14.

“Your e-mail cannot be sent because your signing certificate could not be retrieved” error message

Check the user’s signing certificate

For users to digitally sign e-mail, they must have a valid digital signing certificate. Make sure the user has a signing certificate and that the authentication module you are using to retrieve certificates is configured correctly.

“No signing certificate is available to sign your e-mail. Press Next to continue without digital signature” or “The e-mail cannot be sent because your signing certificate could not be found” error message

E-mail can be digitally signed only if users have a valid digital signing certificate. Users cannot digitally sign e-mail if they do not have a signing certificate or if the login method used does not support retrieving signing certificates.

If you configured the application to allow users to choose whether to digitally sign their e-mail, then the first error message is shown to users who do not have signing certificates. They can either send the e-mail without a digital signature or return to the home screen to cancel the sending of the e-mail.

If you configured the application to require e-mail to be digitally signed, then the second error message is shown to users who do not have signing certificates. These users cannot send e-mail. If you want all e-mail sent from the printer to be digitally signed, then make sure a signing certificate is available for each user.

"The e-mail cannot be sent because an error occurred trying to retrieve user certificates from the LDAP server" error message

Try one or more of the following:

Check the address book setup

For information about configuring address book settings, see "Configuring the address book" on page 6.

Make sure the address book function is secured

For users to search the global address book for e-mail addresses, the address book function must be secured correctly. See "Securing access to the address book" on page 8.

Check the LDAP settings

For information about resolving LDAP issues, see "Secure E-mail LDAP issues" on page 14.

Make sure the printer is connected to the network

Make sure all appropriate network cables are connected securely and the network settings of the printer are configured correctly. For information on networking the printer, see the printer *User's Guide* on the *Software and Documentation* CD that came with the printer.

"Cannot encrypt e-mail for one or more recipients. Choose one of the following" or "Encryption certificate not found for one or more recipients. Press Next to send e-mail only to recipients with certificates" error message

These errors indicate that the user tried to send encrypted e-mail to one or more recipients who do not have encryption certificates. For users to send encrypted e-mail to a recipient, the recipient must be in the global address book and must have a valid encryption certificate. Users cannot send encrypted e-mail to recipients who do not have encryption certificates.

If you configured the application to allow users to choose whether to encrypt their e-mail, then the first error message is shown to users when one or more recipients do not have encryption certificates. Users can choose one of the following on the printer touch screen:

- **Send encrypted e-mail only**—Encrypted e-mail will be sent only to recipients who have encryption certificates. Recipients who do not have encryption certificates will not receive the e-mail.
- **Send all e-mails unencrypted**—Unencrypted e-mail will be sent to all recipients.

Users can also return to the home screen to cancel the sending of the e-mail.

If you configured the application to require e-mail to be encrypted, then the second error message is shown to users when one or more recipients do not have encryption certificates. Users can either send encrypted e-mail only to recipients who have encryption certificates (recipients who do not have encryption certificates will not receive the e-mail), or they can return to the home screen to cancel the sending of the e-mail.

“No encryption certificates could be found for any of the addresses you entered. Press Next to send the e-mail without encryption” or “The e-mail cannot be sent because encryption certificates could not be found for any recipients” error message

These errors indicate that none of the recipients the user tried to send an encrypted e-mail to have encryption certificates. For users to send encrypted e-mail to a recipient, the recipient must be in the global address book and must have a valid encryption certificate. Users cannot send encrypted e-mail to recipients who do not have encryption certificates.

If you configured the application to allow users to choose whether to encrypt their e-mail, then the first error message is shown to users when encryption certificates could not be found for any recipients. Users can either send unencrypted e-mail to all recipients or return to the home screen to cancel the sending of the e-mail.

If you configured the application to require e-mail to be encrypted, then the second error message is shown to users when encryption certificates could not be found for any recipients. If this occurs, then users cannot send e-mail. If you want all e-mail sent from the printer to be encrypted, then make sure each recipient has an encryption certificate in the global address book.

“Unable to connect to the e-mail server” error message

This error usually occurs when there is a problem with the SMTP or e-mail settings on the printer. See “Configuring printer e-mail settings” on page 4, or try one or more of the following:

Make sure the printer is connected to a domain

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Network/Ports** > **TCP/IP**.
3. Under the TCP/IP heading, make sure the information typed in the Domain Name field is correct.
4. Click **Submit**.

Note: For more information about TCP/IP settings, see “Configuring TCP/IP settings” on page 4.

Check the SMTP Server Authentication setting

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **E-mail/FTP Settings** > **SMTP Setup**.
3. Under the Authentication heading, from the SMTP Server Authentication menu, do one of the following:
   - Select **Kerberos 5** if the SMTP server requires user credentials.
   - Select **No authentication required** if Kerberos is not supported.

   Note: If the SMTP server requires user authentication for sending e-mail but does not support Kerberos, then the IP address or host name of the printer must be added to the SMTP server as a relay.
4. Click **Submit**.

Provide the server host name if the SMTP server uses Kerberos

If the SMTP server uses Kerberos for authentication, then you must provide the server host name, not the IP address.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **E-mail/FTP Settings** > **SMTP Setup**.
3. Under the SMTP Setup heading, verify or correct the following settings:
   - **Primary SMTP Gateway**—Type the host name (not the IP address) of the primary SMTP server the printer uses for sending e-mail.
   - **Secondary SMTP Gateway**—If you are using a secondary or backup SMTP server, then type the server host name (not the IP address).
4. Click **Submit**.

Make sure Port 25 is not blocked

Make sure the server and firewall settings are configured to allow communication between the printer and the SMTP server on Port 25.

Make sure the printer is connected to the network

Make sure all appropriate network cables are connected securely and the network settings of the printer are configured correctly. For information on networking the printer, see the printer *User's Guide* on the *Software and Documentation* CD that came with the printer.

"Send me a copy" is not available

For the "Send me a copy" option to appear on the printer control panel, the user's e-mail address must be available in the login session before Secure E-mail starts running.

Make sure all user information is placed in the login session

1. Access the authentication module application configuration settings from the Embedded Web Server.
2. Enable the setting that tells the printer to retrieve all user information before allowing users to access secured applications.
3. Click **Apply**.

Secure E-mail LDAP issues

LDAP lookups fail

Try one or more of the following:

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

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

Verify that the address book setup contains the host name for the LDAP server

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Network/Ports** > **Address Book Setup**.
3. Verify that the host name (not the IP address) of the LDAP server appears in the Server Address field.
4. Click **Submit**.

If the LDAP server requires SSL, then verify or correct the address book setup settings

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

Narrow the LDAP search base

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

Verify that the LDAP attributes being searched for are correct

Make sure all LDAP attributes for the user are correct.

Secure E-mail licensing issues

License error

Try one or more of the following:

Make sure the application is licensed

Applications require a license to run.

For more information on purchasing a license, contact your Lexmark representative.

Make sure the license is up-to-date

Make sure the license for the application has not yet expired. Check the license expiry date using the Embedded Web Server.

Appendix

Configuring applications using the Embedded Web Server

Accessing application configuration settings using the Embedded Web Server

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

Note: An IP address appears as four sets of numbers separated by periods, such as 123.123.123.123.

2. Open a Web browser, and then type the printer IP address in the address field.

   The Embedded Web Server page appears.
3. From the navigation menu on the left, click **Settings** or **Configuration**.
4. Click **Device Solutions** > **Solutions (eSF)**, or click **Embedded Solutions**.
5. From the Installed Solutions list, click the application you want to configure, and then click **Configure**.

Licensing the application

Licensing applications

Applications require a valid electronic license to run on select printers.

For more information on purchasing a license for an application, contact your Lexmark representative.

Exporting and importing configuration files

After configuring an application, you can export your current settings into a file that can then be imported and used to configure that application on one or more additional printers.

Exporting and importing a configuration using the Embedded Web Server

You can export configuration settings into a text file that can then be imported and used to apply the settings to one or more additional printers.

Exporting a configuration

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Device Solutions** > **Solutions (eSF)**, or click **Embedded Solutions**.
3. From Installed Solutions, click the name of the application you want to configure.

4 Click **Configure** > **Export**.

5 Follow the instructions on the computer screen to save the configuration file, and then enter a unique file name or use the default name.

Note: If a **JVM Out of Memory** error occurs, then repeat the export until the configuration file is saved.

Importing a configuration

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

2 Click **Device Solutions** > **Solutions (eSF)**, or click **Embedded Solutions**.

3 From Installed Solutions, click the name of the application you want to configure.

4 Click **Configure** > **Import**.

5 Browse to the saved configuration file, and then load or preview it.

Note: If a timeout occurs and a blank screen appears, then refresh the browser, and then click **Apply**.

Notices

Edition notice

January 2012

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

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

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

For Lexmark technical support, visit **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
USA

Trademarks

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

Mac and the Mac logo are trademarks of Apple Inc., registered in the U.S. and other countries.

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4,

as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commerical Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

LEXMARK SOFTWARE LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Index

U