



Lexmark™

Secure E-mail

Administrator's Guide

April 2013

www.lexmark.com

Contents

- Overview..... 3**
- Configuring Secure E-mail..... 4**
 - Configuring TCP/IP settings..... 4
 - Configuring printer e-mail settings..... 4
 - Configuring SMTP settings 4
 - Configuring e-mail server and scan settings 5
 - Configuring the address book 5
 - Configuring the application settings..... 6
 - Securing access to the application..... 6
- Using Secure E-mail..... 8**
 - Sending secure e-mail..... 8
- Troubleshooting..... 9**
 - Secure E-mail issues..... 9
 - Secure E-mail LDAP issues..... 11
 - Secure E-mail licensing issues..... 12
- Appendix..... 13**
- Notices..... 14**
- Index..... 15**

Overview

Use this application to digitally sign and encrypt e-mails sent from the printer. The application overrides the standard printer e-mail function.

Additional required applications

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

- **Smart Card Authentication Client**—Lets you secure access to the e-mail function by requiring users to log in to the printer when trying to use the function. The authentication module retrieves:
 - The authenticated user e-mail address for sending e-mail from the printer
 - The user certificates for digital signing and encryption
- **eSF Security Manager**—Lets you secure access to the printer e-mail function by associating the function with the authentication module. For more information, see the *eSF Security Manager Administrator's Guide*.

Notes:

- For a list of application requirements, including supported printers and required firmware versions, see the *Readme* file.
- For information on setting up the printer or using the printer features, see the printer *User's Guide*.
- For information on connecting the printer to your network, see the *Networking Guide*.

Configuring Secure E-mail

Configuring TCP/IP settings

- 1 From the Embedded Web Server, click **Settings** or **Configuration**.
- 2 Click **Network/Ports > TCP/IP**.
- 3 From the TCP/IP section, do the following:
 - a Make sure that the domain name is the same as the one assigned to user workstations.
 - b 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.
 - c If the printer is located in a different domain, then list the additional domains in the Domain Search Order field. Use commas to separate each domain. If everything is in the same domain, then leave the Domain Search Order field blank.
- 4 Apply the changes.

Configuring printer e-mail settings

Configuring SMTP settings

- 1 From the Embedded Web Server, click **Settings** or **Configuration**.
- 2 Click **E-mail/FTP Settings > SMTP Setup**.
- 3 Configure the following settings:

From the SMTP Setup section

- **Primary SMTP Gateway**—Type the IP address or host name of the primary SMTP server for sending e-mail.
Note: For Kerberos authentication, use the host name.
- **Primary SMTP Gateway Port**—Enter the port number of the primary SMTP server.
- **Secondary SMTP Gateway**—Type the server IP address or host name of your secondary or backup SMTP server.
- **Secondary SMTP Gateway Port**—Enter the server port number of your secondary or backup SMTP server.
- **SMTP Timeout**—Specify how long before the printer times out if the SMTP server does not respond.
- **Use SSL/TLS**—Select **Disabled**, **Negotiate**, or **Required** to specify whether to send an e-mail using an encrypted link.

From the Authentication section

- **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 authentication but does not support Kerberos, then add the printer IP address or host name to the SMTP server as relay.

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

Note: If authentication is required to send an e-mail, then enter the appropriate information under the Device Credentials heading.

- **User-Initiated E-mail**—If using Kerberos authentication, select **Use Session User ID and Password**. Otherwise, select **None**.

4 Apply the changes.

Configuring e-mail server and scan settings

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

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

3 Configure the following settings:

From the E-mail Server Settings section

- **Subject**—Type a default subject line for each e-mail sent from the printer.
- **Message**—Type a default message for the body of each e-mail sent from the printer.
- **Send me a copy**—This setting is optional.

From the E-mail Settings section

- **Color**—Select **Off** or **Gray** to reduce the file size of scanned documents and images.
- **Resolution**—Set the range between 150 dpi and 300 dpi.
- **Transmission Log**—Select **Print only for error**.
- **E-mail Bit Depth**—Select **8 bit** for grayscale imaging or **1 bit** for black and white.

4 Apply the changes.

Configuring the address book

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 to use for address book lookups.
- **LDAP Certificate Verification**—Select how verification is done for LDAP certification.
- **Use GSSAPI**—Select this check box.
- **Mail Attribute**—Type a name for the mail attribute (usually “mail”).
- **Fax Number Attribute**—Retain the default value.
- **Search Base**—Type one or more values separated by commas to use when querying the LDAP directory.

- **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. This setting is optional.
- **Max Search Results**—Specify the maximum number of search results to be returned from an LDAP query.
- **Use user credentials**—Select this check box to ensure that the address book is protected. For more information, see [step 4 on page 7](#).

4 Apply the changes.

Configuring the application settings

- 1 From the Embedded Web Server, access the configuration page for the application.
- 2 Configure the settings, and then apply the changes.

Notes:

- To digitally sign e-mail, users must have a valid digital signing certificate.
- To receive encrypted e-mail, the recipient must be in the global address book and must have a valid encryption certificate.
- To apply security marking to e-mails, enable the setting, and then type the text that you want to use.

Securing access to the application

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

This application overrides the standard e-mail function on the printer. For the security features of the application to work correctly, use an authentication module to secure access to the e-mail function. Users are required to log in to the printer when trying to use the e-mail function.

After the authentication module has been associated with the e-mail function, specify where to retrieve an authenticated user e-mail address when sending an e-mail. The user e-mail address appears in the From field of the sent e-mail.

- 1 Create a security template.
 - a From the Embedded Web Server, click **Settings** or **Configuration**.
 - b Click **Security > Security Setup**.
 - c From the Advanced Security Setup section, click **Security Template > Add a Security Template**.
 - d Type a name for the security template (for example, **Secure E-mail**).
- 2 Select a security template for the e-mail function.
 - a From the Authentication Setup menu, select the authentication module you want to use to secure access to the e-mail function, and then click **Save Template**.
 - b From the Advanced Security Setup section, click **Access Controls**.
 - c If necessary, expand the **Function Access** folder.
 - d From the E-mail Function menu, select your security template.
 - e Apply the changes.

- 3** Configure the authentication module settings.
 - a** From the Embedded Web Server, access the configuration page for the authentication module application.
 - b** Specify where to retrieve user e-mail addresses when sending e-mail.
 - c** If necessary, configure the other authentication module settings.
 - d** Apply the changes.
- 4** Select a security template for the address book.
 - a** From the Authentication Setup menu, select the authentication module you want to use to secure access to the address book function, and then click **Save Template**.
 - b** From the Advanced Security Setup section, click **Access Controls**.
 - c** If necessary, expand the **Function Access** folder.
 - d** From the Address Book menu, select your security template.
 - e** Apply the changes.

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

Using Secure E-mail

Sending secure e-mail

Note: When using manual login, make sure that the printer retrieves all user information accessing secured applications. Adjust the user authentication settings to let the printer wait for user information.

- 1 Load an original document into the ADF tray or on the scanner glass.

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

- 2 From the home screen, touch the application icon.
- 3 If prompted, enter your authentication credentials.
- 4 Enter the recipients.
- 5 Send the document, and then follow the instructions on the screen.

Note: If necessary, select the security options, including the security marking you want to use.

Troubleshooting

Secure E-mail issues

E-mail address cannot be retrieved

Make sure that the printer e-mail function is secured

For more information, see [“Securing access to the application” on page 6](#).

Make sure that user e-mail addresses are retrieved correctly

- 1 From the Embedded Web Server, access the configuration page for the authentication module application.
- 2 Make sure that the location of e-mail addresses to retrieve is set correctly.
- 3 Apply the changes.

Check the LDAP settings

For more information, see [“Secure E-mail LDAP issues” on page 11](#).

Signing certificate cannot be retrieved

Check the user’s signing certificate

Make sure that the user has a signing certificate and that the authentication module for retrieving certificates is configured correctly.

Signing certificate is unavailable

If the application is not configured to require a digital signature, then send the e-mail without a digital signature or return to the home screen to cancel the e-mail.

If the application is configured to require a digital signature, then make sure that a signing certificate is available for each user.

Cannot retrieve certificates from the LDAP server

Try one or more of the following:

Check the address book setup

For more information, see [“Configuring the address book” on page 5](#).

Make sure that the address book function is secured

For more information, see [“Securing access to the application” on page 6](#).

Check the LDAP settings

For more information, see [“Secure E-mail LDAP issues” on page 11](#).

Make sure that the printer is connected to the network

Make sure that the network cables are connected securely and that the network settings of the printer are configured correctly. For information on networking the printer, see the *Networking Guide*.

Cannot encrypt e-mail for one or more recipients

If the application is not configured to require e-mail encryption, then send unencrypted e-mail to all recipients. You can also return to the home screen to cancel the e-mail.

If the application is configured to require e-mail encryption, then send encrypted e-mail only to recipients who have encryption certificates. Recipients without encryption certificates cannot receive the e-mail.

Make sure that each recipient is in the global address book and has a valid encryption certificate.

Cannot connect to the e-mail server

See [“Configuring SMTP settings” on page 4](#), or try one or more of the following:

Make sure that the printer is connected to a domain

- 1 From the Embedded Web Server, click **Settings** or **Configuration**.
- 2 Click **Network/Ports > TCP/IP**.
- 3 From the TCP/IP section, make sure that the domain name is correct.
- 4 Apply the changes.

Note: For more information, 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 From the SMTP Server Authentication menu, do one of the following:
 - If the SMTP server requires user credentials, then select **Kerberos 5**.
 - If Kerberos is not supported, then select **No authentication required**.
 - If the server requires authentication but does not support Kerberos, then add the printer IP address or host name to the server as a relay.
- 4 Apply the changes.

If the SMTP server uses Kerberos, then provide the host name instead of the IP address

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

- 3** From the SMTP Setup section, check the following settings:
 - **Primary SMTP Gateway**—Type the host name (not the IP address) of the primary SMTP server 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** Apply the changes.

Make sure that Port 25 is not blocked

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

Make sure that the printer is connected to the network

Make sure that the network cables are connected securely and the network settings of the printer are configured correctly. For more information, see the *Networking Guide*.

Cannot send a copy to self

Make sure that all user information is placed in the login session

- 1** From the Embedded Web Server, access the configuration page for the authentication module application.
- 2** Enable the setting that retrieves all user information before allowing access to secured applications.
- 3** Apply the changes.

Secure E-mail LDAP issues

LDAP lookups fail

Try one or more of the following:

Make sure that Port 389 (non-SSL) and Port 636 (SSL) are not blocked

Make sure that the server and firewall settings are configured to allow communication between the printer and the LDAP server on Port 389 and Port 636.

Make sure 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** Make sure that the host name (not the IP address) of the LDAP server appears in the Server Address field.
- 4** Apply the changes.

If the LDAP server requires SSL, then check the address book setup settings

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

Narrow the LDAP search base to the lowest possible scope that includes all necessary users**Check that the LDAP attributes being searched for are correct**

Make sure that all LDAP attributes for the user are correct.

Secure E-mail licensing issues

License error

Try one or more of the following:

Make sure that the application is licensed

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

Make sure that the license is up-to-date

- 1 Open a Web browser, and then type the printer IP address.
Note: View the printer IP address in the TCP/IP section of the Network/Ports menu.
- 2 Click **Settings** or **Configuration**.
- 3 Depending on your printer model, do one of the following:
 - Click **Apps > Apps Management**.
 - Click **Device Solutions > Solutions (eSF)**.
 - Click **Embedded Solutions**.
- 4 Click the license status of the application from the list.
- 5 Update the license.

Appendix

Accessing the configuration page for the application using the Embedded Web Server

1 Open a Web browser, and then type the printer IP address.

Note: View the IP address in the TCP/IP section of the Network/Ports menu.

2 Click **Settings** or **Configuration**.

3 Depending on your printer model, do one of the following:

- Click **Apps > Apps Management**.
- Click **Device Solutions > Solutions (eSF)**.
- Click **Embedded Solutions**.

4 Select the application from the list, and then click **Configure**.

Exporting or importing a configuration file using the Embedded Web Server

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**.

Licensing applications

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

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

Notices

Edition notice

April 2013

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 <http://support.lexmark.com>.

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

© 2013 Lexmark International, Inc.

All rights reserved.

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.

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.

Index

A

- accessing the configuration page
 - using the Embedded Web Server 13
- additional required
- applications 3
- address book
 - securing 6
- address book setup 5
- applications
 - licensing 13

C

- cannot connect to the e-mail server 10
- cannot encrypt e-mail for one or more recipients 10
- cannot retrieve certificates from the LDAP server 9
- cannot send a copy to self 11
- configuration page for the application
 - accessing 13

D

- digital signing
 - configuring 6
- DNS settings
 - configuring 4

E

- e-mail
 - sending 4
- e-mail address book 5
- e-mail addresses
 - retrieving 6
- e-mail function
 - securing 6
- e-mail scan settings
 - configuring 5
- Embedded Web Server
 - accessing the configuration page 13
- encryption
 - configuring 6

- encryption certificate not found 10
- encryption certificate not found for one or more recipients 10
- error trying to retrieve certificates from the LDAP server 9
- exporting a configuration file
 - using the Embedded Web Server 13
- exporting a configuration file using the Embedded Web Server 13
- e-mail
 - sending 8
- e-mail address cannot be retrieved 9
- e-mail cannot be sent because of error retrieving certificates from LDAP server 9
- e-mail cannot be sent because the e-mail address could not be retrieved 9
- e-mail cannot be sent because the signing certificate cannot be retrieved 9
- e-mail cannot be sent because your signing certificate could not be found 9
- e-mail encryption
 - configuring 6

I

- importing a configuration file
 - using the Embedded Web Server 13
- importing a configuration file using the Embedded Web Server 13

L

- LDAP lookups fail 11
- license error 12
- licensing applications 13

N

- no signing certificate is available to sign your e-mail 9

O

- overview
 - Secure E-mail 3

P

- printer e-mail settings
 - configuring 4

S

- scan settings
 - for e-mail 5
- Secure E-mail
 - additional required
 - applications 3
 - configuring 6
 - overview 3
 - secure e-mail
 - using from the printer 8
 - securing access to the address book 6
 - securing access to the application 6
 - security marking
 - configuring 6
 - Send me a copy is not available 11
 - sending e-mail 8
 - signing certificate cannot be retrieved 9
 - signing certificate not available 9
 - signing certificate not found 9
 - SMTP settings
 - configuring 4

T

- TCP/IP settings
 - configuring 4
- troubleshooting
 - cannot encrypt e-mail for one or more recipients 10
 - encryption certificate not found 10
 - encryption certificate not found for one or more recipients 10
 - e-mail cannot be sent because of error retrieving certificates from LDAP server 9

- e-mail cannot be sent because
 - the e-mail address could not be retrieved 9
- e-mail cannot be sent because
 - your signing certificate could not be found 9
- LDAP lookups fail 11
- license error 12
- Send me a copy is not available 11
- signing certificate cannot be retrieved 9
- signing certificate is unavailable 9
- signing certificate not available 9
- signing certificate not found 9
- unable to connect to the e-mail server 10
- users cannot automatically e-mail themselves a copy 11

U

- unable to connect to the e-mail server 10
- user e-mail addresses
 - retrieving 6
- users cannot automatically e-mail themselves a copy 11