Secure E-mail

Version 2.1

Administrator's Guide

Contents

Change history

August 2017

- Added instructions on disabling the Device Quotas application.
- Added support for Brazilian Portuguese, Finnish, French, German, Italian, Simplified Chinese, and Spanish.

July 2016

- Added instructions on how to configure the Email to Self application.

January 2016

- Initial document release for multifunction products with a tablet-like touch-screen display.

Overview

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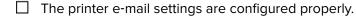
Note: The application overrides the standard printer e-mail function.

Smart Card Authentication Client is required for the security features of the application to work properly. For more information, see the *Smart Card Authentication Client Administrator's Guide*.

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

Deployment readiness checklist

Make sure that:

☐ The printer e-mail settings are configured properly.

☐ You have installed the following applications and drivers:
- Smart Card Authentication Client
- Smart Card Authentication (licensing tool)
- A smart card driver
- CA certificates (.cer file)

Note: For more information, see the *Smart Card Authentication Client Administrator's Guide*.

☐ You have disabled the Device Quotas application:
  1 Obtain the printer IP address. Do either of the following:
  - Locate the IP address on the printer home screen.
  - From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.
  2 Open a web browser, and then type the printer IP address.
  3 Click **Apps** > **Device Quotas** > **Stop**.

Configuring the printer settings

You may need administrative rights to configure the printer settings.

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.
- From the printer home screen, touch **Settings** > **Network/Ports** > **Network Overview**.

2 Open a web browser, and then type the printer IP address.

Securing access to the application

Restricting public access to the application

1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.

2 From the Public section, click **Manage Permissions**.

3 Expand **Function Access**, and then clear **E-mail Function**.

4 Click **Save**.

Allowing users to access the application

1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.

2 From the Additional Login Methods section, click **Manage Permissions** beside Smart Card.

3 Click a user group.

   Note: To configure the default user permission, click **All Users**.

4 Expand **Function Access**, and then select **E-mail Function**.

5 Click **Save**.

Configuring network settings

Configuring TCP/IP settings

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

2 Do any of the following:

- If you are using a static IP address, then type 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, then type the other domains in the Domain Search Order field. Use commas to separate multiple domains.

Note: Use the domain name that is assigned to user workstations.

3 Click **Save**.

Configuring LDAP network account settings

An LDAP network account is needed to send encrypted e-mails. Encryption certificates for recipients are added and configured from the LDAP server. For more information, contact your system administrator.

Note: A Kerberos network account is needed to create an LDAP + GSSAPI network account.

1 From the Embedded Web Server, click **Settings** > **Security** > **Login Methods**.

2 From the Network Accounts section, click **Add Login Method** > **LDAP**.

3 Select **LDAP** or **LDAP + GSSAPI**.

4 From the General Information section, configure the following:

- **Setup Name**—A unique name for the LDAP network account.
- **Server Address**

  Note: Make sure that the address is the same as the Smart Card Authentication Client domain controller address, or the KDC address in the Kerberos configuration file.

- **Server Port**—If you are using SSL, then use port **636**. Otherwise, use port **389**.

5 From the Device Credentials section, clear **Anonymous LDAP Bind**, and then type the authentication credentials used to connect to the LDAP server.

6 If the LDAP server requires SSL, then from the Advanced Options section, set Use SSL/TLS to **SSL/TLS**.

7 From the Address Book Setup section, select **Use user credentials**.

8 Click **Save and Verify**.

Configuring printer e-mail settings

The application overrides the standard printer e-mail function.

Configuring SMTP settings

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

2 Configure the following:

- **Primary SMTP Gateway**—The IP address or host name of the server used for sending e-mail.

    Note: For Kerberos authentication, use the host name.

- **Primary SMTP Gateway Port**

- **Secondary SMTP Gateway**—The server IP address or host name of the secondary or backup SMTP server.

- **Secondary SMTP Gateway Port**

- **SMTP Timeout**

- **Use SSL/TLS**

- **Reply Address**

- **SMTP Server Authentication**

    Notes:

    - If **Kerberos 5** is selected, then type the Kerberos realm.
    - If **NTLM** is selected, then type the NTLM domain.
    - If the SMTP server requires authentication but does not support Kerberos, then in the Reply Address field, type the printer IP address or host name.

- **Device-Initiated E-mail**—The device credentials are required for device-initiated e-mails.

    Note: If **Use Device SMTP Credentials** is selected, then type the authentication credentials.

- **User-Initiated E-mail**—The user credentials are required for user-initiated e-mails.

    Note: If you are using Kerberos authentication, then select **Use Session User ID and Password**.

3 Click **Save**.

Configuring default e-mail and scan settings

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

2 Configure the settings.

3 If necessary, adjust the advanced imaging and the administrative controls settings.

4 Click **Save**.

Configuring Email to Self

Email to Self allows users to send a copy of the e-mail to their e-mail address. For more information, see the *Email to Self Administrator's Guide*.

Depending on your printer model, do either of the following:

For the built-in version of the application

1 From the Embedded Web Server, click **Settings** > **E-mail** > **E-mail Defaults** > **Admin Controls**.

2 Select **Limit E-mail Recipients**.

3 Click **Save**.

For the Embedded Solutions Framework (eSF) application

1 From the Embedded Web Server, navigate to the configuration page for the application:

Apps > **Email to Self** > **Configure**

2 Select **Enable**.

3 Click **Apply**.

Configuring the application

You may need administrative rights to configure the application.

Configuring the Secure E-mail settings

1 From the Embedded Web Server, navigate to the configuration page for the application:

Apps > **Secure E-mail** > **Configure**

2 Configure the settings.

Notes:

- To sign an e-mail digitally, you must have a valid digital signing certificate, and be logged in using a smart card. Signing certificates are available only from the smart card. For more information, contact your system administrator.
- To receive an encrypted e-mail, the recipient must be in the LDAP server address book and must have a valid encryption certificate. For more information, see "Configuring LDAP network account settings" on page 7.
- To apply a security marking to an e-mail, enable the setting, and then type the text that you want to use.
- For more information on each setting, see the mouse-over help.

3 Click **Apply**.

Importing or exporting a configuration file

Note: Importing configuration files overwrites the existing application configurations.

1 From the Embedded Web Server, navigate to the configuration page for the application:

Apps > **Secure E-mail** > **Configure**

2 Click **Import** or **Export**.

Using the application

Sending digitally signed and encrypted e‑mail

Notes:

- When using manual login, configure the Smart Card Authentication Client authentication settings to retrieve all user information. For more information, see the *Smart Card Authentication Client Administrator's Guide*.
- To send an e‑mail, make sure that you have a valid e‑mail address assigned to your account.

1 Log in to the printer.

2 From the printer home screen, touch the application icon.

3 Load a document into the ADF tray or on the scanner glass.

4 Type the e‑mail address of the recipient. Use commas to separate multiple e‑mail addresses.

5 If necessary, configure other e‑mail and scan settings.

6 Touch **Send**.

7 Digitally sign or encrypt the e‑mail.

   Note: To sign an e‑mail digitally, you must have a valid digital signing certificate, and be logged in using a smart card. Signing certificates are available only from the smart card. For more information, contact your system administrator.

8 If necessary, select a security option.

9 Touch **Send**.

10 If an encryption error occurs, then do either of the following:

   - To send an encrypted e‑mail to only recipients with encryption certificates, select **Send Encrypted**.
   - To send an unencrypted e‑mail to all recipients, select **Send Unencrypted**.

11 Touch **Send**.

Troubleshooting

Application error

Try one or more of the following:

Check the diagnostic log

1 Open a web browser, and then type **IP/se**, where **IP** is the printer IP address.

2 Click **Embedded Solutions**, and then do the following:

   a Clear the log file.

   b Set the logging level to **Yes**.

   c Generate the log file.

3 Analyze the log, and then resolve the problem.

   Note: After resolving the problem, set the logging level to **No**.

Contact your Lexmark representative

Cannot send e‑mail using the application

Make sure that the Device Quotas application is disabled

From the Embedded Web Server, click **Apps** > **Device Quotas** > **Stop**.

Cannot retrieve the user e‑mail address

Try one or more of the following:

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 the user e‑mail address is retrieved correctly

1 From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

   Apps > **Smart Card Authentication Client** > **Configure**

2 From the Advanced Settings section, in the E‑mail From Address menu, select where the printer retrieves the user e‑mail address.

3 Select **Wait for user information**.

4 Click **Apply**.

Contact your Lexmark representative

Cannot retrieve the user signing certificate

Try one or more of the following:

Make sure that a signing certificate is available for the user

Install the appropriate signing certificate on the user's smart card.

Make sure that the certificates are retrieved correctly

1 From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

Apps > **Smart Card Authentication Client** > **Configure**

2 From the Advanced Settings section, select **Wait for user information**.

3 Click **Apply**.

Contact your Lexmark representative

Signing certificate unavailable for the user

Try one of the following:

Send the e-mail without a digital signature

Make sure that a signing certificate is available for the user

Install the appropriate signing certificate on the user's smart card.

Contact your system administrator

Cannot retrieve certificates from the LDAP server

Try one or more of the following:

Make sure that the network cables are connected securely and that the network settings of the printer are configured correctly

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

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

If you are using SSL, then use port **636**. Otherwise, use port **389**.

Make sure that the LDAP server address contains the host name, not the IP address

For more information, see "Configuring LDAP network account settings" on page 7.

If the LDAP server requires SSL, then make sure that the SSL settings are correct

For more information, see "Configuring LDAP network account settings" on page 7.

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

Make sure that all LDAP attributes are correct

Contact your system administrator

Cannot encrypt e‑mail for one or more recipients

Try one or more of the following:

Send an unencrypted e‑mail to recipients without an encryption certificate and an encrypted e‑mail to recipients with an encryption certificate

Select **Send to All**. For more information, see "Sending digitally signed and encrypted e‑mail" on page 11.

Send an encrypted e‑mail to only recipients with encryption certificates

Select **Send Encrypted**. For more information, see "Sending digitally signed and encrypted e‑mail" on page 11.

Send unencrypted e‑mail to all recipients

Select **Send Unencrypted**. For more information, see "Sending digitally signed and encrypted e‑mail" on page 11.

Contact your Lexmark representative

Cannot connect to the e-mail server

Try one or more of the following:

Make sure that the printer is connected to a domain

For more information, see "Configuring TCP/IP settings" on page 7.

Make sure that the SMTP Server Authentication setting is correct

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

2 In 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 SMTP server requires authentication but does not support Kerberos, then in the Reply Address field, type the printer IP address or host name.

3 Click **Save**.

Note: For more information, see "Configuring SMTP settings" on page 8.

If the SMTP server uses Kerberos, then make sure that the host names of the primary and secondary SMTP gateways are correct

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

2 In the Primary SMTP Gateway and Secondary SMTP Gateway fields, type the host name of the gateway instead of the IP address.

3 Click **Save**.

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 network cables are connected securely and that the network settings of the printer are configured correctly

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

Contact your system administrator

Cannot send a copy to self

Try one or more of the following:

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

Make sure that the printer is configured to retrieve all user information

1 From the Embedded Web Server, navigate to the configuration page for Smart Card Authentication Client:

Apps > **Smart Card Authentication Client** > **Configure**

2 From the Advanced Settings section, select **Wait for user information**.

3 Click **Apply**.

Make sure that Email to Self is configured correctly

For more information, see "Configuring Email to Self" on page 9.

Contact your Lexmark representative

LDAP lookups fail

Try one or more of the following:

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

If you are using SSL, then use port 636. Otherwise, use port 389.

Make sure that the LDAP server address contains the host name, not the IP address

For more information, see "Configuring LDAP network account settings" on page 7.

If the LDAP server requires SSL, then make sure that the SSL settings are correct

For more information, see "Configuring LDAP network account settings" on page 7.

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

Make sure that all LDAP attributes are correct

Contact your system administrator

Notices

Edition notice

August 2017

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**.

© **2016 Lexmark International, Inc.**

All rights reserved.

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

U
unable to connect to the e-mail
server 15