Overview

*Smart Card Authentication* is a collection of applications used to ensure that only authorized users can access and use restricted printer functions. The applications work together to allow authorized users to log in to a printer and securely perform common tasks, including sending e-mail, scanning documents to a network share, and releasing print jobs. Additional security settings can be configured within each application, such as e-mail signing and encryption, network share authentication, and print job release options.

Smart Card Authentication includes the following security applications. These applications are used to secure access to other installed applications and to built-in printer functions.

- **Smart Card Authentication Client**—This lets you secure access to printers by requiring users to log in using a Smart Card or a user name and password. You can use the application to secure access to all applications and functions on the printer home screen or to individual applications and functions. The application also provides Kerberos authentication options and a Kerberos ticket that can be used by other secured applications.

- **eSF Security Manager**—This lets you associate Smart Card Authentication Client with each application and function to which you want to secure access.

- **Authentication token**—If you are using Smart Cards to secure printer access, then this enables the printer to communicate with the type of Smart Card you are using.

  **Note:** You must use the correct authentication token for your Smart Card type.

- **Background and Idle Screen**—This can be secured through Smart Card Authentication Client to provide a secure idle screen that requires users to authenticate before they can access the printer home screen.

Smart Card Authentication also includes the following user applications that can be protected by the security applications. These applications offer valuable security functionality to users at the printer.

- **Secure E-mail**—This runs in place of the standard printer e-mail function and lets users digitally sign and encrypt e-mail sent from the printer.

- **Scan to Network (Basic)**—This lets users scan documents to network destinations specified by the network administrator. When Scan to Network is secured through Smart Card Authentication Client, the Kerberos ticket from Smart Card Authentication Client can be used to authenticate to network destinations.

  **Note:** A premium version of Scan to Network is also available that offers advanced features in addition to those of the basic application. For information on the two versions of Scan to Network and on configuring the application, see the *Scan to Network and Scan to Network Premium Administrator’s Guide*.

- **Secure Held Jobs**—This lets authenticated users view and release their held print jobs in the printer.

Smart Card Authentication also includes the following permit application:

- **Smart Card Authentication**—This manages the licensing for all of the Smart Card Authentication applications that require a license to run. When this application is licensed and installed on a printer, it automatically allows the use of the other applications instead of requiring a license for each individual application.

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

For information on 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 on how to connect the printer to your network.

For information on licensing the application, see “Licensing applications” on page 42.
Configuring printer settings for use with the applications

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

Changing the panel login timeout

To help prevent unauthorized access if a user leaves the printer unattended with a Smart Card inserted or while logged in, you can limit the amount of time a user stays logged in without activity. If the user does not touch the screen within the specified time, then the session ends and the user is logged out, even if a Smart Card is still inserted.

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

2 Click Security > Miscellaneous Security Settings > Login Restrictions.

3 Set the Panel Login Timeout value (in seconds). The recommended value is 30 seconds.

4 Click Submit.

Installing certificates manually

Note: In select printer models, you can automatically download the CA. For more information, see “Installing certificates automatically” on page 6.

Before configuring Kerberos or domain controller settings, you must install the appropriate certificates on the printer. At minimum, you must install the certificate of the Certificate Authority (CA) that issued the domain controller certificate. The CA certificate is used for domain controller validation. Additional certificates can be installed if needed. For example, if you plan to use chain validation to validate the domain controller certificate, then you must install the entire certificate chain. Each certificate must be in a separate PEM (.cer) file.

For each certificate you want to install, do the following:

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


3 Upload the file containing the certificate, and then click Submit.

Note: The file must be in PEM (.cer) format. The contents of the file should resemble the following:

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3t1Ht1r4gHG85zANBgkqhkiG9w0BAQUFADBs
... 13DTbPe0mnIBq0iWgKeAVne1vwaD16rPy+sOnCaQ==
-----END CERTIFICATE-----
```
Installing certificates automatically
For eSF v4.x printers, the CA certificate can be installed automatically.

Note: Make sure to add the printer to the Active Directory Domain. For more information on how to add the printer to the Active Directory, see the *Embedded Web Server Administrator’s Guide* for your printer.

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security > Certificate Management > Certificate Authority Management > CA Cert Monitor Setup**.
3. Select **Enable CA monitor**.
   - If you want to immediately install the CA certificate without waiting for the scheduled run time, then select **Fetch immediately**.
4. Click **Submit**.

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**.

Setting the date and time
In order for users to log in to the printer using Kerberos authentication, the time on the printer clock must be within five minutes of the time on the domain controller system clock. Printer clock settings can be updated manually, or they can be configured to use *Network Time Protocol* (NTP) to automatically sync with a trusted clock (typically the same clock used by the domain controller).

Setting the date and time manually
1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security > Set Date and Time**.
3. In the “Manually Set Date & Time” field, type the correct date and time in **YYYY-MM-DD  HH:MM** format.
   - **Note:** Entering manual settings automatically disables the use of NTP.
4 Select the correct time zone.

   **Note:** If you select *(UTC+user) Custom*, then you must configure additional settings under the Custom Time Zone Setup heading.

5 If *daylight saving time* (DST) is observed in your area, then select **Automatically Observe DST**.

6 If you are located in a nonstandard time zone or in an area that observes an alternate DST calendar, then adjust the Custom Time Zone Setup settings.

7 Under the Network Time Protocol heading, verify that **Enable NTP** is not selected and that the NTP Server field is cleared.

8 Click **Submit**.

**Using NTP**

**Note:** If your network uses *Dynamic Host Configuration Protocol* (DHCP), then verify that NTP settings are not provided by the DHCP server automatically before configuring NTP settings manually.

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

2 Click **Security > Set Date and Time**.

3 Verify that the “Manually Set Date & Time” field is cleared.

4 Select the correct time zone.

   **Note:** If you select *(UTC+user) Custom*, then you must configure additional settings under the Custom Time Zone Setup heading.

5 If daylight saving time is observed in your area, then select **Automatically Observe DST**.

6 If you are located in a nonstandard time zone or in an area that observes an alternate DST calendar, then adjust the Custom Time Zone Setup settings.

7 Under the Network Time Protocol heading, select **Enable NTP**, and then type the IP address or host name of the NTP server.

8 If the NTP server requires authentication, then do one of the following, depending on the options that are available:

   - Select **MD5 key** or **Autokey IFF** from the Authentication drop-down menu, and then click **Install MD5 key** or **Install Autokey IFF params** to browse to the file containing the NTP authentication credentials. Click **Submit** to install the file.

   - Select **Enable Authentication**, and then click **Install auth keys** to browse to the file containing the NTP authentication credentials. Click **Submit** to install the file.

9 Click **Submit**.
Configuring Smart Card Authentication Client

Smart Card Authentication Client and eSF Security Manager must be configured correctly for the other Smart Card Authentication applications to function securely. Perform all necessary configuration steps in this section before configuring the other applications.

Securing access to the printer

**Note:** Before securing access to the printer, make sure the eSF Security Manager application is installed and running. For more information about eSF Security Manager, see the *eSF Security Manager Administrator’s Guide*.

There are two ways to secure access to the printer:

- Enable a secure idle screen that restricts access to the entire home screen. When users insert a Smart Card or touch the screen, they will be prompted to authenticate before they can access the home screen.
  
  **Note:** The Background and Idle Screen application must be installed and running on the printer to enable this functionality.

- Restrict access to individual applications and functions. Users will be able to access the home screen, but when they touch a secured home screen icon or attempt to use a secured function, they will be prompted to authenticate before they can access that application or function. You can secure access to:
  - Installed applications, such as Scan to Network
  - Individual functions of installed applications, such as the Change Background function of the Background and Idle Screen application
  - Built-in printer functions, such as copy and fax

  Users will still be able to access unsecured applications and functions without having to authenticate.

Setting up a security template

Before you can secure access to applications and functions, you need to create a security template that uses Smart Card Authentication Client to obtain user credentials. You can then assign this security template to each application and function you want to protect.

1. Create a building block.
   a. From the Embedded Web Server, click *Security > Security Setup*.
   b. Under the Advanced Security Setup heading, click the building block (or blocks) appropriate for your environment, and then configure it.

   **Note:** For more information on configuring a specific type of building block, see the “Configuring building blocks” section of the *Embedded Web Server Administrator’s Guide* for your printer.

2. Create a security template.
   a. From the Embedded Web Server, click *Settings or Configuration*.
   b. Click *Security > Security Setup*.
   d. Type a name for the security template (for example, *Smart Card*).
   e. From the Authentication Setup menu, select *Smart Card Authentication Client*, and then click *Save Template*.
   f. Verify that your template appears in the Manage Security Templates list.
Securing access to the home screen

Use this method to require users to authenticate to view and use the printer home screen.

Note: The Background and Idle Screen application must be installed and running on the printer before you can secure access to the home screen.

1. Access the Background and Idle Screen application configuration settings from the Embedded Web Server.

2. Under the Idle Screen Settings heading, make sure Enable is selected.

3. In the Start Time field, enter 0. This prompts the printer to start the secure idle screen immediately (0 seconds) after a user’s login session ends.

4. Under the Home Screen Background heading, make sure Enable is not selected if you do not want users to be able to change the home screen background image from the printer control panel.

5. If you want to add custom idle screen images, then click Add under the Idle Screen Images heading.

6. Type an image name, and then upload the file you want to use.

   Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

7. Click Apply.

8. Repeat step 5 through step 7 to add more idle screen images. You can add up to ten images.

9. If you want to add a custom home screen background image, then under the Home Screen Background heading, select one of the default images, or upload a custom image in the Custom Image field.

   Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

10. If necessary, configure the other application settings. For more information about configuring Background and Idle Screen, see the Background and Idle Screen Administrator’s Guide.

11. Click Apply.

12. Secure access to the idle screen using Smart Card Authentication Client.

   On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

   - Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.

   - From the Embedded Web Server, click Settings > Security > Security Setup.

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

   - If necessary, expand the Device Solutions folder.

   - From the Idle Screen drop-down menu, select your security template.

   - Click Submit.

   On printers running eSF version 2.0:

   - Access the eSF Security Manager application configuration settings from the Embedded Web Server.

   - From the Idle Screen drop-down menu, select Smart Card Authentication Client.
Securing access to individual applications and functions

Securing access to installed applications and functions

Use this method to restrict access to installed applications, such as Scan to Network, or to restrict access to the individual functions of an installed application, such as the Change Background function of the Background and Idle Screen application.

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

1. Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.
3. From Step 3 under the Advanced Security Setup heading, click Access Controls.
4. If necessary, expand the Device Solutions folder.
5. For each application or function to which you want to secure access, select your security template from the drop-down menu.
6. Click Submit.

On printers running eSF version 2.0:

1. Access the eSF Security Manager application configuration settings from the Embedded Web Server.
2. For each application or function to which you want to secure access, select Smart Card Authentication Client from the drop-down menu.
3. Click Apply.

Note: If you are unsure about which version of eSF your printer is running, then see “Checking which version of the Embedded Solutions Framework is installed on a printer” on page 43.

Securing access to built-in printer functions

Use this method to restrict access to built-in printer functions, such as copy and fax.

1. Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.
2. From the Embedded Web Server, click Settings or Configuration, and then click Security > Security Setup.
3. From Step 3 under the Advanced Security Setup heading, click Access Controls.
4. If necessary, expand one or more of the access control category folders.
5. For each function to which you want to secure access, select your security template from the drop-down menu.
6. Click Submit.
Notes:

- If you have used a built-in printer security setup to protect the Use Profiles access control, then any installed applications you secure using Smart Card Authentication Client will prompt users for credentials twice. When users touch a secured application icon, they will first be prompted for the credentials specified by the Use Profiles access control, and then they will be prompted for their Smart Card or user name and password.

- If you need to secure access to profiles you have created and installed on the printer, then you can remove the printer security template applied to the Use Profiles access control, and then apply a security template that uses Smart Card Authentication Client. All of your installed profiles will be secured and users will be prompted for their Smart Card or user name and password when they attempt to access a profile.

Configuring login screen settings

You can use the login screen settings to choose how users will be allowed to log in to the printer and whether they will be prompted for a PIN or a password after inserting a Smart Card.

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Login Screen heading, from the Login Type menu, select how users will be allowed to log in to the printer:
   - Smart Card Only—This allows users to log in using a Smart Card.
   - Smart Card or Manual Login—This allows users to log in using either a Smart Card or a user name and password.
   - Manual Login Only—This allows users to log in using a user name and password.

Notes:

- If you selected Smart Card or Manual Login or Manual Login Only, then configure the Manual Login Domain(s) setting under the Manual Login Setup heading. See “Configuring manual login setup settings” on page 11. If you do not configure this setting, then users will not be allowed to log in to the printer manually (using their user name and password).
- If you selected Smart Card Only, then configure the setting to User Validation Mode. For more information, see “Configuring User Validation Mode settings” on page 14.

3 From the Validate Smart Card menu, select whether users will be prompted to type a PIN or a password after inserting a Smart Card.

4 Click Apply.

Configuring manual login setup settings

Notes:

- If users are allowed to log in to the printer manually (using a user name and password instead of a Smart Card), then specify a list of Windows domains for users to select from during login.
- For eSF v4.x printers, make sure to specify the domain or domains available for manual login to work. To view the complete list of supported printers for each version of the Embedded Web Server, see the Readme file.

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Manual Login Setup heading, in the Manual Login Domain(s) field, specify the domain or domains that will be available for users to select during login. Separate multiple domains with a comma. Domains are case-sensitive and are usually typed in lowercase.

3 Click Apply.
Configuring Smart Card setup settings

Note: This is required only in certain printer models. For other printer models, configuring the Kerberos Authentication system is not required.

Configuring Kerberos settings

In addition to providing the mechanism for validating login credentials, Smart Card Authentication Client can also be configured to provide Kerberos authentication.

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

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2. Under the Smart Card Setup heading, from the Kerberos Information menu, do one of the following:
   - Select Use device Kerberos setup file to use the Kerberos configuration file (krb5.conf) installed on the printer.
   - Select Use simple Kerberos setup to enter Kerberos information manually in the Simple Kerberos Setup fields.

   Note: Only one Kerberos realm can be specified using simple Kerberos setup. If you need to specify multiple realms, then use the device Kerberos setup file.

Using the device Kerberos setup file

If you selected Use device Kerberos setup file, then make sure the Kerberos configuration file is installed on the printer.

a. From the Embedded Web Server, click Settings or Configuration.

b. Click Security > Security Setup.

c. From Step 1 under the Advanced Security Setup heading, click Kerberos 5.

d. Verify that the Kerberos configuration file is installed. If the file is not installed, then under the Import Kerberos File heading, upload the appropriate krb5.conf file, and then click Submit.

Using simple Kerberos setup

If you selected Use simple Kerberos setup, then enter the Kerberos information manually under the Simple Kerberos Setup heading. When you click Apply, the values you entered are used to create a Kerberos configuration file.

- **Realm**—Specify the Kerberos realm as configured in Active Directory. This is typically the Windows domain name. Only one realm can be specified here. To specify multiple realms, customize a Kerberos configuration file and install it on the printer. The realm must be typed in uppercase.

- **Domain Controller**—Specify the IP address or host name of the domain controller or domain controllers used for validation. Separate multiple values with a comma. The domain controllers will be tried in the order listed.

- **Domain**—Specify the domain or domains that should be mapped to the Kerberos realm specified in the Realm field. The domain is the second part of the User Principal Name (UserID@DomainName) on the Smart Card. Type the domain in this format: domain name, comma, period, domain name again. For example, DomainName, .DomainName. Multiple domains that map to the specified Kerberos realm can be added here, separated by a comma. For example, DomainName1, .DomainName1, DomainName2, .DomainName2. The domain is case-sensitive and is usually typed in lowercase.

- **Timeout**—Specify the number of seconds (3 to 30) to wait for a response from the domain controller before trying the next one listed.
Selecting the domain controller validation method

Under the Smart Card Setup heading, from the Domain Controller Validation menu, select the method to use for validating the domain controller certificate:

**Note:** Before configuring this setting, make sure the appropriate certificates are installed on the printer. See “Installing certificates manually” on page 5.

- **Use device certificate validation**—This is the most common method. This method uses the certificate of the Certificate Authority (CA) that issued the domain controller certificate to validate the domain controller certificate. The CA certificate must be installed on the printer.

- **Use device chain validation**—This method uses the entire certificate chain, from the domain controller to the root CA, to validate the domain controller certificate. The entire certificate chain must be installed on the printer.

- **Use OCSP validation**—This method uses the Online Certificate Status Protocol (OCSP) to validate the domain controller certificate. The entire certificate chain, from the domain controller to the root CA, must be installed on the printer, and the settings under the Online Certificate Status Protocol (OCSP) heading must be configured:
  - **Responder URL**—Specify the IP address or host name of the OCSP responder/repeater and the port being used (typically 80). Type the value in this format: `http://ip_address:port_number`. For example, `http://255.255.255.0:80`.
    Separate multiple values with a comma. The values will be tried in the order listed.
  - **Responder Certificate**—Upload the X.509 certificate for the OCSP responder. This certificate is used to validate that the response from the OCSP responder is from a trusted source.
  - **Responder Timeout**—Specify the number of seconds (5 to 30) to wait for a response from the OCSP responder before trying the next one listed.
  - **Allow Unknown Status**—Select this check box to allow users to log in if the OCSP response indicates that the certificate status is unknown. If the certificate status is unknown and the check box is cleared, then users will not be allowed to log in.

When you are done configuring Smart Card setup settings, click **Apply**.

Configuring advanced settings

Not all networks require you to configure advanced settings. If necessary, adjust the settings to enable the printer to communicate on your network.

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2. Under the Advanced Settings heading, configure the following settings:

   - **Session User ID**—Select how the user ID will be obtained when a user logs in:
     - **None**—The user ID is not set. You can select this option if the user ID is not needed by other applications.
     - **User Principal Name**—The User Principal Name (UserID@DomainName) retrieved from the Smart Card or provided during manual login is used to set the user ID.
     - **EDI-PI**—The “UserID” portion of the User Principal Name (UserID@DomainName) retrieved from the Smart Card or provided during manual login is used to set the user ID.
     - **LDAP Lookup**—The user ID is retrieved from Active Directory.
   
   - **E-mail From Address**—Select where the printer should retrieve the user’s e-mail address when sending e-mail.
     - **Smart Card**—This retrieves the e-mail address from the user’s Smart Card.
     - **LDAP Lookup**—This retrieves the user’s e-mail address from Active Directory.
   
   - **Disable Reverse DNS Lookups**—If reverse DNS lookups are not used on your network, then select this check box (if available).
On printers running the Embedded Solutions Framework (eSF) version 3.0 or later, this setting is not available from the application configuration settings. If your printer is running eSF version 3.0 or later, then do the following to disable reverse DNS lookups:

a. From the Embedded Web Server, click **Settings > Security > Security Setup**.

b. From Step 1 under the Advanced Security Setup heading, click **Kerberos 5**.

c. Under the Kerberos Settings heading, select **Disable Reverse IP Lookups**.

d. Click **Submit**.

**Note:** If you are unsure about which version of eSF your printer is running, then see “Checking which version of the Embedded Solutions Framework is installed on a printer” on page 43.

- **Wait for user information**—For some secured applications to work correctly, additional user information must be placed in the login session. Select this option to retrieve all user information before allowing the user to access the home screen or secured application.

  **Note:** If you have enabled manual login and you are using the Secure E-mail application along with Smart Card Authentication Client, then you must select this option. 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 option is not selected, then manual login users cannot send e-mail to themselves automatically. The Secure E-mail “Send me a copy” option will not be available.

- **Use SSL for User Info**—Select this check box to use an SSL connection to retrieve user information from the domain controller. If this check box is cleared, then a non-SSL connection is used.

- **Other User Attributes**—List any other LDAP attributes that should be added to the user's session. These attributes will be used with other applications. Separate multiple values with a comma.

- **Group Authorization List**—List all Active Directory groups that are authorized to use at least one printer function. Separate multiple groups with a comma. Leave this field blank if you are not using group authorization.

- **Hosts File**—If DNS is not enabled on your network, then upload a text file containing the necessary IP address—host name mappings.

  Type the mappings in the text file in this format: IP address, space, server host name. For example, 0.0.0.0 HostName. You can assign multiple host names to an IP address. For example, 0.0.0.0 HostName1 HostName2 HostName3. You cannot assign multiple IP addresses to a host name. To assign IP addresses to groups of host names, type each IP address and its associated host names on a separate line of the text file. For example:

  123.123.123.123 HostName1 HostName2
  456.456.456.456 HostName3

3. Click **Apply**.

### Configuring User Validation Mode settings

You can secure your printer using the Smart Card without the need to maintain a full Kerberos authentication system. The user inserts the Smart Card into the reader and then enters the PIN in the printer home screen. If the Smart Card PIN matches the PIN entered in the home screen matches, then the user can access the application.

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2. Under the Login Screen heading, set “Login Type” to **Smart Card Only**, and then set the Authentication mode to **PIN ONLY**.

3. From the Domain Controller Validation menu, select **Use device certificate validation**.

  **Note:** The Online Certificate Status Protocol (OCSP) must not be configured.
4 Under the Advanced Setting heading, set “E-mail From Address” to Smart Card, and then clear the Wait for user information check box.

Note: Session User ID must be set to None, and the “Other User Attributes” and “Group Authorization List” fields must be empty.

5 Click Apply.

Configuring Secure E-mail

Note: Before configuring Secure E-mail, make sure you have configured all necessary Smart Card Authentication Client security settings. See “Configuring Smart Card Authentication Client” on page 8.

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
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.”

• **Signing Algorithm**—Select the algorithm to use for digital signature. The most common setting is “SHA1.”

• **User can only send to self**—Select this check box to allow users to send e-mail only to themselves.

3 Click **Apply**.

**Securing access to the application**

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 Smart Card Authentication Client 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.

When Smart Card Authentication Client is 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 Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.

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

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

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

5 From the E-mail Function drop-down menu, select your security template.

6 Click **Submit**.

7 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

8 Make sure you have configured the “E-mail From Address” setting.

9 Click **Apply**.

**Securing access to the address book**

For users to search the global address book for e-mail addresses, you must use Smart Card Authentication Client to secure access to the address book function.

1 Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.

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

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

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

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

6 Click **Submit**.
Configuring Scan to Network

**Note:** Before configuring Scan to Network, make sure you have configured all necessary Smart Card Authentication Client security settings. See “Configuring Smart Card Authentication Client” on page 8.

**Using a Kerberos ticket for authentication**

Smart Card Authentication Client provides a Kerberos ticket that can be used to authenticate to network destinations. To configure a Scan to Network destination to use this ticket:

1. Make sure you have configured the Smart Card Authentication Client Kerberos settings. See “Configuring Kerberos settings” on page 12.
2. Access the Scan to Network application configuration settings from the Embedded Web Server.
3. Under the Scan Destination heading, click **Add**.
   
   **Note:** You can also edit an existing destination.
4. Type a name for the destination.
5. Under the Location heading, select **Network Folder**, and then configure the location settings.
6. Under the Authentication Options heading, select **Use Kerberos authentication**. The Kerberos credentials from Smart Card Authentication Client will be used to access the network destination.
   
   **Notes:**
   
   • This option is visible if the location is set to **Network Folder**.
   • If you select this option, then make sure **Use MFP authentication credentials** is also selected.
7. In the sections that follow, adjust the settings.
   
   • Select check boxes to allow users to modify settings.
   • Use radio buttons and drop-down menus to specify the default settings.
8. Under the File heading, in the Name field, type a default base name for the scan file. The file extension is generated automatically according to the value of the Format field in the Scan Settings section.
9. Click **OK**, and then click **Apply**.
10. Secure access to Scan to Network using Smart Card Authentication Client.

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

a. Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.

b. From the Embedded Web Server, click **Settings > Security > Security Setup**.

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

d. If necessary, expand the **Device Solutions** folder.

e. From the Scan to Network drop-down menu, select your security template.

f. Click **Submit**.

On printers running eSF version 2.0:

a. Access the eSF Security Manager application configuration settings from the Embedded Web Server.

b. From the Scan to Network drop-down menu, select **Smart Card Authentication Client**.
c Click Apply.

Note: If you are unsure about which version of eSF your printer is running, then see “Checking which version of the Embedded Solutions Framework is installed on a printer” on page 43.

For more information about configuring Scan to Network, see the Scan to Network and Scan to Network Premium Administrator’s Guide.

Configuring Secure Held Jobs

Note: Before configuring Secure Held Jobs, make sure you have configured all necessary Smart Card Authentication Client security settings. See “Configuring Smart Card Authentication Client” on page 8.

Configuring and securing the application

1 Access the Secure Held Jobs application configuration settings from the Embedded Web Server.

2 In the Icon Text field, type the text that will appear above the application icon on the printer home screen.

3 In the Up Icon field, upload an image for the “up icon” (the image that appears when the application icon is not pressed. To view the default icon image, click View Current Value.

Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

4 In the Down Icon field, upload an image for the “down icon” (the image that appears when the application icon is pressed). To view the default icon image, click View Current Value.

Note: For information about compatible image file types and recommended file sizes, see the mouse-over help next to the field.

5 Under the Release Options heading, configure the following settings to specify how users will be allowed to release print jobs:

- Release Method—Select one of the following:
  - User selects job(s) to print—This lets users to choose the jobs they want to print.
  - All jobs print automatically—This prints all jobs pending for a user automatically when the user touches the application icon and authenticates.

- Display Print Jobs Sorted By—Select Job Name, Date Printed (Ascending), or Date Printed (Descending) to specify the order in which print jobs will be listed on the printer control panel.

6 Under the Job Expiration heading, set the expiration for Verify print jobs and Repeat print jobs.

There are four types of held jobs:

- Confidential—This lets you store print jobs on the printer until you log in and release or delete them.
- Verify—This lets you print one copy of a print job and store the remaining copies on the printer. This enables you to make sure the first copy is satisfactory before printing the remaining copies. The print job is automatically deleted from the printer after all copies are printed.
- Reserve—This lets you store print jobs on the printer. The print jobs are automatically deleted after they are printed.
- Repeat—This lets you print all copies of a print job and store the job on the printer so you can print additional copies later. You can print additional copies as long as the job is stored on the printer.
The expiration of Confidential print jobs and Reserve print jobs is controlled by the printer Confidential Print Setup on the Embedded Web Server (click Settings or Configuration, and then click Security > Confidential Print Setup). By default, only Confidential print jobs can be set to expire. The Job Expiration settings let you set Verify print jobs and Repeat print jobs to expire either at the same time as Confidential print jobs or at another time.

- **Verify Job Expiration**—Select Off, Same as Confidential Print, or one of four intervals ranging from one hour to one week.
- **Repeat Job Expiration**—Select Off, Same as Confidential Print, or one of four intervals ranging from one hour to one week.

7 Under the Advanced Settings heading, configure the following settings if necessary:

- **Require All Jobs to be Held**—Select this check box to require all jobs to remain on the printer until they are released by an authorized user or until they expire.
- **Clear Print Data**—Select this check box to clear the memory associated with each print job when the job is released.

8 Click **Apply**.

9 Secure access to Secure Held Jobs using Smart Card Authentication Client.

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

a. Make sure you have created a security template that uses Smart Card Authentication Client to obtain user credentials. See “Setting up a security template” on page 8.

b. From the Embedded Web Server, click Settings or Configuration.

c. Click Security > Security Setup.


e. Type a name for the security template (for example, Secure Held Jobs).

f. From the Authentication Setup drop-down menu, select the authentication module you want to use to secure access to the Secure Held Jobs, and then click Save Template.

g. Under the Advanced Security Setup heading in step b, click Access Controls.

h. If necessary, expand the Device Solutions folder.

i. From the Secure Held Jobs drop-down menu, select your security template.

j. Click **Submit**.

On printers running eSF version 2.0:

a. Access the eSF Security Manager application configuration settings from the Embedded Web Server.

b. From the Secure Held Jobs drop-down menu, select Smart Card Authentication Client.

c. Click **Apply**.

**Note:** If you are unsure about which version of eSF your printer is running, then see “Checking which version of the Embedded Solutions Framework is installed on a printer” on page 43.
Using the applications

Using Secure E-mail

Note: If manual login is enabled, then the “Wait for user information” option must be selected in the Smart Card Authentication Client application configuration settings. See “Configuring advanced settings” on page 13. 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 option is not selected, 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.

Using Scan to Network

Scanning documents at the printer

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 Select the destination where you want to receive the scanned document. If prompted, enter the credentials required to access the destination. Contact your system support person for login information.

5 Some additional job options may be available depending on how the application has been configured. Follow the instructions on the screen to update the options. Contact your system support person for more information on each option.

6 Touch Scan It or Send It. Depending on how the application has been configured, you may have the option to preview and make adjustments to scanned pages.

7 To scan additional documents, load the next document, and then do one of the following from the confirmation screen:

   - Touch Yes, to same destination to scan the document to the previous destination.
   - Touch Yes, to a different destination to scan the document to a different destination.
   - Touch No to finish the scan job and return to the printer home screen.
Using Secure Held Jobs

Printing held jobs

1. With a document open, click **File > Print**.
   
   **Note:** If you are a Macintosh user, then you may need to click the disclosure triangle to see more options.

2. Select the print-and-hold feature:
   
   - For Windows users, click **Properties**, **Preferences**, **Options**, or **Setup**. Then click **Print and Hold**, or click **Other Options > Print and Hold**.
   
   - For Macintosh users, select **Job Routing** from the print options or the “Copies & Pages” pop-up menu.

3. Select the print job type:
   
   - **Confidential**—This lets you store print jobs on the printer until you log in and release or delete them.
   
   - **Verify**—This lets you print one copy of a print job and store the remaining copies on the printer. This enables you to make sure the first copy is satisfactory before printing the remaining copies. The print job is automatically deleted from the printer after all copies are printed.
   
   - **Reserve**—This lets you store print jobs on the printer. The print jobs are automatically deleted after they are printed.
   
   - **Repeat**—This lets you print all copies of a print job and store the job on the printer so you can print additional copies later. You can print additional copies as long as the job is stored on the printer.

   **Note:** Confidential, Verify, and Reserve print jobs are automatically deleted from memory after printing. Repeat job is held in the printer until you choose to delete them.

4. Type the user name from your Smart Card or the LDAP directory. For a Confidential print job, also enter a four-digit **PIN**.

   **Notes:**
   
   - Because you are required to authenticate to use the printer or the application, you will not be prompted to enter this PIN when you print Confidential jobs using this application. The PIN is needed only for printing Confidential jobs using the built-in held jobs function on the printer.
   
   - Make sure the user name matches the one specified by the Smart Card Authentication Client “Session User ID” setting. See “Configuring advanced settings” on page 13.

5. Click **OK** or **Print**.

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

7. If prompted, enter your authentication credentials.

8. If prompted, select the job or jobs you want to print, specify the number of copies to print, and then print them.

   **Note:** Depending on how the application is configured, all jobs in your print release queue may print automatically when you touch the application icon.

If you want to delete selected jobs from your print release queue, then touch **Delete**.
Troubleshooting

Smart Card Authentication Client login issues

“A card reader was not detected on this device” error message

MAKE SURE A SUPPORTED SMART CARD READER IS ATTACHED

If you want users to access the printer using a Smart Card, then attach a supported Smart Card reader to the printer. See the Readme file for a list of supported card readers.

ALLOW USERS TO LOG IN MANUALLY

If you have enabled manual login, then this error message will prompt users that they can “press Login to manually authenticate.” This indicates that users can still log in to the printer using a user name and password instead of a Smart Card.

“Unsupported USB Device” error message when a Smart Card reader is attached to the printer

Try one or more of the following:

MAKE SURE THE SMART CARD READER IS SUPPORTED

See the Readme file for a list of supported card readers.

MAKE SURE THE REQUIRED FIRMWARE VERSION IS INSTALLED

The minimum required firmware version or a later version must be installed before you can attach a supported card reader to the printer. Remove the card reader, and then see the Readme file for a list of required firmware versions.

MAKE SURE ALL REQUIRED APPLICATIONS ARE INSTALLED AND RUNNING

Smart Card Authentication Client, eSF Security Manager, and the authentication token for your Smart Card must be installed and running before you can attach a supported card reader to the printer.

“An error occurred while reading the card. Remove your card and try again” error message

CHECK THE SYSTEM LOG FOR RELEVANT DETAILS

1 Access the list of installed applications from the Embedded Web Server.
2 Click System tab > Log.
3 From the Filter menu, select an application status.

4 From the Application menu, select the application, and then click **Submit**.

If you are still unable to determine the cause of the error, then you may need to replace the card.

**“Your card has been locked out from future login attempts” error message**

This error occurs after a user enters an invalid Smart Card PIN or password too many times or if a user attempts to authenticate using a card that has already been locked out due to too many invalid PIN/password entries.

**RESET OR REPLACE THE CARD**

When a card is locked out, it will need to be reset or replaced. Find out whether the type of card you are using can be reset. If the card cannot be reset, then it will need to be replaced.

**“An error occurred while checking your PIN. Remove your card and try again” error message**

**CHECK THE SYSTEM LOG FOR RELEVANT DETAILS**

1 Access the list of installed applications from the Embedded Web Server.

2 Click **System** tab > **Log**.

3 From the Filter menu, select an application status.

4 From the Application menu, select the application, and then click **Submit**.

**User is unable to log in manually**

**MAKE SURE THE MANUAL LOGIN DOMAIN(S) FIELD ARE SPECIFIED**

Verify that the domains under Manual Login Domain(s) are specified. See “Configuring manual login setup settings” on page 11.

**User is logged out almost immediately after logging in**

**INCREASE THE PANEL LOGIN TIMEOUT INTERVAL**

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

2 Click **Security** > **Miscellaneous Security Settings** > **Login Restrictions**.

3 Increase the number of seconds specified in the Panel Login Timeout field, and then click **Submit**.
The printer home screen fails to return to a locked state when not in use

Try one or more of the following:

MAKE SURE ALL REQUIRED APPLICATIONS ARE INSTALLED AND RUNNING

Smart Card Authentication Client, eSF Security Manager, and the authentication token for your Smart Card must be installed and running in order to restrict access to the printer home screen or to individual home screen applications and functions. Background and Idle Screen must also be installed and running if you want to secure access to the entire home screen.

MAKE SURE THE HOME SCREEN OR HOME SCREEN ICONS ARE SECURED

Either the entire home screen or individual home screen applications and functions must be secured correctly. See “Securing access to the printer” on page 8.

Smart Card Authentication Client authentication issues

“Authentication failed” error message

This error occurs when Kerberos authentication fails or domain controller validation fails while a user is attempting to log in to the printer.

CHECK THE SYSTEM LOG FOR RELEVANT DETAILS

1 Access the list of installed applications from the Embedded Web Server.
2 Click System tab > Log.
3 From the Filter menu, select an application status.
4 From the Application menu, select the application, and then click Submit.

“Kerberos configuration file has not been uploaded” error message

This system log error indicates that the Kerberos configuration file is not installed on the printer.

MAKE SURE THE Kerberos configuration file is installed

If you want to use the device Kerberos setup file, then make sure the file is installed on the printer.

If you want to use simple Kerberos setup to create the Kerberos configuration file, then manually configure the simple Kerberos setup settings.

For information about installing a Kerberos configuration file or configuring simple Kerberos setup settings, see “Configuring Kerberos settings” on page 12.
“Kerberos configuration file is not properly formatted” error message

This system log error indicates that the Kerberos configuration file contains incorrect information, is missing information, or is not formatted properly.

**MODIFY THE INSTALLED KERBEROS CONFIGURATION FILE**

If you used the device Kerberos setup file, then modify and reinstall the file.

If you used simple Kerberos setup, then modify the simple Kerberos setup settings. For information about configuring simple Kerberos setup settings, see “Using simple Kerberos setup” on page 12.

“Unable to authenticate. Check Kerberos configuration file to verify Windows support enabled” error message

This system log error indicates that the Windows domain is not specified in the Kerberos configuration file.

**MAKE SURE THE WINDOWS DOMAIN IS SPECIFIED**

If you used the device Kerberos setup file, then add an entry to the domain_realm section of the file, mapping the lowercase Windows domain to the uppercase realm. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, add the Windows domain (in lowercase) to the Domain field.

   Example: If the value in the Domain field is `DomainName,.DomainName` and the Windows domain is `x.y.z`, then change the value in the Domain field to `DomainName,.DomainName,x.y.z`.
3. Click Apply.

“Unable to generate certificate from card” or “Unable to read certificate information from card” error message

These system log errors indicate that the Smart Card certificate was not found or that an error occurred while the application was attempting to retrieve data from the Smart Card certificate.

**CHECK THE CERTIFICATE ON THE SMART CARD**

Verify that the certificate information on the Smart Card is correct. If the information is correct and the issue still occurs, then contact your solutions provider.
“The domain controller did not respond within the required time; the domain controller timeout may need to be increased” error message

Try one or more of the following:

**INCREASE THE DOMAIN CONTROLLER TIMEOUT**

If you used the device Kerberos setup file, then increase the number of seconds specified for the timeout entry in the file. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, increase the number of seconds specified in the Timeout field.
3. Click Apply.

**MAKE SURE THE DOMAIN CONTROLLER IP ADDRESS OR HOST NAME IS CORRECT**

If you used the device Kerberos setup file, then:

1. From the Embedded Web Server, click Settings or Configuration.
3. Make sure the domain controller IP address or host name specified in the configuration file is correct.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, verify that the IP address or host name specified in the Domain Controller field is correct.
3. Click Apply.

**MAKE SURE THE DOMAIN CONTROLLER IS AVAILABLE**

This error can occur if the domain controller is not available at the time a user is trying to authenticate to the printer. You can resolve this by specifying multiple domain controllers. If a domain controller is not available, then the next one listed will be tried. You can specify multiple domain controllers in the Kerberos configuration file or in the simple Kerberos setup Domain Controller field. If you are using the Domain Controller field, then separate each value with a comma.

**MAKE SURE PORT 88 IS NOT BLOCKED BY A FIREWALL**

Port 88 must be opened between the printer and the domain controller for authentication to work.
“The domain controller issuing certificate has not been installed” error message

This system log error indicates that the required Certificate Authority (CA) certificate is not installed or that an incorrect certificate is installed.

If an incorrect certificate is installed, then the error message specifies the name of the certificate that is needed: “The domain controller issuing certificate [NAME OF CERTIFICATE] has not been installed.”

MAKE SURE THE CORRECT CERTIFICATES ARE INSTALLED ON THE PRINTER

See “Installing certificates manually” on page 5.

“The realm on the card was not found in the Kerberos configuration file” or “User’s realm was not found in the Kerberos configuration file” error message

These system log errors indicate that the user’s realm in the Kerberos configuration file is missing or incorrect.

ADD THE MISSING REALM OR MODIFY THE INCORRECT REALM

If you used the device Kerberos setup file, then add the missing realm or realms to the file, or modify the incorrect realms. Make sure each realm is typed in uppercase. When you are done, reinstall the file on the printer.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, add the missing realm to the Realm field or correct the realm. Make sure the realm is typed in uppercase.

   Note: The simple Kerberos setup settings do not support multiple Kerberos realm entries. If multiple realms are needed, then install a Kerberos configuration file containing the necessary realms.

“Unable to authenticate. Verify the realm was specified in UPPERCASE” error message

MAKE SURE THE KERBEROS REALM IS IN UPPERCASE

If you used the device Kerberos setup file, then:

1. From the Embedded Web Server, click Settings or Configuration.
3. Make sure the realm entries in the configuration file are in uppercase.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, make sure the realm is correct and that it is typed in uppercase.
3. Click Apply.
“Unable to contact the domain controller for the user’s realm” error message

This system log error indicates that the domain, realm, or domain controller specified in the Kerberos configuration file is incorrect.

**CHECK THE DOMAIN, REALM, AND DOMAIN CONTROLLER IN THE KERBEROS CONFIGURATION FILE**

If you used the device Kerberos setup file, then:

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security > Security Setup > Kerberos 5 > View File**.
3. Make sure all domain, realm, and domain controller information is correct.

If you used simple Kerberos setup, then:

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Simple Kerberos Setup heading, make sure the values typed in the Realm, Domain Controller, and Domain fields are correct. For information about configuring these settings, see “Using simple Kerberos setup” on page 12.
3. Click **Apply**.

“Domain controller and device clocks are different beyond an acceptable range. Check the device’s date and time” error message

This system log error indicates that the printer clock is more than five minutes out of sync with the domain controller system clock.

**CHECK THE DATE AND TIME ON THE PRINTER**

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security > Set Date and Time**.
   - If you configured date and time settings manually, then verify or correct the settings. Make sure the time zone and daylight saving time (DST) settings are correct.
   - If you configured the printer to use a Network Time Protocol (NTP) server, then verify that the NTP settings are correct and that the NTP server is functioning correctly.
     
     **Note:** If your network uses Dynamic Host Configuration Protocol (DHCP), then verify that NTP settings are not provided by the DHCP server automatically before configuring NTP settings manually.
3. Click **Submit**.

“Unable to validate certificate from domain controller” error message

This system log error indicates that the required Certificate Authority (CA) certificate or certificates are not installed on the printer or that you selected the wrong domain controller validation method. Try one or more of the following:

**MAKE SURE THE CORRECT CERTIFICATES ARE INSTALLED ON THE PRINTER**

See “Installing certificates manually” on page 5.
CHECK THE DOMAIN CONTROLLER VALIDATION METHOD

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Smart Card Setup heading, make sure you selected the correct method from the Domain Controller Validation menu. For information about configuring this setting, see “Selecting the domain controller validation method” on page 13.
3. Click Apply.

“An error occurred during domain controller chain validation” or “At least one of the certificates in the domain controller certificate chain has been revoked” error message

These system log errors indicate that there is a problem with one or more of the certificates needed for chain validation. Certificates may be missing, expired, or revoked, or they may contain incorrect information.

CHECK THE CERTIFICATES INSTALLED ON THE PRINTER

1. From the Embedded Web Server, click Settings or Configuration.
3. Make sure all certificates required for chain validation are installed and contain correct information. Make sure none of the certificates have been revoked or are expired.
   If you need to install certificates, then see “Installing certificates manually” on page 5.
   If all certificates are installed correctly and these issues still occur, then contact your solutions provider.

“The OCSP responder URL or certificate has not been configured” error message

This system log error indicates that OCSP settings are not configured correctly.

CHECK THE OCSP RESPONDER URL AND RESPONDER CERTIFICATE

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the values in the Responder URL and Responder Certificate fields are correct. For information about configuring these settings, see “Selecting the domain controller validation method” on page 13.
3. Click Apply.
“An error occurred while trying to connect to the OCSP responder” error message

This system log error indicates that the OCSP responder URL is configured incorrectly or that the responder timed out before the application could connect to it. Try one or more of the following:

**CHECK THE OCSP RESPONDER URL**

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the value in the Responder URL field is correct. For information about configuring this setting, see “Selecting the domain controller validation method” on page 13.
3. Click **Apply**.

**INCREASE THE RESPONDER TIMEOUT**

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, increase the number of seconds specified in the Responder Timeout field.
3. Click **Apply**.

“The status of at least one of the certificates in the domain controller certificate chain is unknown” error message

Try one or more of the following:

**CHECK THE CERTIFICATES INSTALLED ON THE PRINTER**

1. From the Embedded Web Server, click **Settings** or **Configuration**.
2. Click **Security > Certificate Management > Certificate Authority Management**.
3. Make sure all certificates required for chain validation are configured correctly. See “Installing certificates manually” on page 5.

**ALLOW USERS TO LOG IN IF THE CERTIFICATE STATUS IS UNKNOWN**

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, select **Allow Unknown Status**. This allows users to log in to the printer even if the status of one or more of the required certificates is unknown.
3. Click **Apply**.
“The OCSP responder certificate, stored on the printer, does not match the one returned by the responder” error message

Try one or more of the following:

CHECK THE OCSP RESPONDER CERTIFICATE

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Online Certificate Status Protocol (OCSP) heading, make sure the correct certificate has been uploaded in the Responder Certificate field.
3. Click Apply.

CHECK THE CERTIFICATE RETURNED FROM THE OCSP RESPONDER

Make sure the OCSP responder is returning the correct certificate.

“An error occurred while trying to validate the domain controller certificate against the OCSP responder” error message

This system log error indicates that the domain controller is returning an incorrect certificate or that the OCSP responder is not checking the correct certificate. Try one or more of the following:

CHECK THE DOMAIN CONTROLLER CERTIFICATE

Make sure the domain controller is returning the correct certificate.

CHECK THE OCSP RESPONDER

Make sure the OCSP responder is checking the correct domain controller certificate.

“The user is not authorized to use this device. Make sure the user belongs to an Active Directory group that is authorized to use the device” error message

This system log error usually indicates that the user is not in an Active Directory group that is authorized to use the printer. Try one or more of the following:

ADD THE USER TO AN AUTHORIZED ACTIVE DIRECTORY GROUP

If user authorization is enabled for the printer, then add the user to an Active Directory group that is included in the authorization list for the printer.
**ADD THE USER’S GROUP TO THE AUTHORIZATION LIST FOR THE PRINTER**

Make sure the user’s Active Directory group is listed in the Group Authorization List field in the application configuration settings.

1. Access the application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, add the user’s Active Directory group to the Group Authorization List field. Separate multiple groups with a comma.
3. Click **Apply**.

**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 user’s e-mail address could not be retrieved from the Smart Card or the LDAP lookup. Try one or more of the following:

### MAKE SURE THE PRINTER E-MAIL FUNCTION IS SECURED

For Smart Card Authentication Client to retrieve user e-mail addresses, the printer e-mail function must be secured correctly. See “Securing access to the application” on page 18.

### MAKE SURE USER E-MAIL ADDRESSES ARE RETRIEVED CORRECTLY

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, from the E-mail From Address menu, do one of the following:
   - Select **Smart Card** if users log in to the printer using Smart Cards.
   - Select **LDAP Lookup** if users log in to the printer manually (using a user name and password).
3. Click **Apply**.

### CHECK THE LDAP SETTINGS

For information about resolving LDAP issues, see “LDAP issues” on page 40.

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

This error occurs when the digital signing certificate could not be retrieved from the user’s Smart Card.

### CHECK THE SIGNING CERTIFICATE ON THE USER’S SMART CARD

For users to digitally sign e-mail, the Smart Card must contain a valid digital signing certificate. Check the Smart Card to make sure it contains a signing certificate.
“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 log in using a Smart Card that contains a valid signing certificate. Users cannot digitally sign e-mail if they log in manually (using a user name and password) or if they do not have a signing certificate on their Smart Card.

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 16.

**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 18.

**CHECK THE LDAP SETTINGS**

For information about resolving LDAP issues, see “LDAP issues” on page 40.

**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 15, 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 6.
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. For Smart Card users, the e-mail address is retrieved from the Smart Card. For manual login users, the e-mail address must be placed in the login session.

MAKE SURE ALL USER INFORMATION IS PLACED IN THE LOGIN SESSION

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, select **Wait for user information**.
3 Click Apply.

Secure Held Jobs issues

“Unable to determine user id. Contact your system administrator” error message

This error indicates that Smart Card Authentication Client is not setting the user ID for the session.

MAKE SURE THE SESSION USER ID IS SET CORRECTLY

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Advanced Settings heading, configure the Session User ID setting to specify how the user ID will be obtained when a user logs in. For information about configuring this setting, see “Configuring advanced settings” on page 13.

3 Click Apply.

MAKE SURE THE APPLICATION IS SECURED

See step 9 on page 21.

“There are no jobs available for [user]” error message

Try one or more of the following:

MAKE SURE THE SESSION USER ID IS SET CORRECTLY

1 Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.

2 Under the Advanced Settings heading, configure the Session User ID setting to specify how the user ID will be obtained when a user logs in. For information about configuring this setting, see “Configuring advanced settings” on page 13.

3 Click Apply.

MAKE SURE JOBS WERE SENT TO THE CORRECT PRINTER AND HAVE NOT EXPIRED

The user may have sent the job or jobs to a different printer, or the jobs may have been automatically deleted because they were not printed in time.

Jobs print immediately

MAKE SURE THE USER SELECTS THE PRINT-AND-HOLD FEATURE

For jobs to be held at the printer, users must select the print-and-hold feature in the printer driver when printing jobs. See “Printing held jobs” on page 24.
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**.

**DISABLE REVERSE DNS LOOKUPS**

The printer uses reverse DNS lookups to verify IP addresses. If reverse DNS lookups are not used on your network, then do the following:

On printers running the Embedded Solutions Framework (eSF) version 3.0 or later:

1. From the Embedded Web Server, click **Settings > Security > Security Setup**.
2. From Step 1 under the Advanced Security Setup heading, click **Kerberos 5**.
3. Under the Kerberos Settings heading, select **Disable Reverse IP Lookups**.
4. Click **Submit**.

On printers running eSF version 2.0:

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, select **Disable Reverse DNS Lookups**.
3. Click **Apply**.

**Note:** If you are unsure about which version of eSF your printer is running, then see “Checking which version of the Embedded Solutions Framework is installed on a printer” on page 43.

**IF THE LDAP SERVER REQUIRES SSL, THEN ENABLE SSL FOR LDAP LOOKUPS**

1. Access the Smart Card Authentication Client application configuration settings from the Embedded Web Server.
2. Under the Advanced Settings heading, select **Use SSL for User Info**.
3. Click **Apply**.
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.

Licensing issues

License error

A license error can occur if there is a problem with the Smart Card Authentication application or its license. Try one or more of the following:

MAKE SURE SMART CARD AUTHENTICATION IS INSTALLED AND RUNNING

Smart Card Authentication must be installed and running to allow the other applications to run on the printer.

MAKE SURE SMART CARD AUTHENTICATION IS LICENSED

Smart Card Authentication requires 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 Smart Card Authentication has not yet expired. Check the license expiry date using the Embedded Web Server.
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 appears.

3. From the navigation menu on the left, click **Settings** or **Configuration**, and then do one of the following:
   - Click **Apps > Apps Management**.
   - Click **Device Solutions > Solutions (eSF)**.
   - Click **Embedded Solutions**.

4. From the list of installed applications, click the application you want to configure, and then click **Configure**.

Licensing Smart Card Authentication

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.

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, and then import it to apply the settings to other printers.

1. From the Embedded Web Server, click **Settings** or **Configuration**, and then do one of the following:
   - Click **Apps > Apps Management**.
   - Click **Device Solutions > Solutions (eSF)**.
• Click **Embedded Solutions**.

2 From the list of installed applications, click the name of the application you want to configure.

3 Click **Configure**, and then do one of the following:
   - To export a configuration to a file, click **Export**, and then follow the instructions on the computer screen to save the configuration file.
     
     **Note:** If a **JVM Out of Memory** error occurs, then repeat the export process until the configuration file is saved.
   - To import a configuration from a file, click **Import**, and then browse to the saved configuration file that was exported from a previously configured printer.

**Notes:**
   - Before importing the configuration file, you can choose to preview it first.
   - If a timeout occurs and a blank screen appears, then refresh the Web browser, and then click **Apply**.

## Checking the Embedded Solutions Framework version

### Checking which version of the Embedded Solutions Framework is installed on a printer

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.

3 From the Embedded Web Server, click **Reports > Device Settings**.

4 Scroll down until you see “Embedded Solutions” (usually found near the bottom).

5 In the Embedded Solutions section, note the value next to “Framework =”. This signifies the installed version.

**Note:** To view the complete list of supported printers for each version of the Embedded Web Server, see the Readme file.
Notices

Edition notice

October 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 http://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

© 2012 Lexmark International, Inc.

All rights reserved.

Trademarks

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

All other trademarks are the property of their respective owners.

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
a card reader was not detected on this device 25
accessing application configuration settings
  using the Embedded Web Server 42
adding idle screen images 9
address book
  securing 18
address book setup 15
advanced settings
  configuring 13
an error occurred while reading the card 25
application configuration settings
  accessing 42
applications
  securing 10
authentication failed 27
automatic logout 5

B
Background and Idle Screen 9
background image
  adding 9

C
cannot encrypt e-mail for one or more recipients 36
card locked out 26
card reader not detected 25
certificate not installed 30
certificate status unknown 33
certificates
  installing 5
chain validation 12
chain validation error 32
changing the home screen
  background 9
  clocks out of sync 31
confidential print jobs 20, 24
configuring a security template 8
credentials validation failed 26

date and time
  setting 6
deleting held jobs 24
digital certificates
  installing 5
digital signing
  configuring 17
disabling reverse DNS lookups 13
DNS settings
  configuring 6
documents
  scanning at the printer 23
domain controller and device clocks
  out of sync 31
domain controller certificate validation error 34
domain controller did not respond within the required time 29
domain controller issuing certificate
  not installed 30
domain controller validation 12
domains 11, 12
e-mail
  sending 15
e-mail address book 15
e-mail scan settings
  configuring 15
Embedded Solutions Framework
  checking version number 43
Embedded Web Server
  accessing application configuration settings 42
encryption
  configuring 17
  encryption certificate not found for one or more recipients 36
  encryption certificates not found 36, 37
error during chain validation 32
error while reading card 25
eSF Security Manager 9, 10
exporting a configuration
  using the Embedded Web Server 42
exporting a configuration using the Embedded Web Server 42
e-mail
  sending 22
e-mail addresses
  retrieving 18
e-mail cannot be sent because an error occurred trying to retrieve user certificates from the LDAP server 36
e-mail cannot be sent because the e-mail address could not be retrieved 35
e-mail cannot be sent because the signing certificate could not be retrieved 35
e-mail encryption
  configuring 17
e-mail function
  securing 18

H
held jobs
  deleting 24
  printing 24
  releasing 24
types 20, 24
home screen
  changing the background 9
  securing 9
home screen does not lock 27
home screen icons
  securing 10
hosts file
  installing 13

I
idle screen
  securing 9
idle screen images
  adding 9
importing a configuration
  using the Embedded Web Server 42
importing a configuration using the Embedded Web Server 42
Index 47

J
job expiration settings
configuring 20
jobs are not held at printer 39
jobs print immediately 39

K
Kerberos configuration file
installing 12
Kerberos configuration file not uploaded 27
Kerberos file not properly formatted 28
Kerberos settings
configuring 12
Kerberos setup 12
Kerberos ticket
using with Scan to Network 19
krb5.conf file
installing 12

L
LDAP lookups fail 40
license error 41
licensing Smart Card Authentication 0
locking home screen icons 10
locking the home screen 9
login screen settings
configuring 11
logout
automatic 5

M
manual login domains 11
manual login settings
configuring 11
missing Kerberos realm 30

N
Network Time Protocol settings
configuring 6
no encryption certificates could be found for any of the addresses you entered 37
no jobs available for user 39
no signing certificate is available to sign your e-mail 36
notices 44

O
NTP settings
configuring 6
OCSP certificate not configured 32
OCSP responder certificates do not match 34
OCSP responder connection error 33
OCSP responder URL not configured 32
OCSP validation 12
overview 4

P
panel login timeout
changing 5
print and hold enabling 24
print job expiration settings
configuring 20
print release options
configuring 20
printer e-mail settings
configuring 15
printer functions
securing 10
printing held jobs 24

R
realm must be in uppercase 30
realm on card not found 30
releasing held jobs 24
repeat print jobs 20, 24
reserve print jobs 20, 24
reverse DNS lookups
disabling 13
revoked certificate error 32

S
scan settings
for e-mail 15
Scan to Network
securing access to the application 19
using a Kerberos ticket for authentication 19
scanning documents at the printer 23
Secure E-mail
configuring 17
securing access to the application 18
using from the printer 22
Secure Held Jobs
configuring 20
securing access to the application 20
using from the printer 24
securing access to Scan to Network 19
securing access to Secure Held Jobs 20
securing access to the address book 18
securing applications 10
securing home screen icons 10
securing printer functions 10
securing the home screen 9
securing the idle screen 9
security certificates
installing 5
security template
configuring 8
Send me a copy is not available 38
sending e-mail 22
session user ID
configuring 13
setting up a security template 8
signing certificate could not be retrieved 35
signing certificate not available 36
signing certificate not found 36
simple Kerberos setup 12
Smart Card Authentication licensing 0
overview 4
SMTP settings
configuring 15

T
TCP/IP settings
configuring 6
the e-mail cannot be sent because encryption certificates could not be found for any recipients 37
the e-mail cannot be sent because your signing certificate could not be found 36
timeout
automatic 5
troubleshooting
a card reader was not detected on this device 25
an error occurred while reading the card 25
authentication failed 27
cannot encrypt e-mail for one or more recipients 36
certificate not installed 30
certificate status unknown 33
chain validation error 32
clocks out of sync 31
credentials validation failed 26
domain controller and device clocks out of sync 31
domain controller certificate validation error 34
domain controller did not respond within the required time 29
domain controller issuing certificate not found for one or more recipients 36
encryption certificates not found 36, 37
error during chain validation 32
e-mail cannot be sent because an error occurred trying to retrieve user certificates from the LDAP server 36
e-mail cannot be sent because the e-mail address could not be retrieved 35
e-mail cannot be sent because the signing certificate could not be retrieved 35
home screen does not lock 27
jobs are not held at printer 39
jobs print immediately 39
Kerberos configuration file not uploaded 27
Kerberos file not properly formatted 28
LDAP lookups fail 40
license error 41
missing Kerberos realm 30
no encryption certificates could be found for any of the addresses you entered 37
no jobs available for user 39
no signing certificate is available to sign your e-mail 36
OCSP certificate not configured 32
OCSP responder certificates do not match 34
OCSP responder connection error 33
OCSP responder URL not configured 32
realm must be in uppercase 30
realm on card not found 30
revoked certificate error 32
Send me a copy is not available 38
signing certificate could not be retrieved 35
signing certificate not available 36
signing certificate not found 36
the e-mail cannot be sent because encryption certificates could not be found for any recipients 37
the e-mail cannot be sent because your signing certificate could not be found 36
unable to authenticate 28, 30
unable to connect to the e-mail server 37
unable to contact the domain controller 31
unable to determine user ID 39
unable to generate certificate from card 28
unable to log in manually 26
unable to read certificate information from card 28
unable to validate certificate from domain controller 31
unexpected logout 26
unknown certificate status 33
unsupported USB device 25
user e-mail addresses retrieving 18
user is logged out too quickly 26
user is unable to log in manually 26
user not authorized to use the device 34
users cannot automatically e-mail themselves a copy 38
user's realm not found 30
verify print jobs 20, 24
Windows domain specifying 28
your card has been locked out from future login attempts 26