Secure Scan to E-mail

Administrator's Guide

June 2013 A00

www.dell.com | dell.com/support/printers

Contents

Overview

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

Additional required applications

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

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

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

For information on physically setting up the printer or using the printer features, see the printer *User's Guide*. 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.

Configuring Secure Scan to E-mail

Configuring printer settings for use with the application

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

Configuring TCP/IP settings

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

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

Configuring printer e-mail settings

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

Configuring SMTP settings

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

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

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

4 Under the Authentication heading, configure the following settings:

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

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

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

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

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

5 Click **Submit**.

Configuring e-mail server settings

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

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

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

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

4 Click **Submit**.

Configuring scan settings

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

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

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

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

4 Adjust the other scan settings if necessary.

5 Click **Submit**.

Configuring the address book

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

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

2 Click **Network/Ports** > **Address Book Setup**.

3 Configure the following settings:

- **Server Address**—Type the host name (not the IP address) of the LDAP server.
- **Server Port**—Enter the server port number that will be used for address book lookups. The most commonly used values are:
  - Non-SSL connections—Port 389 (the default setting on the printer)
  - SSL connections—Port 636
  - Non-SSL Global Catalog—Port 3268
  - SSL Global Catalog—Port 3269
- **LDAP Certificate Verification**—Select **Never**, **Allow**, **Try**, or **Demand**.
- **Use GSSAPI**—Select this check box.
- **Mail Attribute**—Type a name for the mail attribute (usually “mail”).
- **Fax Number Attribute**—Leave this set to the default value.
- **Search Base**—Type one or more values to be used when querying the LDAP directory. Separate multiple values with a comma.
- **Search Timeout**—Specify the maximum number of seconds allowed for each LDAP query.
- **Displayed Name**—Select the combination of LDAP attributes to use to find the displayed name for an e-mail address (also referred to as the “friendly” name). If you are not sure which option to select, then leave this set to the default value.
- **Max Search Results**—Specify the maximum number of search results to be returned from an LDAP query.
- **Use user credentials**—Select this check box. This ensures that the address book is protected by the credentials that are provided when you secure access to the address book function. See “Securing access to the address book” on page 8.

4 Click **Submit**.

Configuring the application settings

Configuring digital signing

1 Access the application configuration settings from the Embedded Web Server.

2 Configure the following setting:

- **Sign E-mail**—Do one of the following:
  - Select **Prompt User** to let users choose to digitally sign their e-mail.
  - Select **Disabled** to disable digital signing.
  - Select **Always Sign** to require all e-mail to be digitally signed.

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

3 Click **Apply**.

Configuring e-mail encryption

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

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

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

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

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

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

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

8. If necessary, expand the **Function Access** folder.
9. From the E-mail Function drop-down menu, select your security template.
10. Click **Submit**.
11. Access the authentication module application configuration settings from the Embedded Web Server.
12. Configure the setting that specifies where to retrieve user e-mail addresses when sending e-mail.
13. If necessary, configure the other authentication module settings.
14. Click **Apply**.

Securing access to the address book

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

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

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

Using Secure Scan to E-mail

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

Sending secure e-mail

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

1. Load the document into the printer.

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

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

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

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

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

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

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

Troubleshooting

Secure Scan to E-mail issues

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

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

Make sure the printer e-mail function is secured

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

Make sure user e-mail addresses are retrieved correctly

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

Check the LDAP settings

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

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

Check the user’s signing certificate

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

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

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

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

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

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

Try one or more of the following:

Check the address book setup

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

Make sure the address book function is secured

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

Check the LDAP settings

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

Make sure the printer is connected to the network

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

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

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

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

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

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

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

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

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

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

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

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

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

Make sure the printer is connected to a domain

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

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

Check the SMTP Server Authentication setting

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

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

Provide the server host name if the SMTP server uses Kerberos

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

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

Make sure Port 25 is not blocked

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

Make sure the printer is connected to the network

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

"Send me a copy" is not available

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

Make sure all user information is placed in the login session

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

Secure Scan to E-mail LDAP issues

LDAP lookups fail

Try one or more of the following:

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

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

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

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

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

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

Narrow the LDAP search base

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

Verify that the LDAP attributes being searched for are correct

Make sure all LDAP attributes for the user are correct.

Secure Scan to E-mail licensing issues

License error

Try one or more of the following:

Make sure the application is licensed

Applications require a license to run.

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

Make sure the license is up-to-date

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

Appendix

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 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 Dell representative.

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**.

Notices

Edition notice

June 2013

The following paragraph does not apply to any country where such provisions are inconsistent with local law: THIS PUBLICATION IS PROVIDED “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.

Trademarks

Information in this document is subject to change without notice.

Reproduction of this material in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden. Trademarks used in this text: *Dell* and the *DELL* logo are trademarks of Dell Inc.; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation. Other trademarks and trade names may be used in this document to refer to the entities claiming the marks and names of their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

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.

GNU Lesser General Public License

View the GNU Lesser General Public License online at **http://www.gnu.org/licenses/lgpl.html**.

Dell End-User License Agreement

This is a legal agreement ("Agreement") between you, the user, and Dell Products L.P, a Texas limited partnership, or Dell Global B.V. (Singapore Branch), a Singapore branch of a company incorporated in The Netherlands with limited liability, on behalf of Dell Inc. and Dell Inc.’s subsidiaries and affiliates (together "Dell"). This Agreement covers all software (and upgrades, updates and feature enhancements thereto) that is distributed by Dell and for which there is no separate license agreement between you and the manufacturer or owner of the software (collectively the "Software"). This Agreement is not for the sale of Software or any other intellectual property. All title and intellectual property rights in and to Software are owned and retained by the manufacturer or owner of the Software. All rights not expressly granted under this Agreement are reserved by the manufacturer or owner of the Software. By opening or breaking the seal on the Software packet(s), installing, downloading, activating the Software, click-accepting these terms, or using the Software, you agree to be bound by the terms of this Agreement. If you do not agree to these terms, you may not install, download, activate, or otherwise use the Software and must promptly return for a full refund all Software (including accompanying media, written materials, and packaging) or delete any Software, as directed by Dell; for software included with your purchase of hardware, you must return the entire hardware/software package. The right to a full refund does not apply to any updates or upgrades subject to the terms of this Agreement. If you are an entity, you acknowledge that the individual accepting these terms has appropriate authority to do so and to bind you.

Subject to the terms, conditions and limitations of this Agreement, Dell grants you a limited, nonexclusive, nontransferable (except as set forth herein), non-assignable license, to use the Software (in object code only) only on as many computers, devices, or in such configurations as you are expressly entitled, or one computer or device, if no other entitlement is specified, and for only such period as you are entitled, in the case of a term license, and perpetually, if no term is specified. You may use the Software only on Dell computers or devices, with the exception of mobile device application software specifically designed by Dell to be run on non-Dell hardware. "Use" means to install, store, load, execute, and display the Software. If you are a commercial customer of Dell, you hereby grant Dell, or an agent selected by Dell, the right to perform an audit of your use of the Software during normal business hours; you agree to cooperate with Dell in such audit; and you agree to provide Dell with all records reasonably related to your use of the Software. The audit will be limited to verification of your compliance with the terms of this Agreement. The Software is protected by United States and other applicable copyright laws and international treaties and may be protected under the patent laws of the applicable jurisdiction. You may make one copy of the Software solely for backup or archival purposes or transfer it to a single hard disk or storage device provided you keep the copy solely for backup or archival purposes. You shall reproduce and include copyright and other proprietary notices on and in any copies for the Software. You may not sublicense, rent, or lease the Software or copy the written materials accompanying the Software. You may transfer the Software and all accompanying materials on a permanent basis as part of a sale or transfer of the Dell product on which it was preloaded by Dell, where applicable, if you retain no copies and the recipient agrees to the terms hereof. Any such transfer must include the most recent update and all prior versions. You may not reverse engineer, decompile or disassemble, modify, or create derivative works of the Software. If the package accompanying your Dell computer or device contains optical discs or other storage media, you may use only the media appropriate for your computer or device. You may not use the optical discs or storage media on another computer, device, or network, or loan, rent, lease, or transfer them to another user except as permitted by this Agreement.

Limited Warranty and Limitation of Liability

Dell warrants that the Software media (if applicable) will be free from defects in materials and workmanship under normal use for 90 days from the date you receive them. This warranty is limited to you and is not transferable. Any implied warranties are limited to 90 days from the date you receive the Software. Some jurisdictions do not allow limits on the duration of an implied warranty, so this limitation may not apply to you. The entire liability of Dell and its suppliers, and your exclusive remedy, shall be, at Dell's option, either (a) termination of this Agreement and return of the price paid for the Software or (b) replacement of any media not meeting this warranty that is sent with a return authorization number to Dell, within the 90-day warranty period, at your cost and risk. This limited warranty is void if any media damage has resulted from accident, abuse, misapplication, or service or modification by someone other than Dell. Any replacement media is warranted for the remaining original warranty period or 30 days, whichever is longer.

Dell and its suppliers do NOT warrant that the functions of the Software will meet your requirements or that operation of the Software will be uninterrupted or error free. You assume responsibility for selecting the Software to achieve your intended results and for the use and results obtained from the Software. The terms of this Agreement do not entitle you to any maintenance or support for the Software.

DELL, ON BEHALF OF ITSELF AND ITS SUPPLIERS, DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE OR ANY WARRANTY REGARDING TITLE OR AGAINST INFRINGEMENT, FOR THE SOFTWARE AND ALL ACCOMPANYING WRITTEN MATERIALS. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS; YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

IN NO EVENT SHALL DELL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER DATA, OR OTHER PECUNIARY LOSS) ARISING OUT OF USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS DO NOT ALLOW AN EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Hosted and Internet-Accessible Software

Some or all of the Software may be remotely hosted or accessible to you through the Internet. In such case, Dell may suspend, terminate, withdraw, or discontinue all or part of the Software or your access to the Software upon receipt of a subpoena or law enforcement request, or when Dell believes, in its sole discretion, that you have breached any term of this Agreement or are involved in any fraudulent, misleading, or illegal activities. Dell may modify the Software at any time with or without prior notice to you. Dell may perform scheduled or unscheduled repairs or maintenance, or remotely patch or upgrade the Software installed on its and your computer system(s), which may temporarily degrade the quality of the Software or result in a partial or complete outage of the Software. Updates, patches or alerts may be delivered from Dell servers, which may be located outside of your country. Dell provides no assurance that you will receive advance notification of such activities or that your use of the Software will be uninterrupted or error-free.

Open Source Software

The Software may come bundled or otherwise distributed with open source software, which is subject to terms and conditions of the specific license under which the open source software is distributed.

THIS OPEN SOURCE SOFTWARE IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTY REGARDING TITLE OR AGAINST INFRINGEMENT. IN NO EVENT SHALL DELL, THE COPYRIGHT HOLDERS, OR THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS OPEN SOURCE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Under certain open source software licenses, you are entitled to obtain the corresponding source files. You may find corresponding source files for the Software at **http://opensource.dell.com** or at such other locations indicated by Dell.

Export

You are advised that the Software is subject to U.S. export laws as well as the laws of the country where it is delivered or used. You agree to abide by these laws. Under these laws, the Software may not be sold, leased, or transferred to restricted countries (currently Cuba, Iran, North Korea, Sudan, and Syria), restricted end users, or for restricted end uses. You specifically agree that the Software will not be used for activities related to weapons of mass destruction, including but not limited to activities related to the design, development, production, or use of nuclear materials, nuclear facilities, or nuclear weapons, missiles, or support of missile projects, or chemical or biological weapons.

U.S. Government Restricted Rights

The software and documentation are "commercial items" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the software and documentation with only those rights set forth herein. Contractor/manufacturer is Dell Products L.P., One Dell Way, Round Rock, Texas, 78682.

Evaluation Licenses

If you have received Software for trial or evaluation purposes (“Evaluation Software”), despite anything to the contrary in this Agreement, you may use the Evaluation Software solely for such limited evaluation period and for internal evaluation purposes only. Evaluation Software cannot be transferred save with the written authorization of the manufacturer or owner of the Software. You acknowledge that Dell may terminate your right to evaluate or use the Evaluation Software, for any or no reason, effective immediately upon notice to you. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, THE EVALUATION SOFTWARE IS PROVIDED TO YOU "AS IS" WITHOUT INDEMNITY OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. DELL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT OF SUCH SOFTWARE TO YOU.

General

This license is effective until terminated. It will terminate upon the conditions set forth above or if you fail to comply with any of its terms. Upon termination, you agree that the Software and accompanying materials, and all copies thereof, will be destroyed. Except as may be prohibited by local law, this Agreement is governed by the laws of the State of Texas, without regard to principles of conflicts of laws. Each provision of this Agreement is severable. If a provision is found to be unenforceable, this finding does not affect the enforceability of the remaining provisions of this Agreement. This Agreement is binding on successors and assigns. Dell agrees and you agree to waive, to the maximum extent permitted by law, any right to a jury trial with respect to the Software or this Agreement. Because this waiver may not be effective in some jurisdictions, this waiver may not apply to you. You acknowledge that you have read this Agreement, that you understand it, that you agree to be bound by its terms, and that this is the complete and exclusive statement of the Agreement between you and Dell regarding the Software.

Your new Dell printer comes with patented print cartridges specially priced for a single use. Use of this cartridge confirms your agreement to only a single use. After this single use, the license to use the cartridge terminates. The cartridge is designed to stop working after delivering a fixed amount of printing. Regular cartridges, without these license terms, are available for sale that may be refilled. If you do not agree to these terms, contact Dell by visiting **www.dell.com/contactdell**.

Firmware updates may modify Dell printer settings and cause counterfeit and/or unauthorized products, supplies, parts, materials (such as toners and inks), software, or interfaces to stop working. Use of genuine Dell or Dell authorized products will not be impacted.

(Type S—Rev. 040512)

EU5D-0025

Additional copyrights

This product includes software developed by:

Copyright (c) 2002 Juha Yrjola. All rights reserved.

Index