Embedded Document Accounting Solution for User Tracking

Administrator's Guide

April 2013

www.lexmark.com

Contents

Overview

The *Embedded Document Accounting Solution for User Tracking* (eDAS) is an embedded application that can be installed on *single*-*function printers* (SFPs) and *multifunction printers* (MFPs). The application communicates with a designated Pharos Blueprint Server through the *Pharos External Device Interface* (EDI) Web Service. *Simple Object Access Protocol* (SOAP) messages and *Secure Sockets Layer* (SSL) messages authenticate users to access the configuration information established on the Pharos server. This integration provides the flexibility to create and manage customized tracking models applied to frequently used printer tasks such as printing, copying, faxing, and e-mailing, resulting in a comprehensive document accounting solution.

Implementation of the Embedded Document Accounting Solution for User Tracking consists of three parts:

- Installing and configuring the application
- Obtaining and implementing the electronic licenses used to enable the application
- Configuring the Pharos Blueprint Server

This guide is intended for use by service providers and network administrators responsible for the management of this software in their network environment. A thorough knowledge and understanding of Pharos software is required for effective use of this product. As a result, this document does not include information pertaining to the installation and use of Pharos software. For information on installing and configuring Pharos software, see your Pharos documentation.

Notes:

- Print Release is the only feature available on eDAS-enabled SFPs. Copy, fax, and e-mail functionality is available only on eDAS-enabled MFPs.
- Throughout this guide, the word *device* is used interchangeably with the word *printer* to describe both MFPs and SFPs.

Configuring the application

Understanding setup requirements

Prior to setting up the application, the appropriate licensing method must be determined and the necessary electronic license files must be obtained. If a network license server will be used, then the license server should be installed and loaded with the appropriate electronic licenses before setting up the application.

After the licensing prerequisites have been completed, you can proceed with the setup process. Setting up the application involves configuring the application on the appropriate devices. You can access the Embedded Web Server for the devices where the application will be installed.

When the installation is complete, the application must be licensed (using the electronic license obtained prior to setup) and then configured by associating the application with the designated Pharos server. The application receives most of its configuration information through the Pharos EDI Web Service.

Two configuration properties are needed to establish communication channels between the device and the Pharos server:

- The URL that points to the location of the Web Service Description Language (WSDL) file of the Pharos Blueprint Server. This file specifies what SOAP messages the document accounting software can send to the Pharos server.
- The Pharos EDI password, which is required for access to the Pharos EDI Web Service.

When these properties have been properly configured and applied, the application will be able to communicate with the Pharos server.

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.

Configuring applications using the Embedded Web Server (EWS)

Installing the application

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 Click the **Apps** tab > **Install a New App**, or click the **Solutions** tab > **Install**.

5 Click **Choose File** to locate the eDAS flash file.

Note: For more information on choosing the appropriate flash file for use with your printer, see the *Readme* file.

6 Click **Start** or **Start Install**.

Configuring the application

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**.

5 Type the Pharos EDI URL and password.

The configuration page for the device provides the option to configure the release station icon that will be used on the MFP as well as the descriptive text that accompanies the icon. If you do not want to use the default release station icon, then you can browse for new icons to be used for both the pressed and unpressed states.

Notes:

- For SFPs that do not have a touch‑screen display, only the text can be changed.
- If your network requires that the device communicate with the Pharos Server through a proxy server, then you can configure the proxy settings by clicking **Configure** under the System tab of the Embedded Solutions section of the Embedded Web Server for the device.

6 Click **Apply**.

Verifying that the application has been configured correctly

You can use the Test function to verify that basic communication can be established between the device and the Blueprint 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**.

5 Make sure the Pharos EDI URL and password are correct.

If necessary, click **Apply** to save any changes to the Pharos EDI URL and password.

6 Click **Test**.

A message indicating whether the application is able to establish a connection to the Blueprint server appears in the status section on the Configure tab.

Note: The application must be running for the Test button to be available.

Running the application using the Embedded Web Server

Any time that configuration changes are made on the Pharos Server, they will take effect when the Pharos Server session refresh interval has completed. If you want to verify that changes have taken effect before the session refresh interval has completed, then you can stop and then restart the application on the devices to update the configuration.

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 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**.

4 Do one of the following:

To stop the application

- Click **Disable**.
- Select the application, and then click **Stop**.

To restart the application

- Click **Enable**.
- Select the application, and then click **Start**.

To uninstall the application

- Click **Uninstall**.
- Select the application, and then click **Uninstall**.

Configuring the Blueprint Server

The Blueprint Server controls the configuration information for the different tasks performed by the device. For each device function to which document accounting will be applied, a set of configuration steps detailed below must be carried out on the Blueprint Server.

The tasks that document accounting can be applied to are:

- Print Release

  Note: This is the only document accounting task available on SFPs.
- Copy
- Fax
- E-mail

Overview of server configuration

To configure Pharos Blueprint for use with a device, do the following steps. These steps are described in more detail in the sections that follow.

1. Install the appropriate Terminal Type for the version of eDAS you are running:
   - For MFPs running eDAS 1.3.x, install **iMFP 1.3.9**.
   - For MFPs running eDAS 2.6.x, install **iMFP 2.6.11**.
   - For MFPs running eDAS 3.0.x, install **iMFP 3.0.11**.
   - For non-eTask SFPs running eDAS 1.2.x, install **iPR 1.2.3**.
   - For eTask SFPs running eDAS 2.6.x, install **iPR 2.6.11**.
   - For eTask SFPs running eDAS 3.0.x, install **iPR 3.0.11**.
2. Add a printer.
3. Add and then configure a terminal.
4. Set up Secure Release Here.
5. Configure authentication.
6. Create Print Groups.
7. Enable device communication with the Blueprint Server.

Note: For more information on configuring devices and terminals, see your Pharos Blueprint documentation.

Step 1—Installing the iPR or iMFP Terminal Type

Most of the configuration information for the eDAS‑BP application comes from the iPR or iMFP Terminal Types, which must be installed on the Blueprint Server prior to configuring the solution. This custom terminal type allows the solution to integrate with the Blueprint server and adds iPR and iMFP as options when selecting a terminal type in Blueprint Administrator.

1 Copy the contents of the appropriate Terminal Type folder where you extracted the eDAS‑BP package to the PharosBlueprint\bin folder. (Typically C:\Program Files\PharosSystems\BluePrint\bin\)

2 From the PharosBlueprint\bin folder, run **InstallLexmarkTerminalType.bat**.

Step 2—Adding a printer

Using Blueprint with Secure Release Here, print jobs are submitted to print queues on Blueprint Collector Servers in place of actual printers, and each print job must be released before it is printed. These print queues are associated with particular printer drivers and behave like actual printers, but they function only to receive submitted print jobs for release. If using mandatory secure printing, all print queues will be secure. If using optional secure printing, specific print queues may be selected to be secure. To add a print queue for a printer, install that printer on the Blueprint Server using the Printers and Faxes Control Panel in Windows.

A device in Blueprint represents a physical printer to which print jobs can be released and is associated with one or more print queues and a terminal. When configuring a printer as a release station, the device that represents the printer component should be the main device associated with the terminal created for the printer.

1 Using the Printers and Faxes Control Panel on the Blueprint Server, add a print queue for the printer.

2 Print a test page or send a document to the printer from the Blueprint Server.

Blueprint tracks the print job and automatically adds the printer to the Blueprint database.

3 In Blueprint Administrator, click **Device Management** > **Devices**, and then select the printer you just added.

4 On the Device Details tab, select the appropriate model and the Model Confidence setting.

5 For MFP Functions, select **Print**, **Copy**, **Fax**, and **Scan**.

Note: This setting is not available in SFPs.

6 If necessary, configure the remaining device settings.

Step 3—Adding a terminal

Create a terminal for each printer where eDAS‑BP is installed and used as a release station. Select the appropriate iMFP or iPR Network Terminal Object as the terminal type.

For Blueprint to uniquely identify the printer when it is used as a terminal, the printer must pass its network name or IP address to Blueprint, and the terminal record in the Blueprint database must have the same host name or IP address as the printer.

1 In Blueprint Administrator, click **Device Management** > **Devices**.

2 Select the device record for the devices for which you want to create associated terminals.

3 Click **Create Associated Terminal**.

The Create Associated Terminal dialog appears.

4 From the Terminal Type menu, select the Network Terminal Object that corresponds to the version of eDAS you are running:

eDAS version	Blueprint Network Terminal Object
MFPs running eDAS 1.3.x	iMFP 1.3.9
MFPs running eDAS 2.6.x	iMFP 2.6.11
MFPs running eDAS 3.0.x	iMFP 3.0.11
Non-eTask SFPs running eDAS 1.2.x	iPR 1.2.3
eTask SFPs running eDAS 2.6.x	iPR 2.6.11
eTask SFPs running eDAS 3.0.x	iPR 3.0.11
* These Network Terminal Objects contain settings that are not applicable when used with the corresponding version of eDAS.	

5 Click **Apply**.

A iPR or iMFP terminal record is created and automatically associated with the device.

6 In Blueprint Administrator, click **Device Management** > **Terminals**, and then select the terminal just added.

7 On the Settings tab, make sure the host name or IP address of the printer being configured appears for the Terminal setting. This allows eDAS to get configuration information from the Pharos Server.

8 In the “For Terminal Features” section, do either of the following:

- For SFPs, select **Secure Release Here**.
- For MFPs, select **Copy Tracking** and **Secure Release Here**.

9 In the Secure Print menu, select either **Optional** or **Mandatory**.

Note: If optional secure printing is selected, then you must select the secure queues for the device associated with the terminal on the Securable Queues tab of the Devices screen. For more information on configuring Secure Release Here, see “Step 4—Configuring Secure Release Here” on page 14.

10 Configure the remaining settings, as described in the following section.

Settings for the terminal appear on two tabs. The Settings tab contains settings associated with the Blueprint system. The iPR and iMFP Configuration tabs contain settings specific to the iPR and iMFP Terminal Types.

The following sections describe the terminal settings available for SFPs and MFPs.

Configuring the iPR Terminal Type

General section

- **Administrator Contact Info**—This stores the contact information of the system administrator and shows it when the “Contact the system administrator screen” appears.
- **License Expiration Warning**—This specifies the number of days before license expiration that the application begins logging warning messages.
- **Session Ping Interval**—This specifies the interval in minutes between session pings.
- **Session Refresh Interval**—This specifies the interval in minutes that the application waits before refreshing the configuration information requested from the device Network Terminal Object on the Pharos Server.

Authentication section

- **Enable Alternate Authentication**—With the Card Alternate script in place, this prompts users to authenticate themselves using a method other than their ID cards. For more information on creating the Card Alternate script, see "Creating a manual login option for card users" on page 15.

  Note: Although this setting is available on all iPR Terminal Objects, it is used only by eDAS‑enabled SFPs that have a touch‑screen display.

- **First Authentication Token**—This is the initial authentication value the user is prompted for. Possible values include CardSwipe, Username, and PIN.
- **Second Authentication Token**—This is an additional authentication value the user is prompted for. Possible values include Password, PIN, and None.
- **Beep on CardSwipe**—This allows the device to emit an audible beep for each card swipe.
- **Card Authentication Message**—This is the message users see on the printer control panel home screen. The default message is "Please swipe your ID card." If this is left blank, then the default message appears. The field allows messages of up to 64 characters, including spaces.

Print Release section

- **Print Release Type**—This determines how print jobs are released at the SFP when users enter credentials at the device. Possible values include:
  - **Prompt for Print Jobs**—This shows a list of the user's queued print jobs on the printer control panel.
  - **Release All**—This releases all queued print jobs for a user.
  - **Release Most Recent**—This releases the most recent print job that a user sent to the device.
- **Allow User to Delete Print Jobs**—This enables the user to delete queued print jobs from the release station.
- **Display a Release Confirmation Screen**—This prompts the user to confirm the release of the selected print jobs.
- **Display a Delete Confirmation Screen**—This prompts the user to confirm the deletion of the selected print jobs.
- **Display buttons to Select or Deselect all Jobs**—This allows users to select or clear all queued print jobs with the touch of a single button.

  Note: Although this setting is available on all iPR Terminal Objects, it is used only by eDAS‑enabled SFPs that have a touch‑screen display.

Configuring the iMFP Terminal Type

Authentication section

- **Enable Alternate Authentication**—With the Card Alternate script in place, this prompts users to authenticate themselves using a method other than their ID cards. For more information on creating the Card Alternate script, see "Creating a manual login option for card users" on page 15.

  Note: If this setting is selected, then CardSwipe cannot be used as the first authentication token.

- **First Authentication Token**—This is the initial authentication value the user is prompted for. Possible values include Cardswipe, Username, and PIN number.
- **Second Authentication Token**—This is an additional authentication value the user is prompted for. Possible values include Password, PIN, and None.
- **Beep on CardSwipe**—This allows the device to emit an audible beep for each card swipe.
- **Card Authentication Message**—This is the message users see on the printer control panel home screen. The default message is "Please swipe your ID card." If this is left blank, then the default message appears. The field allows messages of up to 64 characters, including spaces.

Copy section

- **Hide Copy Icon if Copy Disabled**—This removes the copy icon from the MFP touch screen.

  Note: This setting applies only when the copy station functionality is disabled and Copy Tracking is not selected for Terminal Features on the Settings tab.

Email section

- **Enable Email Station Functionality**—This makes document accounting available for e‑mail station functionality. If this option is cleared, then normal e‑mail functionality will be available without document accounting.
- **Hide Email Icon if Email Disabled**—If e‑mail functionality is not enabled for the application on the MFP (the Enable Email Station Functionality field is cleared), then selecting this option removes the e‑mail icon from the printer touch screen.
- **Record Each Recipient Separately**—This tracks each e‑mail recipient separately.
- **Restrict/Lock From Address**—This populates the From address field in the e‑mail sent from the MFP with the user's e‑mail address as defined by the Pharos database. The MFP will query the database based on the user's login credentials. If the user's e‑mail address is missing from the Pharos database, then an error message appears on the printer control panel.

  If this option is cleared, then a missing e‑mail address in the Pharos database will not result in an error message on the printer control panel. Instead, the MFP will populate the From address field with the default From address.
- **Scan to Self only**—This queries the Pharos database to determine the user's e‑mail address, based on the user's login credentials. If the e‑mail address is missing from the Pharos database, then an error message appears on the printer control panel.

  If this option is cleared, then a missing e‑mail address will not result in an error message on the printer control panel. Instead, users can type any properly formatted e‑mail address in the To address field.

Fax section

- **Enable Fax Station Functionality**—This makes document accounting available for fax station functionality. If this option is cleared, then normal fax functionality will be available without document accounting.
- **Hide Fax Icon if Fax Disabled**—If fax functionality is not enabled for the application on the MFP (the Enable Fax Station Functionality field is cleared), then selecting this option will remove the fax icon from the printer touch screen.
- **Record each recipient separately**—This tracks each fax recipient separately.

General section

- **Administrator Contact Info**—This stores the contact information of the system administrator and shows it when the “Contact the system administrator” screen appears.
- **License Expiration Warning**—This specifies the number of days before license expiration that the application begins logging warning messages.
- **Session Ping Interval**—This specifies the interval in minutes between session pings.
- **Session Refresh Interval**—This specifies the interval in minutes that the application waits before refreshing the configuration information requested from the device Network Terminal Object on the Pharos Server.

Print Release section

- **Print Release Type**—This determines how print jobs are released at the MFP when users enter credentials at the device. Possible values include:
  - **Prompt for Print Jobs**—This displays a list of the user's queued print jobs on the printer control panel.
  - **Release All**—This releases all queued print jobs for a user.

  - **Release Most Recent**—This releases the most recent print job that a user sent to the device.
- **Allow user to Delete Queued Print Jobs**—This determines whether the user is allowed to delete queued print jobs from the release station.
- **Display a Release Confirmation screen**—This prompts the user to confirm the release of the selected print jobs.
- **Display a Delete Confirmation screen**—This prompts the user to confirm the deletion of the selected print jobs.
- **Display buttons to Select or Deselect all Jobs**—This allows users to select or clear all queued print jobs with the touch of a single button.

Step 4—Configuring Secure Release Here

Secure Release Here allows users to release print jobs to printers securely and conveniently. When using Secure Release Here, a print job is sent to a print queue where it will remain until it is released to a printer from a designated release station. Configuring a device for Secure Release Here establishes the device as a release station from which the delivery of print jobs can be controlled, allowing each print job to be tracked appropriately.

After a print job has been submitted and the user has released it at the device, Blueprint executes the action and records the result.

The records on the Devices screen represent the physical printers to which jobs are released. The print queues that have been detected on the Blueprint Collector Servers for a device appear on the Securable Queues tab of that device and on the Secureable Queues screen of Blueprint Administrator. Some of those queues may not be used with Secure Release Here.

If secure printing to a device is mandatory, all queues relating to the device will hold jobs for release. If secure printing is optional, users can print jobs directly to the device, or they can print and release them securely. Allowing optional secure printing means that security can be applied on a per-job basis. Sensitive jobs can be printed securely, while normal print jobs are sent directly to the device without being held up.

If mandatory secure printing is selected for a device, configuration is complete. All queues associated with the device are secured, and any new queues that are associated with the device are automatically secured.

To configure optional secure printing, make sure each device offering optional secure printing has two or more queues. On the Devices screen, select the device to configure for optional secure printing, and click the **Secured Queues** tab. Select the queue or queues to secure in the Secure column. When at least one secure queue and at least one non-secure queue are provided, users can choose whether to use Secure Release Here for each job by selecting the appropriate queue.

1. From Blueprint Administrator, select **Device Management** > **Terminals**.
2. From the Settings tab, select **Secure Release Here** in the Terminal Features field.
3. Select **Mandatory** or **Optional** in the Secure Print field.
4. Click **Apply**.

Step 5—Configuring authentication

Users interact with a Secure Release Here system by logging in to terminals (iPRs or iMFPs) to release print jobs. Users must also log on to a terminal when copying, e-mailing, or faxing documents from MFPs if these activities are tracked by Blueprint.

The authentication method is determined by the authentication script used by the terminal, as well as the values of the “Card Alternate,” “First Authentication Token,” and “Second Authentication Token” properties on the Network Terminal Object. The script determines the identification information required, the source of authentication, such as the Blueprint database, a network domain, or an online authentication system, and the identifier to associate with the print job.

A variety of sample scripts that demonstrate several common authentication scenarios are included on the Blueprint Enterprise CD. Additionally, the eDAS‑BP package contains a sample script for setting up a manual login option for card users (CardAlternateScript.txt). Contact Pharos Systems for assistance in developing new scripts.

Authentication scripts are managed and associated with terminals on the Authentication Scripts screen in the Device Management section of Blueprint Administrator.

Step 6—Creating print groups

An optional feature of Secure Release Here is the ability to define Print Groups, which are groupings of devices with compatible drivers. A job submitted to one device in a Print Group can be released to any other device in the group using any terminal connected to any device in the group. This allows greater flexibility for mobile users, as well as providing backup printers when one printer is offline.

From the Print Groups screen in the Secure Release Here section of Blueprint Administrator, you can configure existing groups, create new groups, and add devices to them.

A virtual queue may also be created to provide a universal queue for users to submit jobs to a Print Group. For more information about virtual queues, see the Pharos Blueprint documentation.

Note: All devices in a group must all have compatible drivers. Blueprint does not check for compatible drivers; you must ensure that any device you add is compatible with the other devices in the group.

Step 7—Enabling device communication with the Blueprint Server

After configuring the Blueprint Server, the solution must be configured to communicate with the server. For more information about configuring eDAS‑BP to communicate with the Blueprint Server, see “Configuring the application” on page 5.

Creating a manual login option for card users

Setting up a manual login option for MFPs allows users who have forgotten their cards to retrieve print jobs by logging in manually.

1. In Blueprint Administrator, create a new script named `Card Alternate` using the sample script included in the Document Accounting Solution for User Tracking package (*CardAlternateScript.txt*).

   Note: For more information on creating scripts in Blueprint, see your Pharos Help documentation.

2. In Blueprint Administrator, click **Device Management** > **Terminals**.
3. Select the appropriate iMFP terminal from the list.
4. In the Script field on the **Settings** tab, type `Card Alternate`, and then click **Apply**.
5. Click the **Lexmark iMFP Configuration** tab, and then expand the **Authentication** section.

6. Select **Enable Alternate Authentication**.
7. Set the "First Authentication Token" and "Second Authentication Token" fields to the appropriate values. These values determine which alternate authentication methods will be accepted at the device.
8. Restart eDAS-BP.

Note: When the Card Alternate script is in place, you will also need to set up an authentication script on the Blueprint Server that can appropriately handle the two different types of authentication.

Creating a copy policy

Before allowing users to make color copies, you can show either an information message or a warning message. You can also completely restrict users from making color copies.

1. In Blueprint Administrator, click **Policy Print** > **Policies** > **Add Policy**.
2. In the Policy Name field, type the name of the new policy, and then click **Apply**.
3. Select the policy name that you just created, and then from the Rules tab, click **Create**.
4. From the Edit menu, select **Create New**.
5. In the Trigger field, type the name of the trigger.
6. From the Functions section, select **Copy**.
7. From the Conditions column, select **Function**, and then click ➔.
8. From "The user is attempting to" menu, select **copy a document**, and then click **OK**.
9. From the Conditions column, select **Document Contains Color**, and then click ➔ > **OK**.
10. From the "Apply the following action" menu, select an action.
11. In the "And display the following prompt” field, type a message for the user, and then click **OK**.
12. Click the **Groups** tab > **Add** > **Search**.
13. From the Groups column, select the group for which the policy will apply, and then click **OK** > **Apply**.

    Note: You may select all the groups.

Using device features with document accounting enabled

After the application has been installed, the behavior of the device features (Copy, Fax, E-mail, and Print Release) will be altered slightly to accommodate the use of document accounting. As a result, the following instructions have been included as an addition to the existing device documentation to aid administrators in instructing users to perform each task.

Using the Print Release feature

Printing documents on SFPs that do not have touch-screen displays

At any point during an eDAS-BP transaction on an SFP, users will be unable to use the ↺ button to return to a previous screen. Instead, users must press and hold ↺ for three seconds to cancel the transaction and return to the main menu.

Notes:

- These instructions assume that “Prompt for Print Jobs” is set as the Print Release Type in Blueprint Administrator.
- If “Release All” or “Release Most Recent” are set as the Print Release Type in Blueprint Administrator, then the SFP will release print jobs accordingly following successful user authentication.

1. Submit a print job.
2. From the printer control panel, press the down arrow button until `Print Release` appears, and then press ✓.
3. Enter the appropriate user authentication credentials (User ID, password, cardswipe, PIN).
4. Select `Print Documents`, and then press ✓.
5. Use the arrow buttons to scroll through the list of documents. Press ✓ to select documents.
6. After you select the print job(s) you want to release, press the down arrow button until `Done` appears, and then press ✓ to release the job(s).

   Note: Release information is determined by the configuration of the Blueprint Server.

7. If there are more print jobs available for release, select `Yes` and then press ✓ to release more jobs, or select `No` to exit.

Deleting documents on SFPs that do not have touch-screen displays

Note: Users can delete print jobs only if “Prompt for Print Jobs” is set as the Print Release Type in Blueprint Administrator.

1. From the printer control panel, press the arrow buttons until `Print Release` appears, and then press ✓.
2. Enter the appropriate user authentication credentials (User ID, password, cardswipe, PIN).

3 Select `Delete Documents`, and then press ✓.

4 Use the arrow buttons to scroll through the list of documents. Press ✓ to select documents.

5 After you select the print job(s) you want to delete, press the down arrow button until `Done` appears, and then press ✓ to delete the job(s).

6 If `Confirm Delete?` appears, press ✓.

7 If there are more print jobs available for deletion, select `Yes` and press ✓ to delete more jobs. Select `No` and press ✓ to exit.

Printing documents on MFPs, and SFPs with touch‑screen displays

Note: If "Release All" or "Release Most Recent" are selected as a Print Release option in Blueprint Administrator, then the device will release print jobs appropriately following successful user authentication.

1 Submit a print job.

2 At the device, press the **Release Station** icon.

3 Enter the appropriate user authentication credentials (User ID, password, cardswipe, PIN).

4 Select whether to continue with the current print job or to delete it.

5 Select the print job(s) you want to release.

6 Press **Print** to release the job(s).

7 If prompted, press **Yes** to confirm the action. Press **No** to close the session.

> **Note:** Release information is determined by the configuration of the Blueprint Server. See your system support person for more information.

8 The display screen indicates which printer the job has been released to. If there are more print jobs available for release, press **Yes** to release more jobs, or press **No** to exit.

Deleting documents on MFPs, and SFPs with touch‑screen displays

Note: Users can delete print jobs only if "Prompt for Print Jobs" is set as the Print Release Type in Blueprint Administrator.

1 At the MFP, press the **Release Station** icon.

2 Enter the appropriate user authentication credentials (User ID, password, cardswipe, PIN).

3 Select the print job(s) you want to delete.

4 Press **Delete** to delete the job(s).

5 If prompted, press **Yes** to confirm the action. Press **No** to close the session.

6 If there are more print jobs available for deletion, press **Yes** to delete more jobs. Press **No** to exit.

Using the copy feature

Note: Depending on the configuration of the copy policy, you may see either an information message or a warning message on the printer display. You may also be restricted from making a color copy. For information about the configuration of the copy policy, contact your system support person.

1 Load the document into the *automatic document feeder* (ADF) or on the scanner glass, and then press the **Copy** icon.

2 Enter the appropriate user authentication credentials (user ID, password, card swipe, PIN).

3 Select the appropriate copy settings. For more information on the copy settings, see your printer *User's Guide*.

4 Touch **Copy It**.

A confirmation screen indicates whether the document was copied successfully.

5 If you have more documents to copy, then touch **Yes**, load the documents, and repeat steps step 3 through step 5. If you do not have more documents to copy, then touch **No** to complete the task.

Scanning to e-mail

1 Load the document into the ADF or onto the scanner glass, and then press the **Email** icon.

2 Enter the appropriate user authentication credentials (User ID, password, card swipe, PIN).

3 Enter the e-mail address the document will be sent to.

4 Press **Email It**.

5 A confirmation screen indicates whether the document was e-mailed successfully. If you have more documents to scan, press **Yes**, load the documents, and repeat steps 3 through 5. If you do not have more documents to scan, press **No** to finish the operation.

Scanning to fax

1 Load the document into the ADF or onto the scanner glass, and then press the **Fax** icon.

2 Enter the appropriate user authentication credentials (User ID, password, card swipe, PIN).

3 Enter the fax number(s) the document will be sent to. Adjust the fax options as necessary.

4 Press **Fax It**.

5 A confirmation screen indicates whether the document was faxed successfully. If you have more documents to fax, press **Yes**, load the documents, and repeat steps 3 through 5. If you do not have more documents to fax, press **No** to finish the operation.

Troubleshooting

eDAS Troubleshooting

The application cannot be accessed

This error message typically indicates that the application is having difficulty communicating with the Pharos Server. Try one or more of the following:

Make sure the application is properly licensed

To verify that the application is properly licensed:

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. Make sure the license status of the application is `Licensed`.

Make sure the application is configured correctly

The two configuration properties that establish communication between the Pharos Server and the application are:

- The URL that points to the Pharos Server WSDL file
- The Pharos EDI password

Make sure the Pharos Server is configured correctly

Check that the Pharos Server is turned on and ready to receive SOAP messages from the application.

You can also use the Test button to verify that basic communication can be established between the device and the Blueprint 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**.

5 Make sure the Pharos EDI URL and password are correct.

6 Click **Test**.

A message indicating whether the application is able to establish a connection to the Blueprint server appears in the status section on the Configure tab.

Check the system log

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 Click the **System** tab > **Log**.

5 From the Filter menu, select an application status.

6 From the application menu, select an application, and then click **Submit**.

Contact your solutions provider

If you still cannot isolate the problem, then contact your solutions provider for additional help.

An application error has occurred

Try one or more of the following:

Check the system log

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 Click the **System** tab > **Log**.

5 From the Filter menu, select an application status.

6 From the application menu, select an application, and then click **Submit**.

Make sure each of the Pharos objects that have been created for use with the device is configured correctly

Contact your solutions provider

If you still cannot isolate the problem, then contact your solutions provider for additional help.

Configuration changes on the Pharos Server are not showing up on the device

Changes made to the application configuration on the Pharos Server may not be immediately available on the host device. The rate at which configuration is updated is controlled by the Session Refresh Interval set in the device's Network Terminal object. The Session Refresh Interval is one of the advanced properties for the Network Terminal object and is accessible under the General tab by clicking the **More Properties** button.

If you do not want to change the Session Refresh Interval, stopping and then starting the application on the device will automatically refresh configuration changes. For information on stopping and starting the application, see "Configuring the application" on page 5.

If a network is set up to use an Analyst server and multiple Collector servers, the settings on the Analyst server must be manually refreshed on the Collector servers. This ensures that the Collector servers use only new data, rather than data that has been cached from the Analyst server to the Collector server. The new data can include such items as iMFP or iPR settings, and authentication credentials, among other things.

To manually refresh settings on the Collector servers:

1. Open Blueprint Administrator on the Analyst server.
2. From the Blueprint Administrator, click **Servers** > **Servers**.
3. Select the appropriate Collector servers from the list.
4. Click **Clear Replicated Data** on the toolbar near the top of the screen.

Notices

Edition notice

April 2013

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

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

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

For Lexmark technical support, visit **http://support.lexmark.com**.

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

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Trademarks

Lexmark and 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.

Index