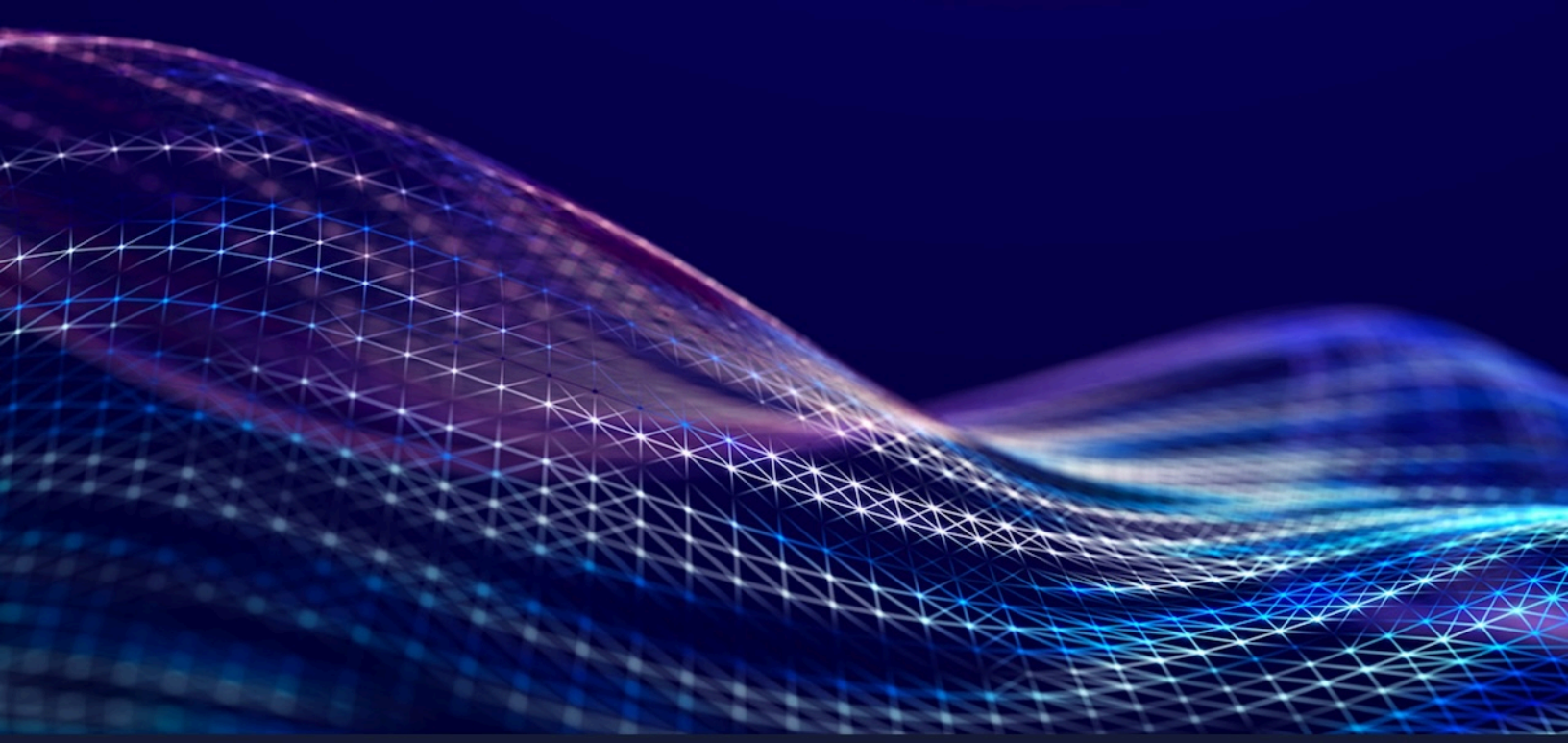

Tungsten Copitrak
Configuration Guide

Version: 3.5.0

Date: 2024-09-12

TUNGSTEN AUTOMATION

Table of Contents

Preface

This guide provides instructions for administrators who are responsible for configuring the Tungsten Copitrak.

System requirements

System requirements are listed in the *Technical Specifications* document, which is available from the Tungsten Copitrak Product Documentation site. The document is updated regularly, and we recommend that you review it carefully before installing your product.

Related documentation

Product documentation for Tungsten Copitrak 3.5.0 is available here:

https://docshield.tungstenautomation.com/Portal/Products/Copitrak/3.5.0-9iemtxkeno/Copitrak.htm

Getting help with Tungsten Automation products

The Tungsten Automation Knowledge Portal repository contains articles that are updated on a regular basis to keep you informed about Tungsten Automation products. We encourage you to use the Knowledge Portal to obtain answers to your product questions.

To access the Tungsten Automation Knowledge Portal, go to https://knowledge.tungstenautomation.com/.

The Tungsten Automation Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Tungsten Automation Knowledge Portal provides:

- Powerful search capabilities to help you quickly locate the information you need.
  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
  To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Tungsten Automation Community (for all customers).
  On the Resources menu, click the **Community** link.
- Access the Tungsten Automation Customer Portal (for eligible customers).
  Go to the Support Portal Information page and click **Log in to the Customer Portal**.
- Access the Tungsten Automation Partner Portal (for eligible partners).
  Go to the Support Portal Information page and click **Log in to the Partner Portal**.
- Access Tungsten Automation support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
  Go to the Support Details page and select the appropriate article.

Chapter 1

PRM configuration files

Before configuring Tungsten Copitrak, you must replace the two PRM configuration files by doing the following:

1. Download the TERMINAL_SETUP.INI.PRM and LT2005_SETTINGS.INI.PRM files from the Tungsten Automation Fulfillment site.
2. Copy TERMINAL_SETUP.INI.PRM to the following location, and overwrite the existing file:
   `C:\ERS\SERVER`
3. Copy LT2005_SETTINGS.INI.PRM to the following location, and overwrite the existing file:
   `C:\ERS\CopitrakDesktop`

- A restart is not required.
- If you have already updated any print tracking or terminal configurations, these changes will have no effect, and further configurations on Copitrak Desktop must be performed.
  For more details, see the *Tungsten Copitrak Desktop Installation and Configuration Guide*.

Chapter 2

Import users and associated attributes

You can import the list of users and associated attributes from the following sources:

- Active Directory (AD)
- Flat File Import
- Microsoft SQL Server

This guide uses AD and user lists as examples.

Import users

1. Open the Copitrak folder on your local computer and select **CSS Manager**.
2. Log in by entering **ers**.
3. Under **System Configuration**, navigate to **Lists** > **Validation lists**.
4. Select **Import** and click **Add** on the top menu bar.
   The **Import Wizard** appears.
5. For an initial import of users, select **Complete List** from the **Import Type** list.
6. Under **Destination table**, select **Users**, and then click **Next**.
7. Select **LDAP** as the source type, and then click **Next**.
8. From the **Setup LDAP parameters** window, in the **Specify server and database** field, enter the base search Distinguished Name (DN) by typing **LDAP://** followed by the location in the LDAP/AD folder where Copitrak should begin its import.
   The following example specifies the topmost folder but an OU can be included. This example is also server-less, which is recommended. You can find this example in the C:\ERS\winers.ini file, by searching for **ldaproot.LDAP://DC=LAW,DC=LOCAL**.
9. In the **Specify query** field, enter the LDAP search filter that determines which accounts are imported.
   This field accepts standard LDAP query expressions.
   Here is an example:
   `(&(objectCategory=person)(sn=*)(sAMAccountName=*)(pager=*))`
   The field cannot be left blank. At a minimum, enter `(objectCategory=person)` or `(sAMAccountName=*)`.
10. Select **Use a specific user name**, and enter the credentials of the Copitrak service account. Click **Next** to continue.
11. Select the LDAP/AD user attributes to import. Expand the different categories and select the check boxes that match the required values.

While the minimum two attributes to map are **cn** (full name) and **PIN** (Copitrak user login), the following attributes are also suggested:

- User full name = cn
- User email address = mail
- User ID = sAMAccountName
- User PIN = (custom attribute determined by customer)

12. Click **Preview** to view the result of the import with the selected parameters.
    Click **Back** to adjust the settings or click **Next** to continue.
13. Map the fields in Copitrak to the values being imported.
14. In the **Formulas and associations** window, assign each user's PIN to the login for Copitrak.
    a. Select the **user_id** field name on the left, and then select the LDAP/AD attribute holding the PIN from the **Field** list.
    b. Click **Add** to complete the mapping.
    If the **user_id** field name is now expanded, the mapping is visible underneath.
15. Select **group_id**.
    A least one user group should be specified, even if a distinction is not required by the user. Complete one of the following steps:
    - Map the user group to one of the specified LDAP attributes using the **Field list**, and then click **Add**.
    - Select the **Constant** radio button on the right, and enter the group name. Click **Add**.
16. Map the **username** attribute to the **CN** field.
17. Map the **department** attribute to the same values as the user_id item.

    A user will be able to log in to the system using the value presented in the department field, so the value must be unique to each user.

18. The **termname** attribute is a legacy attribute and the value entered is not used.
    Complete one of the following steps:
    - Enter a constant value equal to the company's initials (such as "LH" value).
    - Use the same field as mapped to **user_id**.
19. Set the **isuser** attribute to **True**.
    This is a constant value and should not be changed.
20. Set the **islawyer** attribute to **True** unless otherwise specified.
21. Click **Next**.
22. Enter the name for the parameter set.
    For example: "User."
23. Click **Finish** to save the user import parameters.
    The Users Import configuration is added to the Import list.
24. Test the import configuration by doing the following:
    a. Open a Command Prompt window as an administrator.
    b. Go to `C:\ERS\ers.net\win\apps\importer`.
    Change the drive letter if the ERS folder is installed in a different location.

c. Enter the following command:

```
importer.exe c:\ers\ers.net\data\imports\users.dtsx /Debug
```

25. Once the window is closed, return to the **Configuration Manager** window, expand **User**, and then click **Master**.
    The imported users should be displayed.

User profiles

As mentioned in the previous section, a user import might only contain a user name and user ID. It provides a base for other information. The user profiles, by contrast, contain information used elsewhere in Copitrak to determine the behavior of interactions with end users (such as what prompts a user might see at a terminal).

These profile memberships are visible in each user account, where they can be added on a case-by-case basis. However, updating these profiles as part of a batch file is quicker.

Note that when defining imports for this purpose, the profile names are entered manually. As a result, ensure that what is entered matches the pre-determined profile names within Copitrak.

The list of profile names can also be edited from C:\ ERS\ers.net\Data\UserProfiles.xml. If a change is made, test it by opening the .XML file in a Web browser. If an error appears, the problem must be fixed.

The following sections include instructions on creating the import definitions required for a basic installation, followed by the import steps for the previously created import definitions. If other profile information is required, such as badge ID numbers, additional import definitions must be created using the principles behind these specific examples.

Create and import user profile - User ID

To create and import a user profile for identification, do the following:

1. Launch the CSS Manager.
2. Under **System Configuration**, navigate to **Lists** > **Validation lists**.
3. Select **Import**, and click **New Import**.
4. In the **Import Wizard** window, select **User Profile** from the **Destination Table** list and click **Next**.
5. Select **LDAP** as the import source, and click **Next**.
6. Enter the same LDAP parameters as you did in steps 8 to 10 in Import users.
7. In the **Specify fields to include** window, expand **AccountProperties** and select **sAMAccountName**.
8. Select the AD attribute containing user PINs.
9. Click **Preview** to verify that the correct AD attributes are selected. Click **Back** to adjust the settings or click **Next** to continue.
10. In the **Formulas and associations** window, select the **profiletype** item, change the radio button to **Constant**, and then enter a profile name.

If multiple profile groups are required, the import process needs to be repeated for each group of users that require a different profile (and the LDAP query filter is customized each time to pick out each group of users).

11. Click **Add** to complete the entry.
    If a specific group name is not specified ahead of time, it is recommended that the value "NetworkId2" be used as this will simplify subsequent configuration steps.
12. Select the **user_id** item, and then select the AD attribute holding the user PINs. Click **Add** to continue.
13. Select **alternate_id**, and then select the **sAMAccountName** item from the Formula list. Click **Add** to continue.
14. Click **Next**.
15. In the **Import Name** field, enter the name of the import configuration.
16. Click **Finish**.
    The **Import** screen appears with the new import configuration added.

Create and import user profile - Email

1. Repeat steps 7 to 10 in Create and import user profile - User ID.
2. In the **Specify fields to include** window, expand **GeneralProperties** and select **mail**.
3. Select the AD attribute containing the user PINs.
4. Click **Preview** to verify that the correct AD attributes have been selected. Click **Back** to adjust the settings or click **Next** to continue.
5. In the **Formulas and associations** window, select the **profiletype** item. Change the radio button to **Constant** and then enter **E-Mail**. Click **Add** to continue.
6. Select **user_id** on the left followed by the **Formula** radio button on the right. Select the AD attribute name holding the user PIN values. Click **Add** to continue.
7. Select the remaining **alternate_id** item and select **Mail** from the **Fields** list. Click **Add** to continue.
8. Click **Next** to proceed to the next screen, and enter a name for this import configuration.
9. Click **Finish**.
   All the three import configurations are now visible in the CSS Manager.

Import user profiles

1. Go to the `C:\ERS\Validation` folder.
2. Locate the Users.bat file and open it in a text editor.
3. Find any lines that are commented out ("::" at the start of the line) and remove the colons so that all lines are active.
4. Save the changed file and execute it.
   A Command Prompt window appears and then closes automatically when the import process is finished.
5. After the user profiles are imported, return to the Configuration Manager.
6. Under **System Configuration**, navigate to **Lists** > **Validation Lists** > **User**.

7. Select **Master** and select a user.

   The COPITRAK account with the PIN 999999 is created by one of the sqlcm instructions and is commonly used for testing.

8. In the **Edit User** dialog box, from the **Profiles** list, select **E-Mail**.
   The user's email address appears in the field below.
9. Click **Close**.

Common settings

The concept of common settings was introduced in version 3.3.0 to reduce the duplication of configuration parameters and to simplify the process of editing .config files for various components by keeping them in one location. Almost all components need settings such as logging configuration, and they all use the same parameters for those settings but prior to this change, each component had its own .config file.

Common application settings are stored in the following file:

C:\ProgramData\Kofax\Copitrak\Config\CommonSettings.config

Applications that were updated to use common settings:

- SMTP
- Mail Service
- DMS scan connectors (iManage, NetDocs, DM5)
- OneDrive Connector
- SharePoint Connector
- License Manager

These applications read logging settings from CommonSettings.config and do not have those settings in their own .config files, which are located in their respective folders. To configure logging details such as file name, location and level, you only need to edit one file (CommonSettings.config) for all the applications using that file. In addition, the C:\ProgramData\Kofax\Copitrak\Config folder contains further .config files to configure other settings.

To change logging configuration for only one application, copy the logging configuration section from CommonSettings.config into the .config file specific to that application. You can also customize any other parameter from CommonSettings.config this way.

Chapter 3

Client-Matter

The configuration of Client-Matter import depends on the source of the material and the complexity of the requirements.

The source is typically a flat file or a direct query of a database such as Juris. The latter likely requires Tier 2 involvement and falls outside the scope of this guide. The former might need to be prepared for import. While you can complete simple changes, such as removing space or using the Copitrak import, it is best to ensure that the file is fully prepared for importing beforehand.

For the purposes of this guide, Client-Matter falls into two categories: simple and complex. End clients with simple client-matter requirements typically do not have separate client and matter codes, so you need to import only one set of values. Otherwise, separate client and matter codes will need to be imported and combined using the features of the import wizard. The example included in this guide covers the combination of values to produce a single code displayed at the terminal and for billing.

1. Export the client-matter list to a CSV file and save it to the `C:\ERS\Validation` folder. Open the file. Delete the header line if it exists and save the file.
2. Launch CSS Manager, and then navigate to **System Configuration** > **Lists** > **Validation Lists** > **Import**. Click **New Import**.
3. In the **Import Wizard** window, select **Accounts** from the **Destination Table** list and click **Next**.
4. Select **FlatFile** as the import source. Click **Next**.
5. On the **Select the file to import** screen, click the ellipsis next to **Select Source File** to browse for the Client-Matter file.
6. Select the source file and click **Select**.
   As a best practice, store source files in the `C:\ERS\Validation` folder.
7. Customize the parsing parameters and click **Preview** to verify the result.
8. After confirming the result, click **Next**.
9. In the **Formulas and associations** window, select **AccountToValidate**.
   Make sure that the **Fields** list choice corresponds to the first value and click **Add**.
10. Expand the **AccountToValidate** item and select the line that appears.
    This line will be added to the subsequent strings specified.
11. Select **Concat** from the **Functions** list, and enter a dash ("-") in the **String to concatenate** field. Click **Update** to add this character to the value being built.
12. With the **AccountToValidate** item still selected, select **STEP 1** from the **Fields** list.
    This informs the system that what comes next should be added to everything specified in the STEP 1 line displayed on the left.
    Keep **Concat** selected in the **Functions** list and select the **Source Field** radio button.

In the **String to concatenate** list, select **Field 1**. Click on the **Final results step** check box to indicate this is the last operation. Click **Add**.

13. Repeat the previous three steps for **AccountToBill**.
    The **AccountToValidate** and **AccountToBill** items include the same data.
14. Select **group_id** and enter **Billable** as a **Constant** field value. Click **Add**.
15. Select the **client** item. Click the **Formula** radio button and select **Field 2** from the list. Click **Add**.
16. Select the **matter** client and select **Field 3** from the **Fields** list on the right. Click **Add**.
17. Review the result and click **Next** to continue.
18. Assign this import configuration the name "Accounts" and click **Finish**.
19. Open the `C:\ERS\Validation` folder and open the Accounts.bat file.
20. Verify that the importer.exe line has the correct file name (matching the name that was used to save the client-matter import configuration). Close the file and execute the Accounts.bat file. The Command Prompt window will close automatically once the import task completes.
21. Once finished, return to the CSS Manager. Navigate to **Lists** > **Validation Lists** > **Account** > **Master**, you will see the client-matter table appears on the right.

Chapter 4

Eclipse terminal configuration

This chapter covers basic Eclipse terminal configuration and the creation of the three common scan routes: scan-to-folder, copies (with a scan-to-folder option), and scan-to-mail.

Before starting, make sure the Eclipse terminal simulator is configured.

Create terminal groups

1. Open **Configuration Manager**.
2. Log in by entering **ers**.
3. In the main **Configuration Manager** screen, the **Terminal/User Options** button should be available.
   If not, click **Edit**, and then click **Main Menu** at the bottom of the screen that appears. The **Terminal/User Options** button should be now active.
4. Click **Terminal/User Options**.
5. In the **ERS Configuration File Manager** window, select **TERMINAL_GROUP_XX** from the **Enter Key Name** list.
6. Edit **TERMINAL_GROUP_XX** to replace **XX** with the custom name of the terminal group such as **DEFAULT**. Click **Copy Default Group**.

   Use short but descriptive text to easily identify and differentiate one terminal group from another. For example, DA_CLRCOPY or AU_CFXCLR.

7. Repeat the same procedure for users and language groups. Select **USER_GROUP_XX**.
8. Edit **USER_GROUP_XX** to replace **XX** with the User Group Name that was previously assigned to users, such as **REGULAR**. Click **Copy Default Group**.
9. Select **LANGUAGE_GROUP_XX** and replace **XX** with **English**. Click **Copy Default Group**.
10. The following groups are created, but not yet configured:
    - LANGUAGE_GROUP_English
    - TERMINAL_GROUPS
    - TERMINAL_GROUPS_DEFAULT
    - USER_GROUP_REGULAR
11. Select **LANGUAGE_GROUP_English** and click **Set All Missing Entries to Default Values**.
    If the item is now expanded, the default values are displayed.
12. Repeat step 11 for **TERMINAL_GROUP_DEFAULT** and **USER_GROUP_REGULAR**.
    Some settings might not have an associated value. This is normal.

13. In the **Configuration Manager** window, click **Validation Services**.
14. Click **Unit Mappings**.
15. Under the **Eclipse Terminal Group** section, in the **Unit Mask** field, enter a wild card asterisk (*) to cover all terminal units, and in the **Terminal Group** field, enter **DEFAULT**. Click **Add** to create the terminal group.

    This example assumes a single group of terminals with the name "DEFAULT". If multiple terminal groups are required due to different groups of settings, then add those groups here. As a best practice, create as few terminal groups as required, as managing multiple groups can be complex.

16. Click **Save & Back**.
17. In the **Validation Services Options** dialog box, click **Save & Back** again.

Configure the terminal button functions

As part of configuring the terminal button functions, a number must be assigned to each function. This number is used in other configuration areas to refer to the function itself. The **Default Value** button has pre-assigned values to each function, some of which need to be changed. This guide covers the configuration of the following terminal functions/buttons:

- Make Copies (with a Scan-to-network "backup" function in case a user performs a scan after having selected this function)
- Scan-to-email
- Scan-to-network

Note that the number assigned for an active function should start at "1" and increase by one for each subsequent function. "0" is used to indicate an inactive function.

1. With the **TERMINAL_GROUP_DEFAULT** item expanded, scroll down to the **ModeCopy** item and select it.

   This function refers to the dedicated copy function at an MFP. It is typically used only by the operators of a dedicated copy/print room. For general copying at office MFPs, it is highly recommended that users copy using a scan route, to avoid tracking problems when users perform a scan after selecting the copy function. Make sure that a “0” value is displayed on the right. If you changed the value to 0, click **Set In This Group**.

   If a dedicated copy function as discussed is desired, it should be set up in its own Terminal Group. Its value should be set to "1" and all other scan functions should be set to "0".

2. Verify the **ModeDocuret** item value by doing one of the following:
   - If the MyVault printing feature is required, set the **ModeDocuret** value appropriately.
   - If the MyVault printing feature is required, set the **ModeDocuret** value to "0".
3. Continue scrolling and select the **ModeScan** item. Change the value on the right to "1" if necessary.

Determine terminal button functions and order

Set the order in which the buttons appear on the terminal screen and set preferences for their function and appearance. This example uses the following order:

- Copies
- Scan-to-email
- Scan-to-folder

You can change the order as needed.

1. Scroll down and click the **PreMode0** item.

   This item represents the settings for the first button. (PreMode1 is button 2, and so on.) Change the displayed **0** (meaning no value/blank) to **1**, meaning that the first button is assigned to ModeScan, which was set in Configure the terminal button functions.
2. Enter **COPIES%%Make Copies** in the text field below the **1**. Click **Set In This Group** to save the change.

   Make Copies is displayed as the button text at the terminal. The word COPIES is used by Copitrak as an internal identifier. It will be used again when setting the parameters for the function. This text identifier can be anything that uniquely identifies and links the items.
3. Click **PreMode1** and enter the number **1** again (since the mode still being invoked is the scan mode).
4. In the text field, enter **EMAIL%%Scan and email** and click **Set In This Group**.

   The "EMAIL" text should always begin a scan-to-email button since it tells Copitrak what kind of function is to be executed. There are several other function types.
5. Click **PreMode2** and enter **1** again (still invoking the scan mode).
6. In the text field, enter DIRPER%%Scan to Network Share and click **Set In This Group**.
7. Click **Save & Back** until you return to the main screen.
8. Launch or return to the Eclipse terminal simulator to verify the result.

Configure button functionality

1. Return to the **Configuration Manager** and click **Scantrak**.
2. Click **Set 2010 Defaults**.
3. Click **OK** in the confirmation dialog box, and then click **Save & Back**.
4. Click **XML Routing**.

Configure scan-to-folder

To set up the first scan-to-folder, do the following.

1. Select **DIR** from the **Terminal Key Root** list and enter PER into the **Terminal Key Postfix** field.

> The values for the **Terminal Key Root** and **Terminal Key Postfix** fields are concatenated by Copitrak to produce a one-word identifier for this set of configuration options. It must match the value from Determine terminal button functions and order. The identifier can be any string. The values available in the **Terminal Key Root** list are provided as a shortcut for choosing an identifier. They are not required if the combination of the **Terminal Key Root** and **Terminal Key Postfix** fields match what was typed earlier.

2. Select **DIR** from the **Action** list.
   This is an actual Copitrak command and is required for scan-to-folder (directory) functions.
3. In the **Action Postfix** field, enter the path to the network folder destination root provided by the customer such as `\\lhfs\users\`, followed by the code `%N0164`.
   The `%N` value tells Copitrak to insert the value held in Copitrak **userprofile** field of NetworkID2. (In this example, as in most cases, this is the **sAMAccountName** mapped earlier in the import procedure).
   The `0164` value tells Copitrak to use 64 characters of the string starting with the first character. It should normally be set to this value.

   > Clicking on the **?** button will open a help dialog box displaying the various valid commands.

4. In the **Rename** field, enter **%g0160100**. To complete the entry, click **Add**.
   %g016 instructs Copitrak to insert the value from the Scantrak Routing Terminal configuration.
   0100 sets the maximum length of the resulting value to 100 characters.
   The item that you configured appears in the routing list at the top of the dialog box.
5. Click **Save & Back** twice and then return to this dialog box.
   The remainder of this guide assumes that each scan route is fully configured before proceeding. The Description Routing dialog can be populated with all desired scan routes prior to proceeding to Terminal Setup, for all routes.
6. With the newly configured routing selected, click **Terminal Setup** in the bottom-left.
7. In the **Terminal Setup** dialog box, add the appropriate "Available" items to the configuration for this **Active Route** by double-clicking on the item in the **Available** box or selecting it and clicking on the right arrow.
   The item appears in the **Selected** box. Start with the **Available Terminal Groups**, which should display the DEFAULT value determined by our earlier terminal group setup.
8. Repeat the procedure for the **User Group** section.
9. Repeat the procedure for the **Language Group** section.
   Once the three preceding steps have been completed, a new section appears to the right.
10. Click **Set Route Defaults**, and then click **OK** in the confirmation dialog box.
11. The **General** tab appears with default values. Configure the prompts.
    For a scan-to-folder configuration, the following items must be populated:
    - **General 2**: Prompt for file type selection.
    - **General 16**: Prompt for file name.
12. Save the changes in one of the following ways:
    - Click **Save & Back**.

- If configuring multiple scan routes, select the next scan route in the list. Switching scan routes saves the changes automatically. After configuring multiple scan routes, click **Save & Back** twice to save the changes to the last route.

  The remainder of these instructions assume that each scan route is being fully created and configured separately and sequentially.

Configure scan-to-email

1. Return to the **Scantrak Description Routing** dialog box if necessary, and add the scan-to-email scan route. Start by selecting "EMAIL" from the **Terminal Key Route** list. Leave the **Postfix** field empty.
2. Select **SMTP** from the **Action** list.
3. In the **Rename** field, enter **%g0160100** and click **Add**.

   `%g016` instructs Copitrak to insert the value from the Scantrak Routing Terminal Configuration.

   `0100` sets the maximum length of the resulting value to 100 characters.
4. Click **Save & Back** twice and return to this dialog box.
5. With the newly created EMAIL item selected in the **Description Routing** section at the top of the dialog box, click **Terminal Setup**.
6. Move the available items to the **Selected** boxes. Note the automatic addition of the "Scan and E-Mail" entry in the **Route Friendly Name** field at the top.
7. Click **Set Route Defaults** and confirm the change in the verification dialog box that appears.
8. Configure the prompts. For a scan-to-email configuration, complete the following items:
   - **General 2**: Prompt for file type selection.
   - **General 3**: Prompt for email subject line.
   - **General 4**: Prompt for email message.
   - **General 16**: Attachment name
   - Default file name (such as "MyScan").
   - Prompt for file name.
9. Click **Additional Options** tab. The check boxes next to the **Show Bates General <number>** lines determine which of the scan options (General 2-16) will appear at the terminal when someone uses this button.
10. Click **Save & Back** until you return to the main screen.
11. In the **Email Setup** dialog box, enter the general SMTP server information.

    Make sure that the SMTP Relay feature is enabled on the customer's mail server and that it is configured to support anonymous sending of email.
12. Click **Save & Back**.

Chapter 5

Multi-DMS configuration

Starting with Tungsten Copitrak 3.5.0, multiple scan connectors can be configured simultaneously. This is introduced primarily for users to configure and use OneDrive/SharePoint connectors and their DMS scan connectors at the same time. This enhancement requires changes to LcWinService.exe, CandiSim.exe, Eclipse and Edge clients.

Upgraded Eclipse and Edge client route **PreMode** buttons, now let client sessions switch between and interact with different DMS types. Each session may only interact with one DMS type at a time. However, when there are multiple concurrent sessions, it allows different DMS types to be concurrently engaged within the LcWinService.exe process.

Eclipse and Edge clients that remain not upgraded behave in the same way as before when they only engage with the globally configured DMS type.

Configure multiple DMS scan connectors

To configure multiple scan connectors, do the following.

1. Open Config File Manager.
2. Press the **Scantrak** button.
3. Select **DMS System**.

   If you select the DMS type that supports multi-DMS functionality, all other controls in the DMS group box disappear. These are the controls to set the server address, default database and trusted connection. When configuring multiple DMS connectors, these settings are specified in the configuration files specific to the type of DMS you select.

4. Specify the DMS type for each configured PreMode and set the Type parameter to 0.

   Perform this configuration settings in `C:\windows\winersini`.

   For example:

   ```
   [DMS SERVER OPTIONS]
   TYPE=0
   PreMode2DmsType=6
   PreMode3DmsType=7
   ```

   Supported DMS type values are listed in .

5. To enable trusted connection for any DMS type, add **128** to the DMS type value and enter it in the following format: `PreModeXDmsType=Y+128`.

   For example, trusted connection for ProLaw would look like this: `PreModeXDmsType=130`.

6. For all DMS connector types, open `%windir%\winers.ini` and specify the default database in the following format: `PreModeXDsmDatabase=DbName`.

   Where:

   - **X** is the Premode number corresponding to the DMS configured.
   - **DbName** is the name of the database to be used as the default database.

   Database can also be configured in terminal setup if the workspace picklist source is !2-XXD. That setting overrides the default database specified in terminal setup for Database (!1 picklist source) or the database name specified on Open validation.

For the DMS connectors that read configuration from their perspective config files (including iManage, NetDocs, ProLaw, SharePoint, OneDrive), the server address is read from their .config files. Config files are located under `C:\ProgramData\Kofax\Copitrak\Config`. No other configuration is required in `%windir%\winers.ini`.

For all other DMS connectors, the server address can be specified in the text box of the Scantrak configuration UI.

Supported DMS type values

The DMS connectors that are supported with multi-DMS functionality and their values are listed as below.

- **0** - iManage
- **1** - DM5 (eDocs)
- **2** - ProLaw
- **3** - TrialWorks
- **4** - DNA
- **5** - NetDocs
- **6** - SharePoint
- **7** - OneDrive
- **7377747** - Copitrak (Demo)

Chapter 6

Scan settings file configuration

Before performing the first scan, modify the scan settings file to avoid scan quality problems.

1. Open the C:\ERS\WINERS\Scantrak.ini file.
2. Search for the word "despeckle."
3. Replace the value `3` with `0` so that it reads `DESPECKLE=0`.
4. Save the change and close the file.
   The change is applied immediately.

Chapter 7

Pricing

The RAWMon service should be disabled at the end of the installation. This is to avoid any tracking problems for systems where the pricing is not in place prior to the addition of end-points such as terminals.

Return RAWMon to its original state prior to completing the project. A project cannot be closed until price tracking has been verified.

1. Open **Configuration Manager** and click **General Settings**.
2. Click **WorkCode Rates**.
3. In the **Master Rate Table** screen, enter the pricing.
4. If you want to include variable pricing or discount pricing, you can include it in **Copitrak Manager** > **Costing** > **Pricing** or **ERS Admin**.
5. If discounts are entered, perform the following actions:
   a. Go to `C:\ers\winers\` and launch admin32.exe.
   b. Click **System** > **Recompile Discounts**.

Chapter 8

Email notifications

Email messages from all Copitrak applications and workflows are sent using C:\ers\winers\smtp.exe. To configure smtp.exe, you can run it from the command line with parameter -setauth. When executed with that parameter, smtp.exe will prompt for authentication mode, credentials and encryption mode. Settings will be encrypted and saved in C:\ers\winers\smtpinfo.dat.

From CSS 3.3.0, smtp.exe can also be configured to work with Token Vault and authenticate with mail server using user's access token. This feature enables the compatibility with Office 365 after basic authentication becomes disabled. You can find the parameters for this authentication method in C:\ProgramData\Kofax\Copitrak\Config\CommonSettings.config, as shown below.

```
<appSettings>
<add key="TokenVaultSmtpProviderId" value="" />
<add key="TokenVaultSmtpNetworkUser" value=""/>
<add key="TokenVaultMailAccessProviderId" value="" />
<add key="TokenVaultMailAccessNetworkUser" value=""/>
<add key="TokenVaultUrl" value=https://your-css-machine-name:8381 />
</appSettings>
```

After configuring the email provider in Token Vault, the parameters in CommonSettings.config, TokenVaultSmtpProviderId and TokenVaultMailAccessProviderId should be edited to match the values from Token Vault. The Network User settings in this file should be left blank if an email is to be sent using the credentials of the user performing the task, and Token Vault is not used for SMTP authorization.

Configuring mail provider in Token Vault is identical to configuring for OneDrive Scan connector. See the "Configure Token Vault for use with OneDrive Connector" section in the *Tungsten Copitrak OneDrive Connector Installation and Configuration* guide for more details.

Regardless of the authentication method for smtp.exe, various email templates are specified in C:\windows\winers.ini file, in section [STATUS EMAIL].

Chapter 9

Troubleshooting

Issue: Fax transactions are recorded as Copy transactions in the Copitrak Embedded System

Description: The data processing in any Copitrak Embedded System which goes through Copitrak DFI is recording the Fax transactions as Copy transactions.

Workaround: This feature is as designed. Normally, for recording the Transaction Type, Copy is TRANS_TYPE_1 and Fax is TRANS_TYPE_0. In Copitrak DFI, Fax transactions are always recorded as Copy transactions and any embedded system which goes through DFI tracks Scan, Copy and Fax all as TRANS_TYPE_1.

However, this is not a problem because Copitrak has workcodes which are used for billing clients. Scan, Copy and Fax have unique workcodes in DFI. Therefore, even though the Transaction Types are recorded the same for Fax and Copy, the billing and transaction creation for Fax and Copy are still performed correctly based on workcodes.

Issue: An error displayed on the License Information page after upgrading to CSS 3.3.0 or above

Description: After an upgrade from the earlier versions to CSS 3.3.0 or above, the License Manager service fails to start and displays the "Unable to locate License Manager Service" error because some older files are left behind in the License Manager folder.

Workaround: Delete the C:\ERS\Services\LicenseManager\LicenseManager.exe.manifest file and start the CSSLicense Manager service.

Issue: After upgrading CSS from 3.0.0 to 3.3.0 or above, Copitrak DFI is not logging to log files or not running

Description: After an upgrade from CSS 3.0.0 to 3.3.0 or above, Copitrak DFI configuration files are not updated, making it fail to write log files or fail to run.

Workaround: Do the following to resolve the issue:

1. Create backup copies of the following two configuration files and then delete the originals: C:\inetpub\wwwroot\CopitrakDFI\web.config and C:\inetpub\wwwroot\CopitrakDFI\ConsoleDFI\ClientDFI.exe.config.
2. From the administrator's command prompt, run the Copitrak DFI installer to repair it.

   Run C:\CSS\Install\REDIST\CopitrakDFI\CopitrakDFI.<your version number>.msi TARGETAPPPOOL=".NET v4.5 Classic".

   When prompted, select **Repair CopitrakDFI**.

3. Open the backup copies of the configuration files in step 1 and copy the "appSettings" section to corresponding configuration files created after the repair.