Kofax Copitrak
OneDrive Connector Installation and Configuration Guide

Version: 1.0.0

Date: 2023-06-13

KOFAX

© 2010–2023 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface **4**
System requirements 4
Related documentation 4
Getting help with Kofax products 4
Chapter 1: Prerequisites **6**
Chapter 2: Components and common settings **7**
Chapter 3: Kofax Copitrak OneDrive logs **8**
Chapter 4: Kofax Copitrak OneDrive Configuration **9**
Login methods 9
Configure the DMS server 9
Configure the DMS Route in Scantrak 10
Configure the DMS Route Prompts on Eclipse 11
Configure OneDriveCommonSettings.config 18
Configure Token Vault for use with OneDrive Connector 18
Register a new authorization provider for Microsoft 365 in Token Vault 18
Authorize the new authorization provider for OneDrive in Token Vault 19
Configure OneDriveCommonSettings.config for use with Token Vault 20
Configure CommonSettings.config 20
Chapter 5: Scanning workflow **21**

Preface

This guide provides instructions for administrators who are responsible for installing and using Kofax Copitrak OneDrive Connector. Use this guide to get started with the software and become familiar with the product features.

System requirements

System requirements are listed in the *Technical Specifications* document, which is available from the Kofax 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 Kofax Copitrak 3.4.0 is available here:

https://docshield.kofax.com/Portal/Products/Copitrak/3.4.0-csb5nx1k32/Copitrak.htm

Getting help with Kofax products

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

To access the Kofax Knowledge Portal, go to https://knowledge.kofax.com.

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

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

Chapter 1

Prerequisites

The Kofax Copitrak OneDrive Connector is used to access OneDrive and SharePoint document libraries on the cloud via Microsoft Graph Services, which is referred to within this document as the "DMS".

Before starting with the installation and configuration, confirm the following information:

1. Access to Microsoft OneDrive is required.
2. Copitrak CSS Server 3.3.0 or above is required.

Chapter 2

Components and common settings

Kofax Copitrak OneDrive Connector consists of the following primary components:

- OneDriveHelper.dll - Provides read access to OneDrive.
- DMSPlugin.dll - Loads OneDriveHelper.dll.config into LcWinService.exe in the context of a session in which a user browses DMS folders.
- OneDriveTools.exe - Uploads scanned documents to a DMS folder and sends upload notification emails.

Both OneDriveHelper.dll and OneDriveTools.exe are governed by the following configuration files which are further detailed in the subsequent sections of this document:

- %programdata%\Kofax\Copitrak\Config\CommonSettings.config - Provides a common place to configure global settings for Token Vault and logging.

  See Configure Token Vault for use with OneDrive Connector for further details about Token Vault.
- %programdata%\Kofax\Copitrak\Config\OneDriveCommonSettings.config - Provides a common place for OneDrive specific settings.

Chapter 3

Kofax Copitrak OneDrive logs

The %programdata%\Kofax\Copitrak\Config\CommonSettings.config file contains settings for logging by DotNet assemblies that reference it.

Copitrak OneDrive produces the following log files:

- ERS\LogFiles\lcwin\LcWinDotNet.log - Contains log messages from all DotNet assemblies running within LcWinService.exe, including OneDriveHelper.dll, DMSPlugin.dll and LCWIN_NET_EXT.dll. Log settings are configured in CommonSettings.config.
- ERS\LogFiles\DMS\OneDriveTools.log - Contains log messages from OneDriveTools.exe. Log settings are configured in CommonSettings.config.
- C:\ERS\WINERS\debug\smtp\<date>_smtp.log - Contains logs from smtp.exe used to send DMS upload email notifications. DebugLevel is configured in ERS\WINERS\smtp.exe.config.

Chapter 4

Kofax Copitrak OneDrive Configuration

Before configuration, note that Kofax Copitrak OneDrive Connector requires Copitrak CSS Server 3.3.0 or above.

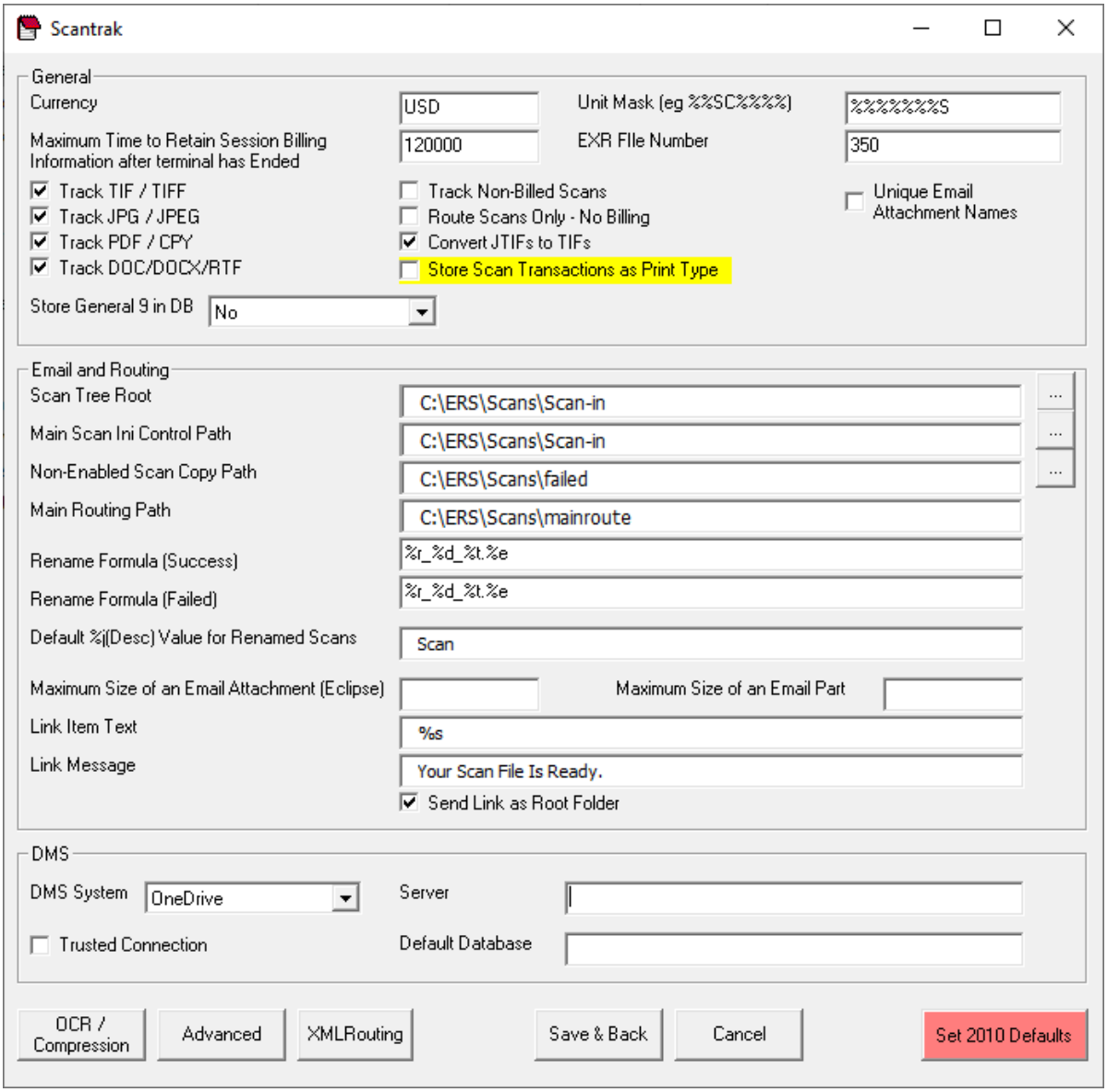
Login methods

In order to log in, the user's network user name must be added to the ERS configuration under the user's NetworkId2 profile. For on-premise OneDrive, the password is then prompted in the Eclipse/Edge user login workflow. For cloud OneDrive on Microsoft 365, the user must authenticate via TokenVault before invoking Eclipse/Edge. See Configure Token Vault for use with OneDrive Connector for details.

If scanned documents are to be stored in OneDrive on behalf of individual users (using their own credentials), each user must provide their credentials by following the link to the authorization page provided to them by their administrator.

Configure the DMS server

1. Open Config File Manager.
2. Press the **Scantrak** button.
   The **Scantrak** configuration page appears.

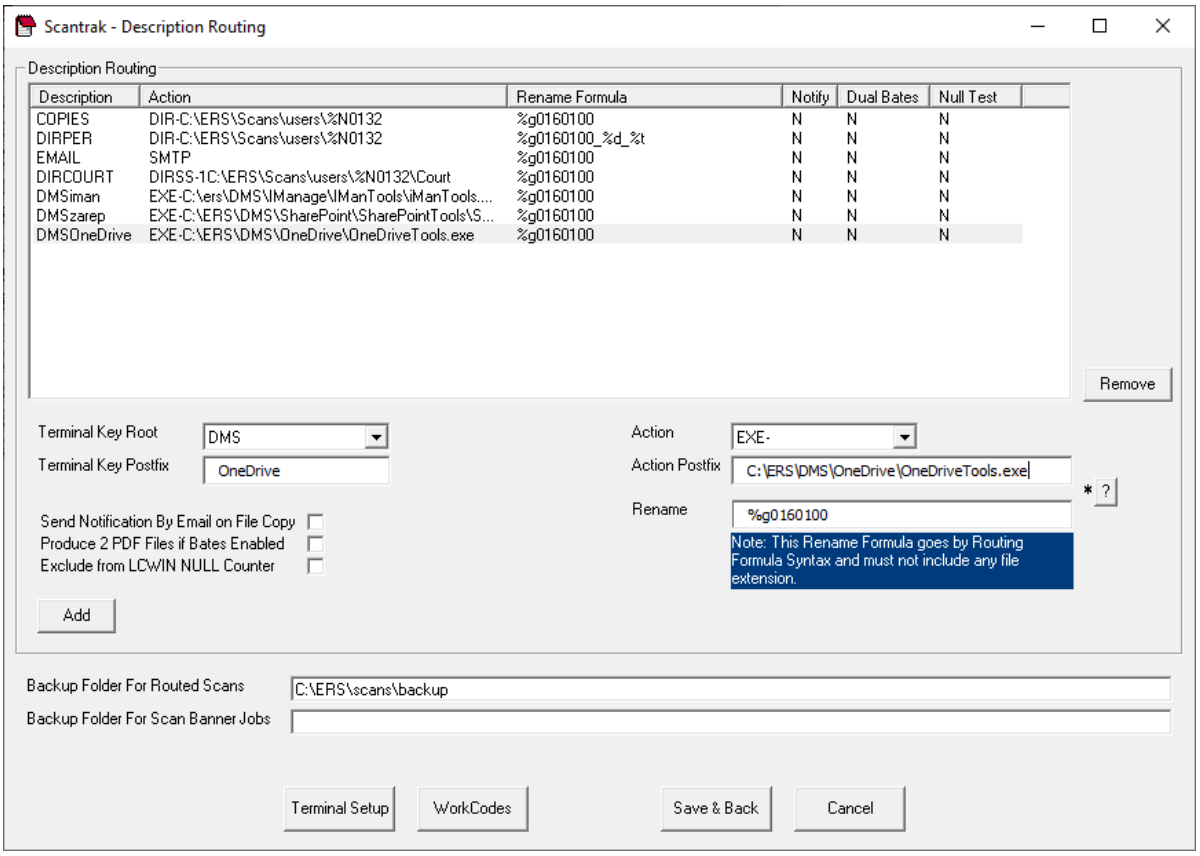


3. Under the **DMS** section, in the **DMS System** drop-down menu, select **OneDrive**.
4. Leave the **Default Database** field blank.
5. Leave the **Server** field blank.
6. Click **Save & Back**.

Configure the DMS Route in Scantrak

1. Open Config File Manager.
2. Press the **Scantrak** button.
3. Press the **XML Routing** button.

The **Scantrak - Description Routing** page appears.



4. Add a route.

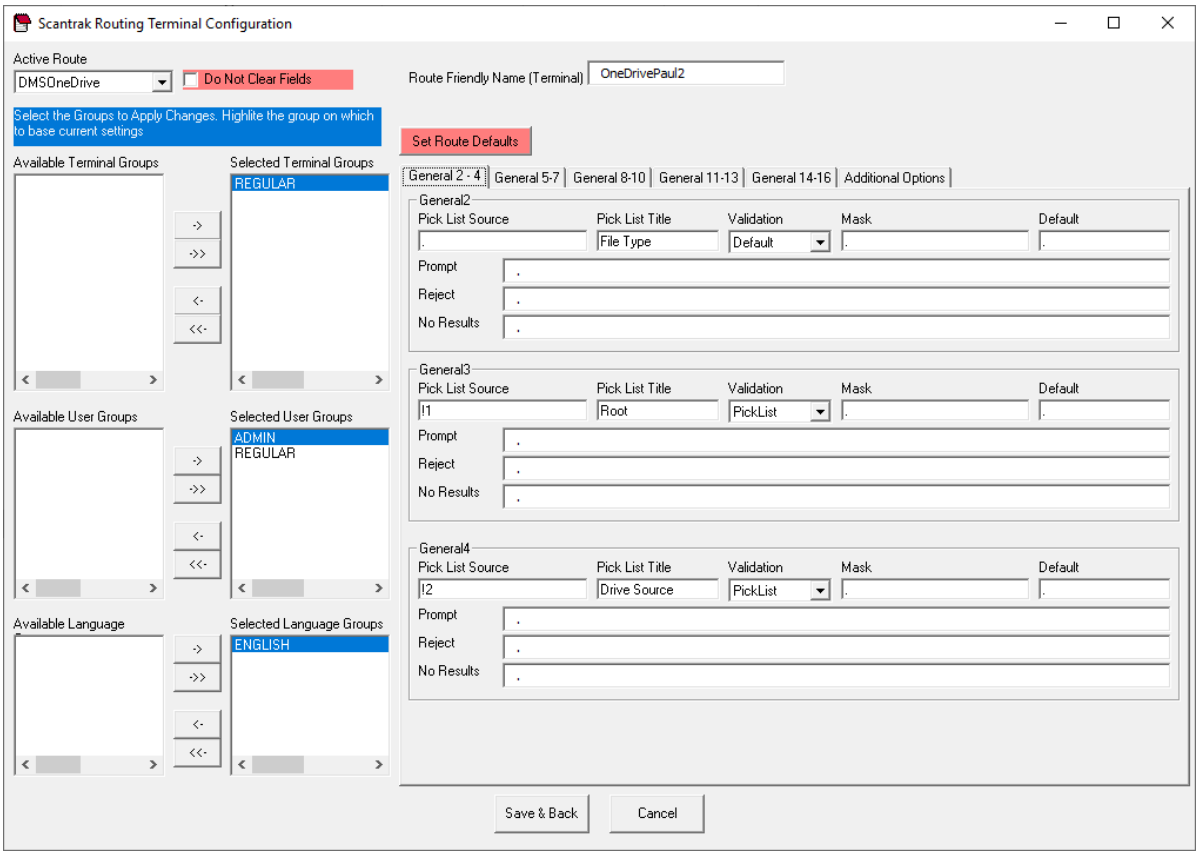
   Typically, DMS is used for the description.

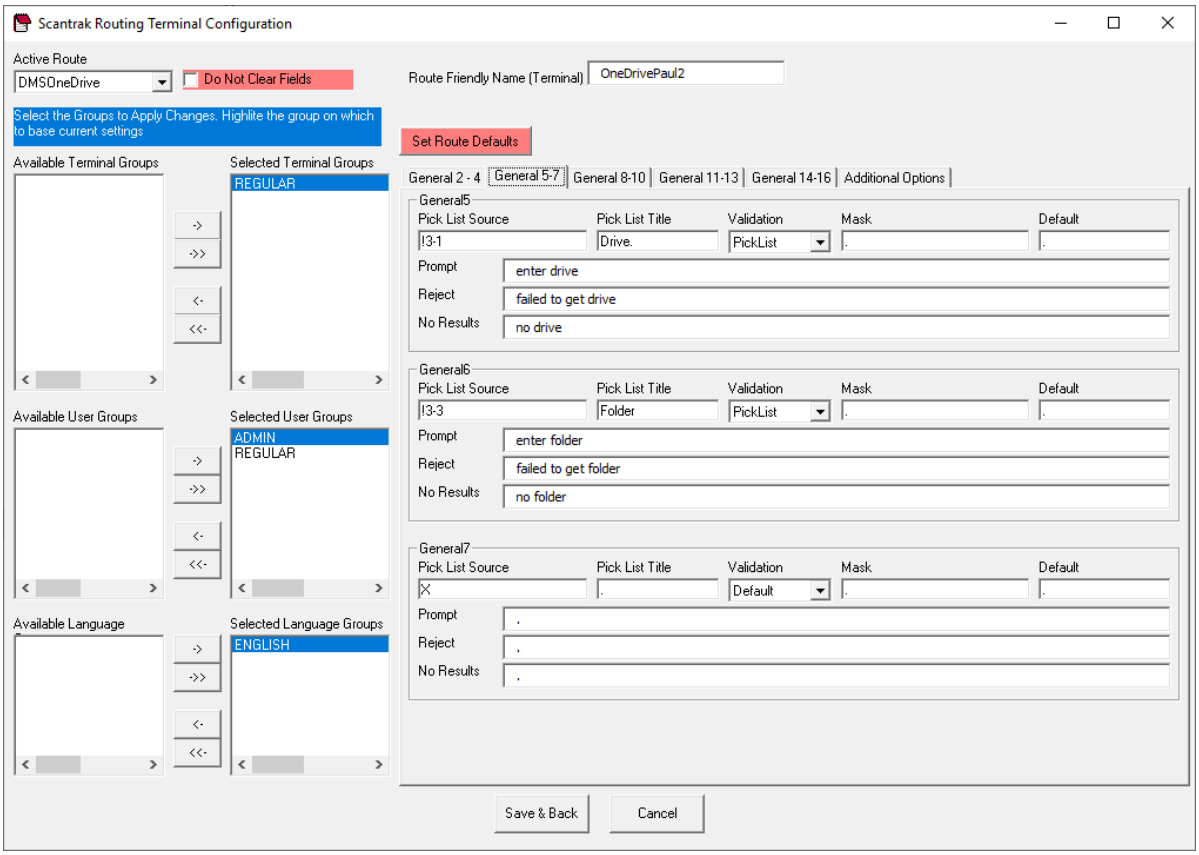
   Action is EXE-"C:\ERS\DMS\OneDrive\OneDriveTools.exe". The drive letter must correspond to your setup.
5. Choose a **Terminal Key Root** of **DMS** if no password prompt is desired in Edge, or **DMSS** if a password prompt is required.
6. Enter a descriptive **Terminal Key Postfix** such as OneDrive.

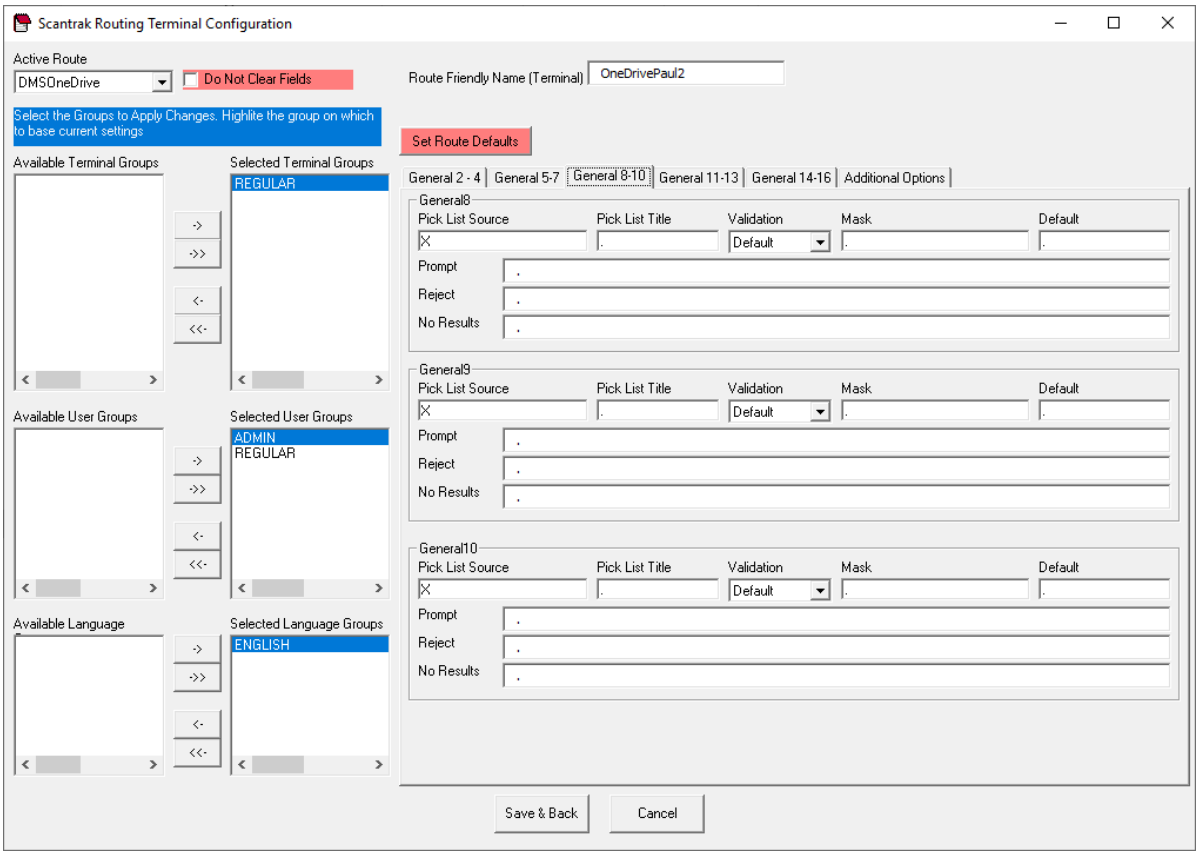
Configure the DMS Route Prompts on Eclipse

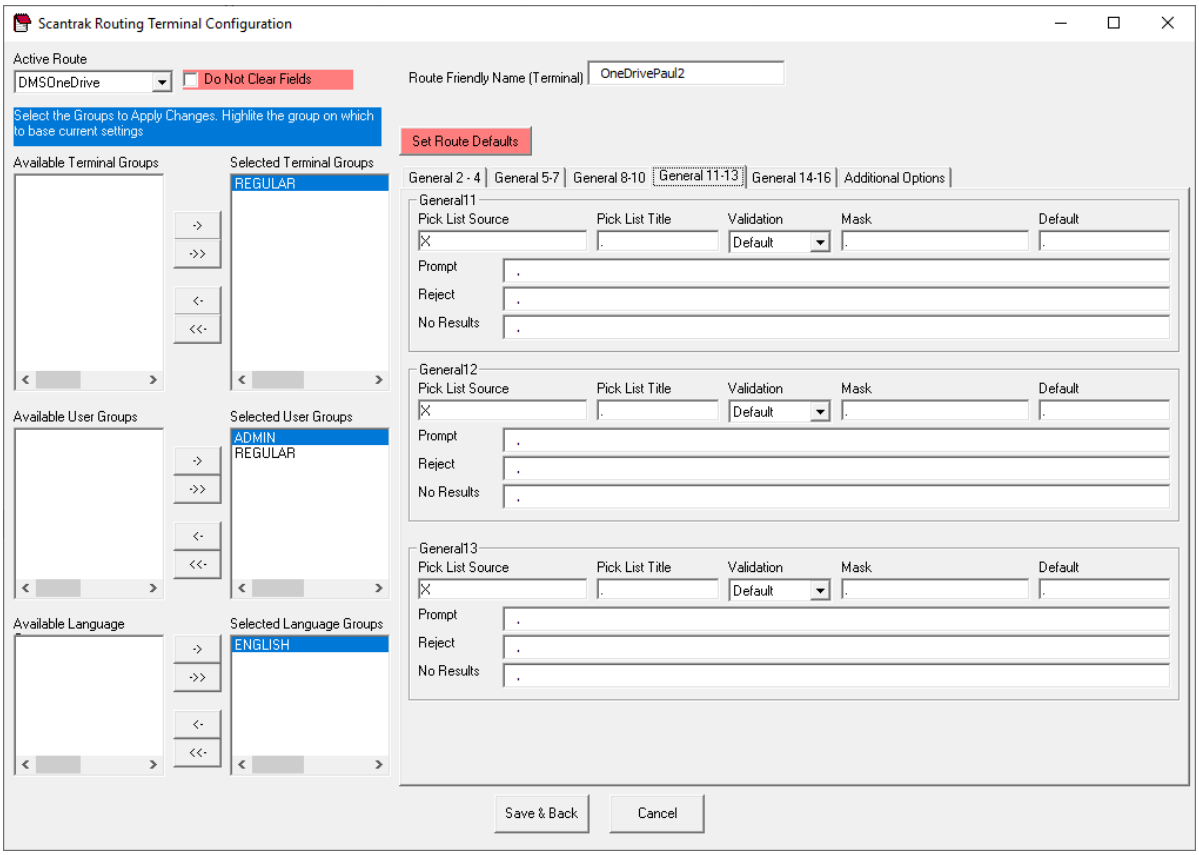
1. Open Config File Manager.
2. Press the **Terminal/User Options** button.
3. Expand the default User group.
4. Set **General1PickXX** to value "1".
5. Set **General1Pick0** to value "DMS%%Scan to OneDrive".
6. Click **Close**.
7. Press the **Scantrak** button.

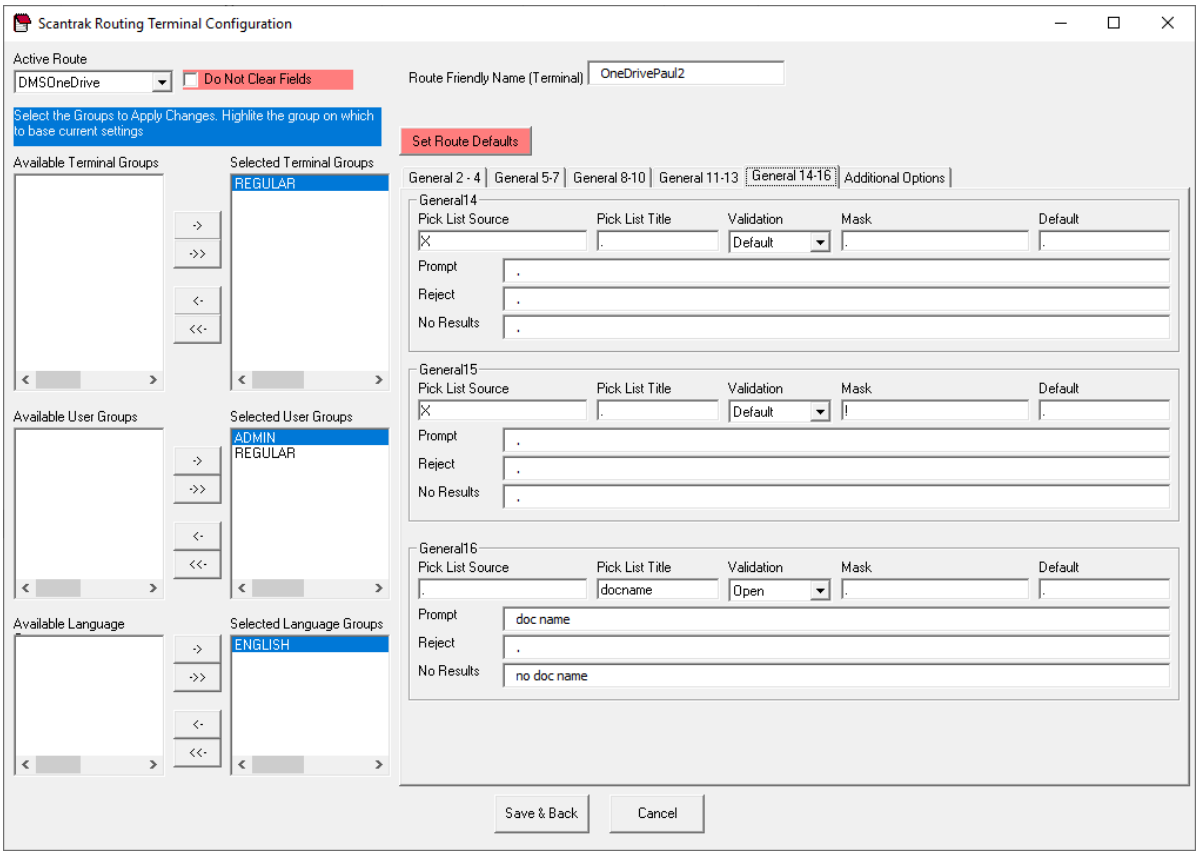
8. Click **XML Routing**.
9. Press the **Terminal Setup** button.
10. Select **DMS** for Active Route.
11. Select the appropriate Terminal group, User group, and Language group.

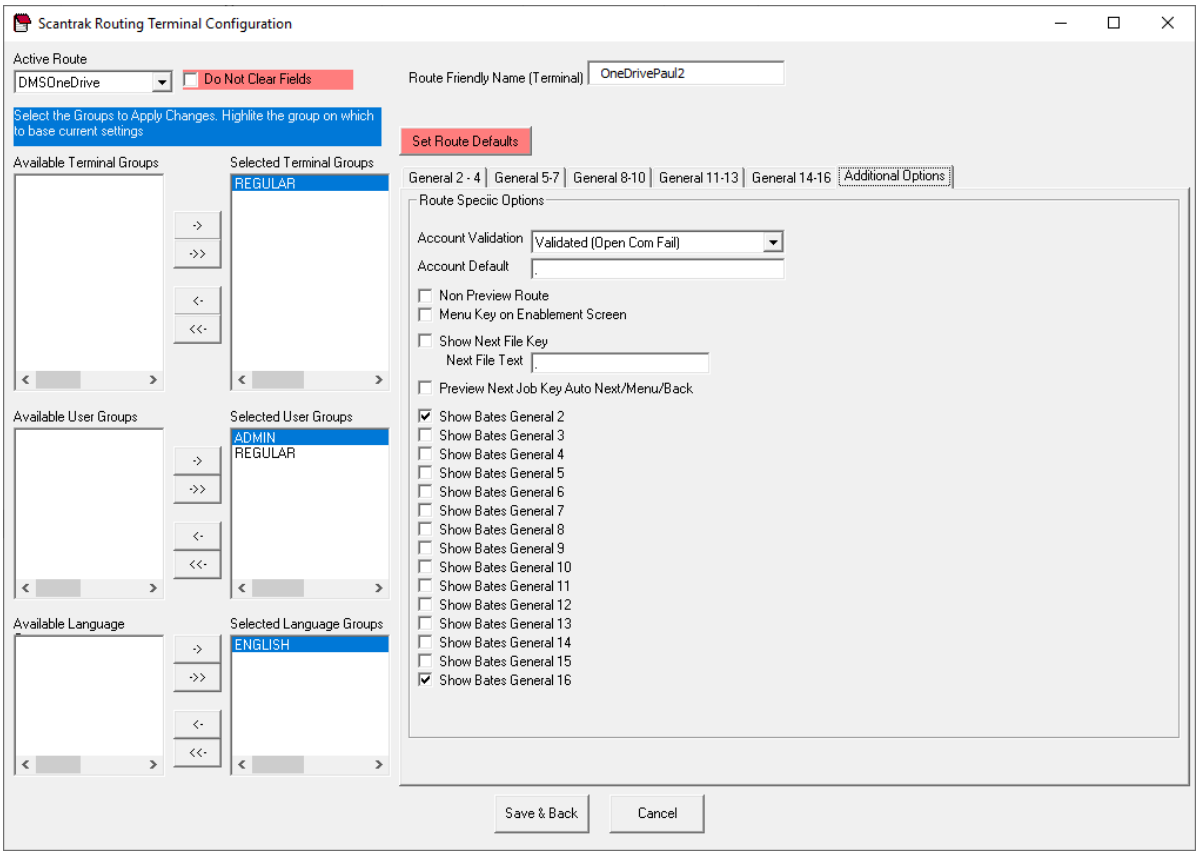



Scantrak Routing Terminal Configuration
Active Route
DMSOneDrive
Do Not Clear Fields
Route Friendly Name (Terminal)
OneDrivePaul2
Select the Groups to Apply Changes. Highlite the group on which to base current settings
Set Route Defaults
Available Terminal Groups
Selected Terminal Groups
REGULAR
General 2 - 4
General 5-7
General 8-10
General 11-13
General 14-16
Additional Options
General5
Pick List Source
Pick List Title
Validation
Mask
Default
!3-1
Drive.
PickList
Prompt
enter drive
Reject
failed to get drive
No Results
no drive
Available User Groups
Selected User Groups
ADMIN
REGULAR
General6
Pick List Source
Pick List Title
Validation
Mask
Default
!3-3
Folder
PickList
Prompt
enter folder
Reject
failed to get folder
No Results
no folder
Available Language
Selected Language Groups
ENGLISH
General7
Pick List Source
Pick List Title
Validation
Mask
Default
X
Default
Prompt
Reject
No Results
Save & Back
Cancel


Scantrak Routing Terminal Configuration
Active Route
DMSOneDrive
Do Not Clear Fields
Route Friendly Name (Terminal)
OneDrivePaul2
Select the Groups to Apply Changes. Highlite the group on which to base current settings
Set Route Defaults
Available Terminal Groups
Selected Terminal Groups
REGULAR
General 2 - 4
General 5-7
General 8-10
General 11-13
General 14-16
Additional Options
General8
Pick List Source
Pick List Title
Validation
Mask
Default
Prompt
Reject
No Results
General9
General10
Available User Groups
Selected User Groups
ADMIN
REGULAR
Available Language
Selected Language Groups
ENGLISH
Save & Back
Cancel


Scantrak Routing Terminal Configuration
Active Route
DMSOneDrive
Do Not Clear Fields
Route Friendly Name (Terminal)
OneDrivePaul2
Select the Groups to Apply Changes. Highlite the group on which to base current settings
Set Route Defaults
Available Terminal Groups
Selected Terminal Groups
REGULAR
Available User Groups
Selected User Groups
ADMIN
REGULAR
Available Language
Selected Language Groups
ENGLISH
General 2 - 4
General 5-7
General 8-10
General 11-13
General 14-16
Additional Options
General11
Pick List Source
Pick List Title
Validation
Mask
Default
Prompt
Reject
No Results
General12
General13
Save & Back
Cancel


Scantrak Routing Terminal Configuration
Active Route
DMSOneDrive
Do Not Clear Fields
Route Friendly Name (Terminal)
OneDrivePaul2
Select the Groups to Apply Changes. Highlite the group on which to base current settings
Set Route Defaults
Available Terminal Groups
Selected Terminal Groups
REGULAR
Available User Groups
Selected User Groups
ADMIN
REGULAR
Available Language
Selected Language Groups
ENGLISH
General 2 - 4
General 5-7
General 8-10
General 11-13
General 14-16
Additional Options
General14
Pick List Source
Pick List Title
Validation
Mask
Default
Prompt
Reject
No Results
General15
General16
docname
Open
doc name
no doc name
Save & Back
Cancel



12. Make changes based on the selected mode.

Picklist Source	Description
!1	Root Selection Choices are **Me** and **Groups**. **Me** stands for your own OneDrives and **Groups** stand for the user groups that own the OneDrives or SharePoint sites.
!2	Drive Source Selection Returns either your user or a list of groups, depending on the selected Root.
!3-1	Drive Selection Returns all drives belonging to the selected Drive Source.
!3-3	Search from Root folder selected in previous general field (!3-1). This prompt only displays subfolders within the Root folders. It also allows the user to drill down to any folder within the tree. Prompt is reused to display the new folders within the previous selected folder.

Configure OneDriveCommonSettings.config

1. Open OneDriveCommonSettings.config file from the %programdata%\Kofax\Copitrak\Config\ folder.
2. Edit the values in the file to reflect the corresponding General Field values from below.

```
<appSettings>
<add key="TokenVaultOneDriveProviderId" value="bbbbbbbb-bbbb-bbbb-bbbb-
bbbbbbbbbbbb" />
<add key="WorkFolder" value="GENERAL6" />
<add key="ClientMatterSplitter" value="-"/>
<add key="Client" value="Client"/>
<add key="Matter" value="Matter"/>
<add key="ClientCode" value="true" />
<add key="SmtpEnabled" value="false" />
<add key="SubjectSuccess" value="Your document ({doctitle}) scan succeeded!" />
<add key="SubjectFailure" value="Your document ({doctitle}) scan failed!" />
</appSettings>
```

   Client, Matter and ClientMatterSplitter settings are ignored.
3. Save the file after making changes.

Configure Token Vault for use with OneDrive Connector

Token Vault is available to create possible workflows where user credentials are required but there is no prompt for credentials, such as scan workflows initiated from the embedded clients and completed by the CSS server.

Register a new authorization provider for Microsoft 365 in Token Vault

Before configuring Token Vault with Kofax Copitrak OneDrive Connector, make sure that you complete the Token Vault installation properly. After installing and configuring TokenVault, the following must be fulfilled on that system:

- You imported all certificates used or generated by TokenVault into the Personal certificate stores.
- You imported the Root CA certificate used or generated by TokenVault into the Trusted Root Certificate Authorities certificate stores.
- Those certificate stores are accessible to the TokenVault service. For more details, see the Kofax Token Vault Installation Guide.

1. In your browser's address bar, open Token Vault manually by entering the Fully Qualified Domain Name of the computer where Token Vault is deployed along with the HTTPS port number.

   For example, *https://computername.mydomain.com:8381/*.

   The **Token Vault Login** page appears.
2. Log in to Token Vault with your Windows user name and password.

   The **Token Vault Configuration** page appears.
3. Select the **Manage authorization providers** tab.

   The **Manage authorization providers** page appears.

4. Click **Register new**.
   The **Select cloud provider** page appears.
5. Select **Microsoft 365** in the list.
   The **New Microsoft 365 authorization provider** page appears.
6. Verify that the **Redirect URL** in this page is added to the **Redirect URLs** in your Mircosoft 365 application by doing the following.
   a. Go to *https://portal.azure.com*.
   b. Navigate to **App registrations** > **Owned applications**, select the application created for Copitrak.
   c. Navigate to **Authentication** > **Web**, and click **Add URL**.
   d. Copy the **Redirect URL** in the **New Microsoft 365 authorization provider** page to the new **Redirect URL** in your Mircosoft 365 application.
7. On the **New Microsoft 365 authorization provider** page, in the **Application (client) ID** field, enter the **Application (client) ID** from the Mircosoft 365 application by doing the following.
   a. Go to *https://portal.azure.com*.
   b. Navigate to **App registrations** > **Owned applications**, select the application created for Copitrak.
   c. Navigate to **Overview** > **Essentials**, and copy the **Application (client) ID** value from this page to the Token Vault **New Microsoft 365 authorization provider** page.
8. On the **New Microsoft 365 authorization provider** page, in the **Client secret (value)** field, enter the **Client secret** from the Mircosoft 365 application by doing the following.
   a. Go to *https://portal.azure.com*.
   b. Navigate to **App registrations** > **Owned applications**, select the application created for Copitrak.
   c. Navigate to **Overview** > **Essentials** > **Client credentials**, and copy the value from the **Value** column in this page to the **Client secret (value)** field in Token Vault **New Microsoft 365 authorization provider** page.
9. On the **New Microsoft 365 authorization provider** page, in the **Supported account types** drop-down menu, select **Single tenant**.
10. In the **Tenant name** field, enter your Mircosoft 365 tenant name.
11. In the **National Cloud** field, select **Azure AD (global service) - https://login.microsoftonline.com**.
12. In the **Scope sets** field, enter **Graph**.
13. Click **Save**.
    The new Microsoft 365 authorization provider is registered.
14. On the **Manage authorization provider** page, click **Enable**.
    The new Microsoft 365 authorization provider is enabled.

Authorize the new authorization provider for OneDrive in Token Vault

1. In **Token Vault Configuration** page, navigate to **Available authorization providers**.
2. In the **New Microsoft 365 authoriztion provider** already registered section, click **Authorize**.

You are redirected to the Microsoft Online login page. After the successful login, you get the message notifying that "You successfully authorized this provider."

3. Click **Close** on the message.

Now you can perform scan jobs without authenticating on the Microsoft Office 365 OneDrive cloud server.

Configure OneDriveCommonSettings.config for use with Token Vault

The OneDriveCommonSettings.config file under %programdata%\Kofax\Copitrak\Config\ provides a common place for OneDrive specific settings. To use Token Vault with OneDrive, open the OneDriveCommonSettings.config file and copy the **Provider ID** from your Token Vault **New Microsoft 365 authorization provider** configuration web page to the following value.

```
<add key="TokenVaultOneDriveProviderID" value="" />
```

Configure CommonSettings.config

The CommonSettings.config file under the %programdata%\Kofax\Copitrak\Config\ folder provides a common place to configure global settings for Token Vault and logging. To use Token Vault, you also need to enter the URL used to run Token Vault to the following key from the CommonSettings.config file.

For example: `<add key="TokenVaultUrl" value=https://myhost.acme.com:8381 />`

Chapter 5

Scanning workflow

The scan workflow proceeds as follows: pick client-matter, pick a root, drive source, drive and folder, and then specify a document name and format.

At each stage, results can be filtered by typing into the text box on the right. Results are displayed 8 at a time, and you can switch between pages of results using the left and right arrows at the top of the list. The arrows are shown in white when you can move forward/ backward.