AccuRoute® v5.1
Release Notes

January 2017

Omtool support and sales

Online resources

The Omtool web site provides you with 24-hour access to documentation, software updates and other downloads, and detailed technical information that can help you troubleshoot issues. Go to http://www.omtool.com/support and log in using your customer number. Then click one of the following:

- **Knowledge Base** to access technical articles.
- **Downloads & Docs** to access online documentation, software updates, and downloads.

Customer service and technical support

Contact Omtool Customer Service or Technical Support using any of the following methods:

- **Phone**: +1/1 978 327 6800 or +1/1 888 303 8098 (toll-free in the US)
- **Fax**: +1/1 978 659 1301
- **E-mail**: customerservice@omtool.com or support@omtool.com

Technical support requires an active support contract. For more information, go to http://w3.omtool.com/support/entitlements.cfm.

Sales, consulting services, licenses, and training

Contact Omtool Sales using any of the following methods:

- **Phone**: +1/1 978 327 5700 or +1/1 800 886 7845 (toll-free in the US)
- **Fax**: +1/1 978 659 1300
- **E-mail**: sales@omtool.com

Contents

Section 3: Omtool Client Updates

Section 4: Issues and Limitations

Section 1: Summary of Features

New Features

The following tables summarize the new Server and Client features specific to AccuRoute® v5.1:

Table 1-1: **AccuRoute v5.1 Server New Features**

Components Affected	Node	New Feature	Description
AccuRoute Server		Disaster Recovery Solution	The AccuRoute Disaster Recovery Solution inherits its configuration from your existing system. Disaster Recovery supports either a single server or a clustered system. It allows switching between the primary data center and failover, and back again.
		Data Encryption	Data Encryption is now available for all messages that move through the server, including the Messages folder, data exchanged between the AccuRoute Server and the SQL server database, and AccuRoute Server Property files. System administrators can enable and disable encryption via Command Line. The current Encryption status (active or inactive) appears in the Server Administrator.
	Messages	New Bookmark Support for PDFs	PDF document bookmarking options are available for both electronic document attachments and hard copies. Bookmarks can be used to separate merged attachments, or to identify sections of hard copy documentation. Bookmark pages can be created by authenticated End User Interface Web Apps users.
	Connectors	New SAP FAX via SMTP Connector	The SAP FAX via SMTP Connector supports inbound and outbound faxing using SAP SMTP-based communications.
		New Secure Print Connector	The new Secure Print Connector works in conjunction with the Brooksnet Remote Print Manager, to allow users to print documents from their desktop to a network folder, with the intention to later access and print the documents from a device, using the MyPrints device button.
		New Bursting Connector	The new Bursting Connector allows you to split up (or burst) document batches. It uses barcodes to identify and break up documents.
		New NetDocuments Connector Features and Updates	The NetDocuments Connector now supports a workflow for Workspace Cabinet delivery and updates Volume List delivery

Table 1-1: **AccuRoute v5.1 Server New Features**

Components Affected	Node	New Feature	Description
AccuRoute Server	RuleSets	Rules Node renamed RuleSets	The Rules Node is renamed RuleSets. The following RuleSet categories are created at installation: • User RuleSets - for user-created Rules • Default RuleSets - previously named Outbound Rules • Received Faxes RuleSets - RuleSets for Inbound Faxes to match **Note:** Routing Rule functionality from prior releases is retained with RuleSets.
		New Rule destinations	New RuleSets destinations include Route to Connector, Route to Embedded Directive Manager, Route to Failure, Route to Lookup, and Advanced Routing.
		Customizing RuleSet workflows	Administrators can now customize their RuleSets workflow by • Defining the Rules' processing order • Configuring notifications associated with Job status
	Configuration	New Table format for User Job Properties	Administrators can associate multiple Job Properties to create a single User Job Property in a table format.
		New Job Property Lookups	System Administrators can now configure Job Properties for Database Lookup and List Lookup.
		New Folder Destination Type: Microsoft® OneDrive® for Business	System Administrators can now configure and assign MS OneDrive for Business Folder access to authorized Web Apps and Device Client user groups.
		New Folder Destination Type: WebDav	System Administrators can now configure and assign WebDav Folder access to authorized Web Apps and Device Client user groups.
		New Search Filters Node	Use Search Filters to configure message searches using message meta-data criteria. Also access Search Filters via the Messages node. Search Filters can be customized and saved for later use
		New Web Apps Node	Web Apps is the new highly-customizable version of the former End User Interface (Web Client). Administrators can assign Applications (such as Inbox, Create Distribution, etc) to Web Apps Profiles, which are in turn associated to specific user groups, defining what a given user will see.
		Web Client Node renamed Legacy Web Views	The prior Web Client Node has been renamed Legacy Web Views. **Note:** The Legacy Web Views Node is the only place to configure Legacy Web Client access to the Help Desk, Archive Search, Deficiencies, and approval.
		New Scan Settings default options in Group Properties	Additional Scan Settings are now available for administrators to apply as user group default settings. Specific setting options vary per device type.
	Devices	New Scan Settings available in Button Properties	Administrators can define Scan Settings values per button, for a specific device group.
		New MyMessages device button	The MyMessages button offers authenticated users the ability to view and print their messages, including faxes. An Administrator configures MyMessages button filters and availability for users.

Table 1-1: **AccuRoute v5.1 Server New Features**

Components Affected	Node	New Feature	Description
AccuRoute Server	Devices	New MyPrints device button	MyPrints button offers authenticated users the ability to view and print messages they have already sent. An Administrator configures MyPrints button availability for users.

Table 1-2: **AccuRoute v5.1 Clients Features**

Components Affected	New Features	Description
End User Interface	New Web Client: Web Apps	The new Web Apps End User Interface provides all the functionality of the prior Web Client, with a new intuitive, Application tile-based display. Individual Application tiles (such as Inbox, Create Distribution, etc) appear on a Homepage.
		Web Apps supports all current browsers and the new PDF Bookmarking feature.
		Note: Note: The Legacy Web Client EUI is the only place authorized users can access the Help Desk, Archive Search, Deficiencies, and approval.
	New Folder Destination Types	Authenticated users can now access the following cloud-based storage applications: • WebDav • Microsoft® OneDrive® for Business
	New Bookmark support for PDFs	PDF Bookmarks can be created by authenticated End User Interface Web Apps users. Bookmarks can be used to identify sections of hard copy documentation.
	New Job Property Lookups	Web Apps users can now use Database Lookup and List Lookup for Job Properties.
Device Client	New Device Support	The AccuRoute Embedded Device Client adds support for the following devices: • HP PageWide Color MFP 586 • HP PageWide Color MFP E58650 • HP PageWide Color Flow MFP 586 • HP PageWide Color Flow E58650 • HP PageWide Managed MFP P57750dw
	New Scan Settings default options	Multiple new Scan Settings are available to users, as defined per user group by the Administrator.
		Specific setting options vary per device type, and may include, for example: Blank Image Removal, Contrast, Darkness, Media Size, and Quality Mode.
	New MyMessages device button	Authenticated Embedded Device Client users can view and print their messages, including those pre-sent from SecurePrint and printers.
	New MyPrints device button	The MyMessages button offers authenticated users the ability to view and print their messages, including faxes.

Table 1-2: **AccuRoute v5.1 Clients Features**

Components Affected	New Features	Description
Device Client	New Folder Destination Types	Authenticated users can now access the following cloud-based storage applications: • WebDav • Microsoft® OneDrive® for Business
	New Search function for Scan to Folders button	A new Search button is available from the Scan to Folders button.
	New Job Property Lookups	Device Client users can now use Database Lookup and List Lookup for Job Properties.

Related AccuRoute v5.1 documentation

For more information about AccuRoute v5.1 and other AccuRoute products, refer to the AccuRoute v5.1 documentation home page to access:

- Readmes and release notes

- DMS Libraries quick start guides

- User guides and online help

- Administrator guides

- Installation and upgrade guides

Section 2: AccuRoute Server Updates

This section describes the new AccuRoute Server features for AccuRoute v5.1.

For more information on using or configuring the new features, refer to the AccuRoute Server Administrator Help and the AccuRoute Web Client Online Help.

This section includes:

Operating System support

The AccuRoute v5.1 server supports

- Microsoft Windows 2012 x64

- Microsoft Windows 2012 R2 x64

- Microsoft Windows 2008 R2 SP-1 x64

Upgrading

AccuRoute v5.1 supports upgrading servers and clients from AccuRoute v5.0 environments. Upgrade (or install new) clients after you upgrade the AccuRoute Server to v5.1.

For instructions on upgrading a legacy AccuRoute environment, consult the AccuRoute Server and Clients Upgrade Guide.

Disaster Recovery Solution

AccuRoute v5.1 now includes a **Disaster Recovery Solution** that inherits its configuration from your existing system. When in use, the Disaster Recovery Server automatically updates names and connections to connectors, components, etc.

The Disaster Recovery solution supports a single server or a clustered system. It allows switching between the primary data center and failover, and back again.

> **Note**   The accuracy of data recovered from your environment depends on the sync timing. For example, if your system syncs 5 minutes behind, there would be a 5 minute data loss in recovery. Also, the database and the files must be synced at the same time to ensure integrity.
>
> Also note, the Disaster Recovery Server is designed to be a "cold" option and is not expected to be used as an active production system.

Requirements

Before you begin setting up your system for Disaster Recovery, make sure you have

- installed a primary AccuRoute Server.
- applied a Disaster Recovery license (and any other licenses needed).

Installing and configuring a Disaster Recovery server

1 Begin by configuring a replication of a FileShare and database(s) for your system.

2 Install AccuRoute on your Disaster Recovery server using the same installation options that you applied to your production server. Set up your Disaster Recovery server to use the replicas you created in Step 1. Your primary production server must be currently on-line.

3 For more information about the standard AccuRoute installation, refer to the [AccuRoute Server Installation Guide](#).

4 When the **AccuRoute Configuration wizard** appears, select **Disaster recovery configuration** on the **Welcome** screen.

5 On the **Disaster Recovery Standby** screen, enter the **Server Name** of your production AccuRoute server and click **Next**.

> **Note**   If you are configuring the Disaster Recovery server as a failover cluster, enter the Primary server name.

6 On the **Existing Database** screen, enter the name of your **SQL Server**.

7 Select either **Use Windows Integrated Authentication** or **Use SQL Authentication Login**. If required, enter the appropriate **Username** and **Password**. Then click **Next**.

8 On the **Select Existing Database** screen, select your preferred database from the list of existing databases and click **Next**.

9   On the **File Share** screen, enter or browse to the **File Share Location** you want associated with your Disaster Recovery Server. Click **Next**.

10 The **Ready to Configure** screen appears. This screen identifies whether you are configuring Disaster Recovery for a single server or a clustered environment. Click **Next** to configure the Disaster Recovery system.

11 The **Completed** screen appears. Click **Finish** to close the Configuration wizard.

Note   If you are configuring a "cold" cluster environment, repeat steps 4 through 10 above, as needed.

12 Power down the Disaster Recovery server(s).

13 In the AccuRoute Administrator, with your Primary server highlighted, select **Action > Recovery Settings...** The **Disaster Recovery Settings** screen appears.

14 Edit the Backup Site entries as needed and select **OK**.

15 To bring your Disaster Recovery server(s) back on-line, first power up the server(s).

16 Open the AccuRoute Administrator. You may need to wait several minutes for Services to start.

17 Select **Action > Recovery Settings...** to return to the **Disaster Recovery Settings** screen. Confirm and/or edit the Backup Site entries as necessary. Click the **Switch Site** button.

18 A message appears warning you that any services running will be stopped. Any other error messages that appear are likely normal, given that the production servers would be off-line in a real disaster.

19 Restart the Disaster Recovery server (or just the services) to bring the server fully on-line.

20 Bring the Disaster Recovery servers off-line.

21 Make needed repairs to the Primary server. Services should be stopped.

22 On the Disaster Recovery Server's AccuRoute Administrator, select **Action > Recovery Settings...** and click **Switch Sites** to return to Primary settings. The Disaster Recovery Server disconnects and services stop.

23 Power down the Disaster Recovery server(s).

24 Perform any manual steps required to sync the Disaster Recovery database & FileShare back with the Primary server.

25 Restart the Production server (or start services).

26 The Disaster Recovery server(s) are ready for the next time.

Data Encryption

AccuRoute v5.1 now makes Data Encryption available for all messages that move through the server. This includes the Messages folder, data as it is exchanged between the AccuRoute Server and the SQL server database, and AccuRoute Server Property files. The System Administrator determines whether Data Encryption is enabled or not.

AccuRoute system files are encrypted using Advanced Encryption Standard (AES). Encryption certificate acquisition and storage is the responsibility of the System Administrator.

Database information is encrypted using Transparent Data Encryption (TDE), which is configured by the SQL Administrator.

Requirements

To use the new AccuRoute Data Encryption feature, you need to acquire an **encryption certificate** from a certificate vendor. Make sure that the encryption certificate is enabled for **Key Exchange**.

Omtool is not responsible for the certificate or the data if the certificate is lost.

Setting up Data Encryption for AccuRoute v5.1 involves:

- Importing the encryption certificate (2-4)
- Enabling Data Encryption (2-4)

Also see steps for

- Disabling Data Encryption (2-5)
- Configuring the SQL Database (2-5)

Importing the encryption certificate

To use the encryption certificate, import the encryption certificate(s) to the server's certificate store.

While you can use the Windows Certificate Manager to do so, AccuRoute recommends using the `omcertutils` tool included in the AccuRoute `server/bin` folder.

To import the certificate, open **Command Prompt** and enter

`omcertutils -import [`*`path to certificate`*`] [`*`password`*`]`

- If the path to the certificate includes spaces, you must quote the path.
- If there is no password on the certificate, no password needs to be supplied.

The `omcertutils` tool must be run as Administrator. If you are on Windows 2008, you need to be logged in as the Service Account to properly import the certificate. (It will succeed if you login as another user, but the services will not be able to find it.)

> **Note**   If your system environment is a server cluster, repeat this step on each individual machine.

Enabling Data Encryption

To enable data encryption:

1   Make sure you are Administrator on the system, open **Command Prompt** and enter

`omcertutils -apply [`*`certificatename`*`]`

The certificate name is the value used for the certificate's **Subject** field when it was created.

2   When it appears, read and agree to the legal warning by typing **YES** to continue.

3   The existing server disk files are encrypted. The process duration varies based on the number of files.

AccuRoute is enabled for encryption and the Services are started.

> **Note**   In the case of a server cluster, perform these steps only on the primary.

Disabling Data Encryption

To disable data encryption:

Make sure you are Administrator on the system, open **Command Prompt** and enter

`omcertutils -remove`

This command stops Services, decrypts all files, disables future encryption, and then restarts the Services. The process duration varies based on the number of files.

> **Note**   In the case of a server cluster, perform these steps only on the primary.

Configuring the SQL Database

SQL database information is encrypted using Transparent Data Encryption (TDE), which needs to be independently configured by the SQL Administrator.

> **Note**   The DSN Server name must exactly match the SQL SSL certificate subject name (most likely a FQDN) . Also, you need to add `Encrypt = yes` to the DSN. To do so, stop Services, make the Registry change, and then restart Services.

For more information on database encryption, refer to:

https://msdn.microsoft.com/en-us/library/bb677241.aspx

http://sqlmag.com/sql-server/transparent-data-encryption-faqs

https://technet.microsoft.com/en-us/library/ms189067(v=sql.105).aspx

Messages

The **Messages Node** has been updated with the following feature:

- New Bookmark Support for PDFs (2-5)

New Bookmark Support for PDFs

AccuRoute v5.1 now offers PDF document **Bookmarking** options, whether you are working with electronic documents or hard copy versions.

AccuRoute offers two PDF document workflows:

- Hard copy documents — You can create bookmark separator sheets to separate multiple scanned documents that may be, for example, from a single binder of documents. Bookmark separators are reusable.

- Electronic Attachments — You can enable several properties as prompts to allow users to merge multiple attachments into a single PDF, using attachment names as bookmarks to annotate the documents. You can also configure the system to use custom template text as bookmarks.
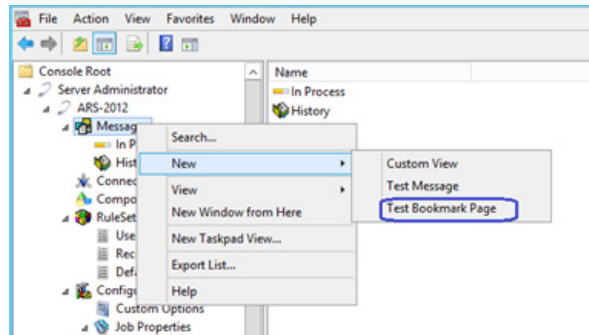
Administrators can assign the **Create Bookmark** button to Web Apps Client users. See below for steps on
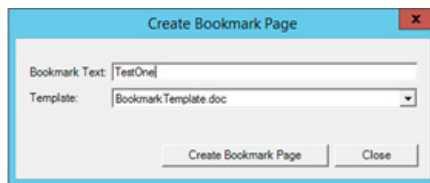

Note   PDF bookmarking requires the Data Extractor License.

## Creating PDF Bookmarks for hard copy documents

1   First, create the Bookmark separator sheets in the AccuRoute Server Administrator.

   **a**   Right-click the **Messages** node and select **New > Test Bookmark Page**.

   **b**   The **Create Bookmark Page** pop-up appears.

   c   Enter a name for your bookmark at **Bookmark Text** and click **Create Bookmark Page**.

   **d**   The system creates and displays the **Bookmark separator page**.
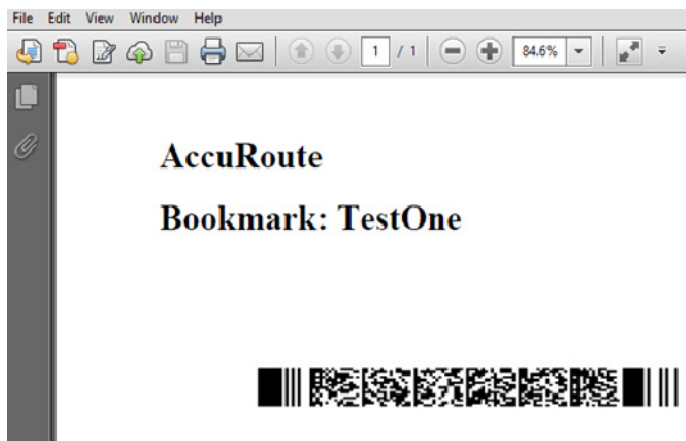
2   Next, you need to set up a rule for the bookmark:

    a   Open the **RuleSets > Default**, and right-click an SMTP rule. Select **Properties**.

    b   In the **Rule Properties** screen, go to the **Actions** tab and double-click the **Compose** Action property. The **Action Properties** screen appears.
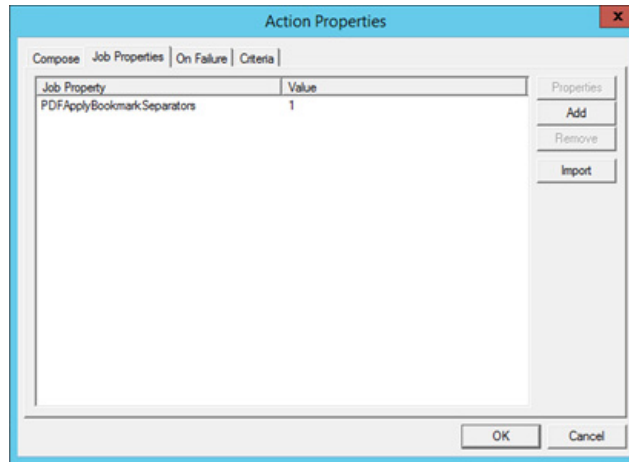
    c   Go to the **Job Properties** tab and click **Add**. Select `PDFApplyBookmarkSeparators` from the **Properties** drop-down list and enter a **Value** of `1`. Click **OK** twice to return to the **Actions** tab.

    d   Double-click the **Data Extractor** Action property. The **Action Properties** screen appears.
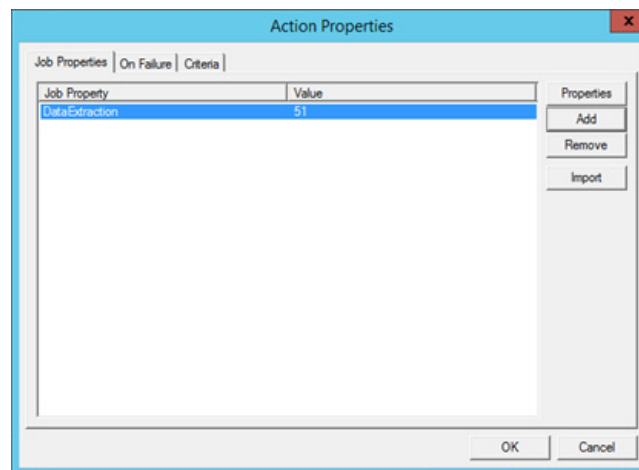
> **e** Go to the **Job Properties** tab and click **Add**. Select `DataExtraction` from the **Properties** drop-down list and enter a **Value** of `51`. Click **OK** twice to return to the **Actions** tab.
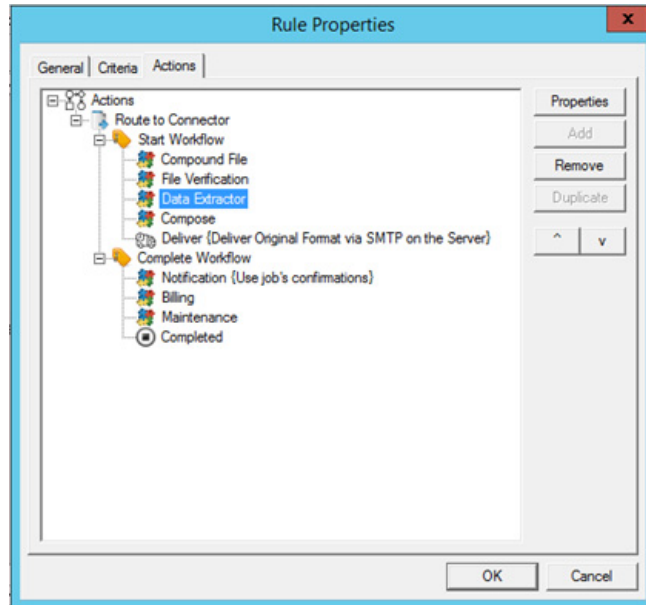
> **f** Make sure the **Data Extractor** appears above **Compose** in the Actions list. If it does not, select **Data Extractor** and click the **up** arrow button. Click **OK**.

3 Scan the Bookmark Separator along with a few other documents, arranged in the following order: *Bookmark Separator > Document > Bookmark Separator > Document*.

4 From the Web Apps Client, send an email message with the scanned document as an attachment.

5 Bookmarks are applied to the delivered document to the page(s) just after the barcode sheet. Bookmark separator pages are removed in the delivered document.

Creating PDF Bookmarks for electronic documents

You can easily use attachment names as PDF Bookmarks directly within the Web Apps Client. For more information, see New Bookmark support for PDFs (3-7).

Alternatively, if you are converting multiple electronic source documents into merged PDF files and want to use the original filenames as bookmarks in the output files, you may want to set up a rule to handle this workflow.

All jobs meeting the criteria in the rule you create will be delivered as PDF with the original attachment name as bookmarks:

1 In the AccuRoute Server Administrator, create a Rule with criteria based on your needs.

2 In the **Action** tab of the **Rule Properties**, make sure that the **DataExtractor** is positioned prior to **Compose**.

3 Click **Properties**. In **Action Properties**, go to the **Job Properties** tab and click **Add**.

4 In the **Set Job Property** pop-up, add the following:

> ▸ `PDFApplyBookmarkFilenames` with a **Value** of `1`.

▸ `PDFApplyBookmarkFilenameTemplate` with a relevant filename.

5 Click **OK** three times.

6 Configure delivery for merged pdf as appropriate for your jobs.

Connectors

The **Connectors Node** has been updated with the following features:
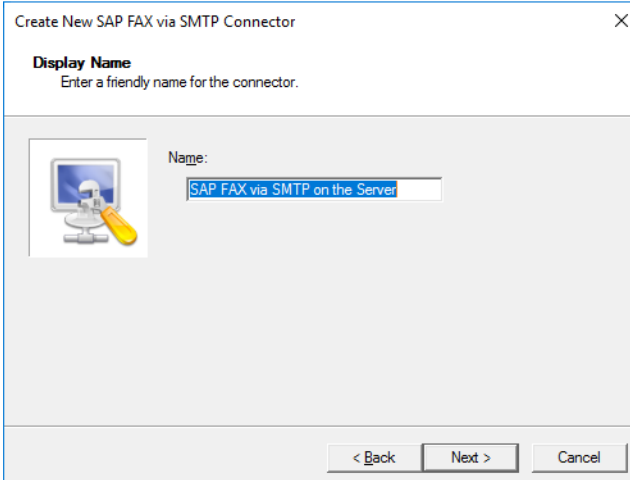
New SAP FAX via SMTP Connector

AccuRoute v5.1 introduces the new **SAP FAX via SMTP Connector**, supporting inbound and outbound faxing using SAP SMTP-based communications. The prior functionality of the SAP Connector (now deprecated) is retained in the new SAP FAX via SMTP Connector. The SAP FAX via SMTP Connector requires an SAP license.

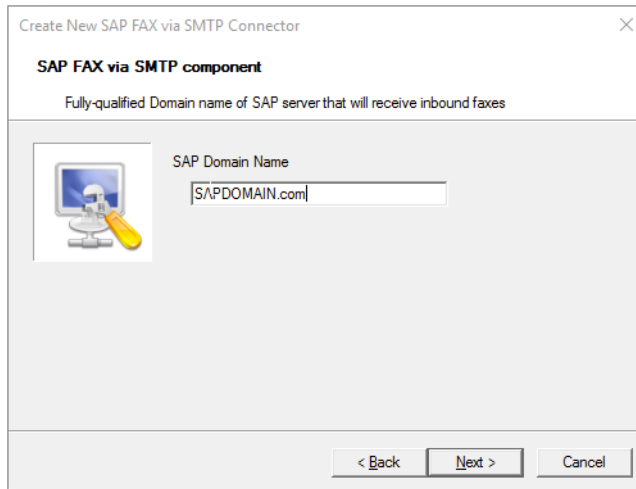> **Note** The SAP SMTP Connector does not support SAP COMServe.

To create and configure the SAP SMTP Connector:

1 Right-click **Connectors** in the console tree and select **New AccuRoute connector > SAP FAX via SMTP**. The **License** page appears. Enter your SAP license number and click **Next**.

2 The **Display Name** page appears. **SAP FAX via SMTP on the Server** appears as the default name.

Accept this or type a friendly name for this connector in the **Name** text box and click **Next**.

3 The **SAP FAX via SMTP component** page appears.

Enter the fully-qualified **SAP Domain Name** of your SAP server and click **Next**.

4 The **Congratulations** page appears. Click **Finish**. The **SAP FAX via SMTP Connector** appears in the details pane.

5 Right-click the new **SAP FAX via SMTP Connector** and select **Properties**. The **Properties for SAP FAX via SMTP on the Server** screen opens.

6 Go to the **Advanced** tab, and enter the **FAX via SMTP domain name** and click **OK**.

The **SAP FAX via SMTP Connector** is now configured.

New Secure Print Connector

AccuRoute v5.1 introduces the new **Secure Print Connector**, which works in conjunction with the **Brooksnet Remote Print Manager (RPM)** to allow users to print documents from their desktop to a local or network folder, with the intention to later access and print the documents from a device, using the **MyPrints** device button.

Note   The **Secure Print** connector is required to be able to use the **MyPrints** button. For more information on using the **MyPrints** device button, see New MyPrints device button (3-11).

In the **Secure Print Connector** workflow, users print documents from their desktop using the RPM, which stores them in a local or network folder. The **Secure Print Connector** monitors that folder and makes documents available upon request from an authenticated device user. Users can print their documents to the Secure Print folder and then later access and print them using the **MyPrints** device button.

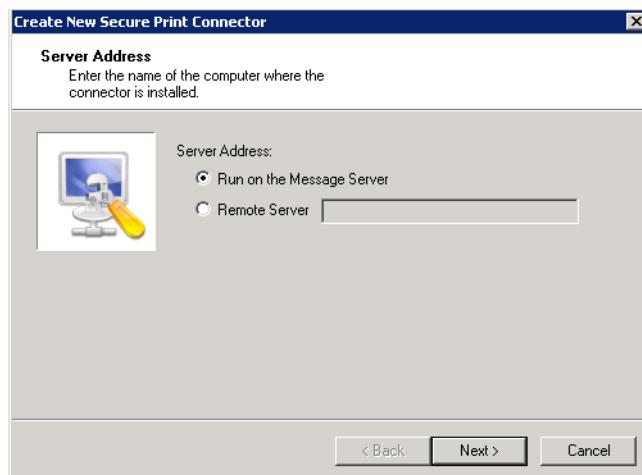The System Administrator assigns authenticated user access and configures the Secure Print connector and folder.

Setting up your system to use the **Secure Print Connector** workflow involves:

- Creating and configuring the Secure Print connector and folder (2-11)
- Installing and configuring the Brooksnet Remote Print Manager (2-16)

Creating and configuring the Secure Print connector and folder

To create and configure the **Secure Print Connector** on the AccuRoute Server:

1   Right-click **Connectors** in the console tree and select **New AccuRoute connector > Secure Print**. The **Server Address** page appears.


Select **Run on the Message Server** to locally install the connector and click **Next**.

**2**   The **Display Name** page appears. **Secure Print on the Server** appears as the default name.
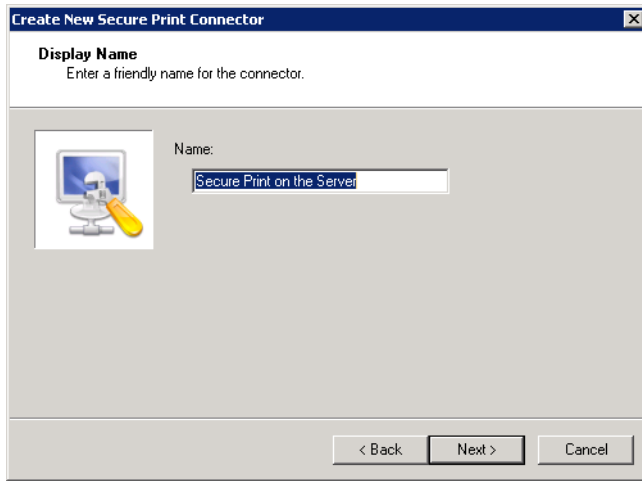
Accept this or type a friendly name for this connector in the **Name** text box and click **Next**.

3   The **Secure Print Folder** page opens. Enter the folder location you want the connector to scan for Secure Print requests, or accept the default location and click **Next**.
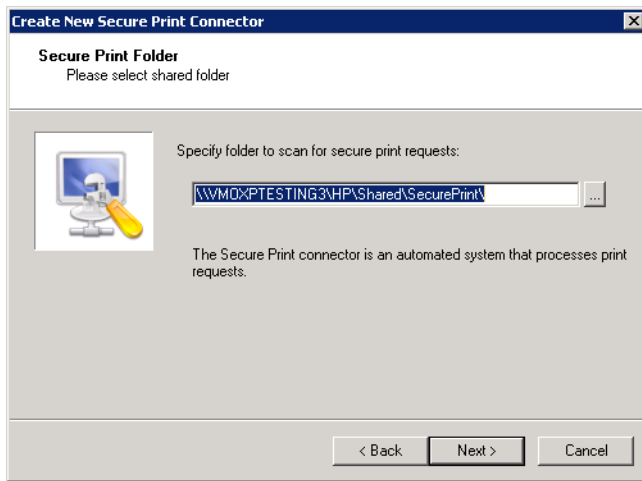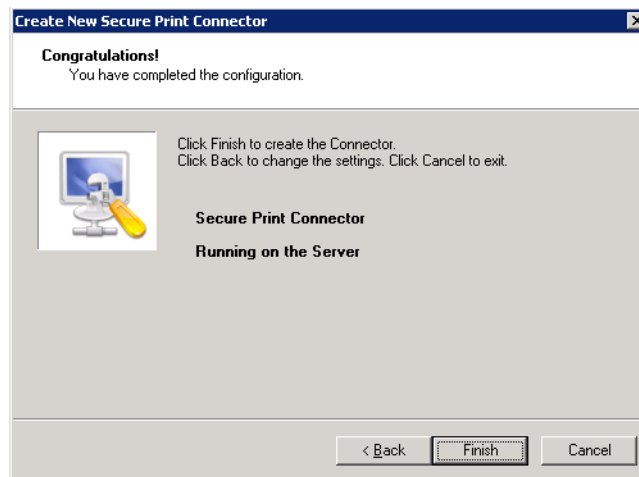
4 On the same page, you are then prompted to enter a default user email address.
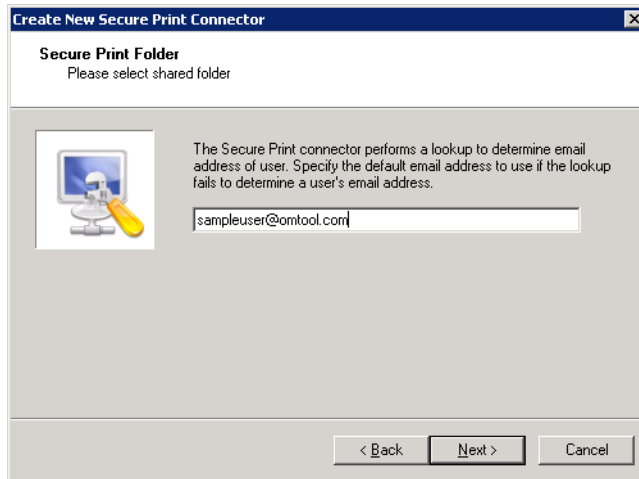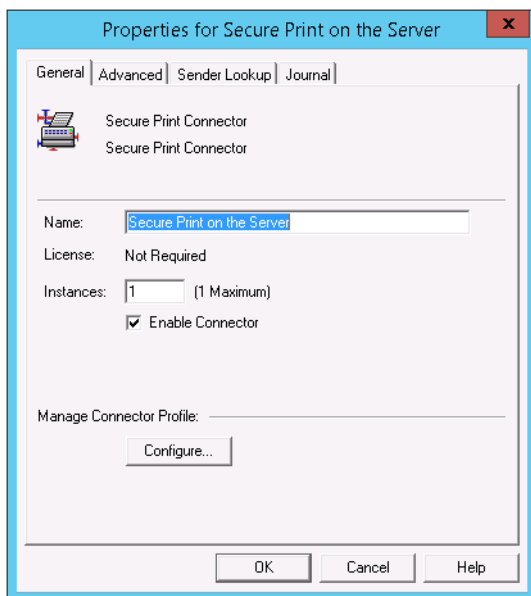

The Secure Print Connector uses the email address to associate an authenticated device user's request with the correct documents.

5 Click **Next**. The **Congratulations** page appears. Click **Finish**.

6 Right-click the new Secure Print Connector and select **Properties**. The **Properties for Secure Print on the Server** screen opens.

7 Go to the **Advanced** tab, and identify the **Secure Print Folder** location for the system to scan for files sent from the Brooksnet printer. Also enter a **Failure Lookup** email address from which any failure notifications will be sent.
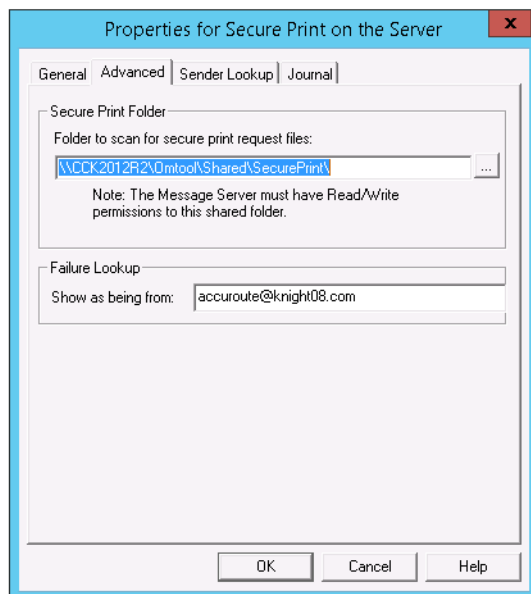
8   Go to the **Sender Lookup** tab and click **Add**. The **LDAP Properties** page appears.

Enter the **Server Address**, **Username** and **Password**.

9   Remaining on the **LDAP Properties** page, go to the **Search** tab.

Enter a **Search Base** address and click **OK**.

10   Click **OK** again. The **Secure Print Connector** is now configured.

For more information on using the **Secure Print Connector** with the **MyPrints** device button, see New MyPrints device button (3-11).

Installing and configuring the Brooksnet Remote Print Manager

The **Secure Print Connector** works together with the **Brooksnet Remote Print Manager (RPM)**. You need to install the **Brooksnet RPM** on your AccuRoute server and activate the RPM license.

> **Note**   If you plan to use AccuRoute v5.1 licensed with the Secure Print Connector, the Omtool Customer Service installation team will provide you with the necessary installation files. These will include the Brooksnet software, plus instructions to install and configure the BrooksNet RPM and to activate the RPM license.

New Bursting Connector

AccuRoute v5.1 introduces support for the new **Bursting Connector**, which provides users the opportunity to break up (burst apart) document batches. It uses bar codes on customer documents to identify and split up documents, with the ability to send documents to multiple locations. No routing sheets are required to use the **Bursting Connector**.

The **Bursting Connector** uses RuleSets to direct document delivery and can only be used with PDF files.

> **Note**   The **Bursting Connector** requires the Data Extractor License.

To create and configure the **Bursting Connector** on the AccuRoute Server:

1   Right-click **Connectors** in the console tree and select **New AccuRoute connector for > Bursting**. The **Display Name** page appears.
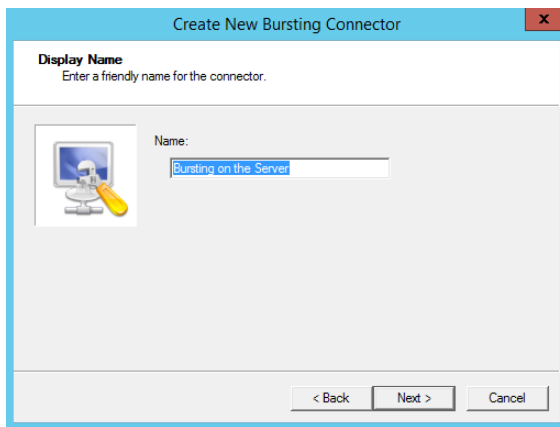
2   **Bursting on the Server** appears as the default name. Accept this or type a friendly name for this connector in the **Name** text box and click **Next**.

3   The **Route to** page opens. Select **Email** from the **Route To:** drop-down list and click **Next**.
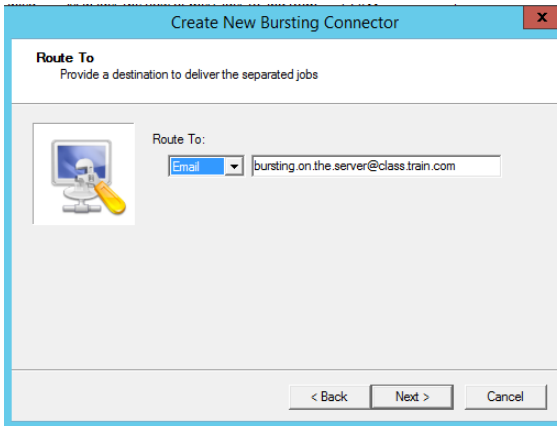
4   The **Congratulations** page appears. Click **Finish**
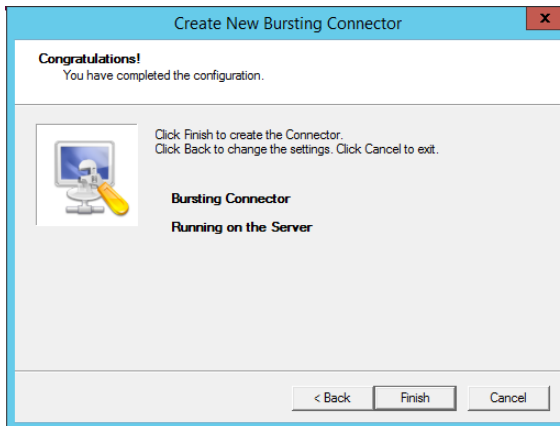
5   Right-click the new connector and select **Properties**. The **Properties for Bursting on the Server** screen opens.
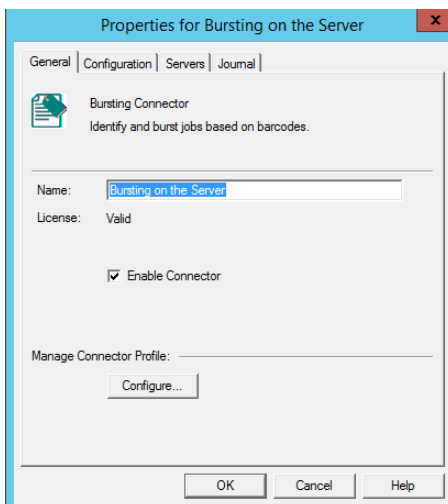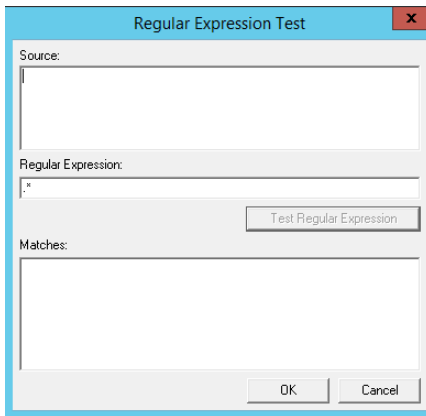
6 Go to the **Configuration** tab, select **Any barcode** and click **Properties**.
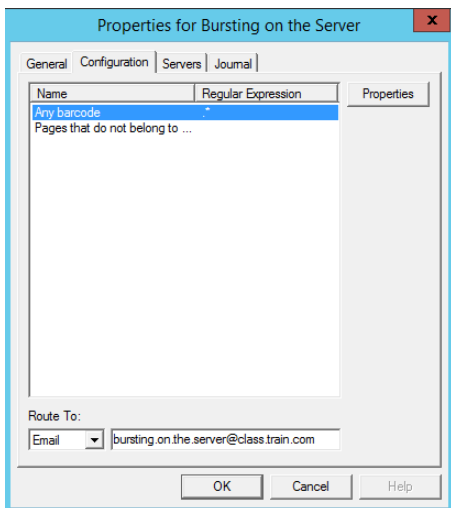
7 The **Barcode Properties** screen appears. On the **General** tab, enter `.*` as a **Regular Expression to match** and click **Test**.
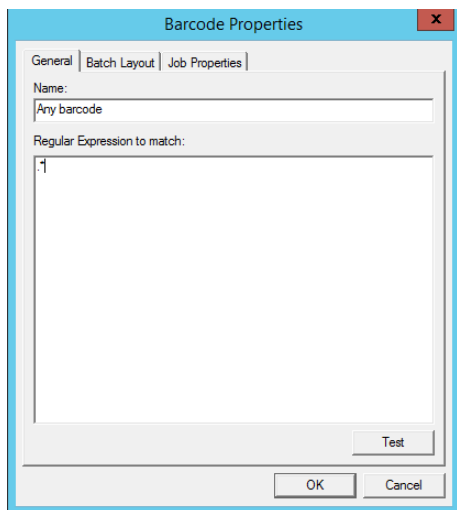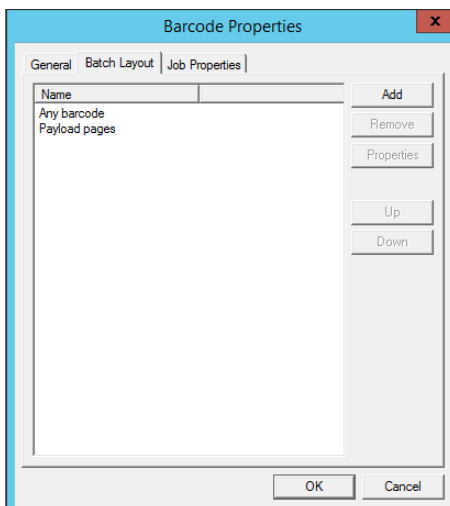
8   The **Regular Expression Test** page opens. Click **OK**.

9   Returning to **Barcode Properties**, go to the **Batch Layout** tab.

10   Select **Any barcode** and click **Add**. The **Barcode Page** pop-up screen appears. You can change the **Name** if you want and click **OK**.

11 Select **Payload pages** and click **Add**. The **Payload Pages** pop-up screen appears.
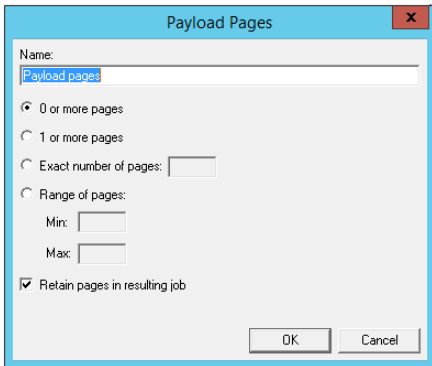
12 You can change the **Name** if you want. Select **0 or more pages** and **Retain pages in resulting job**. Click **OK**.

13 Returning to **Barcode Properties**, you can add any Job Properties you want to use on the **Job Properties** tab.
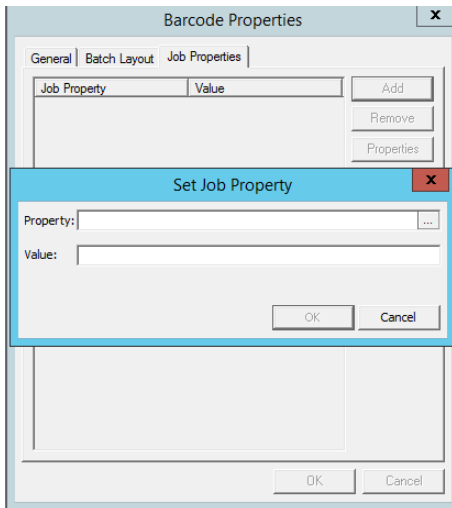
14 Click **OK**. You are returned to the **Properties for Bursting on the Server** screen. Make sure your **localhost** is selected on the Servers tab.
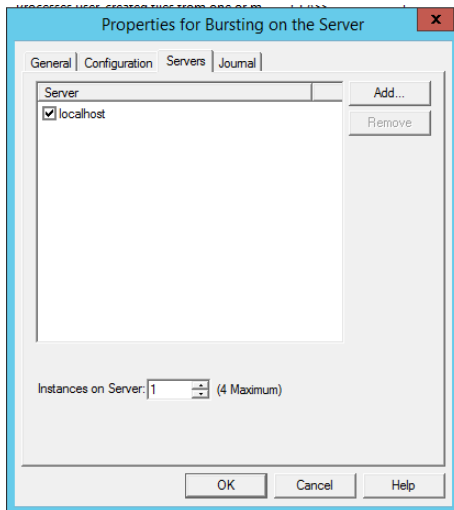
15 Click **OK**. The **Bursting Connector** configuration is ready for use.

New NetDocuments Connector Features and Updates

With AccuRoute v5.1, the **NetDocuments Connector** now supports a workflow for Workspace Cabinet delivery and updates Volume List delivery. The **NetDocuments Connector** authorization process has also been updated. For more information, continue with:

- [Authorization](#)
- [Workspace delivery](#)
- [Volume List delivery](#)

Authorization

The **NetDocuments Connector** configuration screens have changed since the prior release. During the process, you now must authorize AccuRoute with NetDocuments to allow AccuRoute access to your NetDocuments account. After installing the connector, the DMS configuration wizard launches. Use the following steps for configuration:

1 When the DMS configuration wizard opens the **NetDocuments Login Configuration** screen, click the **Authorize** button.
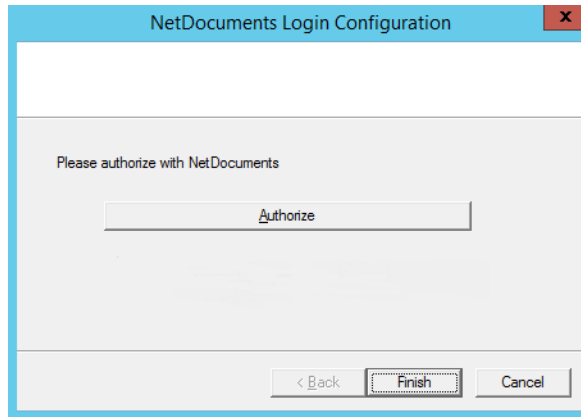
2 An Internet Explorer **Authorization** screen appears. Login to Net Documents with the **username** and **password** with which you will access NetDocuments. Make sure this user has all the rights required to deliver to the necessary Folders and Workspaces.
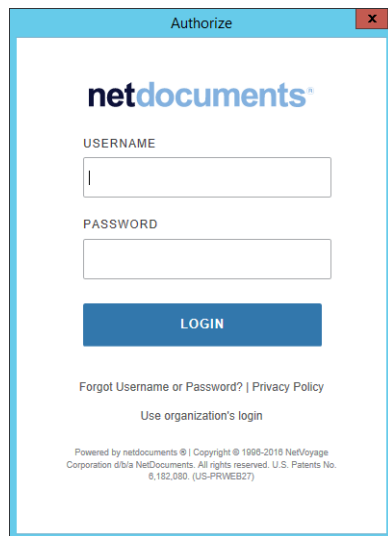
3   After the first time you authorize NetDocuments and successfully login, the following **Authorize**
        screen appears.
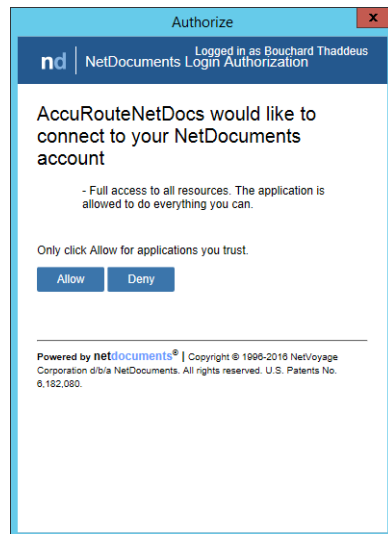
        Click **Allow**.

4   When the **NetDocuments Login Configuration** screen appears again, click **Finish**.
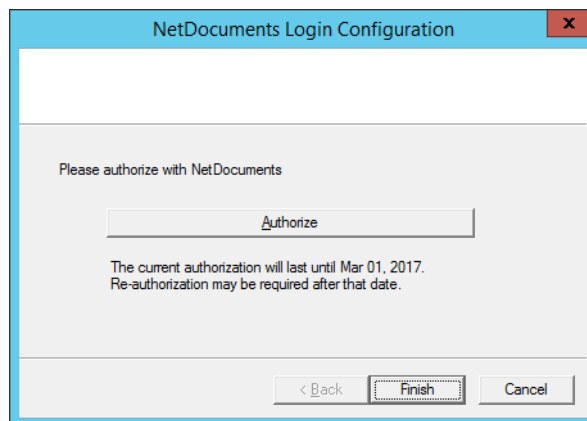
Note   NetDocuments authorizations last one year. After a year, the authorization process needs to take place
            again.

Workspace delivery

With AccuRoute v5.1, the **NetDocuments Connector** now delivers to Workspaces as well as Folders.

To do so, you need to configure a RuleSet to route messages to NetDocuments Workspace. Configure the RuleSet's **Action Properties** as follows:
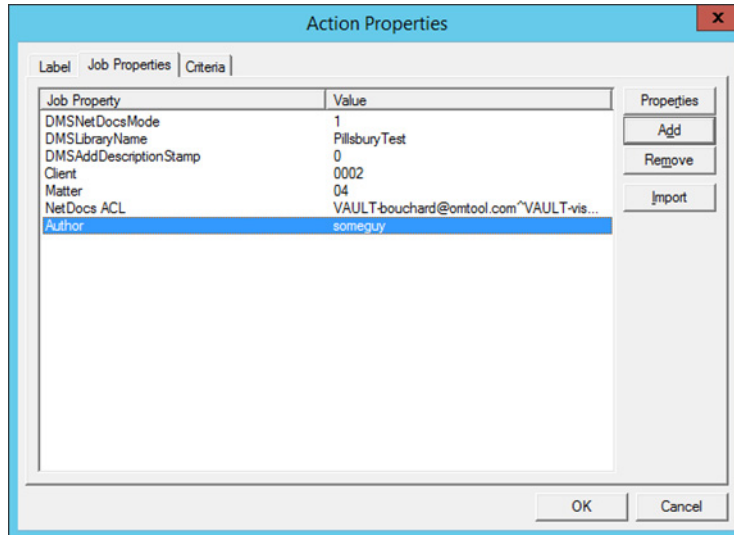
- **DMSNetDocsMode** — Set this property to 1 to allow for Workspace filing to NetDocuments.

- **DMSLibraryName** — Set this property to the name of the cabinet to which you are delivering.

- **DMSAddDescriptionStamp** — Set this property to 0 if you do not want a time stamp appended to the filename.

- **Client** and **Matter** — You need to create the **Client** and **Matter** User Properties in AccuRoute. Setting the proper **Client** and **Matter** in the rule assures your delivery goes to the correct Workspace.

> **Note**   Your organization may have named your **Client** and **Matter** properties something else (for example, **Customer** and **Item**). If so, the Parent and Child properties created in NetDocuments for the cabinet require matching User Properties in AccuRoute. Use them in the rule in place of **Client** and **Matter**.

- All the other properties are custom DMS properties that must match NetDocuments properties. In the example above, **Author** needs to be a custom property and must match (spelling and case) an existing NetDocuments property in order for that data to get into the job when delivered to c. You can add as many custom properties as you like, as long as they have matching properties configured in NetDocuments for cabinet delivery.

> **Note**   If you set an invalid value in any of the fields in which only certain values are valid, subsequent delivery will fail.

The user associated with the **NetDocuments Connector** has full rights to documents delivered to Workspaces. All other users have cabinet-level default rights. However, you can provide full rights to additional NetDocuments users. This only works in Workspace mode. You will need to know the NetDocuments IDs of the relevant users.

1 Create a User Property called `NetDocs ACL` (include the space).

2 **Add** the `NetDocs ACL` User Property as an additional property to the rule described above.

3 Define the value of the property to be all the additional NetDocuments User IDs whom you want to have full access (VESA) to the document. Separate each User ID with a "^". For example:

`IE "VAULT-rouchard@omtool.com^VAULT-mish@omtool.com"`

NetDocuments User IDs are not always based on email addresses. You may need to contact NetDocuments to find out the User ID for a given user.

Volume List delivery

To configure Volume List delivery for the **NetDocuments Connector**:

1 Install a recent version of Internet Explorer.

2 Log in to NetDocuments and install the NetDocuments ActiveX Control.

3 Add a new NetDocuments Volume List.

4 Configure the **NetDocuments Connector** by clicking the **Configure** button and authenticating.

5 Create a new Default Profile, browsing to the folder where you want to store documents.

Note This process does not use the default profile, but Volume Lists require one be created.

---

6 Add any properties you want to index to the **Index** tab.

7 The **DateCreated**, **GUID**, and **SequenceID** properties should appear by default. If they do not auto-populate, exit the tab and return. They will appear.

8 In the **Groups** node, navigate to **Clients > Volume Lists** and enable **Searching** for the NetDocuments Volume List.

9 In the **Search** tab, add the indexed properties for which you want to search (**DateCreated**, **GUID**, etc).

10 Add a **Volume List Connector**, selecting the **NetDocuments Volume List** to which you want to route.

11 Open an Internet Explorer browser and login into NetDocuments. Browse to the folder where you want to store documents.

12 Click the **Folder Options** button on the right and select **All information**. Make note of the folder's ID, as shown in the following screen.
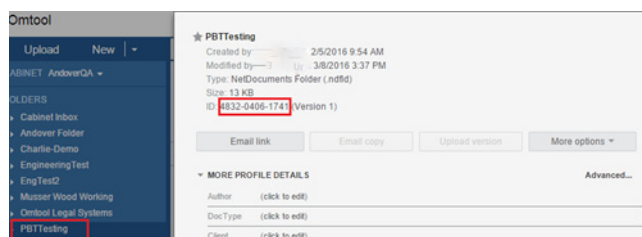
13 Create a RuleSet routing to the Volume List Connector.
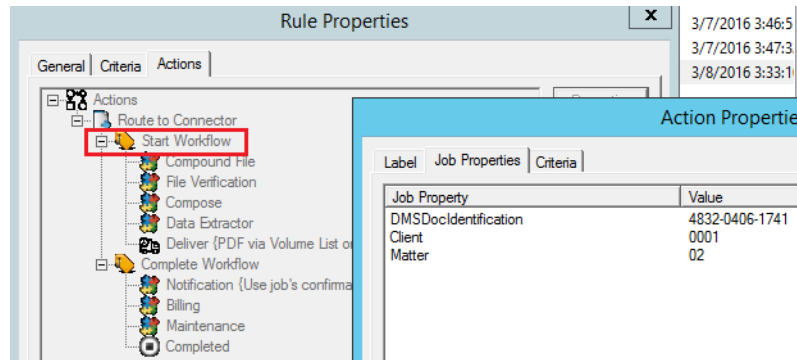
a In **Rule Properties**, at the Start Workflow node, add the property **DMSDocIdentification** in **Action Properties** and enter the Folder ID you noted in the step above.

b Add **Client** and **Matter** properties here as well, if they are being used.

c Set the routing rule to compose to **PDF** in the Deliver node.

14 Test sending messages via this routing rule. The system should deliver Messages to the folder. You should be able to see and preview them in Web Apps.

Note The steps above replace descriptions of Volume List Delivery in prior releases.

RuleSets

AccuRoute v5.1 updates the **RuleSets Node** with the following features:

- Rules Node renamed RuleSets (2-26)
- New Rule destinations (2-27)
- Customizing RuleSet workflows (2-31)

Rules Node renamed RuleSets

With AccuRoute v5.1, the **Rules** Node has been renamed **RuleSets**. Outbound Rules are now called Default RuleSets.

Note Note: Routing Rule functionality from prior releases is retained with RuleSets.

The following RuleSet categories are automatically created at installation:

- **User RuleSets** - for user-customized rules
- **Default RuleSets** - previously-named Outbound Rules
- **Received Faxes RuleSets** - RuleSets for Inbound Faxes to match

New Rule destinations

With new Rule destinations available, administrators now have more flexible options for document routing. These destinations include Route to Connector, Route to Embedded Directive Manager, Route to Failure, Route to Lookup, and Advanced Routing.

For steps on creating (or disabling) Rules using these destinations, go to:

- [Creating a Rule with Route to Connector](#) (2-27)

- [Creating a Rule with Route to Embedded Directive Manager](#) (2-28)

- [Creating a Rule with Route to Failure](#) (2-29)

- [Creating a Rule with Route to Lookup](#) (2-29)

- [Creating a Rule with Advanced Routing](#) (2-30)

- [Disabling a RuleSet](#) (2-31)

Creating a Rule with Route to Connector

1   In the AccuRoute Server Administrator, to create a Rule, navigate to the **RuleSets** Node.

2   Right-click a Rule category, for example, **Users** and select **New > Route to Connector** from the drop-down menu. The **Criteria** screen appears.
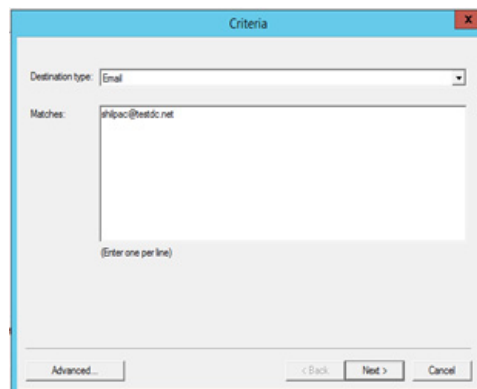
3   On the **Criteria** screen, enter

Destination type: Email
Matches: user@testdc.net

4 Click **Next**. On the **Deliver** screen, select the **Connector** of choice and a **Format**, then click **Next**.
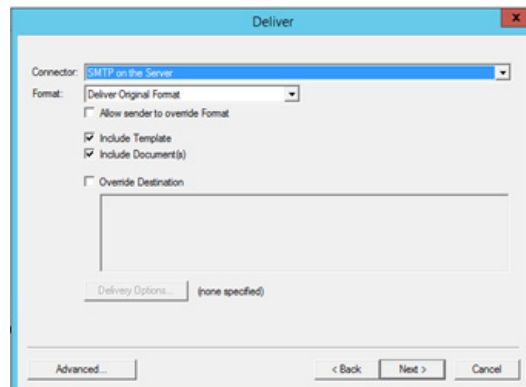
5 The **Full Name** of the Rule appears on the **Complete** screen.
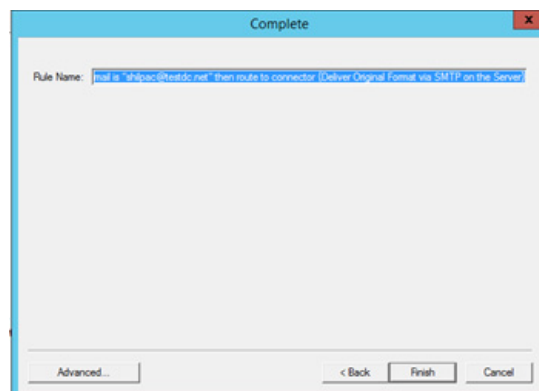
6 Click **Finish**. The newly-created Rule appears in the Administrator.
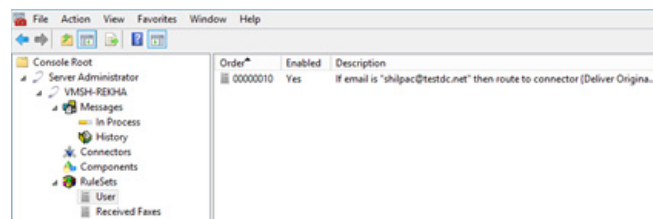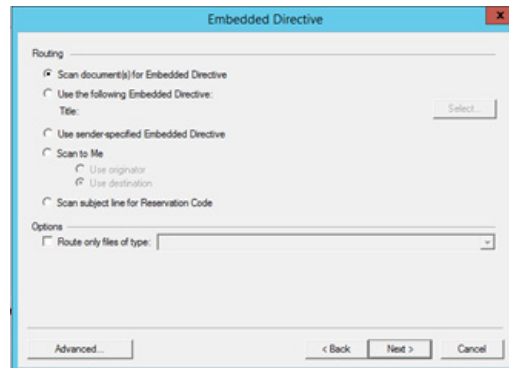
Creating a Rule with Route to Embedded Directive Manager

1 Open the **RuleSets** Node, right-click **Users** (or another rule category) and select **New > Route to Embedded Directive Manager** from the drop-down menu.

2 The **Criteria** screen appears. Enter the following fields and click **Next**.

Destination type: Email
Matches: *user@testdc.net*

3   The **Embedded Directive** screen appears.

Select **Scan document(s) for Embedded Directive** or another choice as needed, and click **Next**.

4   The **Full Name** of the Rule appears on the **Complete** screen. Click **Finish**. The newly-created Rule appears in the Administrator.

Creating a Rule with Route to Failure

1   Open the **RuleSets** Node, right-click **Users** (or another rule category) and select **New > Route to Failure** from the drop-down menu.

2   The **Criteria** screen appears. Enter the following fields and click **Next**.

     Destination type: Email
     Matches: *user@testdc.net*

3   The **Full Name** of the Rule appears on the **Complete** screen. Click **Finish**. The newly-created Rule appears in the Administrator.

Creating a Rule with Route to Lookup

1   Open the **RuleSets** Node, right-click **Users** (or another rule category) and select **New > Route to Lookup** from the drop-down menu.

2   The **Criteria** screen appears. Enter the following fields and click **Next**.

     Destination type: Email
     Matches: *user@testdc.net*

3 The **Lookup** screen appears.
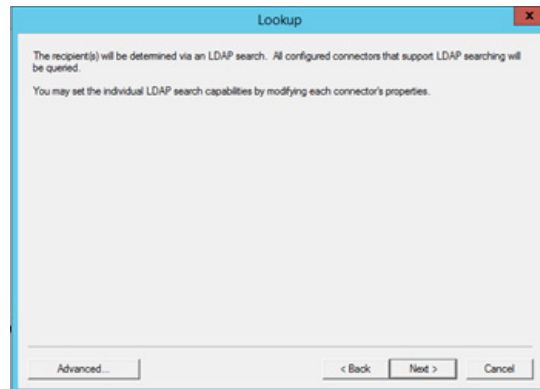
Click **Next**.

4 The **Full Name** of the Rule appears on the **Complete** screen. Click **Finish**. The newly-created Rule appears in the Administrator.

Creating a Rule with Advanced Routing

1 Open the **RuleSets** Node, right-click **Users** (or another rule category) and select **New > Route to Advanced Routing** from the drop-down menu.

2 In the **Rule Properties** screen, select the **Actions** tab.

3 In the **Actions** tab, select **Actions** and click **Add**.

4   Select **Route to Connector > Deliver {Not Configured}**.
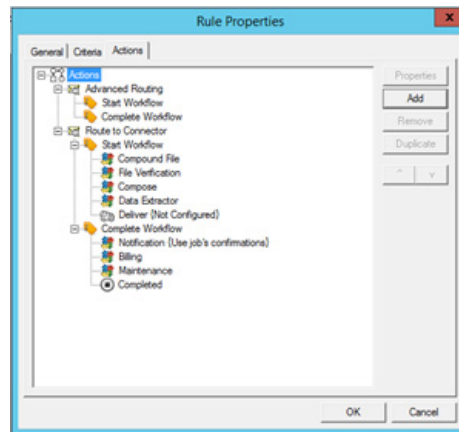
5   The **Action Properties** screen appears.
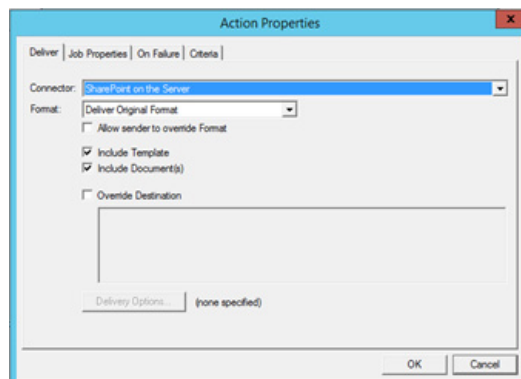
Select **SharePoint on the Server** (for example), from the **Connector** drop-down menu.

6   Click **OK** twice. The newly-created SharePoint Rule appears in the Administrator.

Disabling a RuleSet

When they are empty of Rules, you can delete user-created RuleSets. For example, if you created a RuleSet named Accounting, to remove it you would right-click **RuleSets > Accounting** and select **Delete**.

Customizing RuleSet workflows

AccuRoute v5.1 RuleSets offer administrators more opportunities to customize and interact with their system's workflow. For example, you can configure non-linear processing by defining the order in which Rules are applied. You can also configure criteria to be met in order to send or disable user notifications. For more information, see

-

-

Defining processing order for Rules

The system processes Rules according to how they are arranged on the screen.

- To move a Rule up in the list, right-click the Rule of interest and select **Move Up**.
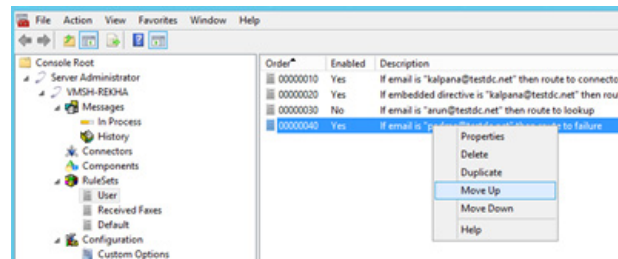
The Rule moves up the list.
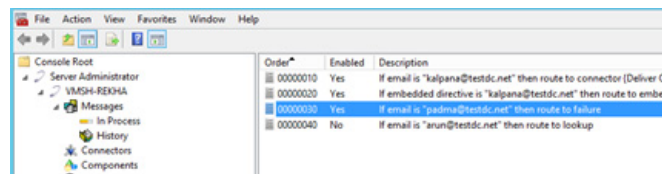
- To move a Rule down in the list, right-click the Rule of interest and select **Move Down**. The Rule moves down the list.

Adding notifications to the workflow

To enable notifications associated, for example, with a Route to Failure rule, first create the rule (see Creating a Rule with Route to Failure). Continue with the following steps:

1   In the **RuleSets** node, double-click the Route to Failure rule of interest. The **Rule Properties** screen appears.

2   In the **Actions** tab, select **Notification {Replace job's confirmations with:}** and click **Properties**.
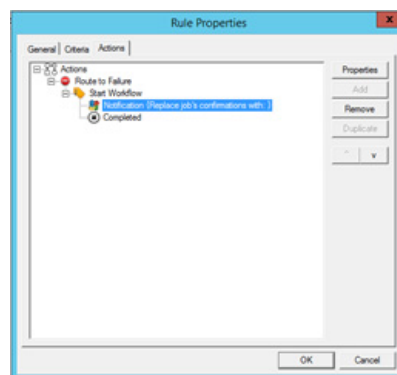
3   The **Action Properties** screen appears. Select **Replace the job's confirmations with the following** and click **Add**.
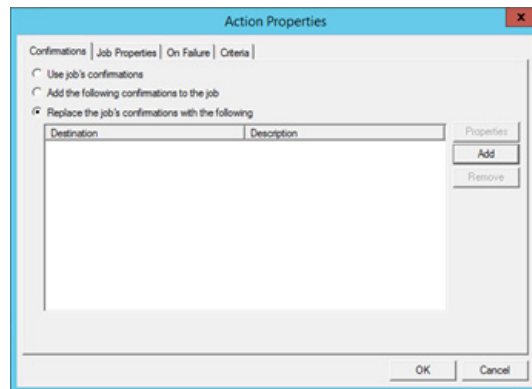
4   In the **Confirmation Destination** screen, select **Email** from the confirmation destination drop-down menu and enter *user@testdc.net*.
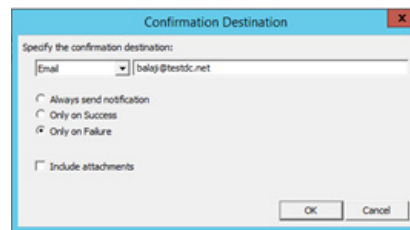
5   Click **OK**. Returning to the **Action Properties** screen, the user's email now appears in the **Destination** list. Click **OK**.
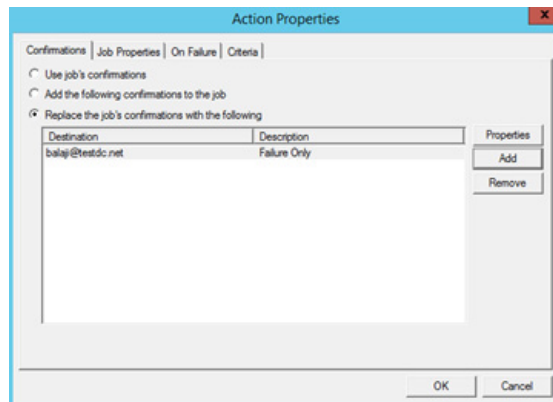
Notifications are now enabled for the selected Rule.

Configuration

The **Configuration Node** has been updated with the following features:

New Table format for User Job Properties

Administrators can collect multiple Job Properties together to create a single **Table User Job Property**.

To create a **Table Job Property**:

1 Navigate to **Configuration > Job Properties**. Right-click **User** and select **New > Job Property**. The **Job Property** screen opens.
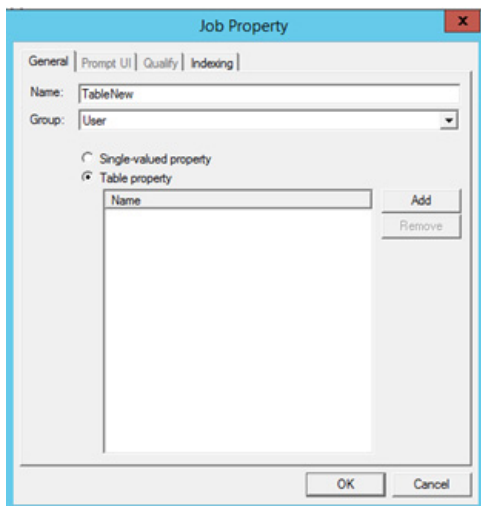
2 Enter a **Name** for the new Table Property, and then select **Table property**.

3 To add a list of the properties you want included in your table, click **Add**.

4   In the **Select Job Property** screen, select a **Job Property** from the list and click **OK**.
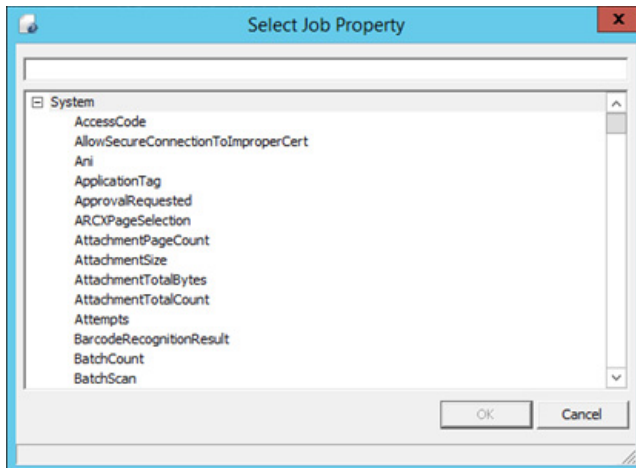
The property is added to the Table property. Continue to **Add** Job Properties as needed.
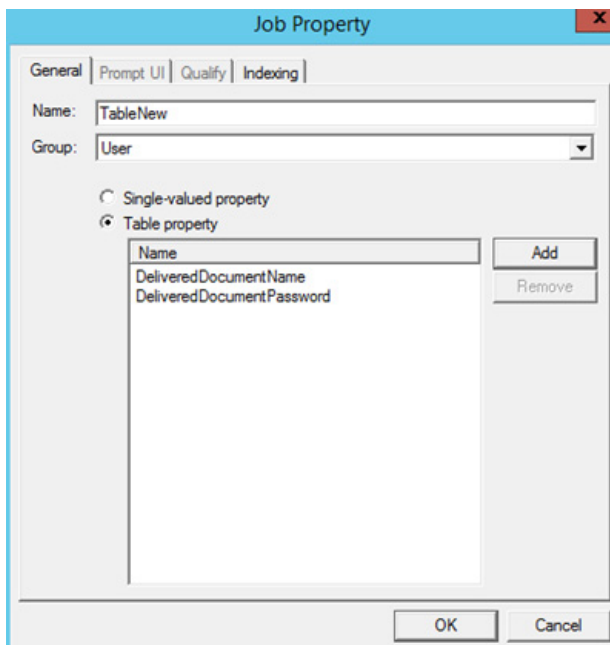
5   When you are finished, click **OK**.

New Job Property Lookups

System Administrators can now configure Job Properties for **Database Lookup** and **List Lookup**. For more information, continue with

- [Configuring a Job Property for Database Lookup](#)
- [Configuring a Job Property for List Lookup](#)

Configuring a Job Property for Database Lookup

1 Execute a Query for the property to be created in the AccuRoute Server and add some values in your SQL Database.
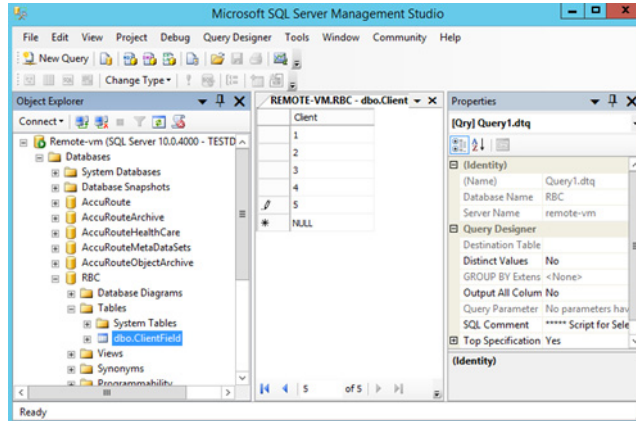
2 In the AccuRoute Server Administrator, navigate to **Configuration node > Job Properties**. Right-click **User** and select **New > Job Property**.

3 In the **Job Properties** screen, enter a **Name** and go to the **Qualify** tab. Select **Database (ADO)** from the **Lookup** drop-down list.
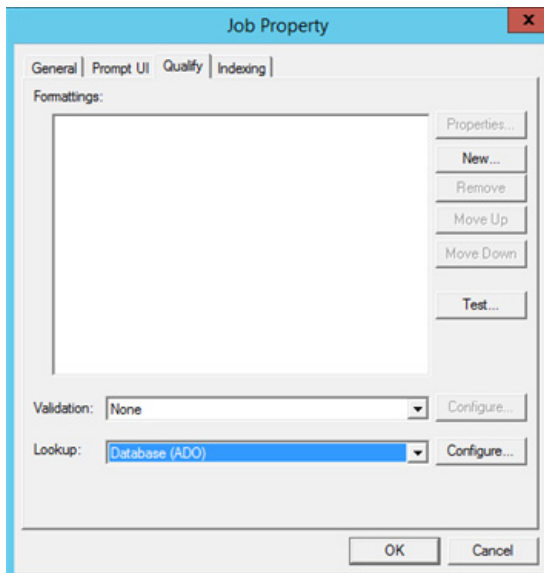
4   Click **Configure**. In the **Lookup Properties** screen, enter **DSN** and **Query** details.
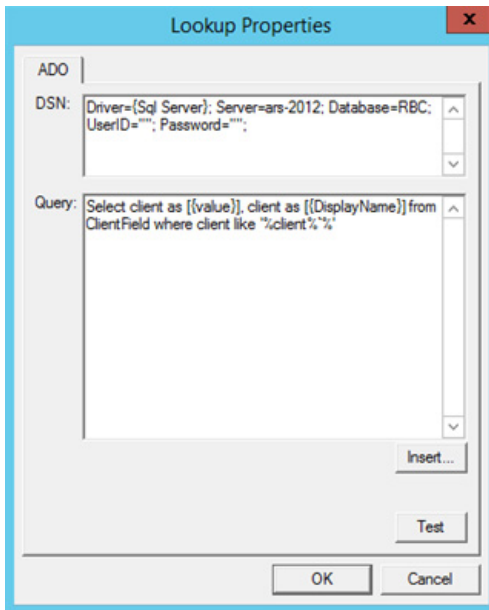
5   Click the **Test** button. The **Test Lookup** screen appears. Enter a value for **Client** (that is present in the database) and click **Test**. The value is returned, and Lookup performs correctly.
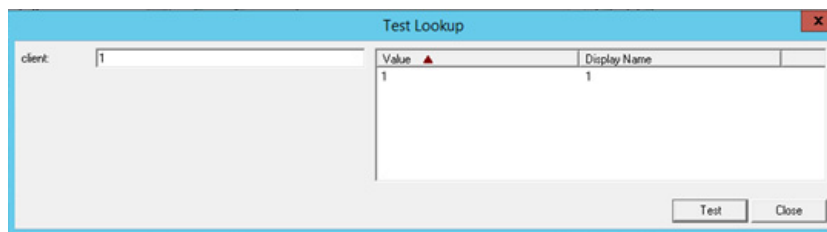
6   Click **Close** and then click **Ok** twice.

The **Client Property** is now configured for **Database Lookup**.

Configuring a Job Property for List Lookup

1   In the AccuRoute Server Administrator, navigate to **Configuration node > Job Properties**. Right-click **User** and select **New > Job Property**.

2   In the **Job Properties** screen, enter a **Name** and go to the **Qualify** tab. Select **List** from the **Lookup** drop-down list.
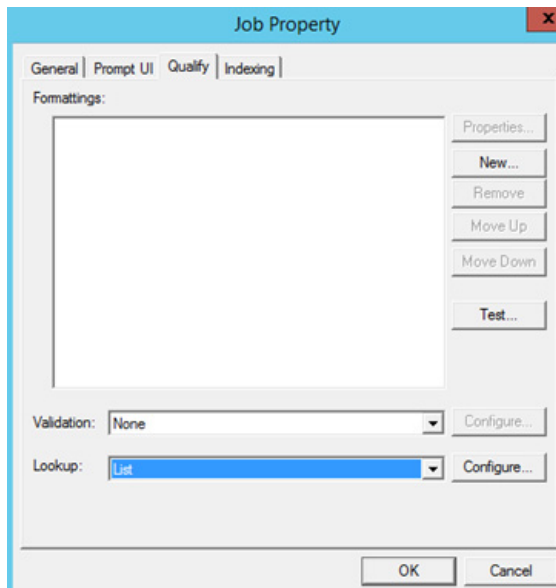
3   Go to the **Prompt UI** tab. Click **New** and add the list of properties.
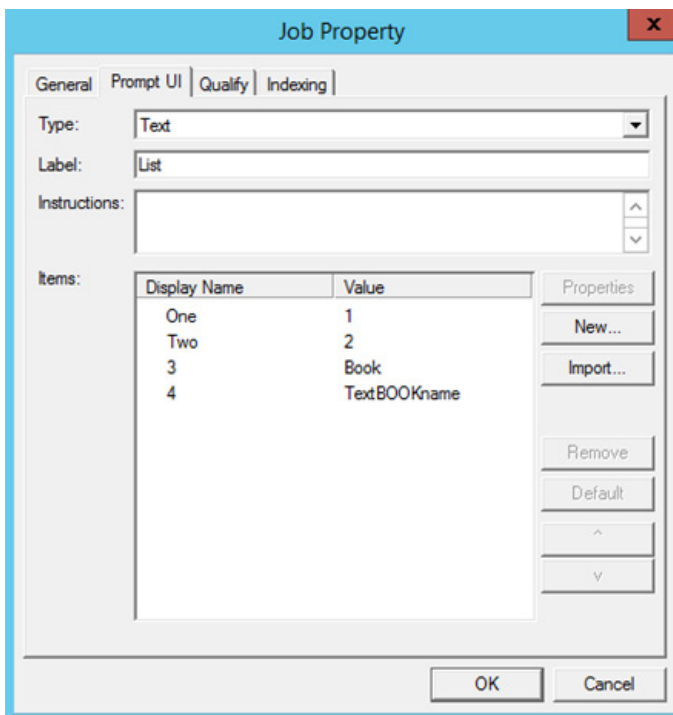
4   Click **OK**.

The **List Property** is now configured for **List Lookup**.

For more information about using Database and List Lookups on the clients, see

- Web Apps End User Interface New Job Property Lookups (3-8)

- Device Client New Job Property Lookups (3-14)

New Folder Destination Type: Microsoft® OneDrive® for Business

System Administrators can now configure and assign MS OneDrive for Business Folder access to authorized End User Interface Web Apps and Device Client user groups.

To configure MS OneDrive for Business in the AccuRoute Server Administrator:

1   Navigate to **Configuration > Folders**. Right-click **Folders** and select **New > OneDrive**. The **Folder Properties** screen opens.
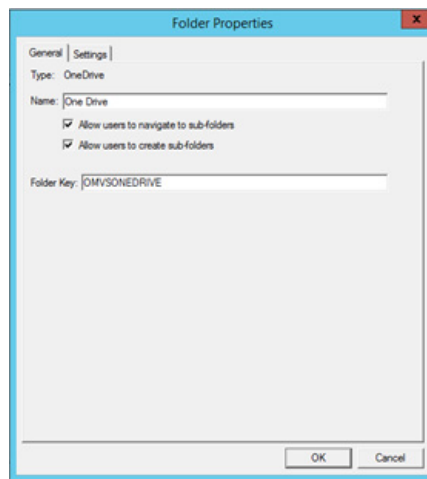
2   In the **Settings** tab, select **OneDrive for Business**. Enter your **Tenant Name** and **Client ID** and click **OK**.
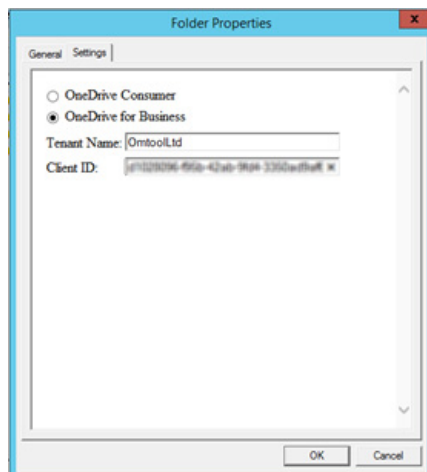
3   Open the **Groups** node and double-click the Default group. The **Group Properties** screen appears. In the **Jobs** section, select **Folders**.
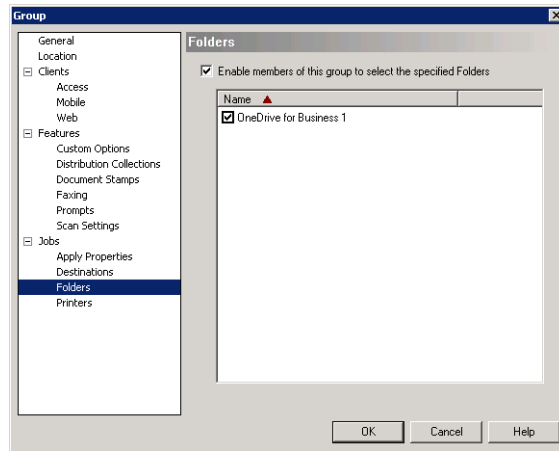
4   Click the **Enable members of this group to select the specified Folders** box and then select the OneDrive Folder of interest. Click **OK**.

5   Open the **Devices** node. Right-click the device of interest and select **Properties**. The **Device Group Properties** screen appears.

6   On the **Buttons** tab, click **Add** and select **Scan to Folder** from the drop-down list on the pop-up. Also enter a **Name** for the new button.
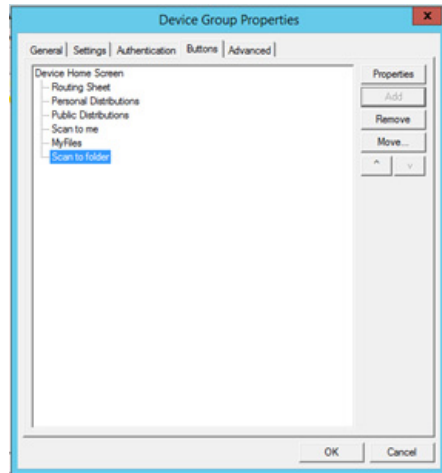
7   With **Scan to Folder** still highlighted, click **Properties**. The **Button Properties** screen appears.
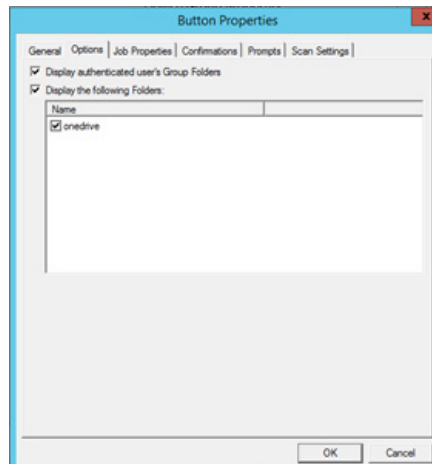
8   In the **Options** tab, select **Display authenticated user's Group Folders** and click **OK**, and **OK** again.

New Folder Destination Type: WebDav

System Administrators can now configure and assign Web Distributed Authoring and Versioning (WebDav) Folder access to authorized End User Interface Web Apps and Device Client user groups.

With WebDav already configured on the AccuRoute Server, follow these steps to enable WebDav in the AccuRoute Server Administrator and Web Apps:

1 Open the AccuRoute Server Administrator and go to **Configuration > Folders**. Double-click the WebDav Folder. The **Folder Properties** screen opens.
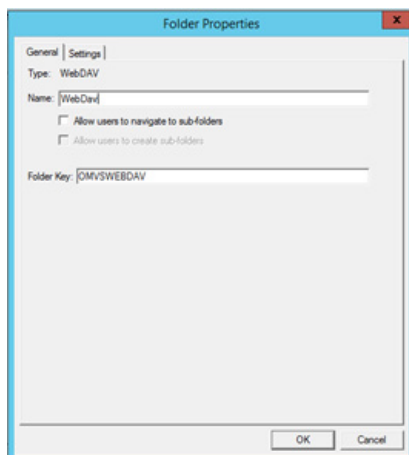
2 In the **Settings** tab, for the **WebDAV URL** field, enter your details, for example: `http://servername/webdav`.
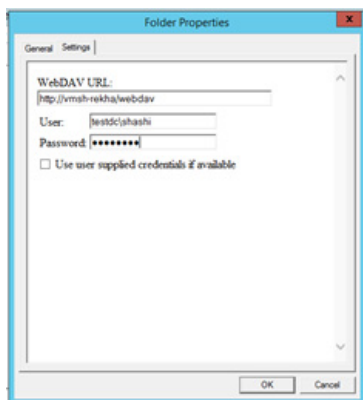
Click **OK**.

3   To enable the added Folder, open the **Groups** node and double-click the **Default** Group.
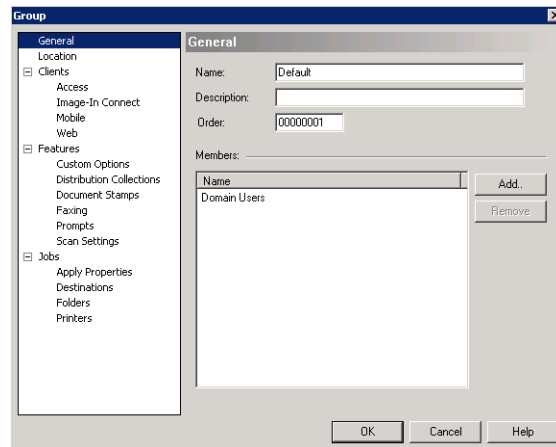
4   The **Group Properties** screen appears. In the **Jobs** section, select **Folders.**
Click the **Enable members of this group to select the specified Folders** box and then select
the WebDav Folder of interest. Click **OK**.

5   Open the **Devices** node. Right-click the device of interest and select **Properties**. The **Device Group Properties** screen appears.

6   On the **Buttons** tab, select **Scan to Folder** and click **Add**.
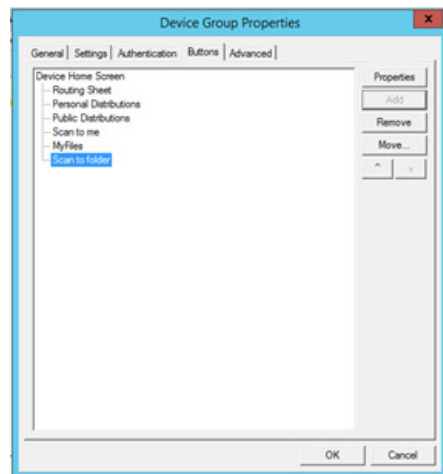
7 With **Scan to Folder** still highlighted, click **Properties**. The **Button Properties** screen appears.
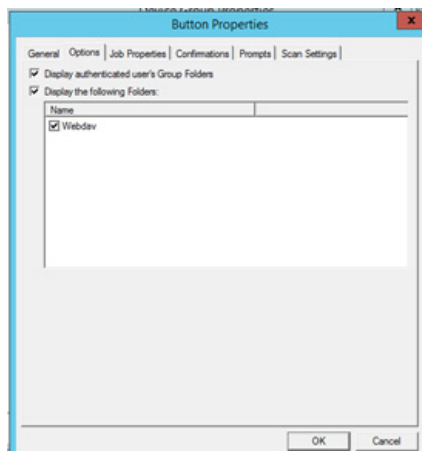
8 In the **Options** tab, select **Display authenticated user's Group Folders** and click **OK**, and **OK** again.

New Search Filters Node

From the **Search Filters** node, you can configure customized message searches using a wide assortment of message meta-data criteria.
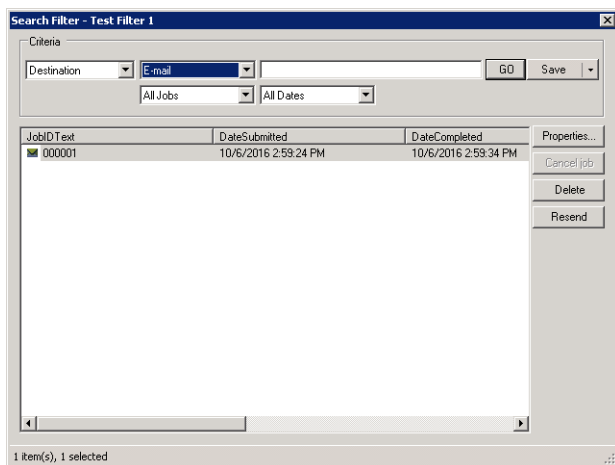
To create a new **Search Filter**:

1 In the AccuRoute Server Administrator, go to the **Configuration** node and right-click **Search Filters > New > Search Filter**. The **Search Filter** screen appears.

2 Select the **Criteria** of interest from the drop-down lists. As you select criteria, other fields on the screen adjust to offer relevant options for further specification.

For example, if you initially select **Destination** and then **E-mail**, you can enter a specific E-mail address.

In addition, you can narrow searches by Job type and/or Dates.

3 With your preferred criteria selected, click **GO**. Search Filter results appear below the **Criteria** section. From the results you can review message Properties, cancel a job, and Delete or Resend messages.

4 Once a Search Filter is created, click the **Save** button to retain it for future use.

The **Search Filters** screen can also be accessed at the **Messages** node, to filter all messages, or for either the **In Process** Queue or **Message History**.

New Web Apps Node

Web Apps is the new highly-customizable replacement of the former Web Client. In the Server Administrator, you can assign Applications (such as Inbox, Create Distribution, etc.) to customized Web Apps Profiles, which are in turn associated to specific user groups, defining what Web Apps users will see.

To create a new **Web Apps Profile**:

1 In the AccuRoute Server Administrator, go to the **Configuration** node and right-click **Web Apps > New > Profile**. The **New Profile Properties** screen appears.
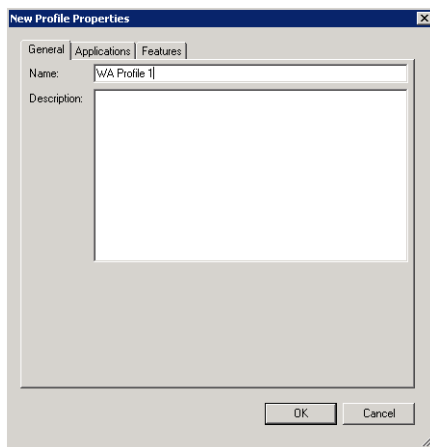
2 Enter a profile **Name**, and optionally, a **Description**.

3 Go to the **Applications** tab, click **Add** and (one at a time) select the applications of interest from the various options in the drop-down menu.
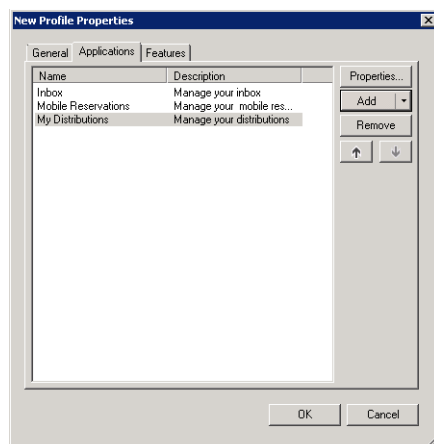
4 For example, click **Add > Messages > Inbox**. The **Inbox Application Properties** screen opens. Here you can further refine specific Inbox properties as needed.
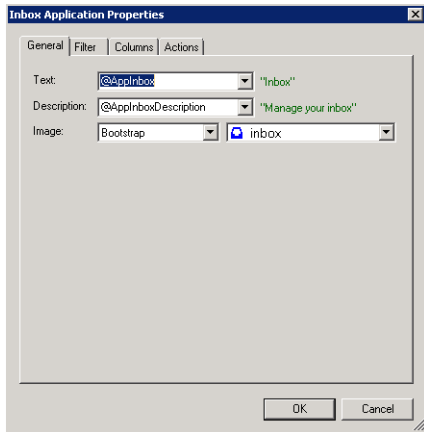
5 Click **OK** to exit the application **Properties** screen. When you return to the **New Profile Properties** screen, you will see the selected Application added to the list.

6 In the **Features** tab, click **Add** and select any Feature you want to associate with the Profile. Options include: **DocumentLink**, **Favorites**, **PrintToWeb**, **ScanToWeb**, and **SendToWeb**.
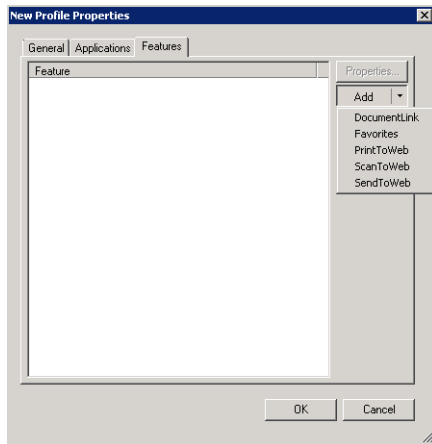
7 As it does with Applications, a **Properties** screen appears for any Feature you select. You can further refine a Feature's characteristics in its **Properties** page.
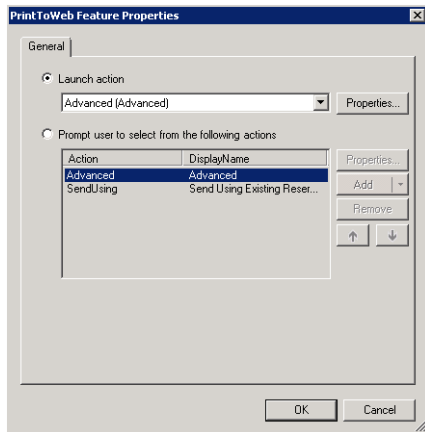
8 Click **OK** to exit the **Features Properties** screen, and click **OK** again.

9 Your new profile appears in the Web Apps list.

To edit properties of an existing Profile, right-click the profile of interest and select **Properties** to access **Profile Properties**.

To add a Web Apps Profile to a User Group:

1 Go to **Configuration > Groups**, right-click the group of interest and select **Properties**.

2 In the **Group Properties** screen, click **Clients > Web**.
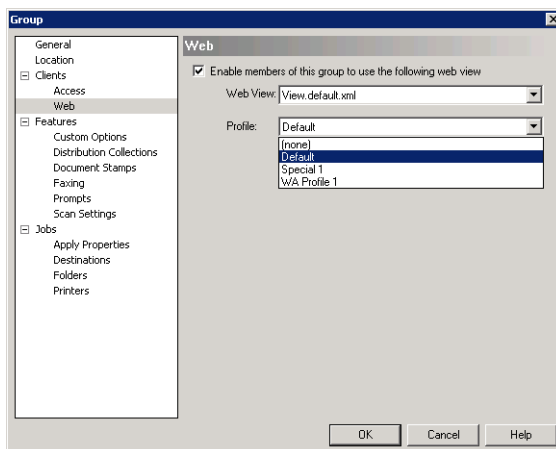
Make sure **Enable members of this group to use the following web view** is selected.

3 Click the **Profile** drop-down list and select the Profile of interest. Click **OK**.

The user group is now updated to use the new Profile in Web Apps.

Web Client Node renamed Legacy Web Views

The Configuration Node for the prior End User Interface, Web Client, has been renamed Legacy Web Views.

> **Note** The Legacy Web Views Node remains the location to configure the Legacy Web Client with access to the Help Desk, Archive Search, Deficiencies, and approval.

New Scan Settings default options in Group Properties

AccuRoute v5.1 provides new Scan Settings for administrators to apply as user group default settings.

> **Note** Scan Settings options vary by device type and may include, for example: Blank Image Removal, Contrast, Darkness, Media Size, and Quality Mode.

To enable or define specific Scan Settings for a selected User Group:

1 In the AccuRoute Server Administrator, go to **Configuration > Groups**, right-click the Group of interest, and select **Properties**.

2 The **Group Properties** screen appears. In the **Features** section, click **Scan Settings**. In the right-hand pane, you will see the range of Scan Settings available for the selected group.

3 Click to open the Setting of interest and select the appropriate box to set a default value.
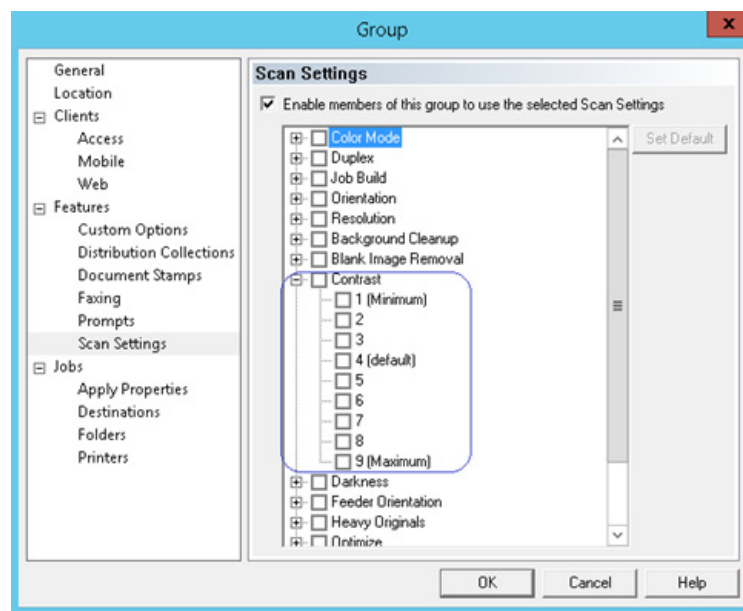
For example, if you pick **Contrast**, a range (1 - 9) of values appear. The values you select will be available for scans made by users in the selected group.

You can set a value as the default using the **Set Default** button.

4 When you have finished with **Scan Settings**, click **OK**.

> **Note** The **Scan Settings** tab in **Button Properties** is the new location of the **Job Build** mode setting. On the **Scan Settings** tab, you can enable or disable **Job Build** mode. The prior location of this setting (**Enable Job Build mode by default**) on the **General** tab of **Button Properties** is inactive.

Devices Node

The **Devices Node** has been updated with the following features:

-

-

-

New Scan Settings available in Button Properties

AccuRoute v5.1 includes new Scan Settings. Administrators can define Scan Settings values per button, for a specific Device Group.

To enable specific scan settings for a Device Group button:

1   In the AccuRoute Server Administrator, open the **Devices** Node. Double-click the device group of interest. The **Device Group Properties** screen appears.

2   In the **Buttons** tab, select the button of interest and click **Properties**. The **Button Properties** screen opens.

3   In the **Scan Settings** tab, you will see the range of scan settings available for the selected device group.
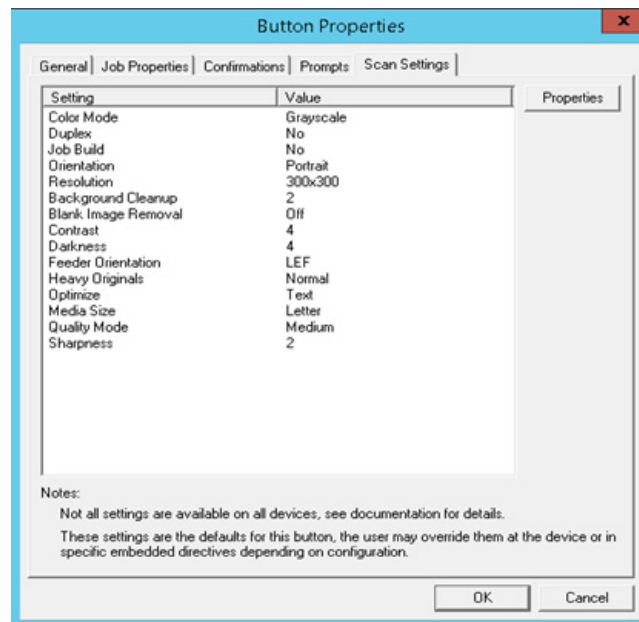
Note   Scan Settings options vary by device type.

4   Select the **Setting** of interest and click **Properties** to change or define its value in the pop-up screen.

For example, you can set **Blank Image Removal** to **On** or **Off**. If set to **On**, when a user scans from an associated device via this button, the system removes any scanned blank page or image from the delivered document. If set to **Off**, such pages or images remain in the delivered document.

New MyMessages device button

AccuRoute v5.1 introduces the **MyMessages** device button. This button offers authenticated users the ability to view and print their messages, including faxes. The System Administrator assigns authenticated user access and configures filtering options for Web Apps and Embedded Device Client users.

Filtering MyMessages

Inbox and **History** are the two default message filters associated with this button. By default, these filters display *unprinted* messages. Users can print these documents from **MyMessages**.

> **Note**   Unprinted, pending documents can also be viewed from the **MyPrints** button.

To be able to view *printed* jobs instead, you need to edit the default filter. To do so,

1   In the Server Administrator, go to the **Devices** node and right-click the device group of interest.

2   In the **Buttons** tab of **Device Group Properties**, highlight **MyMessages** and click **Properties**.

3   In the **Options** tab of **Button Properties**, highlight either **Inbox** or **History** and click **Properties**.

4   In **Filter Properties**, the default filter job property is

   `\\prOriginator = "%AUTH_EMAIL%" AND \\prPrintedByWebSite = 0`

5   To edit the filter, change part of it to `prPrintedByWebSite == 1`, or remove that part of the filter.

6   Click **OK** three times to finish.

You can also configure custom filters. In **Button Properties > Options** tab, click **Add** and customize the **Filter Properties**. You can assign specific filters to specific button views from the **View** drop-down menu.

For more information on adding and configuring **MyMessages** and other buttons, refer to Section 4: Creating Device Groups on the AccuRoute Server Administrator in the AccuRoute Embedded Device Client Installation Guide.

New MyPrints device button

AccuRoute v5.1 introduces the **MyPrints** device button. The **MyPrints** button works in conjunction with the **Secure Print** connector and the **Brooksnet RPM**.

Secure Print users can print documents from their desktop using the RPM. The RPM stores them in a local or network folder, monitored by the **Secure Print Connector**. As authenticated device user, **Secure Print** users can access and print their documents from that Folder using the **MyPrints** device button. For more information on installing and configuring the **Secure Print** connector, see New Secure Print Connector (2-11).

> **Note**   You need to have the **Secure Print** connector installed and configured to be able to use the **MyPrints** button.

After such jobs are printed, authenticated users can view them at the **MyMessages** button, with appropriate system configuration (see section above). The System Administrator assigns authenticated user access and configures the Secure Print connector and Folder(s).

For more information on adding and configuring MyPrints and other buttons, refer to Section 4: Creating Device Groups on the AccuRoute Server Administrator in the AccuRoute Embedded Device Client Installation Guide.

Deprecated items

The AccuRoute v5.1 server no longer supports the following items:

- In prior releases, you could create Collections of Job Properties. Collections have been deprecated and are now replaced by the new feature that allows you to create a Table User Job Property consisting of multiple properties.

- The SAP Connector has been replaced by the new **SAP SMTP Connector**.

Section 3: Omtool Client Updates

This section describes the new AccuRoute Client features for AccuRoute v5.1.

For more information on using or configuring the new features, refer to the AccuRoute Web Client Online Help and the AccuRoute Server Administrator Help.

This section includes:

Client versions in this release

AccuRoute v5.1 includes the following clients:

Table 3-1: **AccuRoute v5.1 Clients**

Client	Version
Mobile Client	5.0
Web Apps	5.1
Legacy Web Views	5.0
AccuRoute Desktop	5.0
AccuRoute Embedded Device Client	1.7.2
Embedded AccuRoute for Xerox (EIP) Device Client	5.0
Embedded AccuRoute for Ricoh (ESA) Device Client	5.1
HP OXPd v1.4	1.4.5
Extension for Worksite	5.1
Extension for MS SharePoint	5.1
Extension for DM	5.0
Image-In Connect	5.0
Image-In Queue	5.0

Table 3-1: **AccuRoute v5.1 Clients**

Client	Version
Image-In Direct Capture	5.0
Image-In Acquisition	5.0
Cost Recovery	5.0
Print to AccuRoute	5.0
FaxCenter	5.0
Fax Service Receiver	5.0

Note   Image-In Direct Capture is only available when the Omtool Healthcare Suite feature is installed.

Operating System support

AccuRoute v5.1 clients support

- Microsoft Windows 8 x32, Windows 8 x64, and Windows 10
- MAC OS X10.8 or newer

Requirements

Review the following requirement before working with the new client features:

- AccuRoute v5.1 installed

  To use the current version, you must uninstall any existing client and then install the new AccuRoute v5.1 Client, or upgrade from v5.0 to v5.1. For more information on upgrading the clients, refer to the AccuRoute v5.1 documentation home page.

Web Apps Client

This section describes the new Web Apps Client features for AccuRoute v5.1:

- Support (3-3)
- Requirements (3-3)
- New Web Client: Web Apps (3-4)
- New Folder Destination Types (3-4)

- [New Bookmark support for PDFs](#) (3-7)
- [New Job Property Lookups](#) (3-8)

For more information on configuring the following features, refer to the [AccuRoute Web Client User Guide](#) .

Support

The AccuRoute v5.1 Web Apps Client is qualified with the following:

Operating systems

- Microsoft Windows 8 x32, Windows 8 x64, and Windows 10
- MAC OS X10.8 or newer

Browsers

- Chrome, Internet Explorer, Edge, Firefox, and Safari browsers

---

Note   Safari browser support requires a minimum of Safari for Mac v6.2.8 or later.
Internet Explorer 11 support requires the compatibility view be disabled.

Requirements

Review the following requirement before working with the new Web Apps Client features:

- To upgrade to the current version, you must uninstall the existing Web Client and then install the new AccuRoute v5.1 Web Apps Client. For more information on upgrading the Web Apps Client, refer to the [AccuRoute v5.1 Server Installation Guide](#).

New Web Client: Web Apps

AccuRoute v5.1 introduces the new **Web Apps**, a highly-customizable replacement for the former Web Client. **Web Apps** provides all the functionality of the prior Web Client, now with an intuitive, tile-based display. Individual Application tiles appear on the Homepage, as shown below.
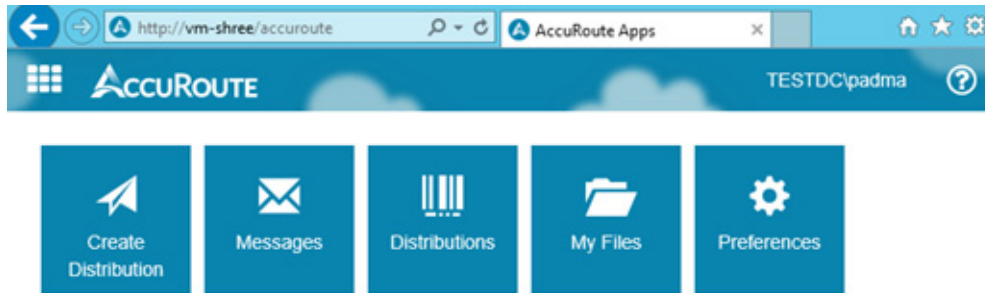
Administrators can assign specific Applications (such as **Inbox**, **Create Distribution**, **Mobile Reservations**, etc.) to Web Apps Profiles, which are in turn associated to specific user groups, thereby defining what a given member of that user group will see.

> **Note** The Legacy Web Client is the only place authorized users can access the Help Desk, Archive Search, Deficiencies, and approval.

New Folder Destination Types

Authenticated Web Apps users can now access the following cloud-based storage applications:

- Microsoft® OneDrive® for Business
- WebDav

For more information, see

- [Configuring Web Apps user access to MS OneDrive for Business](#)
- [Sending documents to MS OneDrive for Business](#)
- [Sending documents to WebDav](#)

Configuring Web Apps user access to MS OneDrive for Business

1 Launch Web Apps and click **Preferences > Authorizations**.
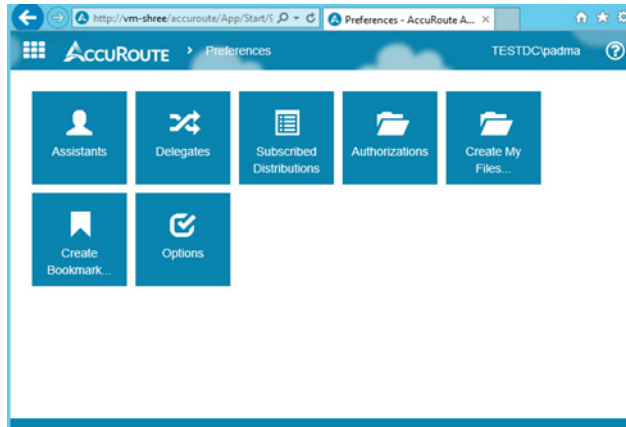
2 On the **Authorizations** screen, select your OneDrive Folder and click **Properties**.
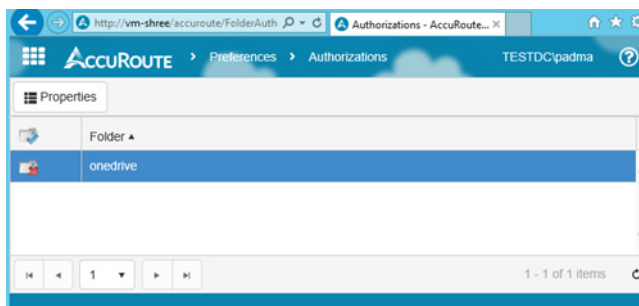
3 Read the **Folder Authorization Properties** dialog box that appears and click **OK**.
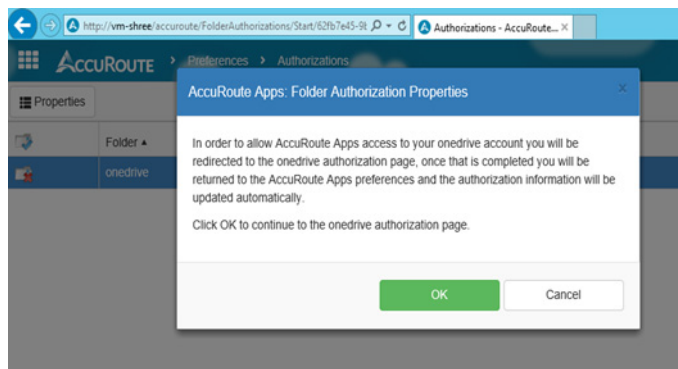
4   The **Login** screen for OneDrive for Business appears.
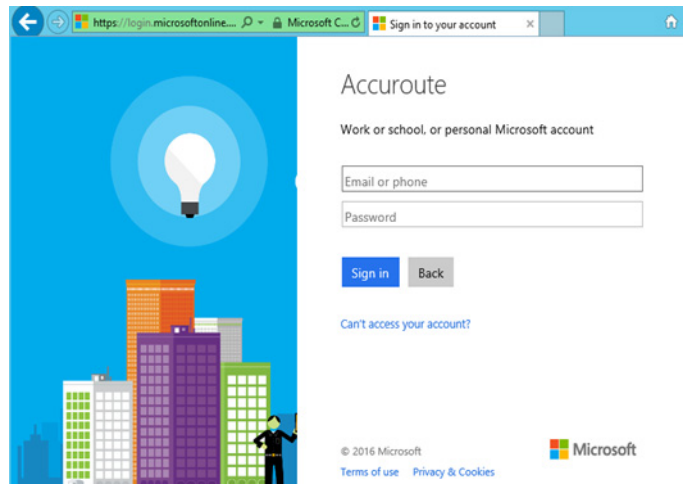
Enter your **Account** and **Password** credentials and click the **Sign In** button.

5   The OneDrive **Authorization** screen appears.
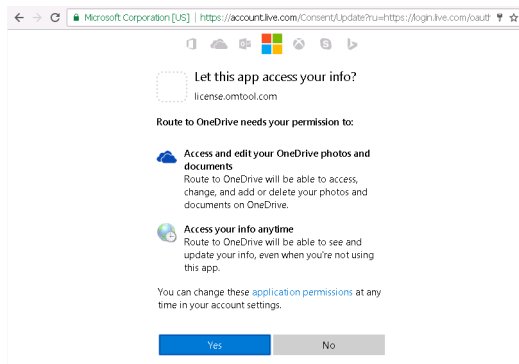
Click **Yes**. OneDrive for Business is now authorized.

Sending documents to MS OneDrive for Business

1   Launch Web Apps. To create a new message, click **Create Distribution**.

2   At the end of the **Destinations** field, click the **+** sign. Select **OneDrive**.

3   On the **Recipient Properties** screen, enter the relevant **Subject** and **Comments**, attach your file(s), and click **OK**.

4   Click **Send**. The message is submitted to the AccuRoute Server and document attachments are delivered to the OneDrive for Business repository.

Sending documents to WebDav

1   Launch Web Apps. To create a new message, click **Create Distribution**.

2   At the end of the **Destinations** field, click the **+** sign. Select **WebDav**.

3   On the **Recipient Properties** screen, enter the relevant **Subject** and **Comments**, attach your file(s), and click **OK**.

4   Click **Send**. The message is submitted to the AccuRoute Server and document attachments are delivered to the **WebDav** repository.T

Note   The **WebDav Folder** requires no authorization and appears blue.

New Bookmark support for PDFs

In AccuRoute v5.1, authenticated Web Apps users can add bookmarks to PDF documents. Bookmarks can be used to separate merged attachments, or to identify sections of hard copy documentation. You can configure the system to apply documents' attachment names as bookmarks.

To bookmark documents with their attachment names within Web Apps:

1   Launch the Web Apps client and select **Create Distribution**. Click the **+** sign at the end of the **Destinations** field and select **E-mail**.

2   The E-mail **Recipient Properties** window opens. Enter the **Email** address and an optional **Filename**.

3   Go to the **Advanced** tab and click the check box for **Bookmark individual documents using: %ATTACHMENT_NAME%**.

4 Click **OK**. The **Email destination** is added. You can enter other details in the message and add attachments.

5 Back in **Create Distribution**, click the **+** sign at the end of the **Attachments** field. Browse to and select any attachment(s) you want to include and click **Open**.

6 When finished, click **Send**. The message is submitted to the AccuRoute Server for further processing.

7 When you check the delivered document, attachment name(s) will be used for the Bookmark(s) in the delivered document.

This option is supported for all destinations to which PDF is delivered.

New Job Property Lookups

Web Apps users can now use **Database Lookup** and **List Lookup** for Job Properties.

Client and **List** properties need to be already set up for use in the AccuRoute Administrator. For more information, see New Job Property Lookups (2-35).

To configure and use Database and List Lookups:
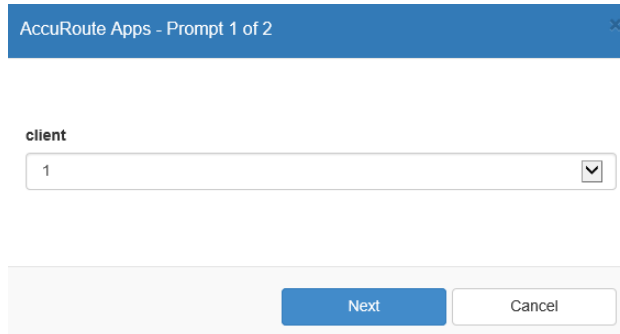
1 Launch the Web Apps client and select **Create Distribution**. Click **Options** and go to the **Prompts** tab.

2 Enable the Prompts **Client** and **List** and click **OK**.
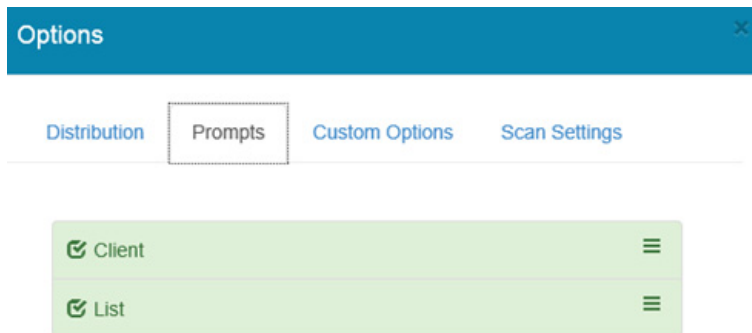
3 Enter the **Email destination** and attach an attachment. Save the distribution.
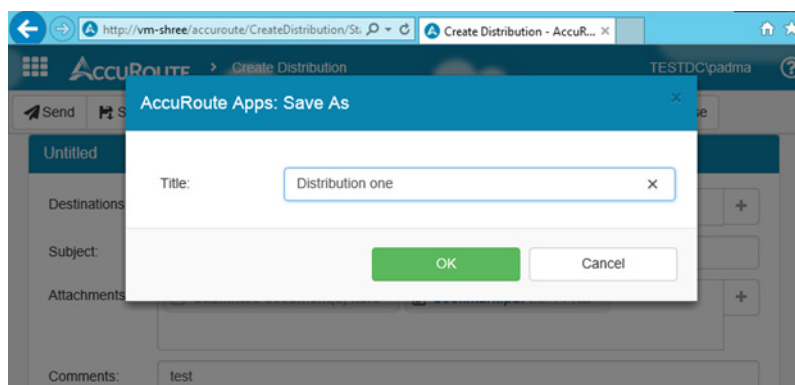
4   Click **Send**. **Client** is prompted. The prompt includes a **Search** button, indicating that the property is configured for Lookup.
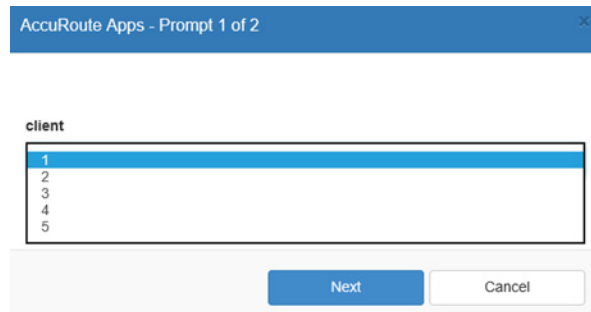
5   Click the **Search** button. All the values associated with the **Client** property appear in the drop-down list.
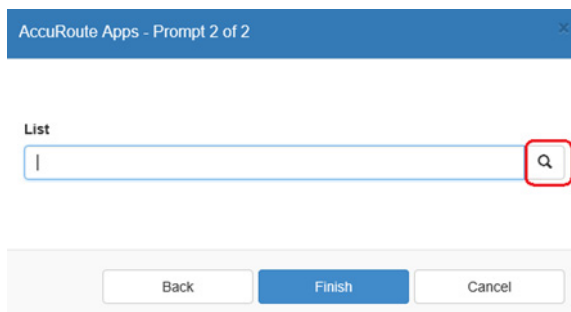
6   Select a value and click **Next**. **List** is prompted. The prompt includes a **Search** button, indicating that the property is configured for Lookup.

7   Click the **Search** button. All the values associated with the **List** property appear in the drop-down list.
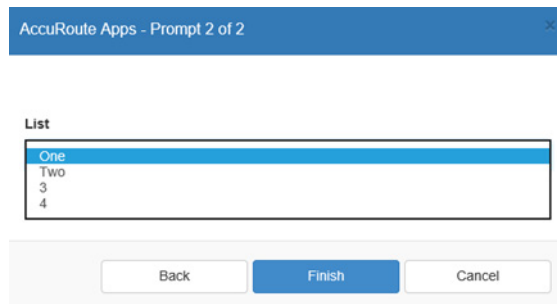
Embedded Device Client

AccuRoute v5.1 introduces the following new features for the AccuRoute Embedded Device Client:

- [Requirements](#) (3-10)
- [New Device Support](#) (3-11)
- [Installing the Embedded Device Client for Ricoh](#) (3-11)
- [New Scan Settings default options](#) (3-11)
- [New MyMessages device button](#) (3-11)
- [New MyPrints device button](#) (3-11)
- [New Folder Destination Types](#) (3-12)
- [New Search function for Scan to Folders button](#) (3-12)
- [New Job Property Lookups](#) (3-14)
- [Upgrading to AccuRoute v5.1](#) (3-15)
- [Deprecated items](#) (3-15)

Refer to the [AccuRoute Embedded Device Client Installation Guide](#) for more information on installation and configuration of these features.

Requirements

Review the following requirement before working with the new Device features:

- Devices must be upgraded to AccuRoute Embedded Device Client v5.1. Install or upgrade the clients from the Clients directory after the AccuRoute Server is upgraded to v5.1.

  To upgrade the Embedded Device Client to the current version, you can uninstall the existing Device Client and then install v5.1, or upgrade it from the existing 5.0 version. For information on upgrading the devices, refer to the Embedded AccuRoute Software installation guides on the [AccuRoute v5.1 documentation home page](#).

New Device Support

The AccuRoute v5.1 Embedded Device Client now supports the following new devices:

- HP PageWide Color MFP 586
- HP PageWide Color MFP E58650
- HP PageWide Color Flow MFP 586
- HP PageWide Color Flow E58650
- HP PageWide Managed MFP P57750dw

Installing the Embedded Device Client for Ricoh

If you use Ricoh devices, in addition to the AccuRoute Embedded Device Client, you also need to install the Embedded AccuRoute for Ricoh (ESA) Device Client.

- For full steps to install the AccuRoute Embedded Device Client, see *Section 3: Installation* in the [AccuRoute Embedded Device Client Guide](#).
- For full steps to install the Embedded AccuRoute for Ricoh (ESA) Device Client, see *Section 3: Installation and Configuration on a Local AccuRoute Server* in the [Embedded AccuRoute for Ricoh (ESA) Device Client v5.1 Installation Guide](#).

New Scan Settings default options

AccuRoute v5.1 adds new Scan Settings for device users, which can be configured per user group or per button (for device groups) in the Server Administrator.

> **Note**   Scan Settings options vary by device type, and may include, for example: Blank Image Removal, Contrast, Darkness, Media Size, and Quality Mode.

New MyMessages device button

AccuRoute v5.1 introduces the **MyMessages** button. Embedded Device Client users can view and print all their own messages. Messages are listed (those already printed or still pending printing, for example) according to filters defined in the Server Administrator. If multiple filters are configured, users can select one from the list at the device button.

For more information on adding and configuring buttons, refer to *Section 4-2 Specifying buttons for devices* in the [AccuRoute Embedded Device Client Guide](#).

New MyPrints device button

AccuRoute v5.1 introduces the **MyPrints** device button. The **MyPrints** button works in conjunction with the **Secure Print** connector. Authenticated device users with a Secure Print Folder can access and print their documents already sent to the Folder, by using the **MyPrints** device button. For more information on configuring the **MyPrints** device button, see [New MyPrints device button](#) (2-50).

> **Note** You need to have the **Secure Print** connector installed and configured to be able to use the **MyPrints** button.

The System Administrator assigns authenticated user access and configures the **MyPrints** button and the **Secure Print** connector and Folder(s). For more information on adding and configuring buttons, refer to *Section 4-2 Specifying buttons for devices* in the [AccuRoute Embedded Device Client Guide](#).

New Folder Destination Types

Authenticated Device Client users can now access the following cloud-based storage applications:

- Microsoft® OneDrive® for Business

- WebDav

To scan documents to a MS OneDrive for Business Folder:

1   Log in to the device of interest and select **Scan to Folder**.

2   Select **OneDrive for Business**.

3   Scan your documents.

4   Your message is sent to the AccuRoute Server and the documents delivered to the OneDrive for Business Folder associated with your user group.

To scan documents to a WebDav Folder:

1   Log in to the device of interest and select **Scan to Folder**.

2   Select **WebDav**.

3   Scan your documents.

4   Your message is sent to the AccuRoute Server and the documents delivered to the WebDav shared Folder associated with your user group.

New Search function for Scan to Folders button

AccuRoute v5.1 adds a new **Search** button, available to Embedded Device Client users on the **Scan to Folders** button. Use this to search for Folders.

To use the **Search** button:

1   Log in to the device of interest and select **Scan to Folder**.
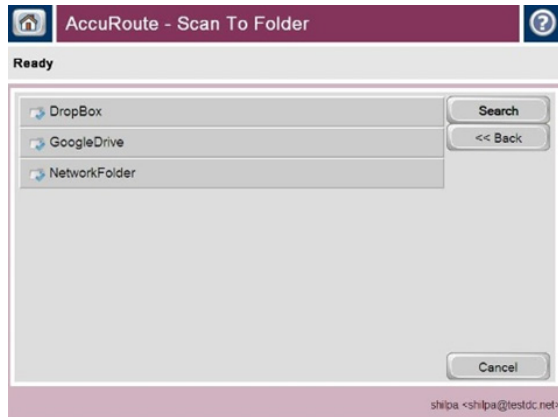
2   Click the **Search** button in the top-right corner.
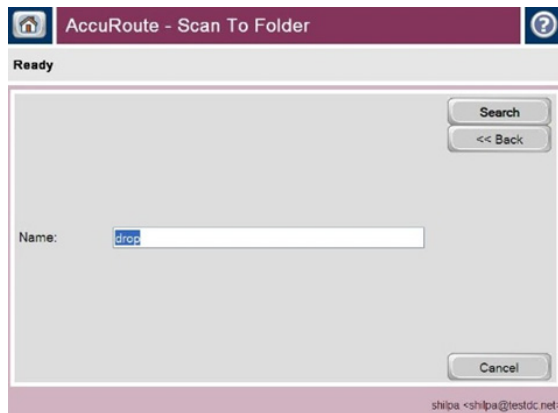
3   Enter the text for which you want to search in the **Name** field, and click **Search**.
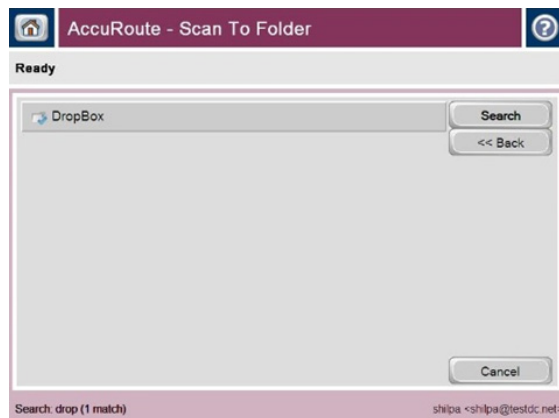
4   The **Search** result(s) appear on the display. Select the match of interest, or click **Search** to search again.

New Job Property Lookups

Embedded Device Client users can now use **Database Lookup** and **List Lookup** for Job Properties.

> **Note** **Client** and **List** properties need to be already set up for use in the AccuRoute Administrator. For more information, see New Job Property Lookups (2-35).

To configure **Database** and **List Lookups** for the Device Client:

1 In the AccuRoute Server Administrator, go to the **Devices** node, right-click the **Device Group** of interest and select **Properties**.

2 From **Device Group Properties**, go to the **Buttons** tab and double-click on the button of interest, for example, **Myfiles**.
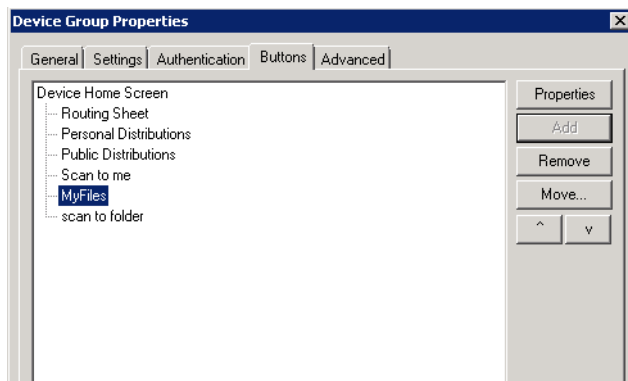
3 In **Button Properties**, go to the **Prompts** tab. Click **Add** and add the properties `Client` and `List`. Click **OK** twice.
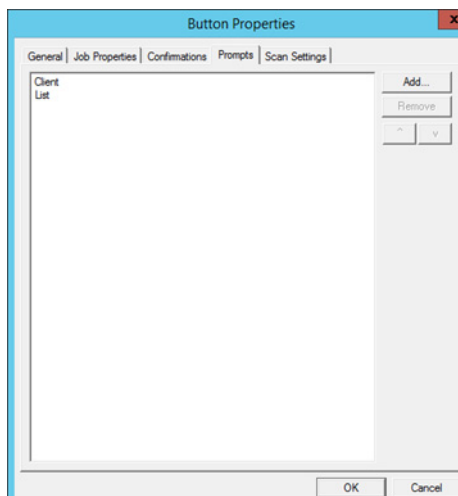
4   Walk up to the device of interest. Press the **Scan to My Files** button. Login to the button. You will
        see a **Client** property field and a **Search** button.
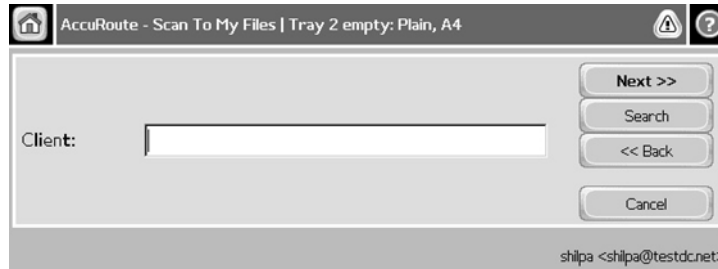
5   Enter the **Client** of interest and click **Search**. All Clients associated with the search term are listed.

6   Select a Client from the list. You will see a **List** property field and a **Search** button.
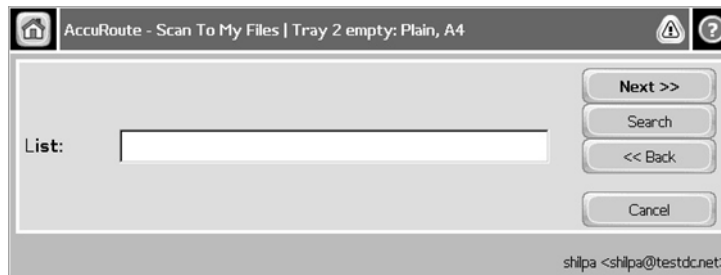
7   Enter the **List** of interest and click **Search**. All the entries associated with the search term appear.
        Select the List item of interest.
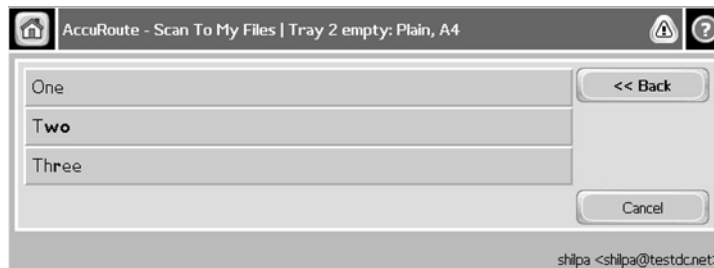
Upgrading to AccuRoute v5.1

To upgrade clients to AccuRoute v5.1, Extensions must first be uninstalled. You can uninstall the Embedded Device
Client or upgrade it from the existing 5.0 version. Install or upgrade the clients from the Clients directory after the
AccuRoute Server is upgraded to v5.1.

For information on upgrading the devices, refer to the Embedded AccuRoute Software installation guides on the
AccuRoute v5.1 documentation home page.

Deprecated items

The AccuRoute v5.1 Server no longer supports the following item:

- In prior releases, you could create **Collections** of Job Properties. Collections have been deprecated and are now replaced by the new feature that allows you to create a **Table User Job Property** consisting of multiple properties.

- The SAP Connector has been replaced by the new **SAP SMTP Connector**.

Section 4: Issues and Limitations

Resolved issues

The following Server and Client issues were found in the Omtool test laboratory during testing and are resolved in AccuRoute v5.1:

Table 4-1: **Resolved Server Issues**

Issue	Description
AR-7131	When a second user is configured as an assistant to the first, the assistant receives duplicate email messages.
AR-7294	An image viewed in Meditech PCI that was archived in Image-In Queue is slow to appear and of poor image quality.
AR-7724	When multiple modem servers are used within a single Telco connector, the Receive tab within the Telco Connector properties windows will only allow the channels of the modem server first detected to be configured.
AR-7735	When a PDF source file is composed to Tiff output using Ghostscript engine, the message fails with an error message.
AR-7746	An incomplete list of Existing Assignable Distributions was appearing in the AccuRoute Desktop.
AR-7771	Inbound faxes routed to email from DID lookup appear with the email address override configured in the Telco Connector, but display the message recipient name as the sender name, instead of using the name override configured in the Telco Connector.
AR-7774	When using the DMS Conversion Tool to extract TIF images from a legacy ObjectArchive database, the MessageContents field contained a corrupted .pdf image.
AR-7775	The Fax Sr. Filescan Connector was previously unavailable for AccuRoute v5.0.
AR-7785	Message Cleanup was too slow to keep up with the message volume passing through the DMS Conversion Tool server.
AR-7818	User credentials captured at the device were not properly transmitted for use by the Scan to Me Home Folder.
AR-7914	Server conversion of documents from PDF to OCR-PDF occurred too slowly.
AR-7942	Able to scan only the first page of a document for a barcode.
AR-7977	In Volume List Properties, the ability to change the Indexing the DSN database was unavailable.
AR-7982	When using the ObjectArchive Extractor with Alias objects, the Extractor should include the parent object's OA Key as a job property, not the binary object, and include the smallest dummy attachment possible.
AR-8002	Image retrieval times for Meditech PCI from ObjectArchive are inappropriately long.
AR-8003	In ObjectArchive, the ability to save MRP files using compression is unavailable.
AR-8009	Jobs sent to the Worksite Connector using the default profile fail to properly deliver the message.
AR-8024	ObjectArchive is in write-disabled mode.
AR-8036	Cost Recovery is not running properly in AccuRoute v5.0.
AR-8146	When using a routing sheet created using the AccuRoute Extensions for HP iManage, the system does not deliver the job from Image-In Queue to WorkSite.
AR-8153	Applying the document splitting feature in a routing rule causes a significant delay in document delivery.
AR-8163	Jobs en route either to an archive in a Volume List destination or as a notification to a Meditech destination get stuck in the Image-In Queue barometer instead of being promptly delivered. This also causes other jobs to become stuck in turn.
AR-8164	The ObjectArchive Migration tool inappropriately increases the size of the archived data, due to alias objects.

Table 4-1: **Resolved Server Issues**

Issue	Description
AR-8174	Scans within ObjectArchive cannot be retrieved by the Meditech PCI console.
AR-8206	When a bad text file exists in a folder for FaxSr FileScan, the FaxSr FileScan connector crashes when trying to process it, instead of marking it bad.
AR-8214	Ability to query or install buttons on a Lanier MP 3554 device is unavailable.
AR-8281	Jobs workflow ceases with jobs stuck in various barometers.
AR-8332	When Server Compression is set to Normal, scans from Lexmark scanners appear blacked out.
AR-8397	When using Image-In Queue, having Message Server logging enabled causes slowness.
AR-8457	Memory usage issues occurring with services.
AR-8534	When using a profile to send a document to WorkSite with the WorkSite connector, the AccuRoute Desktop is not automatically populating the Author, Client, and Matter fields with the relevant data.
AR-8539	The WorkflowStateID property is missing from the list of available System properties.
AR-8648	AccuRoute is currently missing claims-based authentication support for SharePoint 365 with the SharePoint connector.
AR-8680	AccuRoute is currently missing a rollup of resolved issues for Aspose.
AR-8786	Memory usage issues occurring with the ObjectArchive Migration tool.
AR-8876	FineReaderOCR document conversions fail to complete for documents over 800 pages.
AR-8880	Licensing errors occur during disaster recovery server installation.
AR-8953	Support for SharePoint is currently unavailable in the Folders node on the Administrator.
AR-8954	Folder support for SharePoint 365 is unavailable.
AR-8999	Omtool Admin account, instead of being appropriately available to users with Client Matter cabinet access.
AR-9046	When sending documents to NetDocuments, only the Admin account user was able to access the document, excluding the scanning user or others with cabinet access.
AR-9062	When routing a document through Image-In Queue for quality assessment, the system cannot continue to properly route that document onward to a subfolder.
AR-9063	An issue with the Xeroxscan Connector caused it to become disabled, leaving jobs stuck in Dispatch.
AR-9133	When using Image-In Connect and ProLaw, the ability to view the values of Custom Properties on the Routing Sheet is not currently available.
AR-9169	When using the DMS Extraction tool for OCR with WorkSite, and set to ignore PDF images that contain text, PDF XFA documents were improperly extracted.
AR-9263	When using the Collection Locator and Image-In Queue, extra duplicate jobs appear in the Web Client.
AR-9265	When sending a message through Image-In Queue to an archive, property values can be overwritten by the Collection Locator when there is an archived document with matching properties.
AR-9292	The Back and Cancel functions accessible in nested buttons on Xerox devices are not properly functioning, displaying an error message instead of returning to the prior device button screen.
AR-9295	There is a problem enabling Image-In Connect for some users when another server (besides the default server) is providing the User Principal Name (UPN) for those users. In the Administrator, the Provider Properties are missing a UPN tab to allow users to specify the server searched for this information.
AR-9301	When converting documents to PDF/A (with normal compression and JPEG format settings), the resulting text appears fuzzy.
AR-9307	When using a date property in a prompt, the value (date) selected by the user is not retained by the system with the delivered job, regardless of destination.
AR-9343	During Batch scanning, attachments including bar codes similar to those used on routing sheets and separator pages cause the batch scans to get stuck in the Embedded Directive Manager.

Table 4-1: **Resolved Server Issues**

Issue	Description
AR-9349	When using the Scan to Me feature, customized to deliver documents to DFS Folders, the delivery is not completed.
AR-9432	Additional Confirmations variable settings applied to Outbound rules in the Administrator are not properly applied by the system.
AR-9483	FineReader update process is not working properly.
AR-9580	An ObjectArchive service times out and fails to start during updates.

Table 4-2: **Resolved Client Issues**

Client	Issue	Description
ObjectArchive Migration Tool	AR-7297	ObjectArchive Migration Tool unavailable for AccuRoute v5.0.
AccuRoute Embedded Device Client	AR-7634	Samsung PAR file is unavailable.
	AR-9193	When entering device authentication information (username and password) as required to use a customized button such as Scan to Me, the device was improperly presenting the user with multiple screens of login fields.
	AR-9336	When the Button property setting to allow Scan Preview by default (for supported devices) is enabled, using it at the device causes the device to hang.
	AR-8434	A Job Property Verification component needed to be created for the Server Administrator's Process and Components nodes.
AccuRoute Extensions for iManage	AR-8471	When using the AccuRoute Extensions for iManage with FileSite 9, if you right-click on a file or folder, Import Scan options are available, but there is also a blank space in the drop-down menu.
AccuRoute Extensions for OpenText DM	AR-9013	Right-click functionality is missing when working with the client extension for Open Text Document Management (DM).
Web Client	AR-7723	When two Web Client users attach separate documents to messages at the same time (with a second of each other), both attachments are added to each File Attachment section.
	AR-8748	When working with a document without a name in WorkSite, the AccuRoute Web Client flashes for a moment and nothing happens, no scan sheet appears, nor an error message.
Image-In Acquisition Client	AR-7777	The Image-In Acquisition Client failed when users tried to access scanner settings.
Image-In Connect	AR-8688	Image-In Connect is currently missing support for Generic Lists.
Image-In Direct Capture Client	AR-8134	When scanning documents from the Image-In Direct Capture Client, the document cannot be saved via the Scanner pane.
	AR-8799	Invalid scan resolution settings in the Image-In Direct Capture configuration file cause a scanning error to occur.

Table 4-2: **Resolved Client Issues**

Client	Issue	Description
Image-In Queue	AR-7422	When documents are routed to an Image-In Queue collection, with Folder level edit data permissions, an error message appears when you try to edit a property via the Edit Data screen. The message reads "Failed to set viewer zoom level."
	AR-7750	In Image-In Queue, the type-ahead function for drop-down lists behaved improperly, only working for the initial letter.
	AR-8004	Image-In Queue licenses are based on a user name (email address) instead of a workstation ID.
	AR-8051	When upgrading Image-In Queue from v3.01 Feature Pack 6 to v5.0, Image-In Queue cannot connect to the server.
	AR-8396	The current version update for Image-In Queue is missing the correct version number as it appears in Add/Remove Programs.
	AR-8872	Image-In Queue is unable to properly open attachments composed of multiple PDFs.
	AR-9067	More flexibility is required for validation of Edit Data properties, in particular, an Image-In Queue setting to allow the user to save document meta-data that has not yet passed validation.
	AR-9091	When documents are processed by Image-In Queue en route to WorkSite, and you Extract Data, DMS properties are lost and the document delivery to WorkSite fails.
	AR-9284	When a document that includes the subsection symbol (§) in its description is transferred from Image-In Queue to WorkSite, an extra Â is prefixed to the subsection symbol.
	AR-9472	When Image-In Queue is extracting pages, it only retains properties configured in the Administrator's Queue properties, and is excluding properties set outside of Image-In Queue, such as configured with Image-In Connect or a Watch folder.

Known issues

The following issues are known for AccuRoute v5.1:

Table 4-3: **Known issues**

Issue	Description
AR-6497	The prior version of the Universal Output connector is neither supported nor updated by this release. You need to manually enable the connector after installation of AccuRoute v5.1.
AR-6498	When using the AccuRoute v5.1 Server with a prior version of the Web Client, if you add Job Properties for a Volume List search, for which you want the results to appear in the Web Client Archive Node, those properties do not appear.
AR-7074	When connecting to the Mobile Client, users receive the error message 'Failed to get user's group information - unauthorized.' As a solution, verify that on the IIS server all IIS Roles, including security, are installed.
AR-7197	On localized MFPs, when an incorrect username and/or password are entered for authentication, the response 'The user name or password is incorrect.' is not localized.
AR-9593	Device settings are tailored to HP devices. Other vendor's device models may not be able to take advantage of all available device settings.

Table 4-3: **Known issues**

Issue	Description
AR-10190	Print w/prompts now automatically occurs when you select the Send or Routing Sheet action. There was no "useful value" in sending or creating a routing sheet without the configured prompts, so we have integrated this into one step.
AR-10484	When users have multiple email addresses associated with their login, they can no longer select a specific account's messages to appear. They must select a primary email, and the system displays all messages associated with that user.

Limitations

The following limitations are known for AccuRoute v5.1:

Table 4-4: **Limitations**

Limitation	Description
AR-5978	In Image-In Direct Capture, if you add a new pane without properly configured system connections, the new pane appears blank with a red x and an incorrect date/time stamp.
AR-6066	On a LaserJet Flow M525 MXP device, there is a 75-character limit for a prompt field associated with a button.
AR-6532	If you have upgraded from AccuRoute v4.1 Feature Pack 1 to v5.0 without upgrading your Image-In Queue client, any existing messages no longer appear in Image-In Queue. For compatibility, the Image-In Queue Client needs to be upgraded to v5.0.
AR-6735	On HP OXPd v1.4 devices, support is unavailable for • Job Queue button • Device Information button • Mobile Reservations button (existing Mobile reservations appear under Personal Distributions) • Fax button feature 'User may modify their Sender Name' option in Fax properties
AR-7094	Take the following steps to hide the Watch Folder tray icon: 1 Configure the Watch Folder for Launch to AccuRoute. 2 Check whether the AccuRoute Desktop launches when dropping a file. 3 Close the tray icon application. 4 Open %appdata%\Omtool\AccuRouteWatchFolder\AccuRouteWatchFolder.xml and edit the configuration to use a prVisible node in the top level (a good location is after prServer) and set it to 0. 5 Enable the Watch folder. 6 Verify that it still functions normally and that the icon is no longer visible in the tray.
AR-7110	When using a Remote Intelligent Device Client and HP OXP v1.4 devices, an error message appears if you try to login to a HP v1.4 device and use the Personal Distribution button. Instead, on the Remote Intelligent Device Client system, launch IIS and select Application Pools. Select the OXPAppPool and change the Identity to the AccuRoute Service Account.
AR-7215	In a Windows 2012 environment, the pre-installation pack neither includes nor configures MS.NET 3.5 SP1.
AR-7216	In order for cloud-based Folders (such as Microsoft OneDrive or box) to properly appear in the Web Client, restart the browser after configuring user permissions. This reloads the configuration for the Web Client.
AR-10261	In Web Apps, using the Internet Explorer browser when opening a Routing Sheet alters the typical workflow. When the user clicks the Open button, instead of the Routing Sheet opening, they must also click the Open Folder button that appears.

Table 4-4: **Limitations**

Limitation	Description

AR-7759	In order for messages sent from the Native button via the HP LAN Fax Connector to appear in a device's Job Queue button > All My Faxes filter, you need to appropriately configure the LDAP lookup. To do so:
	
	 1 In the Server Administrator, expand Connectors and double-click the HP LAN Fax Connector.
	 2 In Properties, select the Sender Lookup tab.
	 3 Click Add and enter the server's IP address, user name, and password.
	 4 In the Search tab, enter the search base as dc=testdc;dc=net
	 5 Test by entering any user name and complete the configuration.
	 6 In the device EWS's Digital Sending tab, configure the Fax Settings for the device.
	 7 Also configure LDAP Authentication:
	   a LDAP Server Bind Method: Simple
	   b LDAP Server: IP address
	   c Port: Port number
	   d Credentials: Select Use LDAP Administrator's Credentials
	   e LDAP Adminstrator's DN: cn=administrator,cn=users,dc=testdc,dc=net, and enter the password
	   f Bind and Search Root: CN=USERS,DC=testdc,DC=net
	   g Match the name entered with the LDAP attribute of: CN
	   h Retrieve the device user's email address using attribute of: mail
	   i and name using the attribute of: displayName
	 10 To test, send a Native Fax message from the Server.
	 11 On the device of interest, login to the ob Queue button and check the All my faxes filter.
	     The Native Fax message sent should appear in the All my faxes filter list.

AR-8478	When using the Ricoh Embedded Device Client, to set the default Color Mode to Color, you also need to set the File Intermediate format to JPEG. If it is set to TIFF instead, the default color mode will be Monochrome. To set the default Color Mode to Color: 1 In the Server Administrator, expand Devices and right-click the Ricoh Device Group. 2 Select the Properties menu option. 3 In the Buttons tab, highlight the button of interest and click Properties. 4 On the Device Settings tab, highlight File Intermediate Format and click Properties. 5 In the Device Settings Properties popup, select the JPEG File Intermediate format and click OK. 6 Highlight Color Mode and click Properties again. 7 Select Color for the Color Mode, click OK, and click OK again. 8 When you test the button on the device, the Color Option should be Color mode.

Table 4-4: **Limitations**

Limitation	Description
AR-8800	When using the Ricoh Embedded Device Client with MPC 401 v12 or similar devices, you need to change the Scan Size setting in Button Properties in order to avoid an "Illegal Attribute set" error message during scanning. The required setting for these devices is NA_Letter_SEF (for Short Edge First). To configure this setting exclusively for Short Edge First devices, place them in a separate Ricoh Device Group. The default Scan Size is set to NA_Letter_LEF (for Long Edge First). For V12 MP c401 or similar devices: 1 In the Server Administrator, expand Devices and right-click the Ricoh Device Group of interest. 2 Select the Properties menu option. 3 In the Buttons tab, highlight the button of interest and click Properties. 4 On the Device Settings tab, highlight Scan Size and click Properties. 5 In the Device Setting Properties pop-up, select NA_Letter_SEF from the drop-down menu. 6 Click OK three times.
AR-8538	If you need to re-add the MyFiles button to a Xerox device (after initially adding a new Group), you need to select the Scan to Destination button and rename it MyFiles. The MyFiles button appears as a default choice only when adding a new group. To re-add the MyFiles button: 1 Remove the existing MyFiles button from the device group of interest. 2 In Device Group Properties > Add Button, select Scan to Destination from the drop-down Type list, edit the Name to MyFiles, and click OK. This updates the button name display in the ScanFacts Server Administrator. 3 With Scan to Destination still selected, to update the displayed name and image for the button on the device, click Device Group Properties > Properties. On the Button Properties screen, enter Name: MyFiles Display Text: @buttonmyfiles Text Image: myfiles 4 Click OK and OK again.
AR-8816	If you are adding a DM connector after an update, and you see the message "Failed to create the DOCSObject," you need to uninstall and reinstall the Windows Explorer DM Extensions (the DM client) on the server and then reboot.

Table 4-4: **Limitations**

Limitation	Description
AR-8847	If you want to send a message to a remote server with DCOM connectivity, you need to first make sure that you are either signed in as the Administrator or as Everyone or a specific user or user group with DCOM Launch and Activation Permissions enabled. Otherwise, error messages warning of failure to queue the message will appear. To enable DCOM permissions, **1** Open Component Services. **2** Right-click My Computer > Properties and select the COM Security tab. **3** In Launch and Activation Permissions Security Limits, select Everyone or a specific user or user group and enable (check the Allow check boxes) all the Permissions for that user. **4** Click Add and select Anonymous Logon and then enable all the same permissions for the Anonymous user. **5** Click OK, Apply, and OK.
AR-8884	If you want to add a remote server to a SharePoint 365 connector, you need to first make sure that you are either signed in as the Administrator or that Everyone or your specific user or user group has DCOM Launch and Activation Permissions enabled. Otherwise, an error message warning of product installation failure will appear and you cannot add the remote server. To enable DCOM permissions, **1** Open Component Services. **2** Right-click My Computer > Properties and select the COM Security tab. **3** In Launch and Activation Permissions Security Limits, select Everyone or a specific user or user group and enable (check the Allow check boxes) all the Permissions for that user. **4** Click Add and select Anonymous Logon and then enable all the same permissions for the Anonymous user. **5** Click OK, Apply, and OK.