Embedded AccuRoute® for Ricoh (ESA) Device Client v5.0 Installation Guide

For AccuRoute v5.0

January 2015

Omtool, Ltd.
6 Riverside Drive
Andover, MA 01810
Phone: +1/1 978 327 5700
Toll-free in the US: +1/1 800 886 7845
Fax: +1/1 978 659 1300

Omtool Europe
25 Southampton Buildings
London
WC2A 1AL
United Kingdom
Phone: +44/0 20 3043 8580
Toll-free in the UK: +44/0 80 0011 2981
Fax: +44/0 20 3043 8581

Web: http://www.omtool.com

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://www.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 4: Remote Installation and Configuration

Section 5: Optional Configuration

Section 6: Testing

Section 7: Troubleshooting

Appendix: Installation and Configuration using the Embedded Web Server

Contents

Section 1: Introduction

This guide contains instructions on deploying Embedded AccuRoute for Ricoh (ESA) Device Client v5.0 to multifunction devices running Ricoh SDK. This guide is written for systems administrators with detailed knowledge of the AccuRoute server and the device. This section of the guide includes:

Overview of Embedded AccuRoute for Ricoh (ESA) Device Client

Embedded AccuRoute for Ricoh (ESA) Device Client v5.0 is compatible with AccuRoute Server v5.0 environments. It is built against the SDK/J version 10.x and runs on supported Ricoh, Lanier, Savin, and Gestetner 4.x, 5.x, 6.x, 7.x, 10.x and 11.x devices as a Java xlet called the Omtool Xlet v2.0.

This integration brings the versatile document routing capabilities of AccuRoute to supported Ricoh, Lanier, Savin, and Gestetner devices. These capabilities are founded on Omtool's distribution technology.

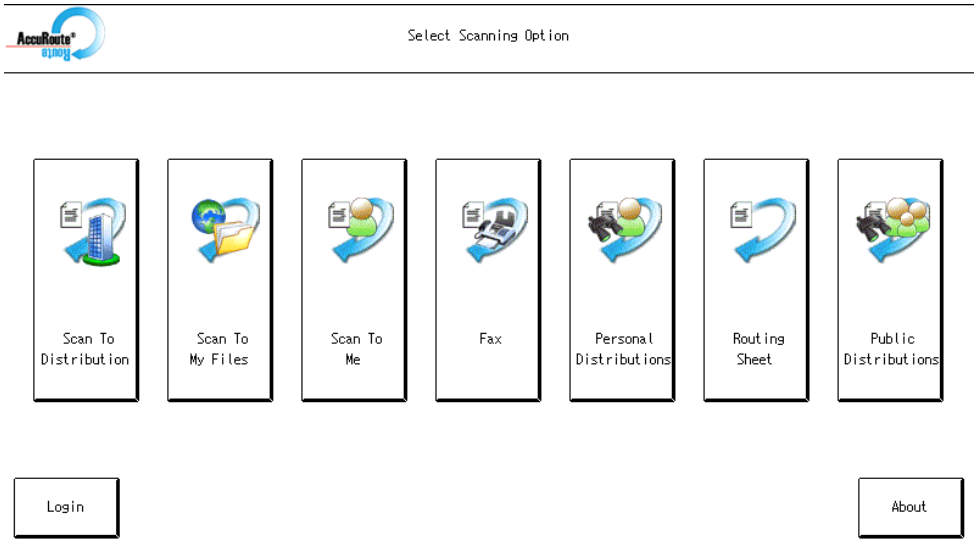


Figure 1-1: **AccuRoute scanning features on the Ricoh device running the Embedded AccuRoute for Ricoh (ESA) Device Client**

Each feature has a unique function that is detailed in the following table. (To see how each feature works on the device, go to Section 6: Testing, for the complete screen sequence of each feature.)

Table 1-1: AccuRoute scanning features in Embedded AccuRoute for Ricoh (ESA) Device Client

Feature	Description	Login required	Notes
Fax	This option allows the user to perform a walk-up fax. The user enters the fax number and can additionally add a cover page to fax. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The AccuRoute server sends the fax to the intended recipients.	No	
Personal Distributions	The user selects Personal Distributions, logs in to the device, and selects a personal distribution option or Distribution Rule. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.	Yes	The device user must be able to create Distribution Rules. This requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets).
Public Distributions	The user selects Public Distributions and then selects a public distribution option or Distribution Rule. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server decodes the Distribution Rules and distributes the document to the intended recipient.	No	Public distribution options are associated with a special user account that is set up for this purpose. The user account associated with this feature must be able to create Distribution Rules. This requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets).
Routing Sheet	After the user selects Routing Sheet, the device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server then decodes the Distribution Rule and distributes the document to the intended recipients.	No	The device user must be able to generate Routing Sheets. This requires access to AccuRoute Web Client (where the user can create the Routing Sheets).
Scan to Destination (formerly Scan to Folder, see Notes)	The device scans and delivers the document to the AccuRoute folder via HTTP/HTTPS protocol. The server picks up the scanned document from the network folder, processes it, and delivers it to the intended folder.	No	If you previously used "Scan to Folder" for this button, you must change the display text of the Scan to Destination button. This will be described during the device configuration.
Scan to Distribution	After the user selects Scan to Distribution, the device scans and delivers the documents to a configured distribution.		
Scan to Folder	The device scans and delivers the document to a folder (Dropbox, FTP, or network folder share) predetermined by your system administrator. The AccuRoute server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	

Table 1-1: **AccuRoute scanning features in Embedded AccuRoute for Ricoh (ESA) Device Client**

Feature	Description	Login required	Notes
Scan to Me	The user selects Scan to Me and logs in to the device. The device scans and delivers the document to the AccuRoute server via HTTP/HTTPS protocol. The server processes the document using the device user's personal Scan to Me directive and distributes the document to the intended recipients. Or, the scanned document is emailed to the sender (the default).	Yes	Scan to Me is an advanced feature of AccuRoute Web Client. It enables the server to process all AccuRoute messages from the same user with the same Distribution Rule. Scan to Me requires access to AccuRoute Web Client (where the user can create the Distribution Rules and Routing Sheets). In addition, Scan to Me must be configured in the AccuRoute Web Client and on the server. For more information on this feature, consult Section 2: Requirements.
Scan to My Files	The user selects Scan to My Files button and logs in to the device. The device scans and delivers the document to the AccuRoute server (via HTTP/HTTPS protocol) where it is processed and distributed to the My Files section of the user AccuRoute Web Client.	Yes	All jobs scan.
Nested Buttons	The Nested Buttons feature provides the ability to configure one top-level button that all other AccuRoute buttons will appear under, minimizing the front panel home screen real estate. For example, one button can be configured and labeled "AccuRoute." This button would be the only AccuRoute button to display on the home screen. Pressing this button would then display any other enabled buttons (such as Routing Sheets, Personal Distributions, etc.).	Yes	Login is required only if using Device Authentication and if one of the Nested Buttons needs authentication.

Main components of the environment

The Embedded AccuRoute for Ricoh (ESA) Device Client environment consists of the following components.

- **AccuRoute Server** - The main back end server for processing and routing documents.
- **Embedded AccuRoute for Ricoh (ESA) Device Client v5.0** - See Section 3: Installation and Configuration on a Local AccuRoute Server for installation instructions.
- **Ricoh Device** - See Supported devices (2-1) for a list.

Installation components

The Embedded AccuRoute for Ricoh (ESA) Device Client setup includes multiple components detailed in this table.

***Table 1-2:* Description of installation components with locations and functions**

Component	Location	Function
Embedded AccuRoute for Ricoh (ESA) Device Client Install	`...\Omtool\Omtool Server\Clients`	The setup contains the setup.exe file for Ricoh ESA. Use this file to install the Embedded AccuRoute for Ricoh (ESA) Device Client.
Embedded AccuRoute for Ricoh (ESA) Device Client Configuration Manager	Devices node in the AccuRoute Server Administrator.	The Device Client Configuration node is a management tool installed with the AccuRoute Server Administrator, and is used to manage settings and options that will be available on the device. **Note:** A device license must be installed in order for the Device Client Configuration manager node to be used.

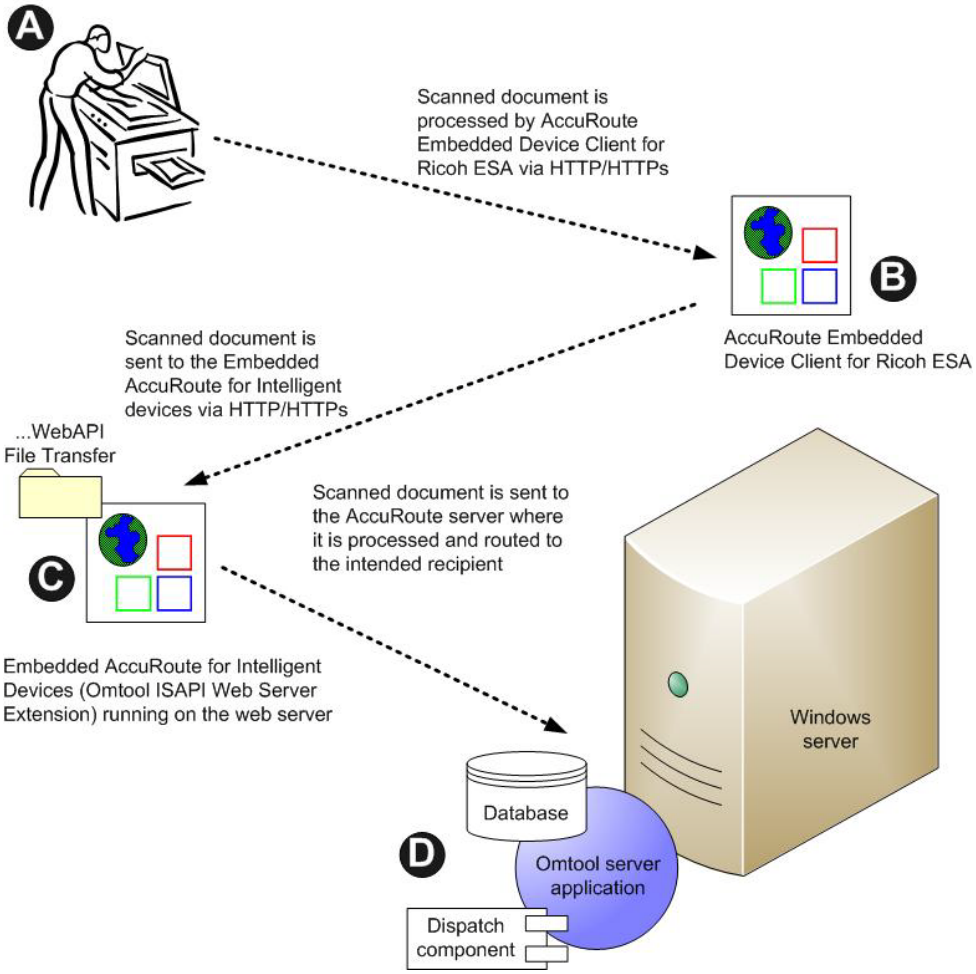
Document workflow

The workflow that moves a document from the device to its final destination involves the user, the device, the Embedded AccuRoute for Ricoh (ESA) Device Client, Embedded AccuRoute for Intelligent Devices (Omtool ISAPI web server extension), and the AccuRoute server. An understanding of this workflow can be helpful in troubleshooting Embedded AccuRoute for Ricoh (ESA) Device Client integration.

Basic workflow is:

- When a device user scans a document, the device submits the document to Embedded AccuRoute for Ricoh (ESA) Device Client via HTTP/HTTPS protocol.
- The Embedded AccuRoute for Ricoh (ESA) Device Client then routes the document to the AccuRoute server via HTTP/HTTPS protocol.
- The Dispatch component applies rules to the message.
- AccuRoute server processes the message and routes it to the intended recipients.

Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features



A - The user selects an AccuRoute scanning feature and scans a document.

B - The document is processed by Embedded AccuRoute for Ricoh (ESA) Device Client via HTTP/HTTPS protocol.

C - Embedded AccuRoute for Ricoh (ESA) Device Client sends the document to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) via HTTP/HTTPS protocol which in turn routes the document to the AccuRoute server.

D - The Dispatch component applies rules to the message, and the server processes the message accordingly.

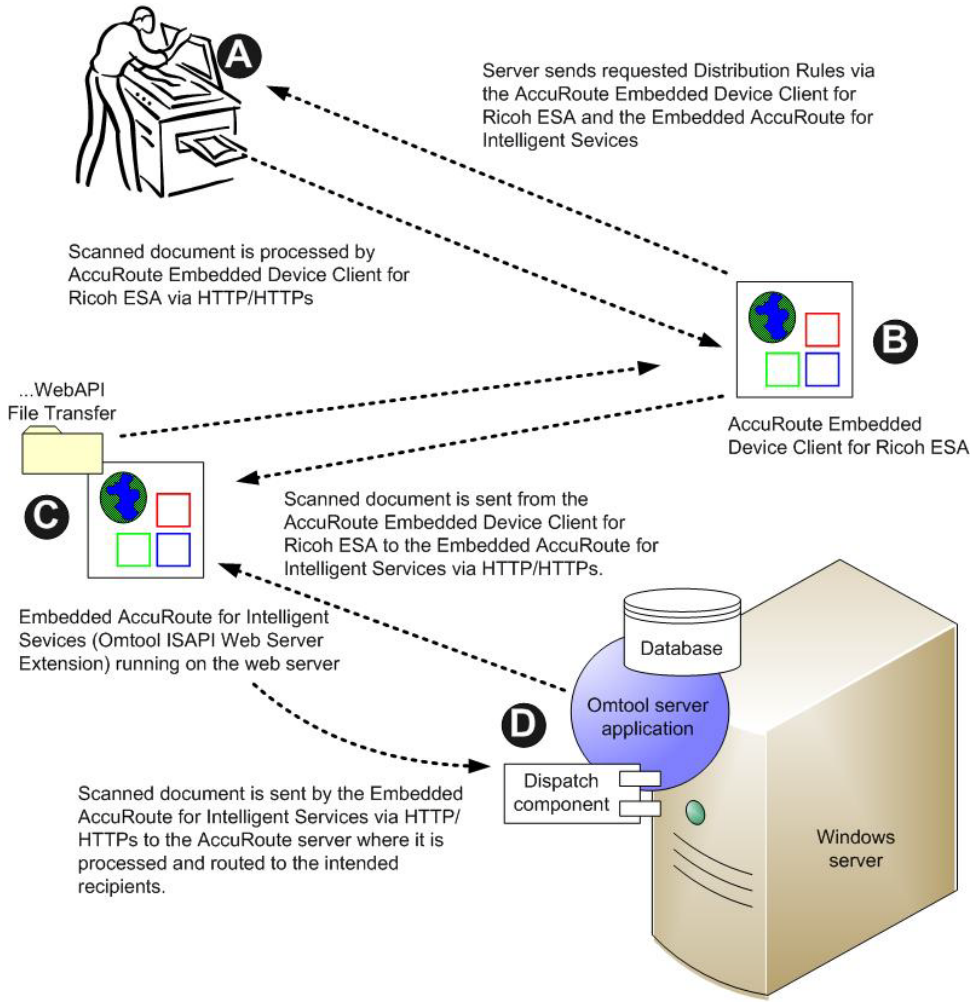
Figure 1-2: **Workflow for Fax, Routing Sheet, Scan to Destination, and Scan to Distribution**

Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features

When a user begins a scan session with one of these options, the device requests the Embedded AccuRoute for Ricoh (ESA) Device Client to retrieve Distribution Rules.

> **Note** For Personal Distributions, Scan to Me, and Scan to MyFiles, the user must authenticate himself at the device using the configured authentication type. See Configuring Ricoh device authentication [rewrite] (5-8).

The Embedded AccuRoute for Ricoh (ESA) Device Client then submits a request to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI web server extension) which retrieves the data from the AccuRoute server and supplies it to the Embedded AccuRoute for Ricoh (ESA) Device Client. As soon as the Embedded AccuRoute for Ricoh (ESA) Device Client returns the data to the device, the workflow resumes.



A - The user selects the Personal, Public Distribution, Scan to Me, or Scan to My Files feature. (If the user chooses Personal Distribution, he logs into the device.) The device requests the list of Distribution Rules from the server. The AccuRoute server returns the requested data. The user selects a Distribution Rule from the list and scans the document.

B - The document is processed by Embedded AccuRoute for Ricoh (ESA) Device Client via HTTP or HTTPS protocol.

C - Embedded AccuRoute for Ricoh (ESA) Device Client sends the document to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) via HTTP/HTTPS protocol which in turn routes the document to the AccuRoute server.

D - The Dispatch component applies rules to the message, and the server processes the message accordingly.

Figure 1-3: **Workflow for Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files**

Deploying Embedded AccuRoute for Ricoh (ESA) Device Client

1. Verify the server and device installation requirements. (Section 2: Requirements)
2. Complete the installation process. (Section 3: Installation and Configuration on a Local AccuRoute Server)
3. If relevant to your environment, instead complete the remote installation and configuration steps. (Section 4: Remote Installation and Configuration)
4. Test the AccuRoute scanning features on the device. (Section 6: Testing)
5. Troubleshoot the setup, if necessary. (Section 7: Troubleshooting)

Related documentation

- AccuRoute v5.0 Server Installation Guide
- Omtool Server Administrator Help
- Ricoh ESA Device Client Quick Start Guides

> **Note** The quick start guides have been designed to be posted near the device, distributed to device users, and published on your organization's intranet.

For all documentation related to AccuRoute v5.0, consult the AccuRoute v5.0 documentation page.

Section 2: Requirements

This section includes:

Supported devices

The following devices are supported by default when the Embedded AccuRoute for Ricoh (ESA) Device Client is installed. Check with Omtool Sales if you have a device not listed below.

Table 2-1: **List of devices supported by Embedded AccuRoute for Ricoh (ESA) Device Client**

Model	Minimum Firmware
Aficio MP 2550	Group4X
Aficio MP 2851 SP	Group4X
Aficio MP 3350	Group4X
Aficio MP 3351 SP	Group4X
Aficio MP 2550	Group4X
Aficio MP 2851 SP	Group4X
Aficio MP 3350	Group4X
Aficio MP 3351 SP	Group4X
Aficio MP 2550	Group4X
Aficio MP 2851 SP	Group4X
Aficio MP 3350	Group4X
Aficio MP 3351 SP	Group4X
Aficio MP 2550	Group4X
Aficio MP 2851 SP	Group4X
Aficio MP 3350	Group4X
Aficio MP 3351 SP	Group4X
Aficio MP 2550	Group4X
Aficio MP 2851 SP	Group4X
Aficio MP 5000	Group4X
Aficio MP 5001 SP	Group4X
Aficio MP C2050	Group4X
Aficio MP C2050 SP	Group4X

Model	Minimum Firmware
Aficio MP C2550 SP	Group4X
Aficio MP C2800	Group4X
Aficio MP C3300	Group4X
Aficio MP C4000	Group4X
Aficio MP C5000	Group4X
Aficio MP C6000	Group4X
Aficio MP C7500	Group4X
Aficio MP W5100	Group4X
Aficio MP W7140	Group4X
Aficio MP W5100en	Group4X
Aficio MP W7140en	Group4X
Aficio MP 4000	Group4X
Aficio MP 4001 SP	Group4X
Aficio MP 6001 SP	Group5X
Aficio MP 7001 SP	Group5X
Aficio MP 8001 SP	Group5X
Aficio MP 9001 SP	Group5X
Imagio MP 6001 SP	Group5X
Imagio MP 7501 SP	Group5X
Aficio MP 171	Group6X

Model	Minimum Firmware
Aficio MP 171 SPF	Group6X
Aficio MP 201	Group6X
Aficio MP 201 SPF	Group6X
Aficio MP 2352	Group7X
Aficio MP 2852	Group7X
Aficio MP 3352	Group7X
Aficio MP 5200S	Group7X
Aficio MP 5210SF	Group7X
Aficio MP 5210SR	Group7X
Aficio MP C300	Group7X
Aficio MP C400	Group7X
Aficio MP C2051 SP	Group7X
Aficio MP C2551 SP	Group7X
Aficio MP C3001SP	Group7X
Aficio MP C3501SP	Group7X
Aficio MP C4501	Group7X
Aficio MP C5501	Group7X
Aficio MP C6501SP	Group7X
Aficio MP C7501SP	Group7X
Aficio MP W2401	Group7X
Aficio MP W3601	Group7X

Table 2-1: **List of devices supported by Embedded AccuRoute for Ricoh (ESA) Device Client**

Model	Minimum Firmware
Imagio MP 2552	Group7X
Imagio MP 3352	Group7X
Imagio MP C2201	Group7X
Imagio MP C2801	Group7X
Imagio MP C3301	Group7X
Imagio MP C4001	Group7X
Imagio MP C5001	Group7X
Imagio MP C6001SP	Group7X
Imagio MP C7501SP	Group7X
Imagio MP W2401	Group7X
Imagio MP W3601	Group7X
Aficio MP 301	Group10X
Aficio MP 4002	Group10X

Model	Minimum Firmware
Aficio MP 5002	Group10X
Aficio MP C305	Group10X
Aficio MP C3002	Group10X
Aficio MP C3502	Group10X
Aficio MP C4502	Group10X
Aficio MP C5502	Group10X
Aficio MP 6002	Group10.08.00X
Aficio MP 7502	Group10.08.00X
Aficio MP 9002	Group10.08.00X
Imagio MP 4002	Group10X
Imagio MP 5002	Group10X
Imagio MP 6002	Group10X
Imagio MP 7502	Group10X
Imagio MP 9002	Group10X

Model	Minimum Firmware
Imagio MP 9002T	Group10X
Imagio MP C2802	Group10X
Imagio MP C3302	Group10X
Imagio MP C4002	Group10X
Imagio MP C5002	Group10X
Imagio MP W4001	Group10X
MP C3003	Group 11X
MP C3503	Group 11X
MP C4503	Group 11X
MP C5503	Group 11X
MP C6003	Group 11X
SP C730DN	Group 11X

Pro C720S	Group4X
Pro C900S	Group4X
Pro C901S	Group4X

Ricoh Pro 907EX	Group5X
Ricoh Pro 1107EX	Group5X
Ricoh Pro 1357EX	Group5X

Pro C651EX SP	Group7X
Pro C751EX SP	Group7X

Supported SDK/J platform versions

Ricoh Corporation certified the following devices with the SDK/J platform versions listed in the table below.

The SDK/J platform, known as Embedded Software Architecture, must be installed on an SD card that remains in the service slot whenever the device is powered on. To check the version of the SDK/J platform installed on your Ricoh device, start the Application Manager. The version is displayed in the top right corner.

Note OmtoolXlet version 1.4 supports Ricoh, Lanier, Savin, and Gestetner 2.x, 4.x, 5.x and 7.x devices. It will also continue to support 2.x devices that were certified previously.

Table 2-2: **List of Ricoh devices and the minimum SDK/J platform versions supported by Ricoh as well as SDK/J platform versions included in the Ricoh ESA Device Client kit.**

Minimum SDK/J platform version supported	SDK/J platform version included in the Ricoh ESA Device Client kit	Device Model
7.0x	7.03	• Ricoh - MP C6501, MP C7501, • Gestetner - MP C6501, MP C7501 • Lanier - C9065, C9075 • Savin - LD365C, LD375C **Note:** The 7.0x devices have Java VM Card pre-installed.
5.0x	5.08	• Ricoh - SP 4210, SP C820DN, SP C821DN, SP 6330N • Gestetner - SP 4210N, C8140nD, C8150nD, SP 6330N • Lanier - LP137N, LP540c, LP550c, LP235N • Savin - MPL37N, CLP340D, CLP350D, MLP235n
5.0x	5.08	• Ricoh - MP 6001 SP, MP 7001 SP, MP 8001 SP, MP 9001 SP, Pro 907EX, Pro 1107EX, Pro 1357EX • Gestetner - MP 6001 SP, MP 7001 SP, MP 8001 SP, MP 9001 SP, Pro 907EX, Pro 1107EX, Pro 1357EX • Lanier - LD360sp, LD370sp, LD380sp, LD390sp, Pro 907EX, Pro 1107EX, Pro 1357EX • Savin - 9060sp, 9070sp, 9080sp. 9090sp, Pro 907EX, Pro 1107EX, Pro 1357EX
4.1x	4.20	• Ricoh - MP C2050**, MP C2550**, MP C2800, MP C3300, MP C4000, MP C5000 • Gestetner - MP C2050**, MP C2550**, MP C2800, MP C3300, MP C4000, MP C5000 • Lanier - LD520C**, LD525C**, LD528C, LD533C, LD540C, LD550C • Savin - C9020**, C9025**, C2828, C3333, C4040, C5050 ** - Requires 512 MB memory upgrade to run solutions.
4.1x	4.20	• Ricoh - MP C2800 (E-3100)##, MP C3300 (E-3100)##, MP C4000 (E-5100)##, MP C5000 (E-5100)## • Gestetner - MP C2800 (E-3100)##, MP C3300 (E-3100)##, MP C4000 (E-5100)##, MP C5000 (E-5100)## • Lanier - LD528C (E-3100)##, LD533C (E-3100)##, LD540C (E-5100)##, LD550C (E-5100)## • Savin - C2828 (E-3100)##, C3333 (E-3100)##, C4040 (E-5100)##, C5050 (E-5100)## ## - Fiery products.
4.1x	4.20	• Ricoh - SP C420DN • Lanier - SP C400DN • Savin - SP C400DN

Table 2-2: **List of Ricoh devices and the minimum SDK/J platform versions supported by Ricoh as well as SDK/J platform versions included in the Ricoh ESA Device Client kit.**

Minimum SDK/J platform version supported	SDK/J platform version included in the Ricoh ESA Device Client kit	Device Model
4.1x	4.20	• Ricoh - SP 8200DN • Gestetner - SP 8200DN • Lanier - LP150dn • Savin - MLP150DN
4.1x	4.20	• Ricoh - MP 2550 SP, MP 3350 SP, MP 4000 SP, MP 5000 SP, MP C6000, MP C7500, Pro C900S, MP 2851SP^^, MP 3351SP^^, MP 4001SP^^, MP 5001SP^^ • Gestetner - MP 2550, MP 3350, MP 4000, MP 5000, MP C6000, MP C7500, Pro C900S, MP 2851SP^^, MP 3351SP^^, MP 4001SP^^, MP 5001SP^^ • Lanier - LD425, LD433, LD040, LD050, LD260C, LD275C, Pro C900S, 9228SP^^, 9233SP^^, 9240sp^^, 9250sp^^ • Savin - 9025, 9033, 9040, 9050, C6055, C7570, Pro C900S, LD528SP^^, LD533SP^^, LD140SP^^, LD150SP^^ ^^ - Java VM Card Pre-installed

AccuRoute server requirements

The Embedded AccuRoute for Ricoh (ESA) Device Client requires:

- ❒ AccuRoute server
- ❒ At least one fax-enabled connector to support fax-based features
- ❒ Embedded AccuRoute for Ricoh (ESA) Device Client device license installed (per device)
- ❒ AccuRoute ISAPI Device Client (included with default server install)

Device authentication requirements

Embedded AccuRoute for Ricoh (ESA) Device Client supports the following authentication methods. It is recommended that an authentication is selected and verified before installing the device client. See the *AccuRoute v4.1 Server Installation Guide* on the AccuRoute v4.1 documentation page.

The types of authentication are:

- **Email** or **Email with Password** authentication occurs when a user logs into the device with a valid email address that was created in Active Directory.
- **Login** authentication occurs when a user logs into the device with a user name and password as defined in the Active Directory.

- **Pin** or **Pin with Password** authentication displays on the device a text box into which a user enters a PIN login.
- **Device** authentication is not supported at this time.

Note PIN refers to an attribute of Active Directory and it can be changed to point to any other Active Directory field by modifying the LDAP Lookup Settings Filter field values on the **Authentication** tab of the **Device Group Properties**. The default attribute is set to use **employeeID**.

Section 3: Installation and Configuration on a Local AccuRoute Server

This section includes:

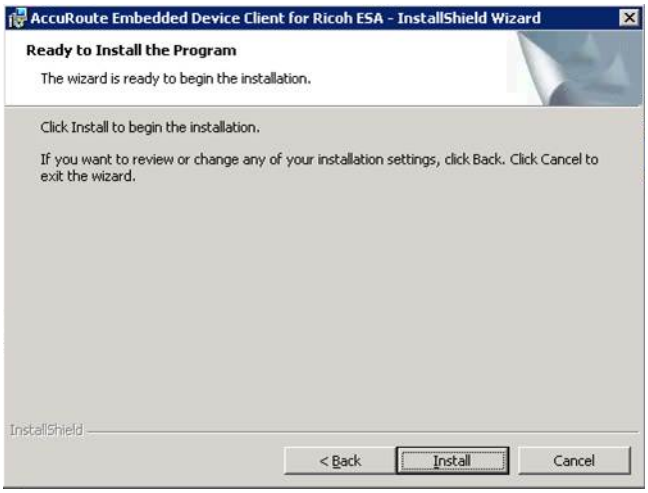
Installing Embedded AccuRoute for Ricoh (ESA) Device Client

To install the AccuRoute Embedded Device Client for Ricoh ESA onto the AccuRoute server, complete the following procedure:

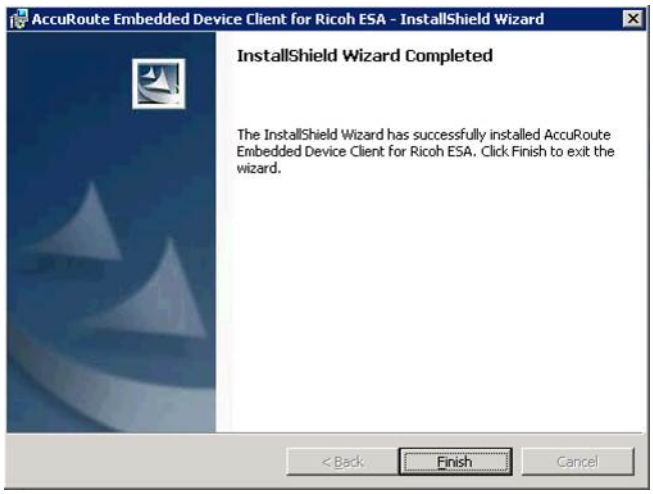
1. Log on to the system running the AccuRoute server using an account that belongs to the local Administrators group.

2 Navigate to the folder `...\Omtool\Omtool Server\Clients\Ricoh ESA` and run **setup.exe**. The InstallShield wizard launches with the **Welcome** message.

3 Click **Next** and then **Install**.



4 Click **Finish**.



5 Continue to Entering a license for Embedded AccuRoute for Ricoh (ESA) Device Client (3-3).

Entering a license for Embedded AccuRoute for Ricoh (ESA) Device Client

Note If you do not have a license, contact Omtool Sales for more information.

You can activate the Embedded AccuRoute for Ricoh (ESA) Device Client license in one of two ways:

- **Automatically** when you enter an activation code and the AccuRoute server is on a system that has access to the internet.
- **Manually** if the AccuRoute server does not have access to the internet. In this case, you will:
  - Submit and validate the activation code.
  - Create an Export file into which the activation code is copied.
  - Create an Import file and use this file for activation from a system that does have internet access.

Automatic license activation

Be sure the AccuRoute server has access to the internet. Have available a copy of the device license activation code.

1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2 Expand the tree view and select the server name.

3 Right-click and select the **Licensing** option**.** The **Licensing** page is displayed.

4 Click the **Activate License...** button. The **License Activation** page is displayed.

5 Select the **Automatically activate via the Internet** option.

6 Enter your license activation code in the **Activation Code** text field.

7 Click **OK**. The server is updated with your license.

8 Click **Close** to complete the procedure.

Manual license activation

Have available a copy of the activation code.

> **Note** Although the AccuRoute server may not have access to the internet, to complete this procedure you will need a system that does have access.

1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2 Expand the tree view and select the server name.

3 Right-click and select the **Licensing** option**.** The **Licensing** page is displayed.

4 Click the **Activate License...** button. The **License Activation** page is displayed.

5 Select the **Export activation file for manual activation** option.

6 Create an Export license file:

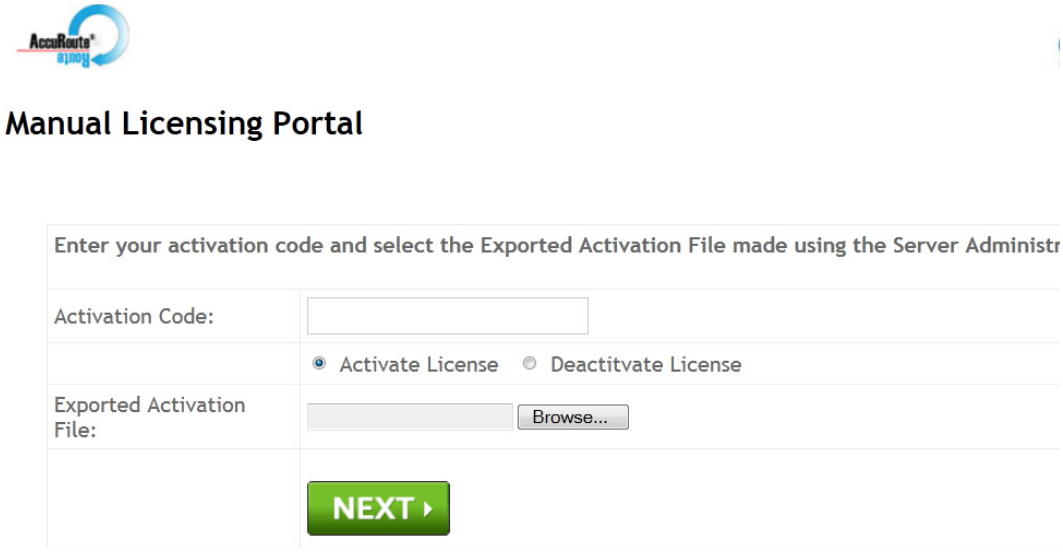
   a Browse to a location where you want to save the license file. By default, the file is an Export file named `ManualActivation.exp`. After specifying the file name and location, click **Save**.

   b The path will appear in the **Export Filename** field on the **License Activation** page. Click **OK**.

7 From a system with internet access, launch the web browser and go to:

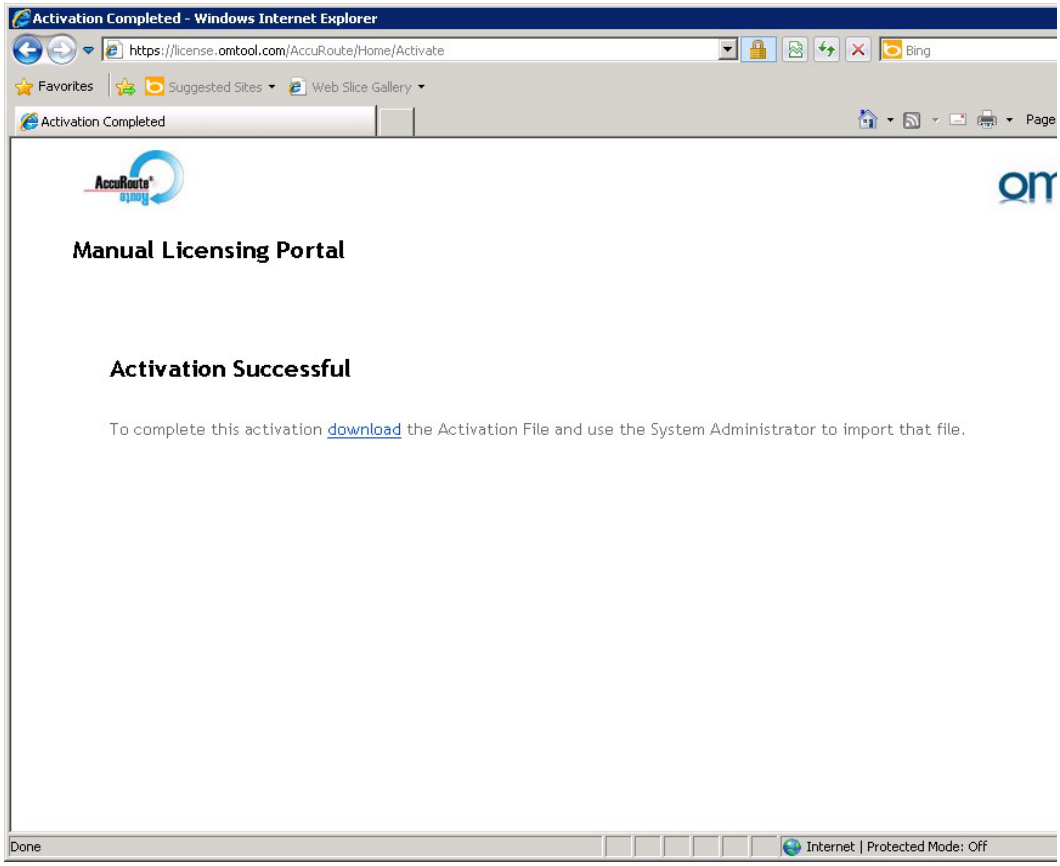
   `https://license.omtool.com/accuroute`

The **Manual Licensing Portal** page opens.



8. Enter your device license activation code in the **Activation Code** text field.
9. Be sure the **Activate License** option is selected (the default).
10. Click the **Browse** button to select the `ManualActivation.exp` file created in Step 6. With the file name selected (highlighted), click **Open**.
11. Verify that the license information is entered correctly on the **Manual Licensing Portal** page.

12 Click **NEXT** and the **Activation Successful** message is displayed.



13 To complete the device activation, click **Download**. The **File Download** page is displayed.

14 Click **Save** to create the Import file. By default, the file is named with the device activation code. You can change this (for example, `ManaulActivation.imp`) and select a location for the file on the AccuRoute server.

15 Click **Save**. The **Download Complete** page shows that status of the file download.

16 Click **Close**.

Note You can minimize or close the browser.

17 On the **Licensing** page, click the **Activate License...** button.

18 Select the **Import activation file from manual activation** option.

19 Browse to the saved `ManaulActivation.imp` file. Select the file and click **Open**.

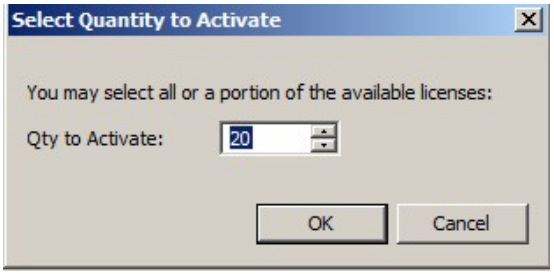
20 Click **OK** on the **License Activation** page. The license is updated.

21 Click **Close** to complete the procedure.

Activating or deactivating multiple clients or a subset of licenses

When activating a multiple device license, you will be prompted to indicate the number of devices to be activated.

Note Multiple device licenses can be used on multiple servers.



When deactivating a multiple device license, highlight the device license activation code and click **Deactivate License**. Then, choose the number of licenses to deactivate.

Modifying the DeviceLoader.xml

Verify that your device is listed in Table 2-1 to be sure it will be added by default with the Embedded AccuRoute for Ricoh (ESA) Device Client. The installation will fail if your device is not listed within the `Deviceloader.xml`. In this case, you must manually add your device to the `Deviceloader.xml` prior to installation of the client application.

Important If you have multiple devices that are the same model, for example, if you have three Aficio MP 3000 devices in your environment, you need to add the model number only once in the `Deviceloader.xml` file.

Before you add any device model number, check the `Deviceloader.xml` to see if the model number information was previously entered. If so, you will not need to add the information.

To modify the `DeviceLoader.xml`:

1. Go to the directory:

   `C:\Program Files (x86)\Omtool\Ricoh ESA`

2. Open the `Deviceloader.xml` file with Notepad for editing purposes.

3. Under the **Models** node, add the appropriate information for Model type and `GroupnumberX` into a new Model type as follows:

```
<Model type = "Aficio MP C3003 SPF"
minimumFirmware="">Group11X</Model>
```

For example:

```
      Value for Model node specifies the configuration listed under
- <Models>
   <Model type="Aficio MP C2050" minimumFirmware="">Group4X</Model>
   <Model type="Aficio MP C2500" minimumFirmware="">Group2X</Model>
   <Model type="Aficio MP C6501" minimumFirmware="">Group7X</Model>
   <Model type="Ricoh MP6001SP" minimumFirmware="">Group7X</Model>
  </Models>
  <!-- - Contains various configurations which could be mapped to a sp
         Any number of child nodes may be specified.   -->
```

For a list of supported devices, see the Supported devices (2-1) section.

4 Save your changes and close the file.

Creating a group of devices

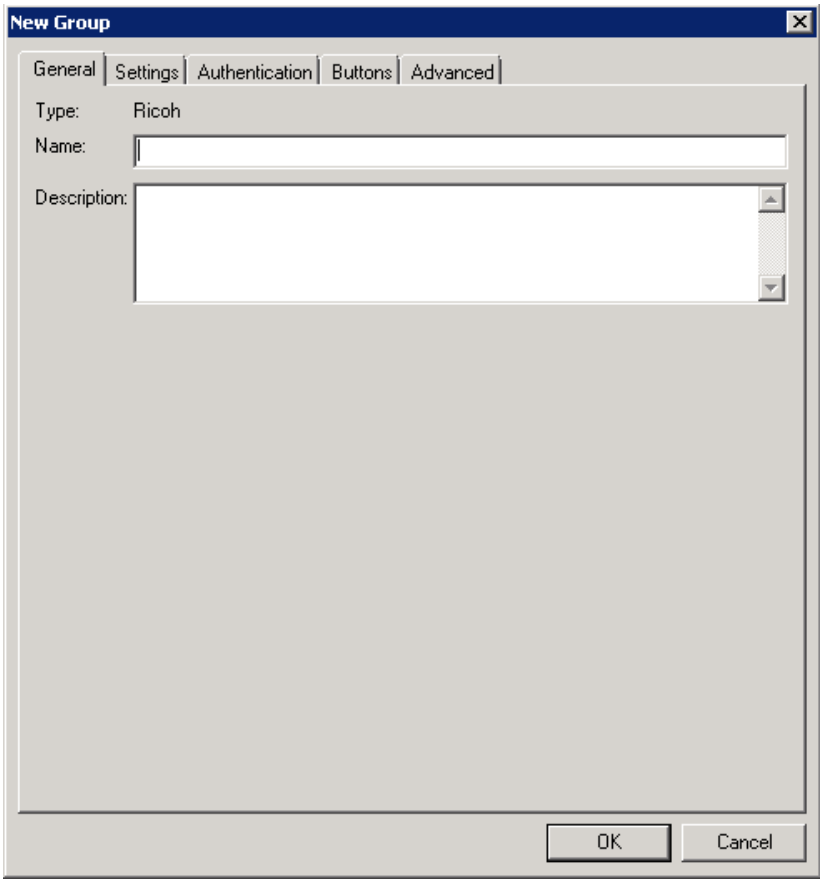
Before you can install the Embedded AccuRoute for Ricoh (ESA) Device Client on any devices, you first need to create a new Group for them on the AccuRoute Server Administrator. While each group may have the same configuration, you can configure groups to be completely different from one another. For example, you might create a group named “Marketing” and configure it to use only the Routing Sheets and Fax features. An additional group named “Sales” might be configured for PIN authentication with the ability to use only the Routing Sheet, Personal Distributions, and Scan to Me features.

The following procedure explains how to create and configure a group. This is completed on the AccuRoute Server.

1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2 In the console tree, expand the AccuRoute Server Administrator and right-click **Devices**.

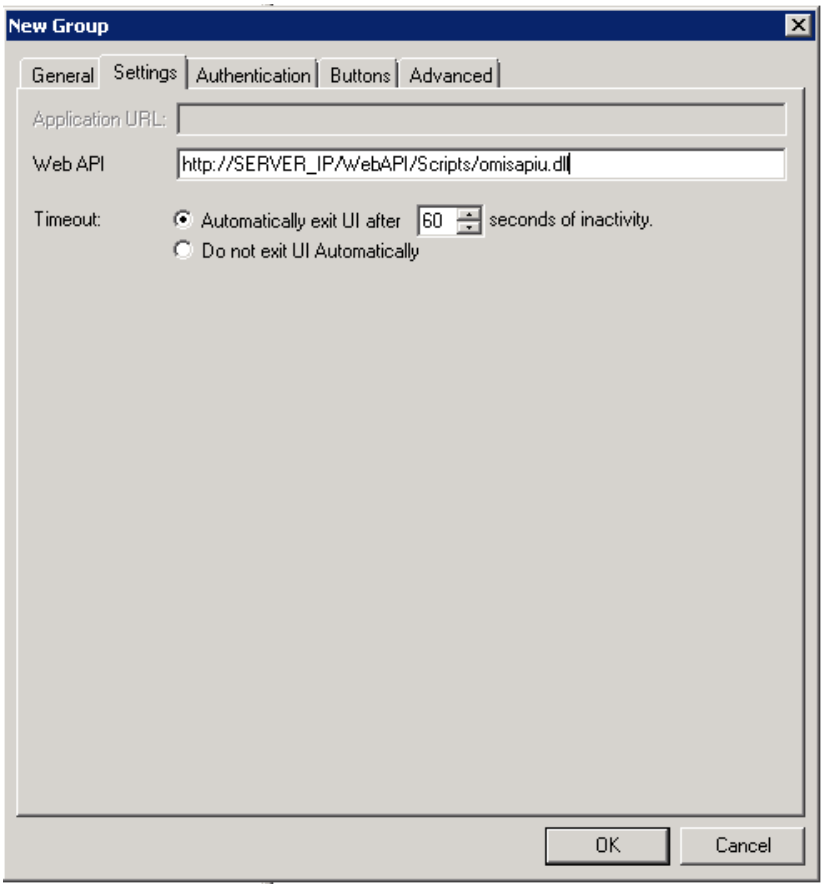
3 Select **New > Ricoh group**. The **New Group** page opens.



4 In the **Name** text box, enter a name for the device.

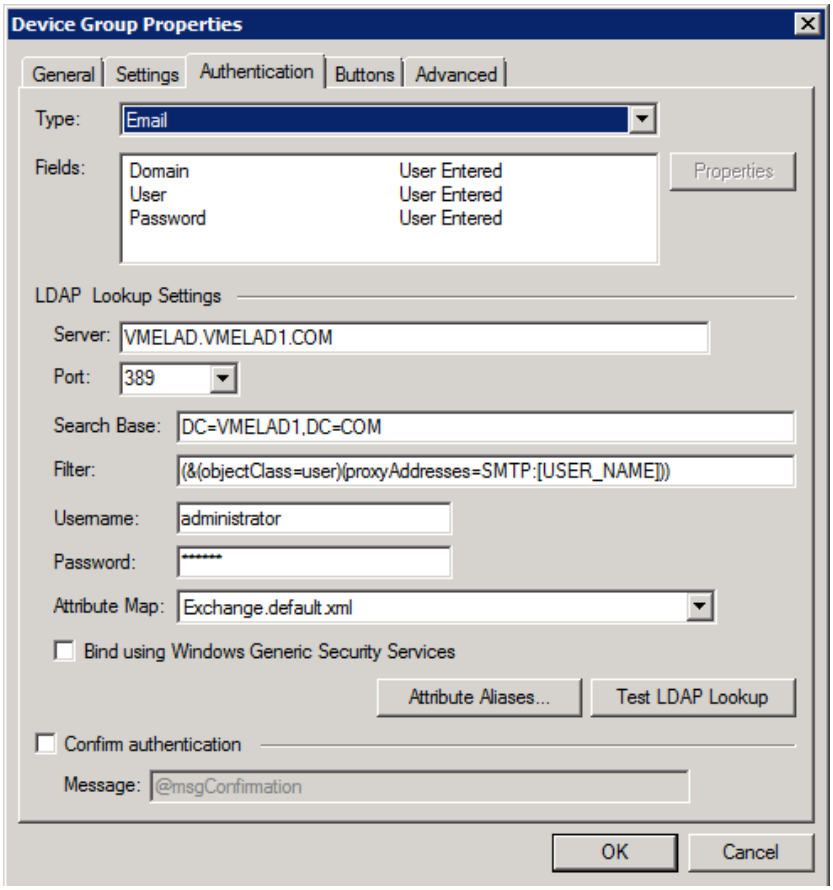
5 Optionally, in the **Description** text box, enter a device description.

6 Click the **Settings** tab. Change the **Web API** url to point to the Intelligent Device Client server..



Note When the Intelligent Device Client is installed on a remote system, you must manually enter the IP address of that system in the **Web API** section of the **Settings** tab in the **Device Group** node.

7 Click the **Authentication** tab to specify the type of user authentication required for the group of devices.

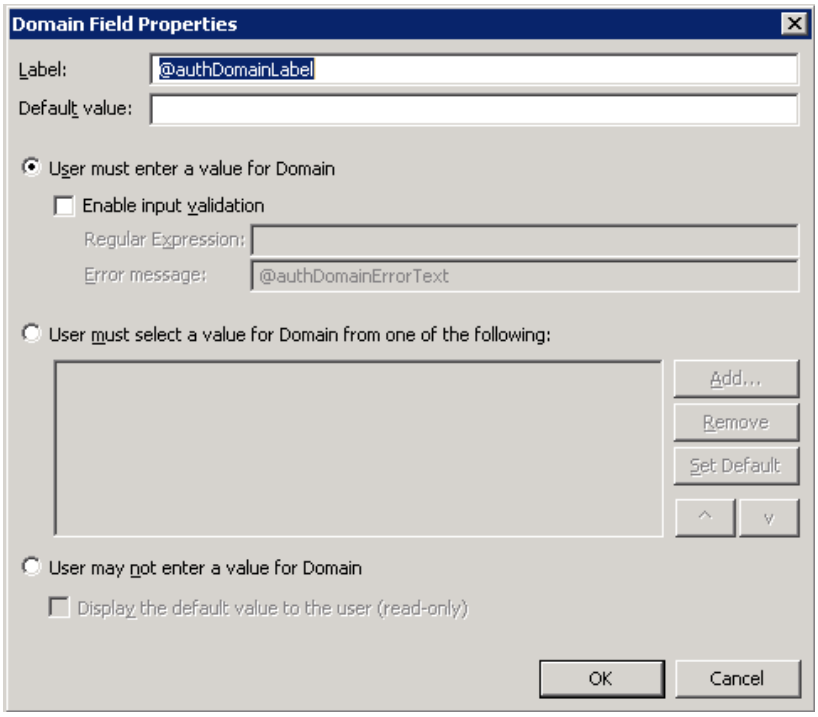


8 From the **Type** drop-down, select one of the four authentication options: **Email**, **Login**, or **PIN**.

If you select **Email**, **Login**, or **PIN** as the authentication type, you can define the properties for the **Domain**, **User**, and **Password**. For example, if you select **Email**, notice that the **Fields** section is active.

Defining Domain Properties

To define domain properties, double-click **Domain** (or click **Domain** and then click the **Properties** button). The **Domain Field Properties** dialog is displayed:



Note Domain definition is optional for all authentication types.

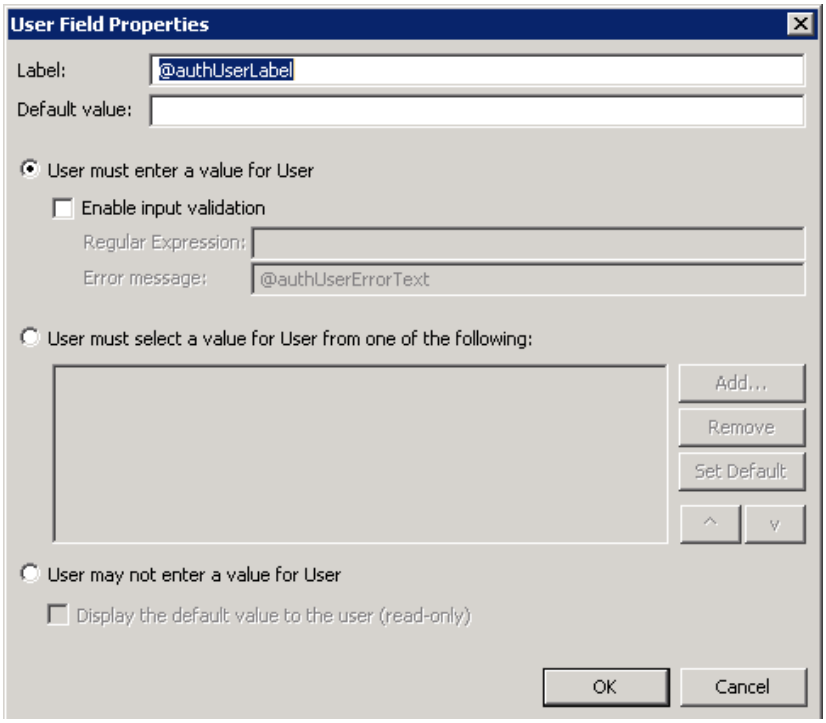
When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Domain** - The device user will need to enter a domain for authentication during login at the device.
- **User must select a value for Domain from one of the following** - If there are multiple domains in the environment, use this option to create a list of domains from which the user can select.
- **User may not enter a value for Domain** - This option prohibits the user from entering a domain value. When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it.

Continue with Defining User Properties (3-13).

Defining User Properties

To define user properties, double-click **User** (or click **User** and then click the **Properties** button). The **User Field Properties** dialog is displayed:



Note User definition is required for **Login** authentication and optional for all other authentication types.

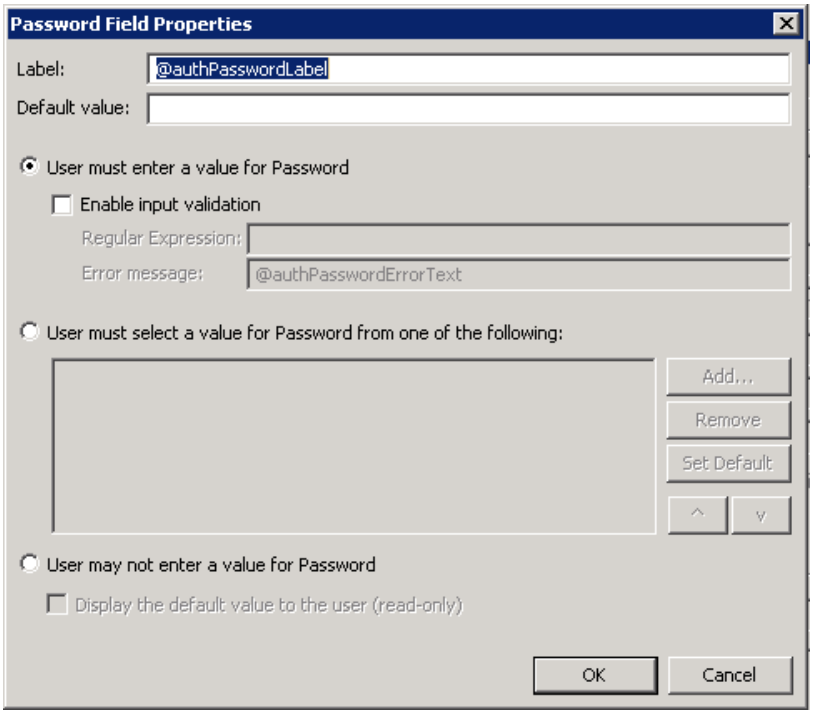
When you define a user, you can specify a **Default value** (user) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for User** - The device user will need to enter a user for authentication during login at the device.
- **User must select a value for User from one of the following** - If there are multiple users in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for User** - Do not select this option if you are using Email, Login, or PIN authentication. This option prohibits the user from entering a user value.

Continue with Defining Password Properties (3-14).

Defining Password Properties

To define password properties, double-click **Password** (or click **Password** and then click the **Properties** button). The **Password Field Properties** dialog is displayed:



Note Password definition is required for **Login** authentication and optional for all other authentication types.

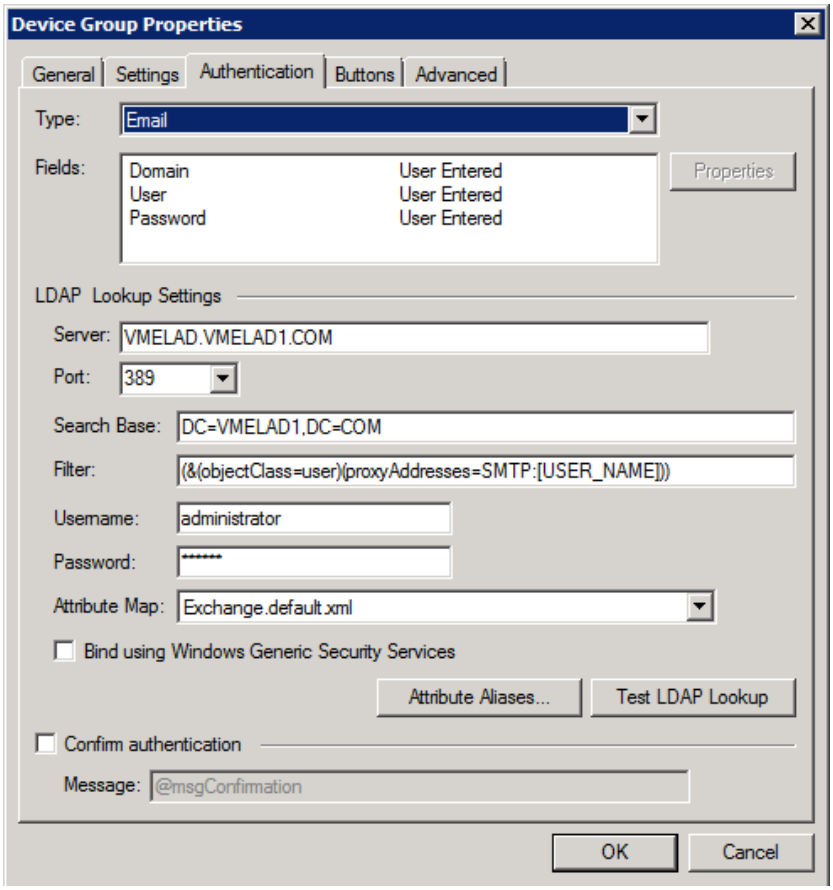
When you define a password, you can specify a **Default value** (password) that will be displayed at the device. In addition, you can specify one of the following:

- **User must enter a value for Password** - The device user will need to enter a password for authentication during login at the device.
- **User must select a value for Password from one of the following** - If there are multiple passwords available in the environment, use this option to create a list from which the user can select.
- **User may not enter a value for Password** - This option prohibits the user from entering a password. Use this option only when PIN authentication is used without a password. Do not select this option if you are using Email (with password), Login, or PIN (with password) authentication.

  When you select this option, you can indicate that the device will **Display the default value to the user (read-only)**. The user will see the **Default value**, but cannot change it. Although this option is provided for configuration flexibility, use of the option is not recommended.

Continue with Step 9 on page 3-15.

9 On the **Device Group Properties** page, keep the defaults for **Server**, **Port**, **Search Base**, and **Filter** (under the **LDAP LookUp Settings** heading)..



10 In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.

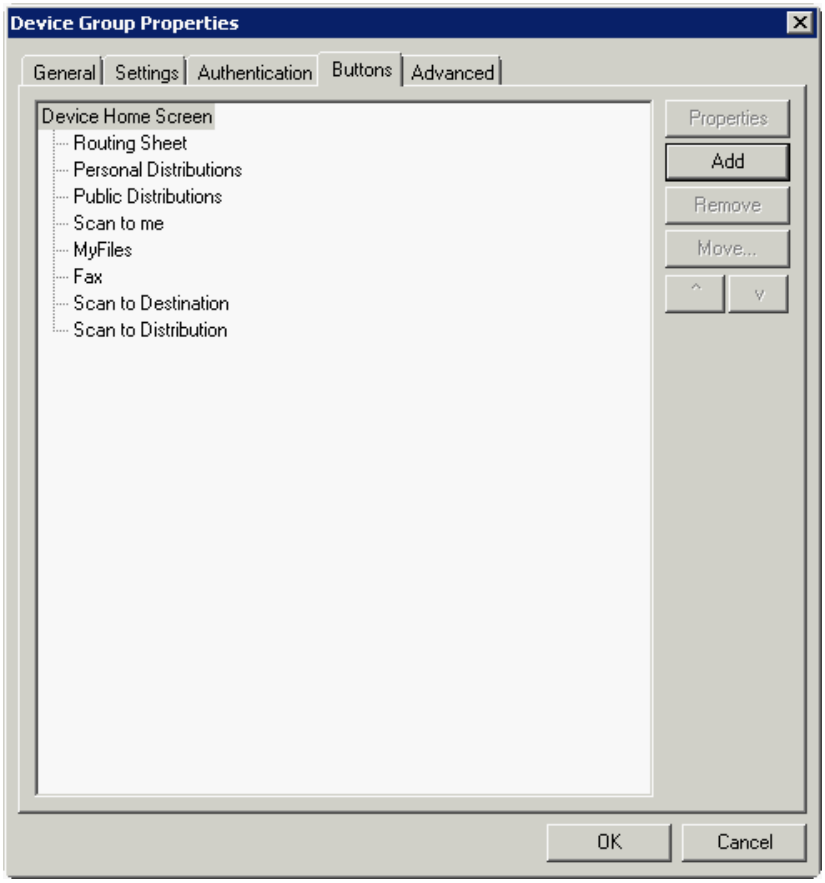
11 In the **Password** text box, enter the Windows user with permissions to the active directory password.

12 If you are working in an Exchange environment, select Exchange.default.sml (Exchange Attributes) from the **Attribute Map** drop-down.

13 In some cases, it is necessary to select **Bind using Windows Generic Security Services**.

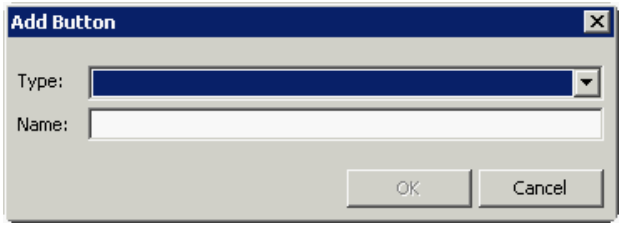
14 Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user's information when authenticating.

15 Click the **Buttons** tab to add or remove buttons that appear on the device.



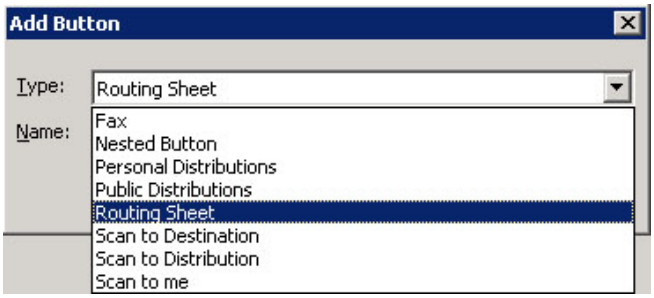
Note It is best to add or remove all previously set buttons before installing to the device. All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Reinstallation is required only if a new button is added or if the text on a currently installed button is modified. Uninstallation is required only if buttons are removed.

16 To add a button, click **Add**. The **Add Button** dialog is displayed.



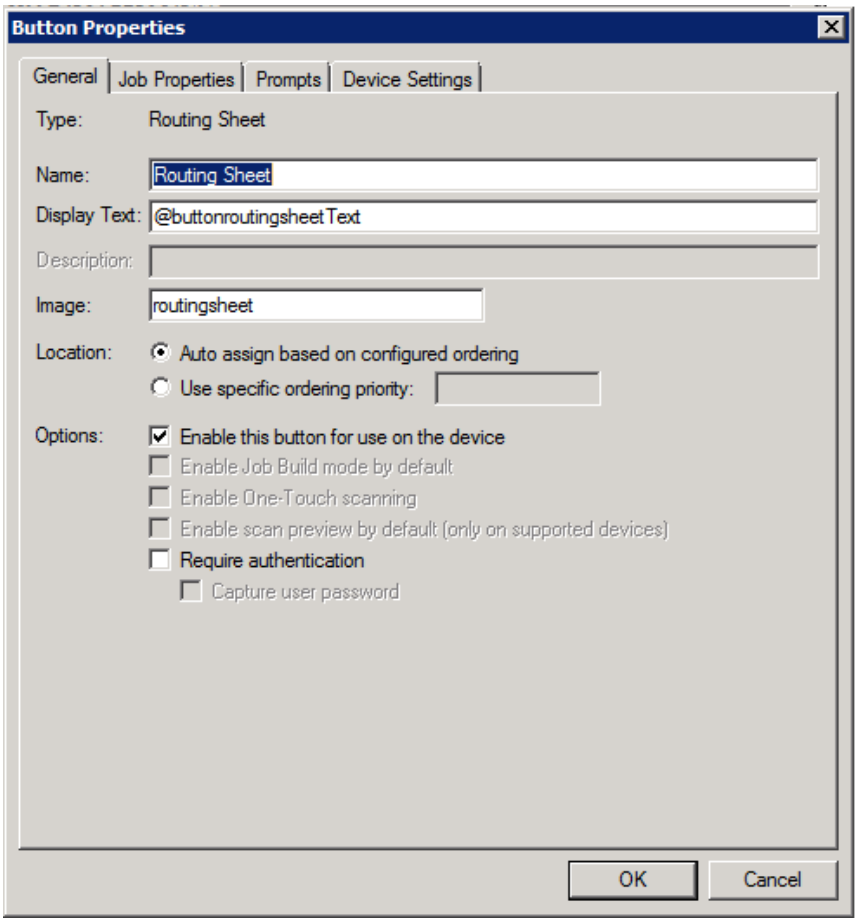
Note If the **Add** button is not active, click on **Device Home Screen**.

17 From the **Type** drop-down, select a button type.



18 Enter a **Name** for the button. Then, click **OK**.

19 You will need to define properties for the button. With the button highlighted on the list, click **Properties**.



Each button has a default **Name** and **Display Text** that you can edit.

Note Do not change Image from the default value.

Note To change "Scan to Destination" to "Scan to Folder," change the **Display Text**.

20 Specify a location for the button. Select either of these options:

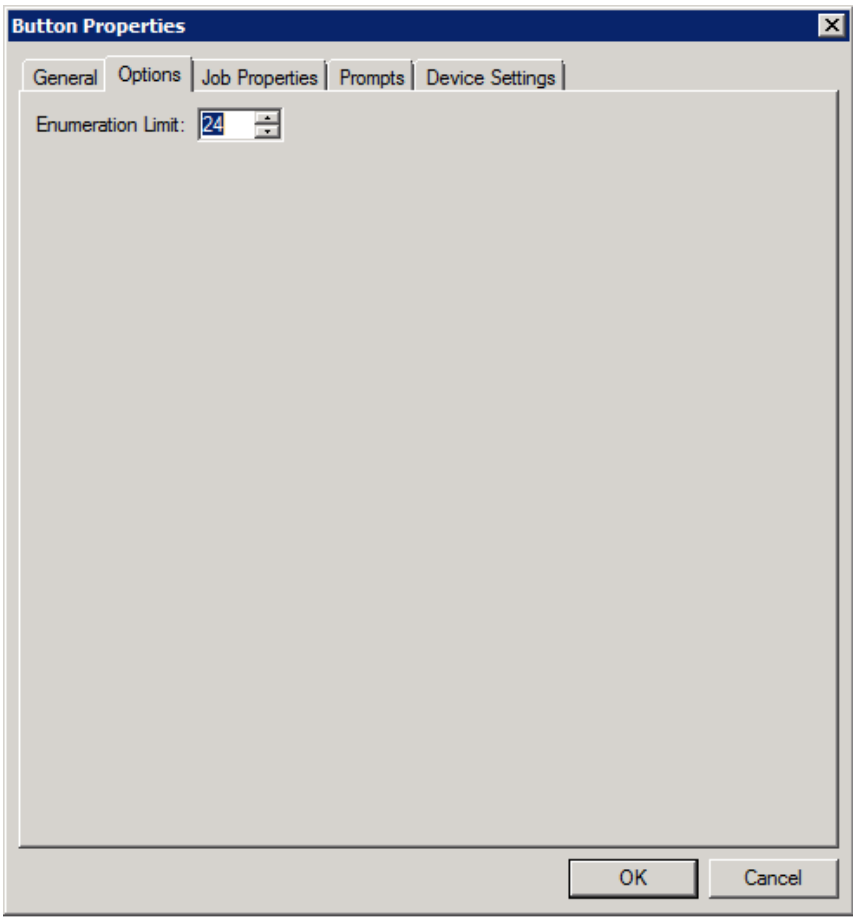
- **Auto assign based on configured ordering** - The button is positioned based on a predefined order.
- **Use specific ordering priority** - You can enter a value to indicate the button placement. Position 1 is in the upper left location and position 2 is in the upper right location, in a Z-order layout. The pattern is as follows:

  1 2
  3 4
  5 6
  etc.

21 Select additional options for the button:

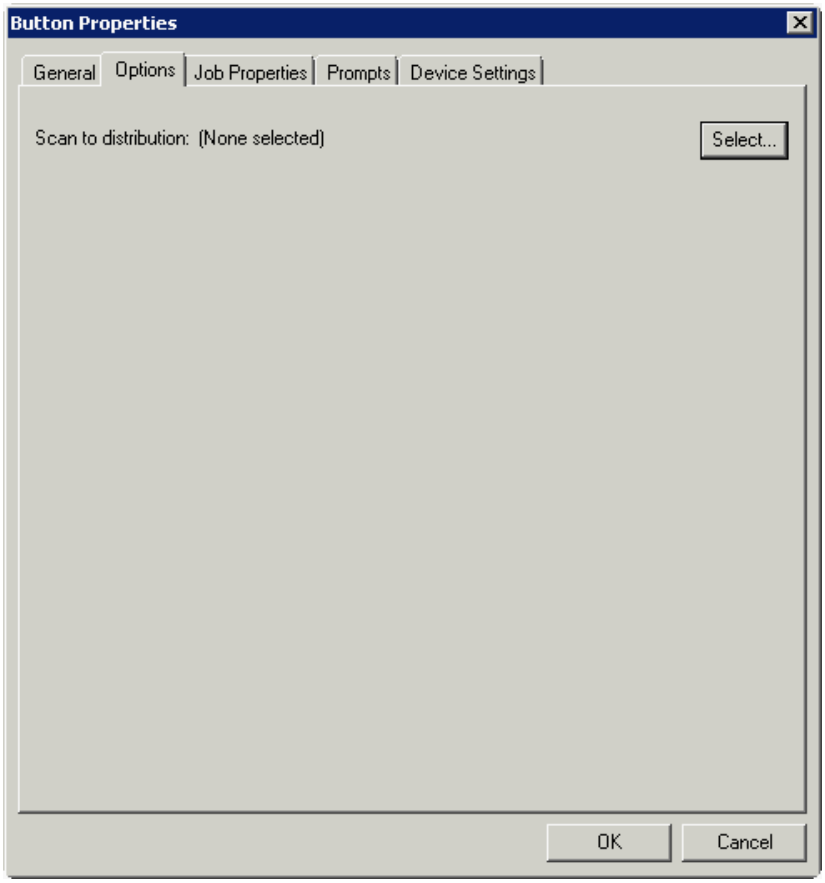
- **Enable this button for use on the device** - Self-explanatory.
- **Require authentication** - If you select this option, you can then indicate that the button should capture the user's password. Note that although the Routing Sheet feature typically does not require authentication, you can configure this requirement here.

22 If you are adding a **Personal Distributions** or **Public Distributions** button, click the **Options** tab.

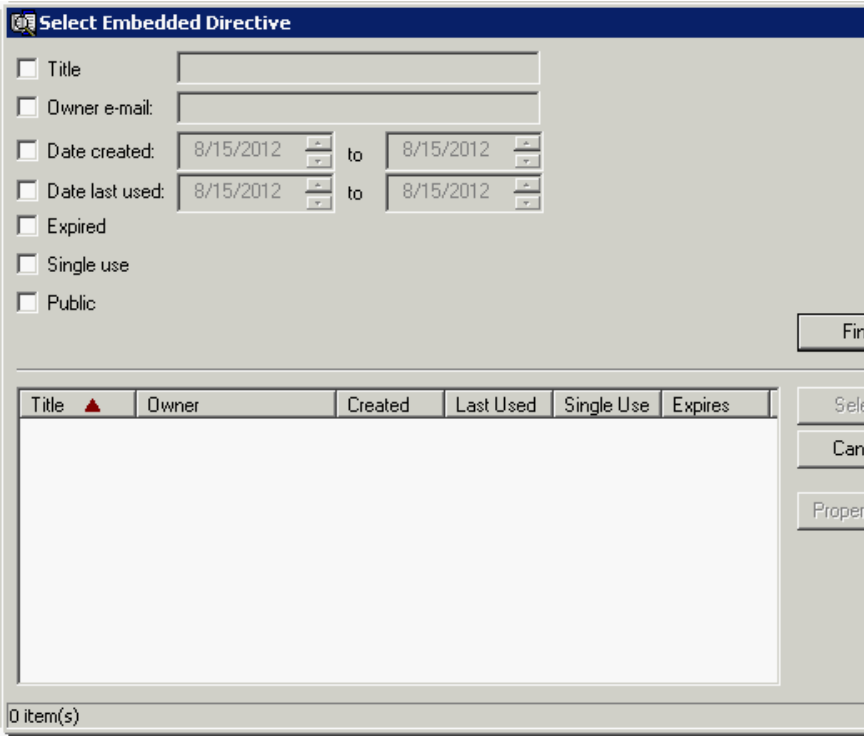


Set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

23 If you are adding a **Scan to Distribution** button, click the **Options** tab to route using an existing (already created) distribution.



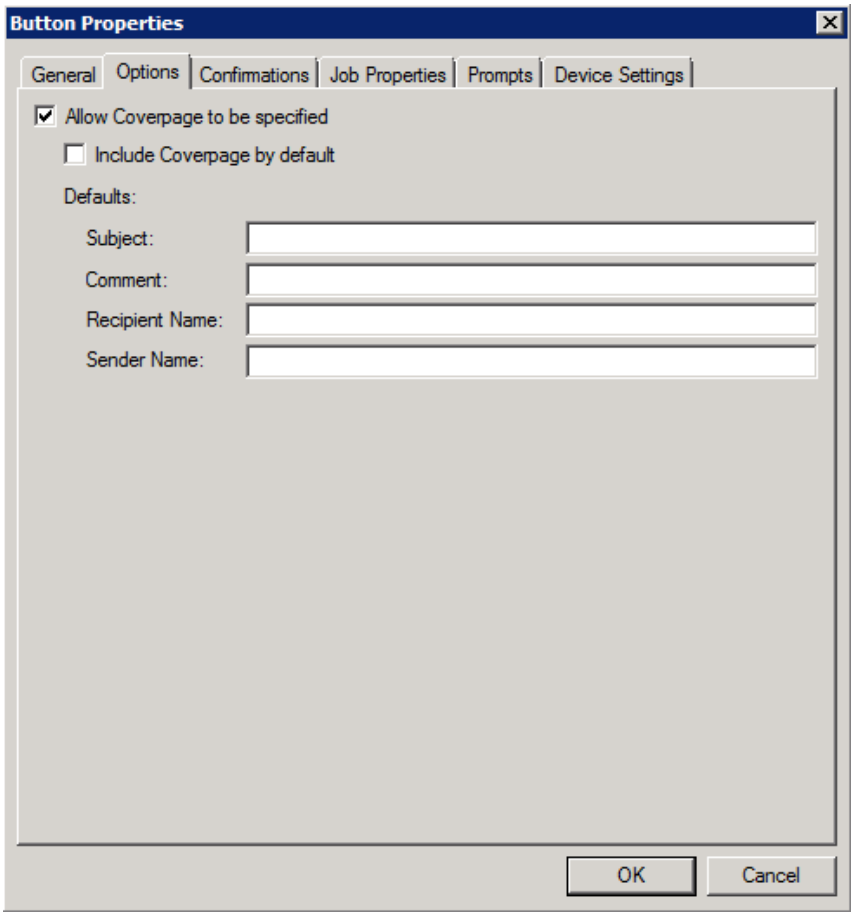
a Click **Select** and the **Select Embedded Directive** dialog is displayed enabling you to select a Distribution Rule.



b Click the **Find** button to display all distributions.

c Select the distribution and then click the **Select** button to choose the distribution that will be used when that button is selected from the device.

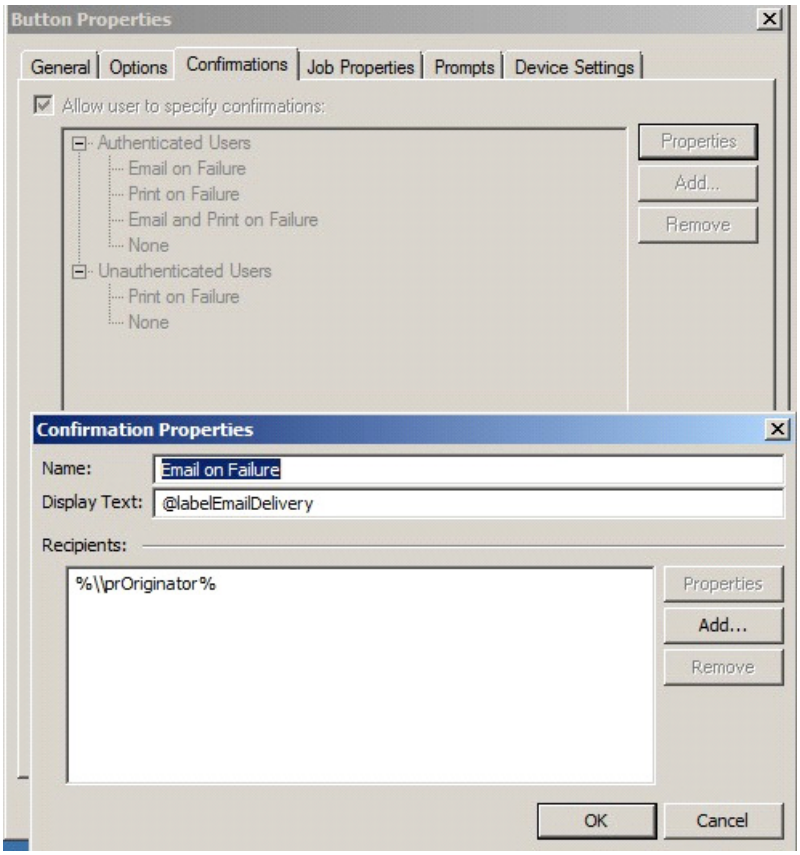
24 If you are adding a **Fax** button, click the **Options** tab to configure fax cover pages. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.



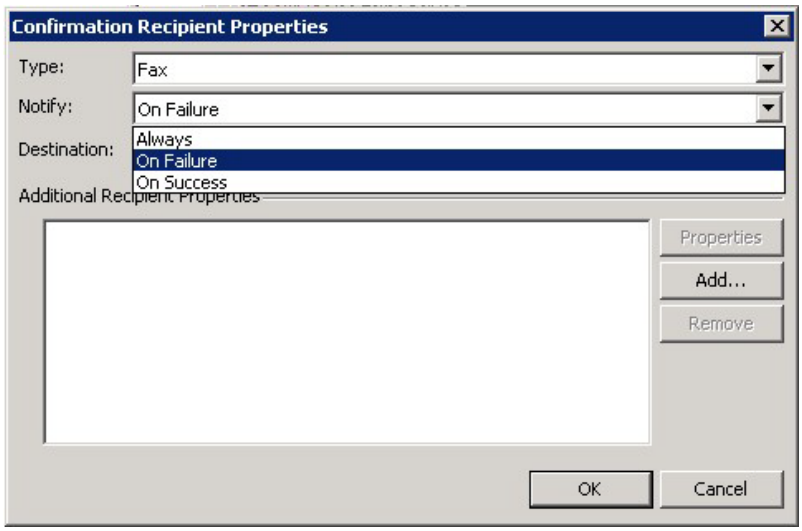
25 If you are adding a **Fax** button, click the **Confirmations** tab to:

- Allow authenticated and non-authenticated users to select the button.
- Define the type of fax confirmations (select a field and click **Properties**).
- Add recipients for confirmations (click the **Add** button).

For example, you can edit the fields for the Originator for faxes:



To change the recipient notifications, double-click the recipient. The **Confirmation Recipient Properties** page opens.



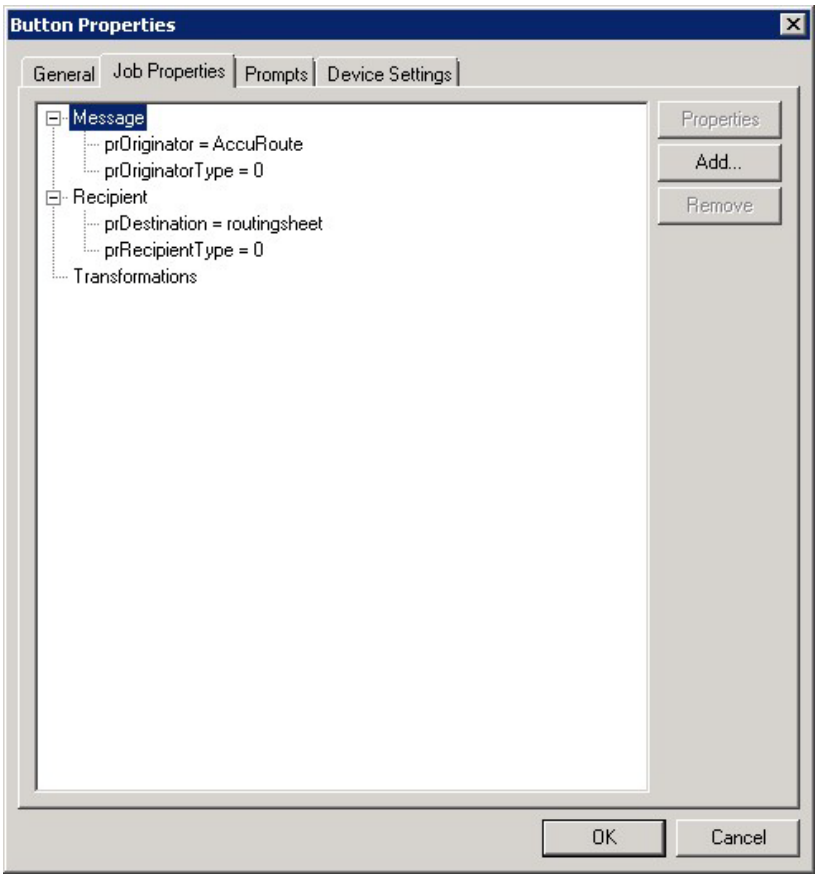
Type. - Leave this as the default.

Notify - Select **Always**, **On Failure**, or **On Success**.

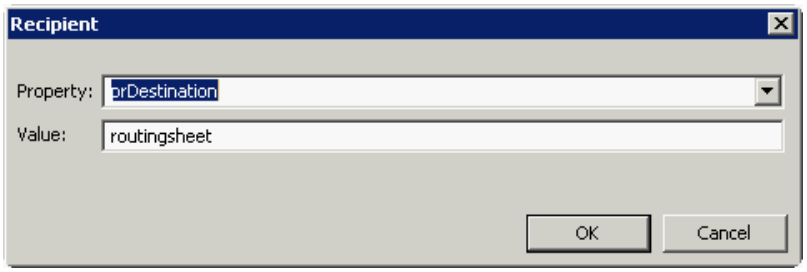
Destination - This is the recipient you selected.

Additional Recipients Properties - You can add additional recipients for this confirmation property.

26 If you are adding a **Routing Sheet**, **Scan to Destination**, **Scan to Distribution**, **Scan to Me**, or **Scan to My Files** button, click the **Job Properties** tab.



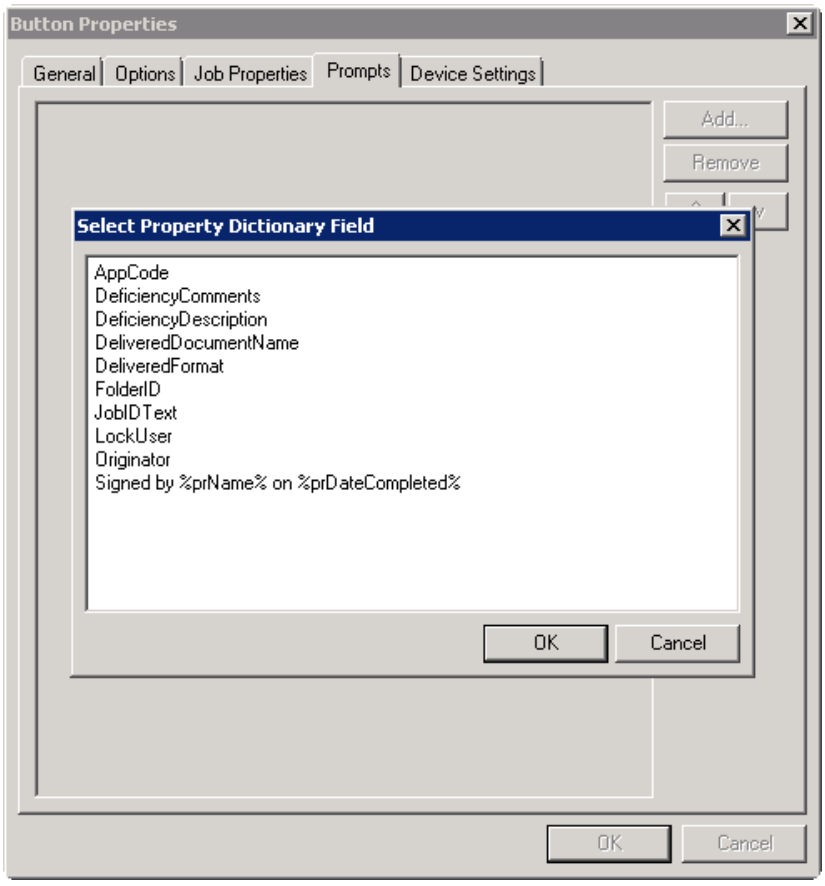
You can add, remove, or change a property. This example shows the property of a **Destination**.



You can change an **Originator**, **Destination**, or **Recipient**.

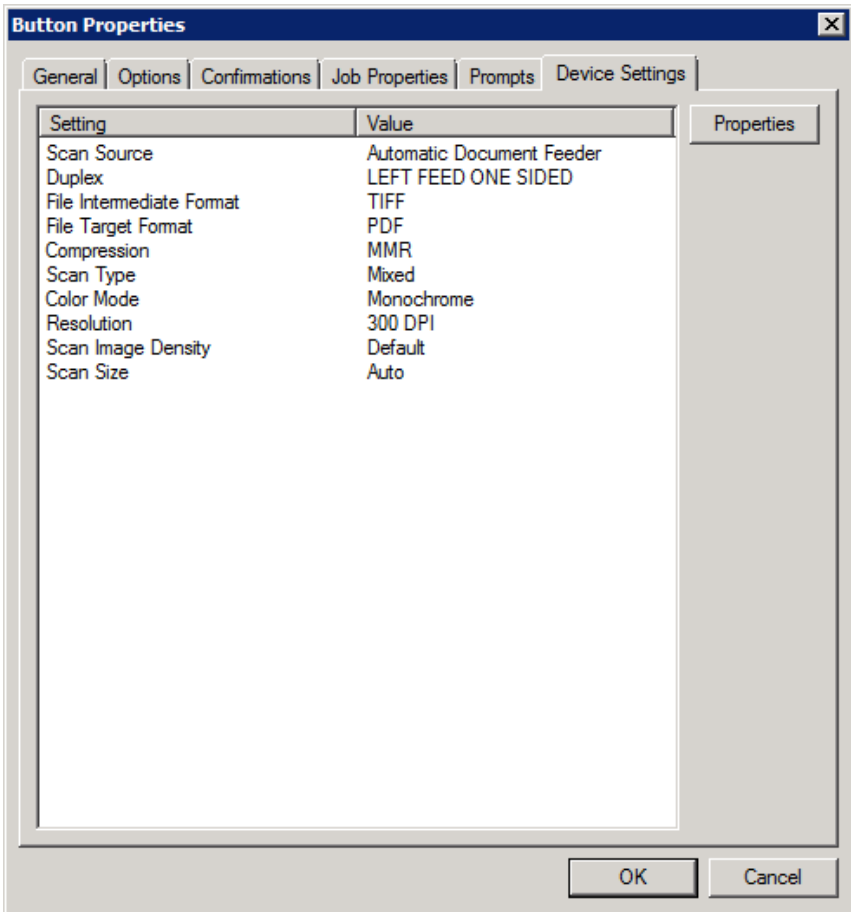
Note that the **Scan to Destination** button allows for message routing based on routing rules. The default is set to send to a destination of MyFiles, which can have an outbound rule associated with that destination to route to any location to which the AccuRoute server can route messages. This destination value can be edited.

27 Click the **Prompts** tab. Click **Add** to select a prompt configured on the AccuRoute server. The **Select Property Dictionary Field** is displayed.

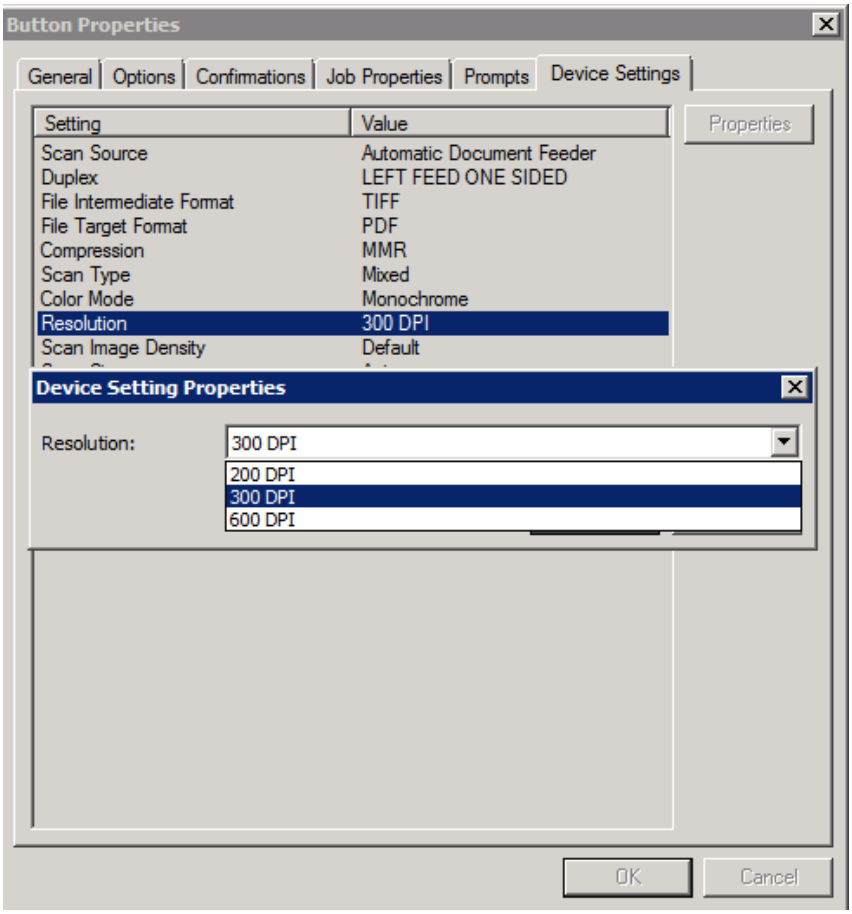


Select a prompt and click **OK**.

28 Click the **Device Setting** tab to configure native device scan settings. This is used for configuring a fleet of monochrome or color machines to use the same scanning settings. For example, the Fax button should only use Monochrome scan settings for better output quality.



29 Select a setting and click **Properties** to change the setting value. For example::

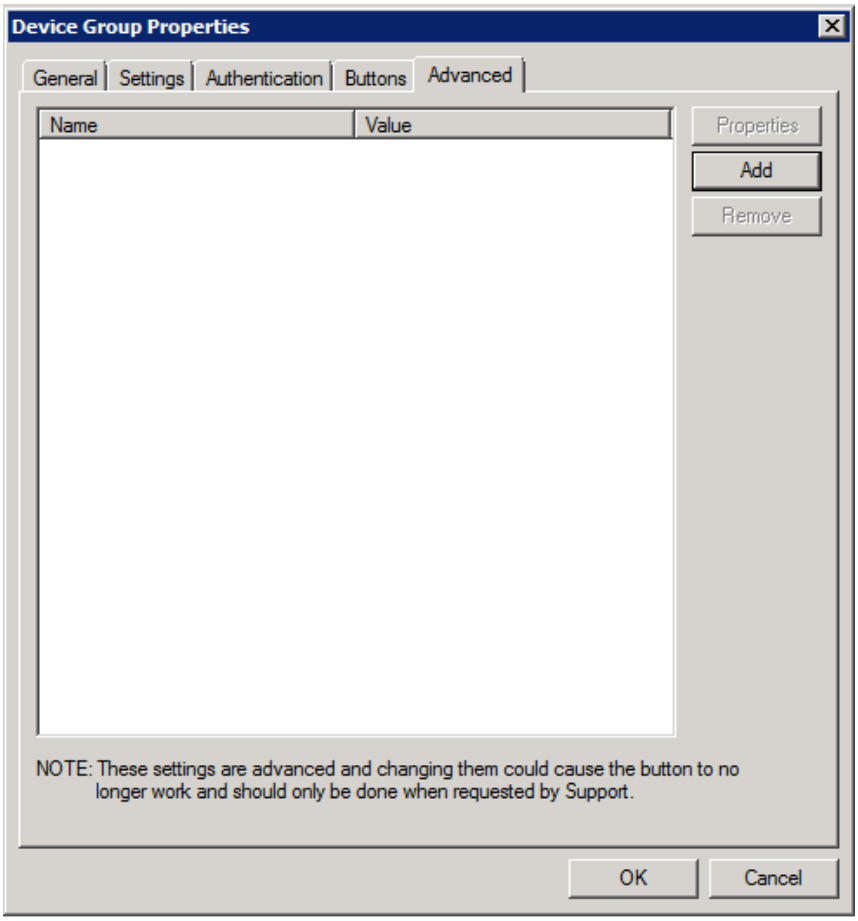


30 Click **OK** to return to the **Device Group Properties**.

Note It is best to add or remove all previously set buttons before installing to the device. All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Reinstallation is required only if a new button is added or if the text on a currently installed button is modified. Uninstallation is required only if buttons are removed.

31 Click the **Advanced** tab to modify settings that control the device's native settings for connectivity timeouts and job refresh settings.

Note It is strongly suggested that these settings are NOT changed. Take note of all defaults before changing any of these values.



32 Click **OK** to end your work with the **Device Group Properties**.

Configuring for HTTPS support

This section describes how to configure HTTPS support from the AccuRoute Server Administrator using a signed certificate.

The configuration process on the AccuRoute Server Administrator includes:

Creating a self-signed certificate (3-28)

Exporting and saving the certificate (3-28)

Creating an SSL binding (3-28)

Verifying the SSL binding (3-29)

Adding the certificate to the Embedded AccuRoute Ricoh Device Client (3-29)

Adding the SSL binding configuration to the server (3-31)

Alternatively, you can configure HTTPS support using either of the following methods:

- from the device by using an SD card with a modified DALP file
- from the device Embedded Web Server interface with a modified DALP file pointing to a (zipped) `xletrepository.zip` file

For more information on these methods, refer to Configuring HTTPS support from the Embedded Web Server or an SD Card (A-5).

Creating a self-signed certificate

1. Open **Internet Information Services Manager** (IIS).
2. Click the local machine and open **Server Certificates**.
3. Right-click in the **Server Certificates** dialog and select **Create Self-Signed Certificate**.
4. Enter a **Friendly** name matching the name of the server and click **OK**.

   The self-signed certificate is created based on the fully-qualified name.

Exporting and saving the certificate

1. In the **Server Certificate** dialog in IIS, right-click the certificate created in the procedure above (*Creating a self-signed certificate*) and select **View**.
2. In the **Certificate** dialog, click the **Details** tab.
3. Select **Copy to File**. The **Certificate Export Wizard** appears.
4. Click **Next**.
5. In the **Private Key** dialog, select **No, do not export the private key** and click **Next**.
6. In the **File Formats** dialog, select **Base-64 encoded X.509 (.CER)** and click **Next**.
7. In the **Filename** dialog, browse to a location at which to save the `.cer` file and enter a filename.
8. Click **Save** and then **Next**.
9. Verify the settings and click **Finish**. The export is complete.

Creating an SSL binding

1. Open **Internet Information Services Manager**.

2. Click the **Default** website and click **Edit Site > Bindings**, in the top right-hand corner. The **Site Bindings** dialog appears.
3. Click the **HTTPS** type and select **Edit**. The **Edit Site Bindings** dialog appears.

> **Note** If the HTTPS does not yet exist, select **Add** (instead of **Edit**) to create one.

4. From the **SSL certificate** drop-down menu, select the certificate you created earlier and click **OK**.
5. Click **Close**.

Verifying the SSL binding

1. In **Internet Information Services Manager**, expand the tree view and select **OmtoolWebAPI**.
2. Click **Browse *:443 (https)** under **Manage Application/Browse Application**, in the top right-hand corner of the IIS dialog.
3. A message stating `There is a problem with this website's security certificate` appears. This is normal and you can continue the configuration.
4. Click the `Continue to this website` option.
5. Verify that the **IIS 7** dialog appears.

Adding the certificate to the Embedded AccuRoute Ricoh Device Client

1. On the AccuRoute server, navigate to:

   `C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository`
2. Use WinZip to open the `cacerts.jar` file.
3. Create a folder at the root of `C:\` (for example, `C:\certs`).
4. Locate the `jdk-certs` file within the `cacert.jar` file and extract it to the local system.
5. Place both the certificate file and the `jdk-cacerts` file in the newly created folder.

> *Important* Java™ is included in the AccuRoute installation. Instructions below require use of the Java Keytool. The AccuRoute installation places Java in `C:\Program Files (x86)\Omtool\Ricoh ESA\JRE\bin`.
> If your Java installation is in a different location, alter the path used below to match.

6. Open the command prompt and enter

```
C:\Program Files (x86)\Omtool\Ricoh
ESA\JRE\bin;C:\Program Files (x86)\Omtool\Ricoh
ESA\JRE\bin;%path%
```

This adds the Java Path Variable to the current command screen.

7 In the command prompt, change the directory to the newly created folder (for example, `C:\certs`).

8 Using the Keytool, run the following command:

```
keytool -keystore jdk-cacerts -storepass changeit -
import -alias <commonname> -file <certificatename> -
trustcacerts
```

where *<commonname>* is the fully-qualified domain name and *<certificatename>* matches the name of the certificate.

Select **Yes** to import the certificate.

9 Add `jdk-cacerts` back into `cacerts.jar`. To do so:

a Open `cacerts.jar` using WinZip.

b Delete the `jdk-cacerts` file located within `cacerts.jar`.

c Right-click `jdk-cacerts` and select **WinZip > Add to Zip File** (the one with the certificate added) into the `cacerts.jar` file. Add the file to the `cascerts.jar` file.

d In the `cacerts.jar` file, verify that the `jdk-cacerts` file has the proper date and time stamp.

e Open `C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository` and delete the `cacerts.jar` file.

f Copy the `cacerts.jar` file into:

```
C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository
```

10 Verify that the fully-qualified domain name is correct in `OmtoolXlet.dalp`. To do so:

a Open the `OmtoolXlet.dalp` file.

b Change `-servicepath` from `%URL_ISAPI%` to `https://<fully-qualified AccuRoute server domain name>/WebAPI/Scripts/omisapiu.dll` in the following line:

```
<argument>-servicepath:%URL_ISAPI%</argument>
```

c Change `-sourcename` from `%GROUP_NAME%` to the group name of interest, as it appears under **Devices** in the server, in the following line:

```
<argument>-sourcename:%GROUP_NAME%</argument>
```

d Change `display-mode` from `%DISPLAY_MODE%` to `VGA` in the following line:

```
<display-mode size="%DISPLAY_MODE%" />
```

e Proceed to the directory `C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts:` and edit the `OmISAPIU.xml` file to reflect the URL change.

f Replace the URL to `https` along with the fully-qualified domain name of the AccuRoute server.

```
<FileTransfer>https://<fully-qualified AccuRoute server domain name>/WebAPI/FileTransfer/</FileTransfer>
```

11 Require SSL for the WebSite:

a Open **Internet Information Services Manager**.

b Expand `local machine\Default WebSite` and select **WebAPI**.

c Open **SSL Settings** and select **Require SLL**.

d Under **Client Certificates**, select **Ignore**.

12 Change device settings on the Ricoh device under **User Tools > System Settings > Interface Settings** as follows:

- **Select DNS configuration**: Enter the DNS IP address.
- **Select Domain Name**: Enter a fully-qualified domain name for the DNS server.

Adding the SSL binding configuration to the server

1 In the AccuRoute server console tree, expand the AccuRoute Server Administrator and click **Devices**.

2 Right-click the **Device Group** of interest and select **Properties**. The **Device Group Properties** screen appears.

3 Select the **Settings** tab and enter the following in the Web API text box:

```
https://<fully-qualified AccuRoute server domain name>/WebAPI/Scripts/omisapiu.dll
```

4 Click **OK**.

Continue with Installing the Ricoh (ESA) Device Client on the device (3-31).

Note If Embedded AccuRoute for Ricoh is already installed on the device it must be uninstalled and then reinstalled for the changes to be reflected.

Installing the Ricoh (ESA) Device Client on the device

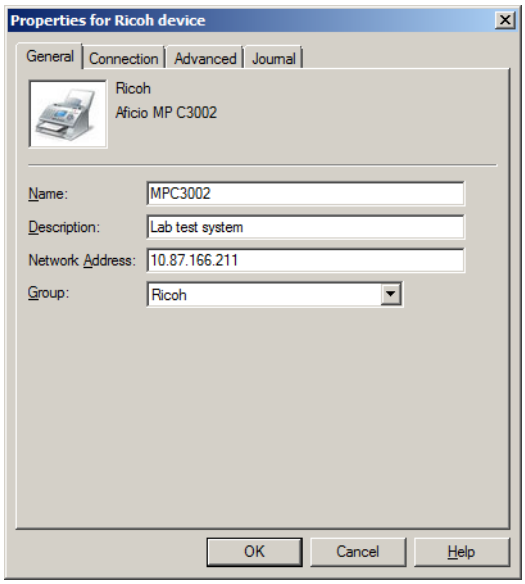
The installation of a Ricoh ESA device client using the AccuRoute Server Administrator includes the following steps:

- Add the Ricoh device to the Ricoh group in the Devices node.
- Verify that the device was properly added to the group.

- Install the device from the AccuRoute Server Administrator.
- Reboot the device from the Administrator to push the AccuRoute buttons out to the Ricoh MFP.

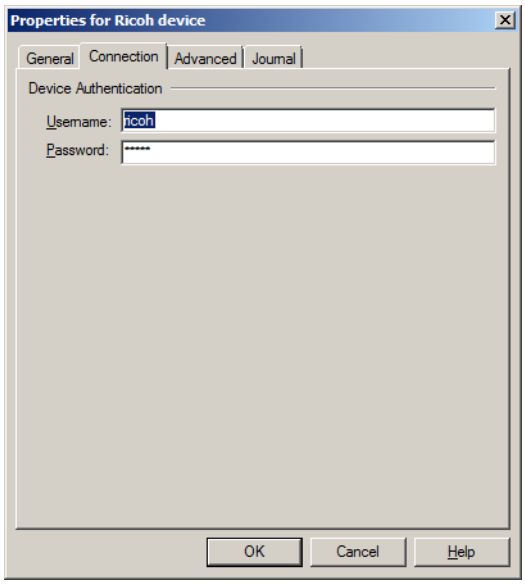
To install the Embedded AccuRoute for Ricoh (ESA) Device Client using the AccuRoute Server Administrator:

1. Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
2. In the console tree, expand the AccuRoute Server Administrator.
3. Go to the **Devices** node.
4. Right-click the **Ricoh** device group and select **New > Device**. The **Properties for Ricoh device** page appears.



5. In the **General** tab, enter the appropriate device information, including its **Name**, a **Description** of the device, and in the **Network Address** text box, enter the IP address of the Ricoh device.
6. Select **Ricoh** from the **Group** drop-down menu.

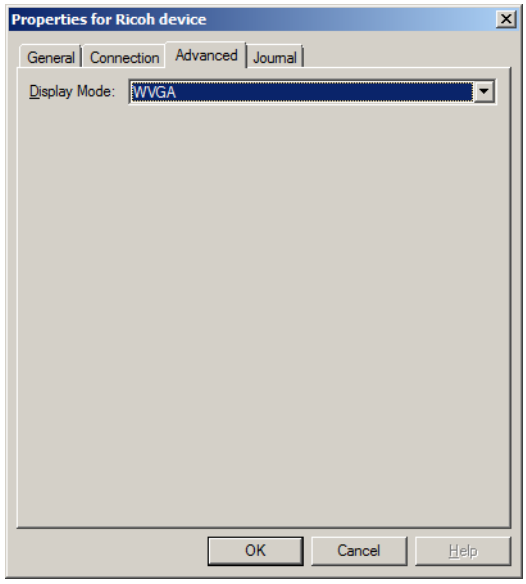
7 Select the **Connection** tab.



8 Enter the **Username** and **Password** for the device of interest.

> **Note** **Admin** and **No Password** appear as default values for devices. However, AccuRoute software requires a password when setting up the devices.

9 Go to the **Advanced** tab and select **WVGA** from the **Display Mode** drop-down menu.



10 Click **OK** to add the device to the Ricoh device group.

11 To verify that the device was successfully added to the **Group** listing, right-click on the device and select **Query** from the drop-down menu.

Verify that the query is successful.

12 Right-click the device again and select **Install**.

Verify that the system successfully installs the device from the MMC console.

13 Then right-click the device and select **Reboot**.

Note The installation adds the Ricoh Device Client to the device with an Auto-Start status. The device client does not initially start automatically, but does start when you next reboot the device.

If you do not reboot the device, you need to manually start the Ricoh Device Client via Ricoh's Web Image or from the device itself under **Extended Feature Settings**.

Verify that the device reboots and that the **AccuRoute** button now appears in the control panel of the device.

Upgrading the Ricoh (ESA) Device Client

Important Omtool does not support a specific upgrade process for the AccuRoute Embedded Device Clients at this time.

Instead, to update your existing Device Clients, you must first uninstall the old version and then install the new version.

Uninstalling the Ricoh (ESA) Device Client from the Ricoh device

To uninstall the Ricoh (ESA) Device Client using the AccuRoute Server Administrator:

1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2 In the console tree, expand the **AccuRoute Server Administrator**.

3 In the **Devices** node, identify the device from which you want to uninstall the client.

4 Right-click the device and select **Uninstall** from the drop-down menu. The system uninstalls the AccuRoute buttons from the device.

Section 4: Remote Installation and Configuration

This section includes:

Configuring the Embedded AccuRoute for Ricoh (ESA) Device Client when the Intelligent Device Client is on a remote system

In environments where the IIS server is remote from the Omtool Server, the Intelligent Device Client must be installed on the remote system. The Ricoh ESA client must be installed on the Omtool Server, and you will need to modify files to point to the remote Intelligent Device Client, so that the installed buttons on the physical device can communicate to the server from the remote Intelligent Device Client.

The steps to install the Intelligent Device Client on a remote system include the following:

- Setting required COM permissions for remote AccuRoute Intelligent Device Client
- Adding the remote server's name to DCOM
- Installing the AccuRoute Intelligent Device Client on the remote system
- Installing the Embedded Device Client for Ricoh on the AccuRoute Server
- Creating the Device Group for the remote Device Client

Setting required COM permissions for remote AccuRoute Intelligent Device Client

When performing a typical AccuRoute server installation, the AccuRoute Intelligent Device Client is installed by default. No separate installation of the client is necessary. For custom installations, the installer can un-check the AccuRoute Intelligent Device Client option from the list of components to install.

If you need to install the AccuRoute Intelligent Device Client on a separate system, you must configure the following DCOM permissions for the Anonymous_User user.

To give Anonymous_Logon COM permissions:

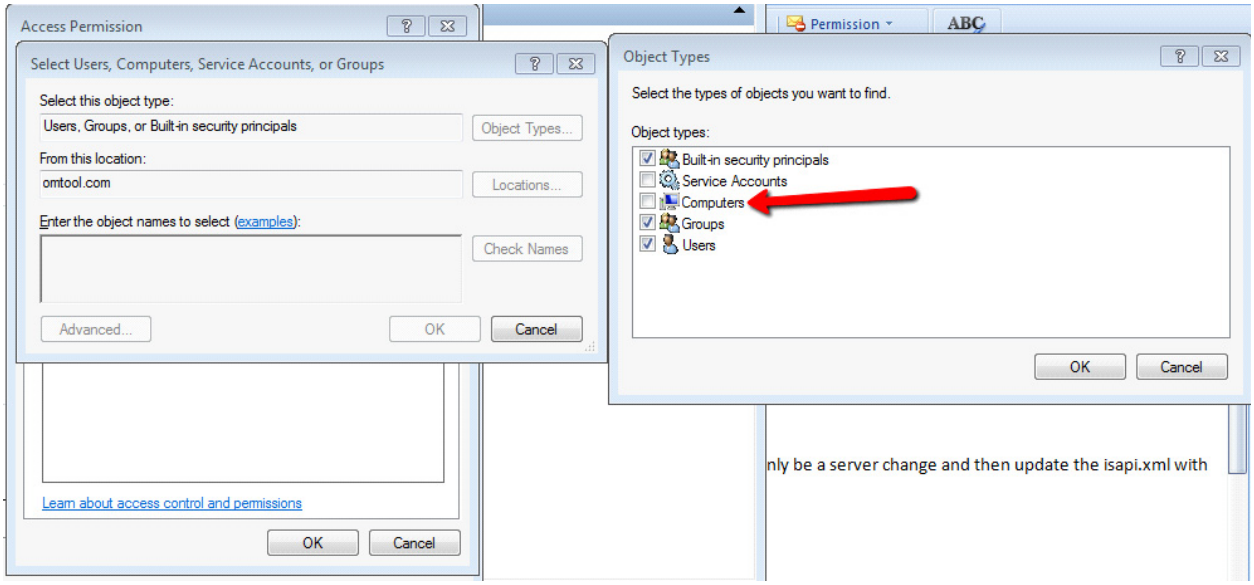
1. Log in to the system where you will install the AccuRoute server using an account that belongs to the Administrator.
2. Click **Start > Control Panel > Administrative Tools > Component Services**.
3. In the console, expand **Component Services > Computers**.
4. Right-click **My Computer** and select **Properties** from the drop-down menu.
5. Click **COM Security**.
6. In the **Access Permissions** section, click **Edit Limits**. The **Access Permission** page opens.
7. For user **Anonymous_logon**, select **Local Access** and **Remote Access** permissions.
8. Click **OK** to close the page.
9. In the **Launch and Activate Permissions** section, click **Edit Limits**. The **Launch Permissions** page opens.
10. For user **Anonymous_logon**, select **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** permissions.
11. Click **OK** twice to close the **Properties** page.

Adding the remote server's name to DCOM

1. Add the remote server's name to DCOM on the AccuRoute server. For example: `VMTesting$`

   Note You must append the name with a dollar sign ($).

2. Select Computers in the Object types when adding the server name.



3. Reboot the AccuRoute server.

Installing the AccuRoute Intelligent Device Client on the remote system

For steps to install the AccuRoute Intelligent Device Client on a remote system, see the 'AccuRoute Intelligent Device Client' chapter of the AccuRoute Server Installation Guide.

Installing the Embedded Device Client for Ricoh on the AccuRoute Server

For steps to install the Embedded Device Client for Ricoh, see Installation and Configuration on a Local AccuRoute Server (3-1).

Creating the Device Group for the remote Device Client

To create a Device Group for the remote environment, follow all the steps described in Creating a group of devices (3-8), with the addition of the following note:

> **Note** In the Device Group Settings tab, change the IP address in the Web API window to reflect the IP address of the remote Intelligent Device Client.

Section 5: Optional Configuration

This section includes:

Setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster

You must configure this on the Web server of the cluster.

1. Click **Start > Run**.
2. Enter `dcomcnfg`. Click **OK**.

   The **Component Services** console opens.
3. Expand **Component Services > Computers > MyComputer > DCOM Config**.
4. Browse down to find the application **OmGFAPIServer**.
5. Right-click the application and select **Properties** from the drop-down menu.

   The **Properties** page opens.
6. Click **Security** to open the **Security** page.
7. Click **Edit** for all three levels: **Launch and activation permissions**, **Access Permissions** and **Configuration Permissions**.
8. Add **Anonymous** to the list of users and give it full permissions.

Additional procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the AccuRoute Server Installation Guide.

Configuring for AccuRoute to remain the priority application after power off or standby

If the AccuRoute does not display on the LCD panel after power off or standby, you can set it as the priority application.

1. Press the **User Tools/Counter** Button.
2. Press the **System Settings** button.
3. On the **General Features** tab, select the **Function Priority** button.
4. Select **JavaTM/X** to set AccuRoute as the priority.

Configuring a Distribution Rule to appear at the top of the device listing

When creating a Distribution Rule in AccuRoute Desktop or AccuRoute Web Client, you can mark it to appear at the top of a device listing. Distribution Rules that are used most frequently can be marked to appear on top of listings so that the device user can easily see and use the Distribution Rule, rather than needing to scroll through a list.

To configure Distribution Rules to appear on top of a device listing:

1. Click the **Options** tab to open the **Message Options** page.
2. Check the **Sort at top of device listing** option.
3. Save your changes.

Note The newer Distribution Rules appear first in the list, then the Distribution Rules are listed alphabetically. Finally, the rules marked to show at the top of a device appear.

Configuring scan settings in Distribution Rules

You can configure scan settings in the Distribution Rules you create. When a user goes to a device and scans a document using a Distribution Rule with previously-defined scan settings, the document is scanned using the settings defined in the server. The scan settings at the device are ignored.

To configure scan settings in a Distribution Rule:

1. Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
2. In the console tree, expand the AccuRoute Server Administrator and enable scan settings for the group of users who will use the settings:
   a. Open the **Group Properties** page and select the **Scan Settings** tab.
   b. Check the **Enable members of this group to use the selected Scan Settings** option.
   c. Select the settings and save your changes.
3. Open AccuRoute Desktop or AccuRoute Web Client and create Distribution Rules. The scan settings enabled in the server are available under the **Options > Scan Settings** menu.
4. Select the scan settings for the Distribution Rule.
5. Log in to the Ricoh device and select a Distribution Rule with which to scan a document. The scan settings in the Distribution Rule override any device scan setting.

For example, if "Mono" is selected as the color mode in server, the **Mono** option will be available:

- On the **Tools > Message Options > Scan Settings** tab of the AccuRoute Desktop Client.
- On the **Distributions > Options > Scan Settings** tab of the AccuRoute Web Client.

You can create and save a Distribution Rule with the Mono scan setting and then select that Distribution Rule on the device (under **Public** or **Personal** distributions). You can verify the Color mode on **More options** screen for the Distribution Rule. The Color mode set for that Distribution Rule will be Black.

Configuring the Universal Input connector for Ricoh ESA file processing

AccuRoute Universal Input connector is a connector that can pick up and process orphaned Ricoh ESA files and route them to the AccuRoute server. An AccuRoute server supports multiple connectors, all managed by the **Connector** component on the AccuRoute server.

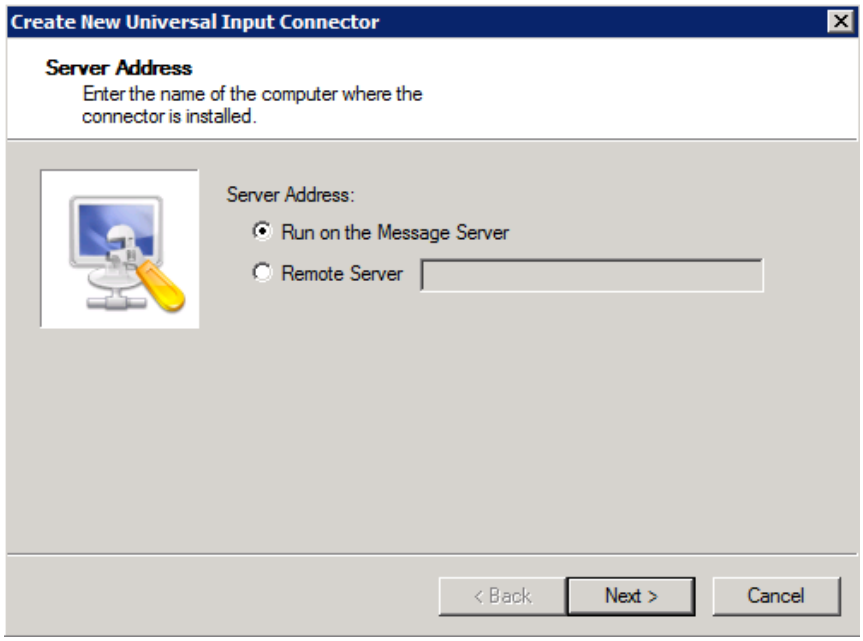
If the Ricoh ESA application fails to route scanned files to the AccuRoute server, this new connector will be able to pick up and process the Ricoh ESA files for processing on the AccuRoute server.

Requirements for the Universal Input Connector

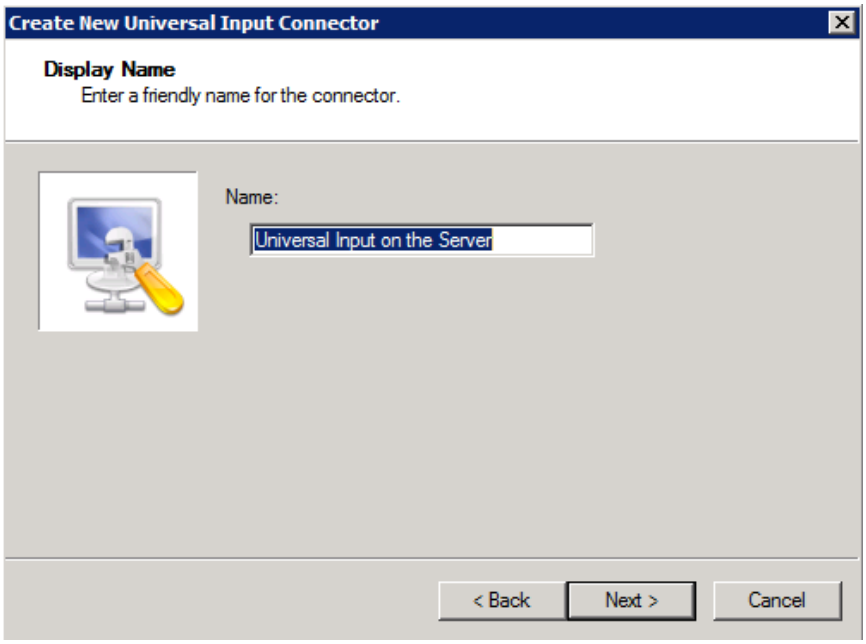
- AccuRoute v5.0
- AccuRoute Embedded Device Client for Ricoh ESA
- Universal connector license

Installing the Universal Input connector license

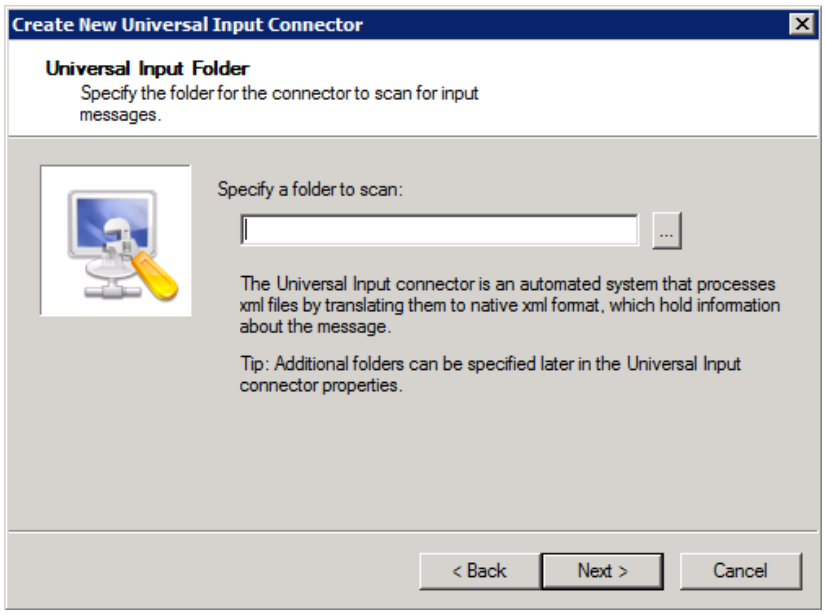
1. Log in to the AccuRoute v5.0 server using an account that belongs to the AccuRoute Administrators group.
2. Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
3. In the console tree, expand the AccuRoute Server Administrator and right-click **Connectors**. Select **New AccuRoute connector for > Universal Input**.



4 Enter a name for the connector or keep the default name. Click **Next**.

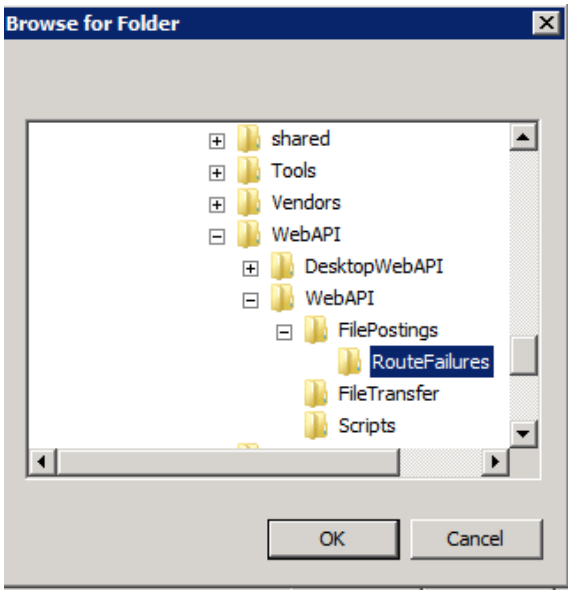


5 Browse to the folder from which the Universal Input connector will be processing files. Click **Next**.

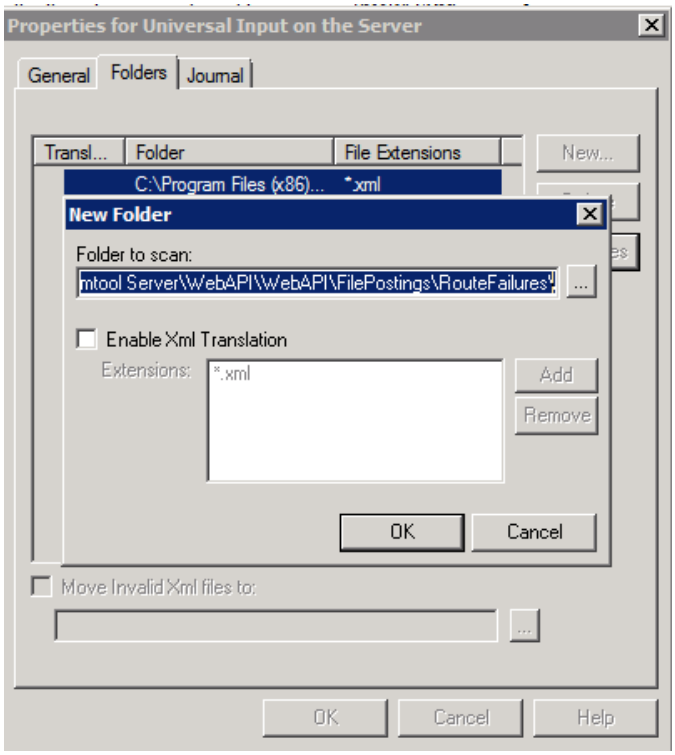


a If the Ricoh ESA application already had a processing failure and has automatically created a **RouteFailures** folder, browse to that folder in this location:

```
C:\Program Files (x86)\Omtool\Omtool
Server\WebAPI\WebAPI\FilePostings\RouteFailures
```

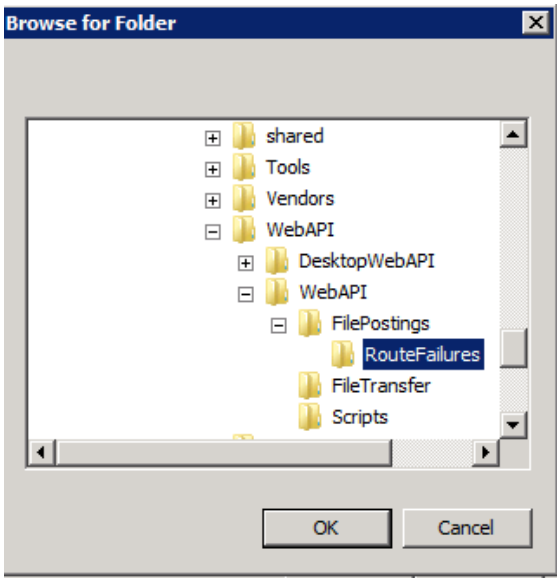


Click **OK** and verify on the **Folders** tab that the **RouteFailures** folder has **Enable Xml Translation** unchecked. Click **OK** twice to save the connector configuration.



b If you are setting up the Universal Input connector prior to any processing failures, create a folder named **RouteFailures** in this location:

```
C:\Program Files (x86)\Omtool\Omtool
Server\WebAPI\WebAPI\FilePostings\RouteFailures
```



Click **OK**.

6 Once the folder is selected, leave the **Enable Xml Translation** box unchecked.

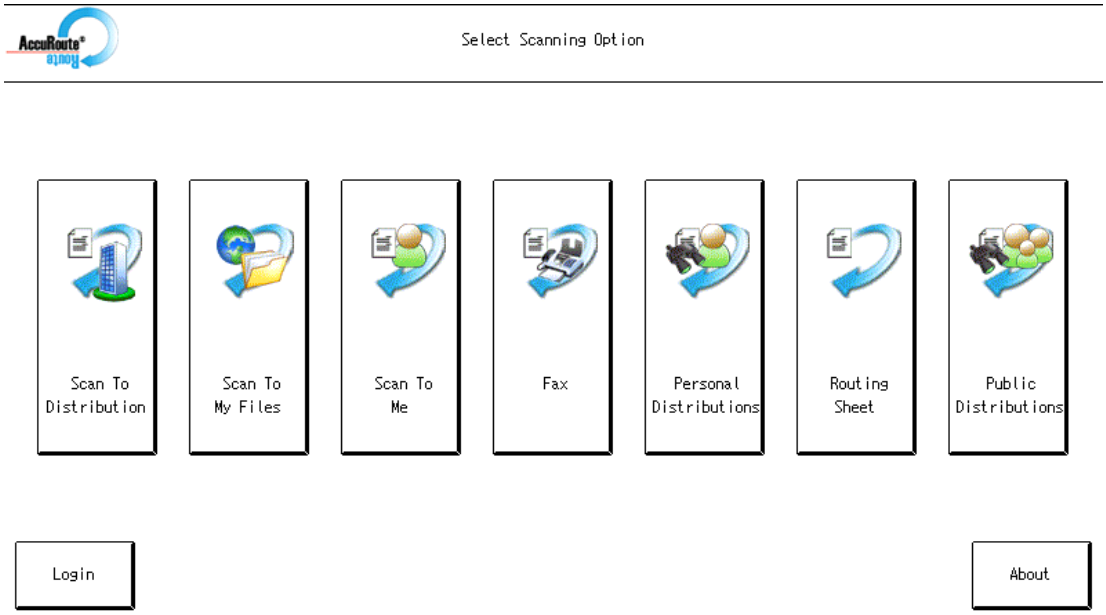
7 Select **OK** twice to save the connector configuration.

Section 6: Testing

The following section provides a procedure for testing the Routing Sheet feature. This will ensure that your installation is operational. This section includes:

Testing the Routing Sheet feature

1. Create at least one Distribution Rule with your user account.
2. Generate and print a Routing Sheet using the AccuRoute Desktop or the AccuRoute Web Client application.
3. Assemble a test document. Add the Routing Sheet to the front or back of the document, and go to the device. The main screen looks like this:



4. Load the document into the document feeder.
5. Press **Routing Sheet**.

Note If you have configured prompts, you will see the them now. Enter the appropriate prompt values and click **Next**.

The device indicates it is ready to scan.

6 To begin scanning, press **Start** on the hard keypad.

Alternately, to change the scan attributes, click **Setup**.

For example, you can specify the page size for the scanned document. The default page size is Letter. After you have made your modifications, click **Start** to begin scanning.

To stop the scan job, press the **Clear/Stop** hard key. Otherwise wait for the job to finish. When scanning is complete, the device shows the scan completed message.

The message is transferred to the AccuRoute server via HTTP/HTTPS where it is processed and routed to the intended recipient. If the document does not arrive at the destination, troubleshoot the setup. Go to Section 7: Troubleshooting.

Important If you see that the AccuRoute server cannot decipher or interpret the Distribution Rule instructions on the Routing Sheet, you must change the device setting from **mixed** to **text**. For instructions, see Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet (7-6).

Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for Creating a group of devices (5-5).

You can set up tests to test all authentication types at once by configuring groups on the AccuRoute server, with each group having a different authentication type:

- Email
- Email with Password
- PIN
- PIN with Password
- Login

Then, test one device by uninstalling and reinstalling from each authentication type group to verify that all authentication types will work at once.

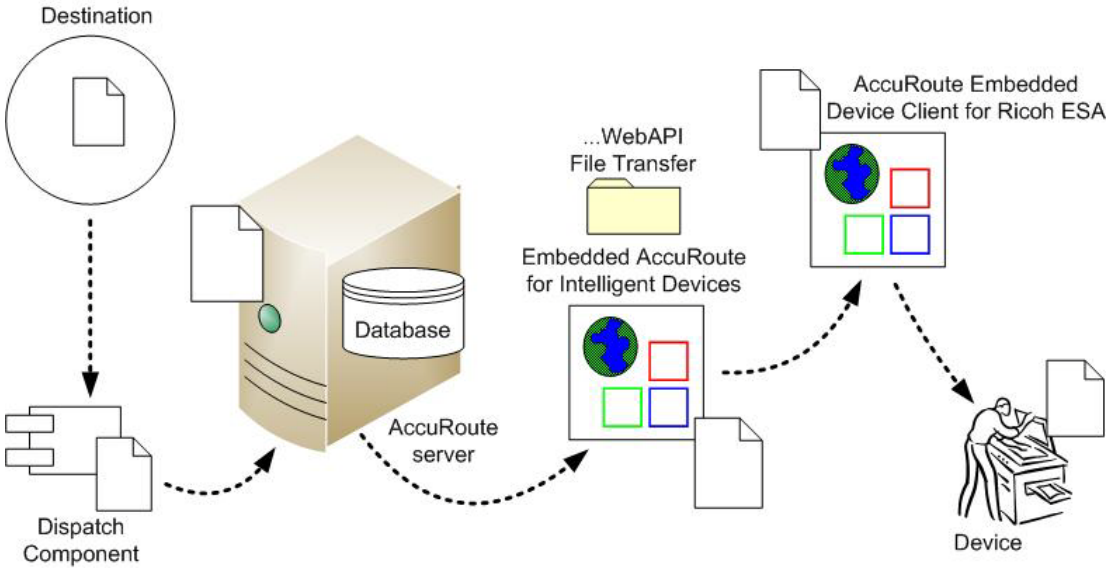
Section 7: Troubleshooting

This section includes:

If you cannot resolve an issue, contact Omtool support.

Detecting workflow issues

After a document has been scanned on the device, the document should arrive at its destination momentarily but can take up to several minutes when the server workload is high. If a document does not arrive at its destination within a reasonable period of time, begin troubleshooting the environment. Omtool recommends troubleshooting the workflow in reverse order because this is the easiest way to troubleshoot the setup on your own.



When a document does not arrive at its destination, troubleshooting starts with the delivery mechanism such as the mail server or DMS application, and then continues to the AccuRoute server, the Embedded AccuRoute for Ricoh (ESA) Device Client, the Web server, and the device.

Figure 7-1: **Troubleshooting the workflow in reverse order**

Troubleshooting the delivery mechanism

When the AccuRoute server finishes processing a message, an outbound connector routes the message directly to its destination or passes the message onto a delivery agent. If a delivery agent such as a mail server or DMS application is involved in the delivery process, do some basic troubleshooting on the delivery agent. If the delivery agent is functioning correctly, troubleshoot the message on the AccuRoute server. Continue to Troubleshooting messages on the AccuRoute server.

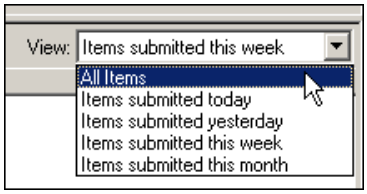
Troubleshooting messages on the AccuRoute server

There are two important questions that can be resolved when troubleshooting a message on the AccuRoute server:

- Was the message submitted to the AccuRoute server?
- Assuming the message was submitted to the AccuRoute server, what caused the delivery failure? The state and status of the message, along with details in the message journal, provide some important clues.

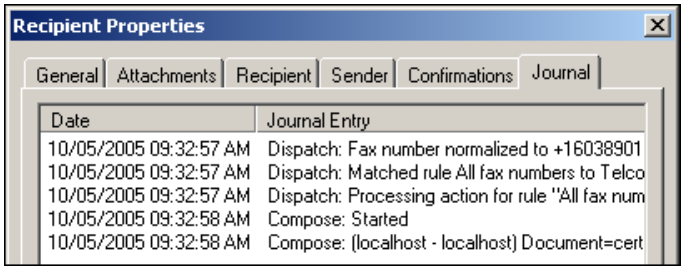
Start troubleshooting by trying to locate the message on the AccuRoute server:

1. Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
2. In the console tree, expand the AccuRoute Server Administrator and go to **[ServerName] > Messages**.
3. Look for the message in the In Process queue:
   a. Click **In Process**.
   b. View **All Items**.



   c. Sort all items by the date submitted.
   d. Look for the message.

   - **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If the AccuRoute server stops processing the message (for example, the message seems to be stuck in a processing queue), restart all the Omtool services.

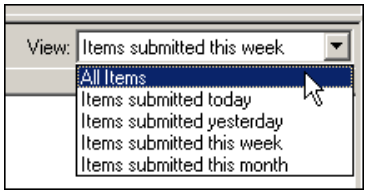


   - **Message not found** - Go to step 4 and look for the message in the History queue.

4 Look for the message in the History queue:

a Click **History**.

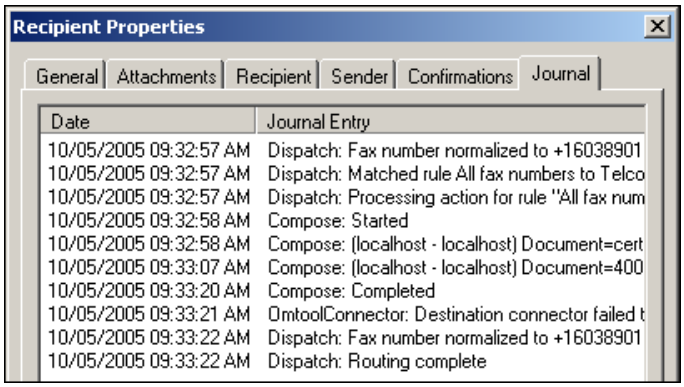
b View **All Items**.



c Sort all items by the date submitted.

d Look for the message.

- **Message found** - View the message journal to determine the cause of the failure.



If the message failed, correct the issue and send the message again. Contact Omtool if you are unable to resolve the issue.

If the journal states that AccuRoute server delivered the message but it still has not arrived at its destination, this indicates that the AccuRoute server transferred the message to the delivery agent successfully. Do some advanced troubleshooting on the delivery agent to determine why the message is not being delivered to its destination. Contact Omtool if you are unable to resolve the issue.

- **Message not found**

Troubleshooting the Web server

The *Embedded AccuRoute for Intelligent Devices Installation Guide* has instructions on troubleshooting the Web server. For documentation related to AccuRoute v4.1, consult the AccuRoute v4.1 documentation page.

If you cannot identify any issues with the Web server, troubleshoot the device. Continue to Troubleshooting the multifunction device.

Troubleshooting the multifunction device

After troubleshooting all other components in the workflow, troubleshoot the device. Consult the Ricoh documentation.

Troubleshooting .NET error when installing Embedded AccuRoute for Ricoh (ESA) Device Client

Problem:

When installing Embedded AccuRoute for Ricoh (ESA) Device Client v5.0 on a Windows 2008 R2 system, this message appears:

```
.NET Framework 3.5.1 must be installed using Server Roles before
continuing.
```

Solution:

.NET Framework v3.5.1 is not installed in your system. Install .NET Framework v3.5.1before proceeding with the AccuRoute Embedded Device Client for Ricoh ESA installation.

For information on how to install .NET Framework v3.5.1, consult:

http://blogs.msdn.com/b/sqlblog/archive/2010/01/08/how-to-install-net-framework-3-5-sp1-on-windows-server-2008-r2-environments.aspx

Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster

Problem:

Issues related to permissions occur when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster environment.

Solution:

When setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster, you must configure permissions for the Anonymous user.

Procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the AccuRoute v4.1 Server Installation Guide.

Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet

Problem:

When using a Ricoh device to scan a document with a Routing Sheet, the AccuRoute server cannot decipher the instructions on the Routing Sheet and process the document.

Solution:

Change the device setting from scanning a Mixed document to scanning a Text document. To do so:

1. Open a Web browser and enter the IP address of the device.
2. Click **Log In** and login to the device using the device administrator name and password.
3. Click **Digital Sending > Preferences**.
4. For **Document Type**, change the chosen option from **mixed** to **text**.

Troubleshooting default page setting issue during scanning

Problem:

For Ricoh MP 301 SPF and MP 305 SPF (A4-type) devices, scanning at the default page setting (and some other settings) results in an error message: 'Message: Current Scan Setup is invalid.'

Solution:

As a workaround, set page size to 8.5x11_SEF. To do so:

1. In the AccuRoute Server Administrator, right-click on **Device Groups** and select **Properties**.
2. In the **Buttons** tab, select a button and click **Properties**.
3. In the **Device Settings** tab, double-click **Scan Size** and change the setting from **Auto** (default) to **8.5x11_SEF**.
4. Click **OK**.
5. Double-click **Duplex** and change the setting from **LEFT FEED ONE SIDED** (default) to **TOP FEED ONE SIDED**.

Troubleshooting Java issues when configuring HTTPS

Problem:

While configuring your environment to use HTTPS, you are unable to add the self-signed certificate to the device client.

Solution:

The Embedded AccuRoute for Ricoh Device Client installation includes a version of Java™. Adding the certificate to the device client [see Adding the certificate to the Embedded AccuRoute Ricoh Device Client (3-29)] requires using Java tools. The instructions as written assume Java is in the default location to which it was installed by Omtool.

However, if Java was independently updated before configuring HTTPS, any prior Java installations (including that installed with the device client) may have been uninstalled. Also, new versions may be installed to a different location.

Given either of these situations, you will not find the Java tools at the default location. You can either place Java in the default location for the Ricoh device client or alter the HTTPS configuration steps to use the correct path to your Java installation.

Appendix: Installation and Configuration using the Embedded Web Server or an SD Card

This section includes:

Entering a license for Embedded AccuRoute for Ricoh (ESA) Device Client

Note If you do not have a license, contact Omtool Sales for more information.

You can activate the Embedded AccuRoute for Ricoh (ESA) Device Client license in one of two ways:

- **Automatically** when you enter an activation code and the AccuRoute server is on a system that has access to the internet.
- **Manually** if the AccuRoute server does not have access to the internet. In this case, you will:
  - Submit and validate the activation code.
  - Create an Export file into which the activation code is copied.
  - Create an Import file and use this file for activation from a system that does have internet access.

Automatic license activation

Be sure the AccuRoute server has access to the internet. Have available a copy of the device license activation code.

1. Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
2. Expand the tree view and select the server name.
3. Right-click and select the **Licensing** option**.** The **Licensing** page is displayed.
4. Click the **Activate License...** button. The **License Activation** page is displayed.

5 Select the **Automatically activate via the Internet** option.

6 Enter your license activation code in the **Activation Code** text field.

7 Click **OK**. The server is updated with your license.

8 Click **Close** to complete the procedure.

Manual license activation

Have available a copy of the activation code.

> **Note** Although the AccuRoute server may not have access to the internet, to complete this procedure you will need a system that does have access.

1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

2 Expand the tree view and select the server name.

3 Right-click and select the **Licensing** option**.** The **Licensing** page is displayed.

4 Click the **Activate License...** button. The **License Activation** page is displayed.

5 Select the **Export activation file for manual activation** option.

6 Create an Export license file:

   a Browse to a location where you want to save the license file. By default, the file is an Export file named `ManualActivation.exp`. After specifying the file name and location, click **Save**.

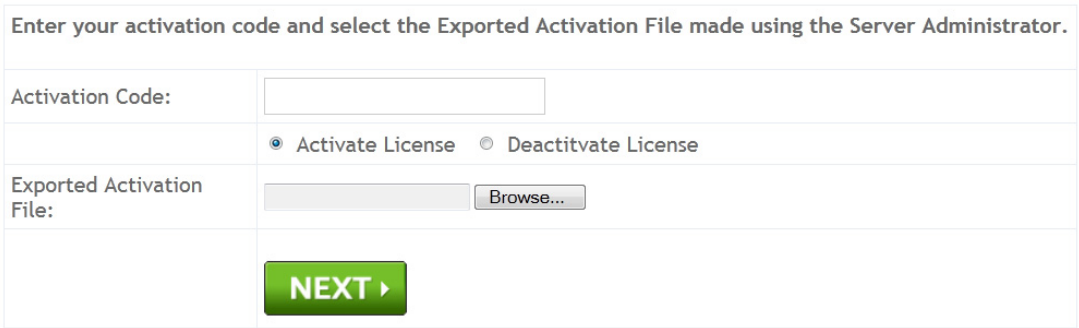
   b The path will appear in the **Export Filename** field on the **License Activation** page. Click **OK**.

7 From a system with internet access, launch the web browser and go to:

   `https://license.omtool.com/accuroute`

   The **Manual Licensing Portal** page opens.

Manual Licensing Portal



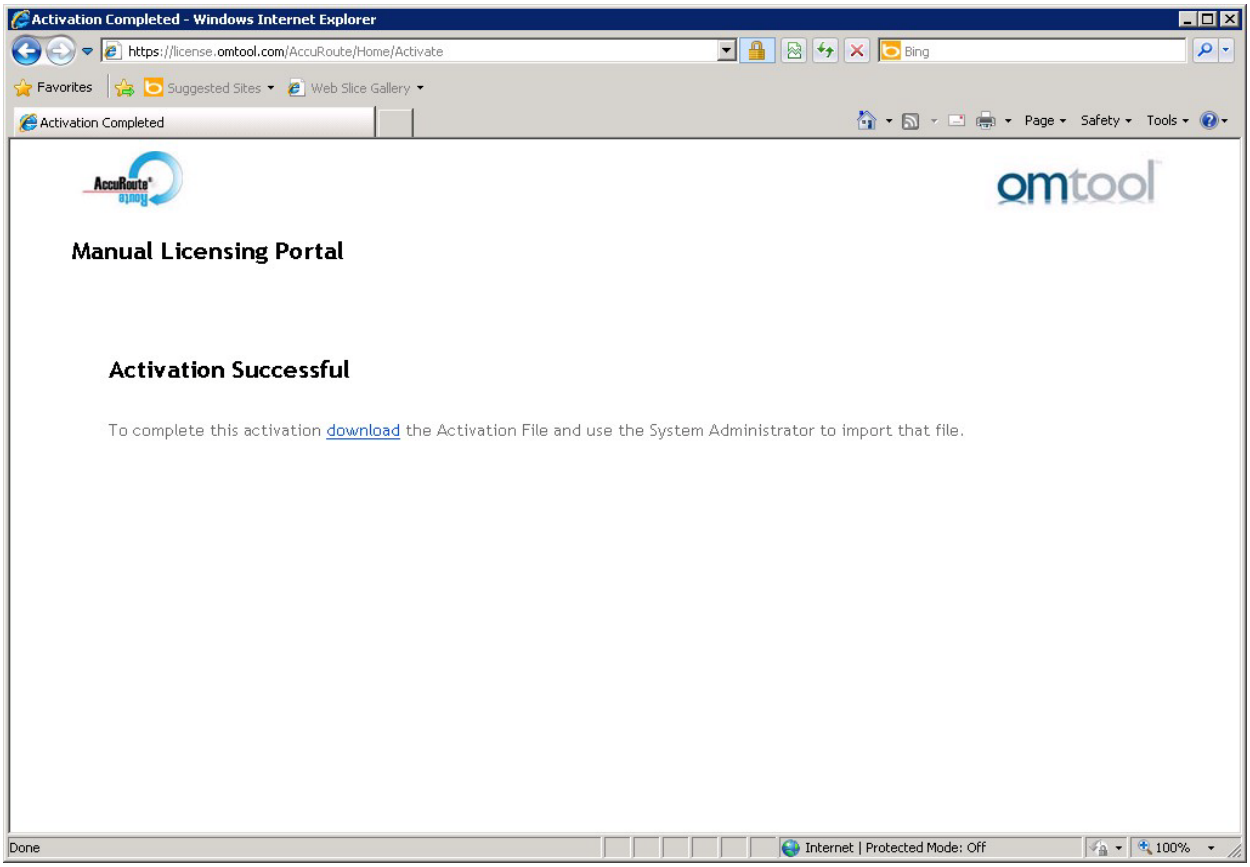
8 Enter your device license activation code in the **Activation Code** text field.

9 Be sure the **Activate License** option is selected (the default).

10 Click the **Browse** button to select the `ManualActivation.exp` file created in Step 6. With the file name selected (highlighted), click **Open**.

11 Verify that the license information is entered correctly on the **Manual Licensing Portal** page.

12 Click **NEXT** and the **Activation Successful** message is displayed.



13 To complete the device activation, click **Download**. The **File Download** page is displayed.

14 Click **Save** to create the Import file. By default, the file is named with the device activation code. You can change this (for example, `ManaulActivation.imp`) and select a location for the file on the AccuRoute server.

15 Click **Save**. The **Download Complete** page shows that status of the file download.

16 Click **Close**.

Note You can minimize or close the browser.

17 On the **Licensing** page, click the **Activate License...** button.

18 Select the **Import activation file from manual activation** option.

19 Browse to the saved `ManaulActivation.imp` file. Select the file and click **Open**.

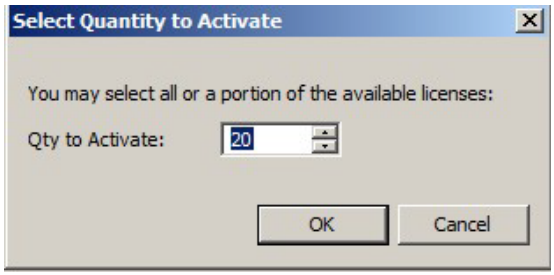
20 Click **OK** on the **License Activation** page. The license is updated.

21 Click **Close** to complete the procedure.

Activating or deactivating multiple clients or a subset of licenses

When activating a multiple device license, you will be prompted to indicate the number of devices to be activated.

Note Multiple device licenses can be used on multiple servers.



When deactivating a multiple device license, highlight the device license activation code and click **Deactivate License**. Then, choose the number of licenses to deactivate.

Installing Embedded AccuRoute for Ricoh (ESA) Device Client v5.0

Two methods for installation and configuration are described in this chapter:

- Using the Embedded Web Server method
- Using the SD card method

Note For the SD card method, obtain an SD card to use while installing AccuRoute Embedded Device Client for Ricoh ESA v5.0 onto the device. You will need a card reader on the computer that will be used to transfer the files to the SD card.

For either method, install AccuRoute Embedded Device Client for Ricoh ESA onto the AccuRoute server by completing this procedure:

1 Log on to the system running the AccuRoute server using an account that belongs to the local Administrators group.

2 Navigate to the folder `...\Omtool\Omtool Server\Clients\Ricoh ESA` and run **setup.exe**. The InstallShield wizard launches with the **Welcome** message.

3 Click **Next** and then **Install**.

4 Click **Finish**.

5 Continue with Configuring HTTPS support from the Embedded Web Server or an SD Card.

Configuring HTTPS support from the Embedded Web Server or an SD Card

Configuring from the Embedded Web Server

Before you install the Embedded AccuRoute for Ricoh (ESA) device client on the device from the Embedded Web Server, you need to modify the `OmtoolXlet.dalp` as follows:

- %URL_ISAPI% should be replaced by the URL to the ISAPI found in the **Settings** tab for the Ricoh node in the Administrator.
- %GROUP_NAME% should be the group you created under the Ricoh node in the Administrator.
- %DISPLAY_MODE% should be replaced with WVGA.

You can now install the Embedded AccuRoute for Ricoh (ESA) device client to the device.

Configuring from an SD card

Before you install the Embedded AccuRoute for Ricoh (ESA) device client on the device from an SD card, you need to add the XLet Repository directory to the SD card as follows:

1. On the SD card, create the following directory structure:

   `E:\sdk\dsdk\dist\33960192`

2. Copy the contents of:

   `C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository`

   to the `33960192` directory.

You can now install the Embedded AccuRoute for Ricoh (ESA) device client to the device.

Installation using the Embedded Web Server or SD card method

If you plan to install the Embedded AccuRoute for Ricoh (ESA) Device Client using the Embedded Web Server method, continue with Installation using the Embedded Web Server method, below.

If you plan to install using the SD card method, continue with Installation using the SD card method (A-9).

> **Note** To configure remote systems for the Ricoh device client installation, conduct the following steps on the remote AccuRoute server.

Installation using the Embedded Web Server method

1. On the AccuRoute server browse, to:

   `C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository`

   Locate the `OmtoolXlet.dalp` file.

2. Open the `OmtoolXlet.dalp` file with Notepad for editing.

3. Locate the following `<application-desc main-class="OmtoolXlet" visible="true">` sections and make the appropriate changes:

   - **Service Path**: Locate `<argument>-servicepath:%URL_ISAPI%</argument>`. Replace `%URL_ISASPI%` with the WebAPI URL. This URL address can be found in the AccuRoute server in the Device Group Properties under the Settings tab. Example:

     `<argument>servicepath:http://<accuroute_server_IP>/WebAPI/Scripts/omisapiu.dll</argument>`

   - **Group Name**: Locate `<argument>-sourcename:%GROUP_NAME%</argument>`. Replace `%GROUP_NAME%` with the name of the Ricoh group (from Creating a group of devices), for example:

     `<argument>-sourcename:Ricoh</argument>`

4. Locate the `<display-mode size "=%DISPLAY_MODE%" >` after the `</shortcut>` section and make the appropriate change:

   - **Display Mode**: Locate `<display-mode size="%DISPLAY_MODE%" />`. Replace `%DISPLAY_MODE%` with the proper display mode size. Example:

     `<display-mode size="WVGA" />`

5. Save the changes to the `OmtoolXlet.dalp` file.

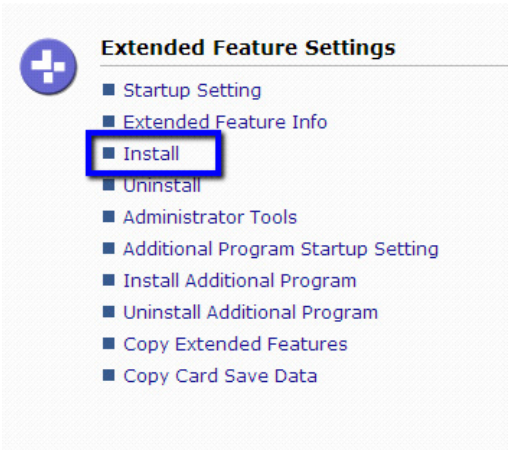
6. Copy the entire `XletRepository` directory and create a Zip file called `XletRepository.zip` containing all the files.

7. Open the Embedded Web Server for the device in a web browser.

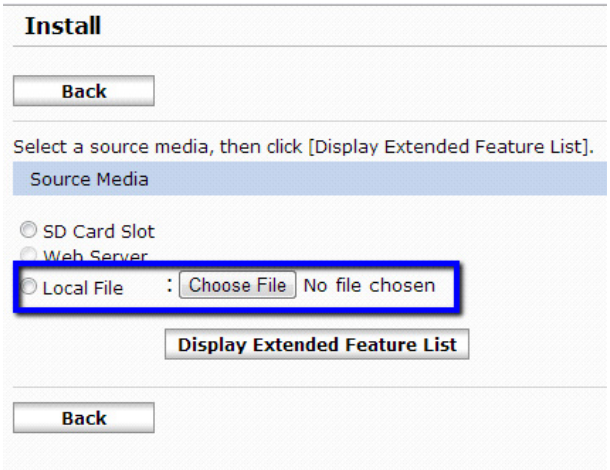
8. Log into the device using the Administrator credentials.

9. Once logged in, locate the **Device Management** button on the left side of the screen. Hover over the button and select **Configuration**.

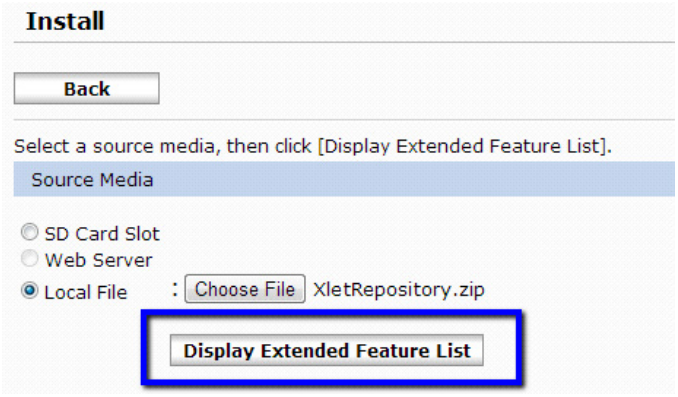
10 Locate the **Extended Feature Settings** and select **Install**:



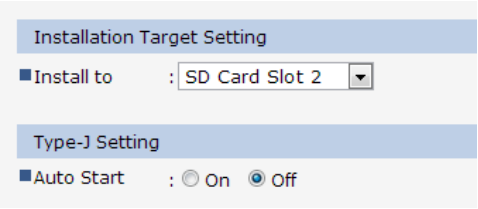
11 Under **Source Media**, select **Local File** and click the **Choose File** button.



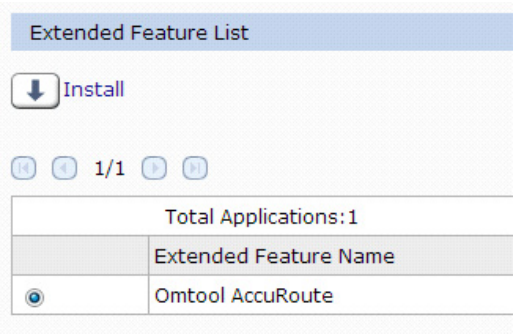
12 Browse to the XletRespository.zip file and select it. Once the file is selected, click the **Display Extended Feature List** button:



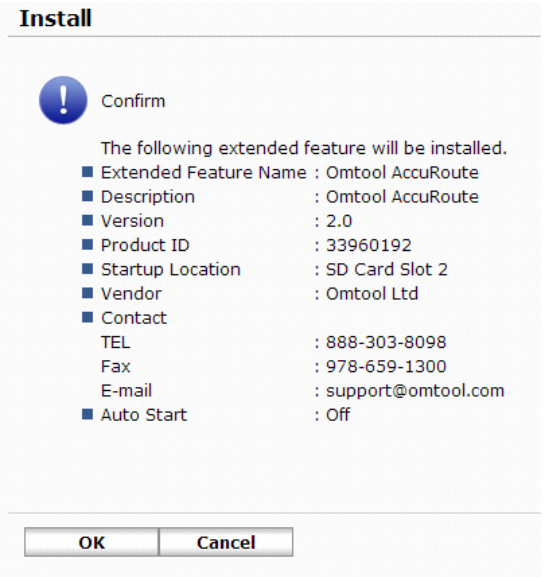
13 Indicate where the Omtool application is to be installed (Device HHD or SD card slot) and whether or not it is to **Auto Start** (Auto Start is recommended):



14 In the **Extended Feature List**, click the radio button next to **Omtool AccuRoute**. Verify that all settings are correct (from above) and click the **Install** button (down arrow):

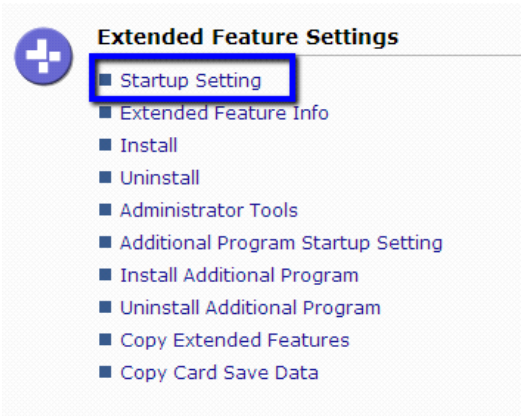


15 Verify that all the installation settings are correct on the confirmation page and click **OK** to install Omtool AccuRoute to the device:

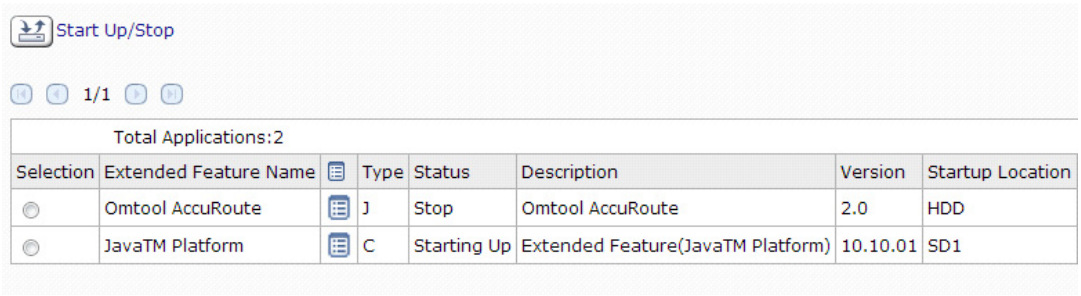


16 Verify that the application was properly installed. Once the application installs, click the **Back** button.

17 Locate the **Extended Features Settings** section and click **Startup Setting**.



18 Verify that the Omtool AccuRoute application is present.



Selection	Extended Feature Name		Type	Status	Description	Version	Startup Location
○	Omtool AccuRoute		J	Stop	Omtool AccuRoute	2.0	HDD
○	JavaTM Platform		C	Starting Up	Extended Feature(JavaTM Platform)	10.10.01	SD1

If the application is not started, click the **Omtool AccuRoute** radio button. Then, click the **Start Up/Stop** button.

Installation using the SD card method

1 On the AccuRoute server, browse to:

`C:\Program Files (x86)\Omtool\Ricoh ESA\XletRepository`

Locate the `OmtoolXlet.dalp` file.

2 Open the `OmtoolXlet.dalp` file for editing.

3 Locate the following sections and make the appropriate changes:

- **Service Path**: Locate `<argument>-servicepath:%URL_ISAPI%</argument>`. Replace `%URL_ISASPI%` with the WebAPI URL. This URL address can be found in the AccuRoute server in the Device Group Properties under the Settings tab. Example:

  `<argument>servicepath:http://<accuroute_server_IP>/WebAPI/Scripts/omisapiu.dll</argument>`

- **Group Name**: Locate `<argument>-sourcename:%GROUP_NAME%</argument>`. Replace `%GROUP_NAME%` with the name of the Ricoh group (from Creating a group of devices), for example:

  `<argument>-sourcename:Ricoh</argument>`

- **Display Mode**: Locate `<display-mode size="%DISPLAY_MODE%" />`. Replace `%DISPLAY_MODE%` with the proper display mode size. Example:

  `<display-mode size="WVGA" />`

4 Save the changes to the `OmtoolXlet.dalp` file.

5 On the local system, create a directory structure as follows:

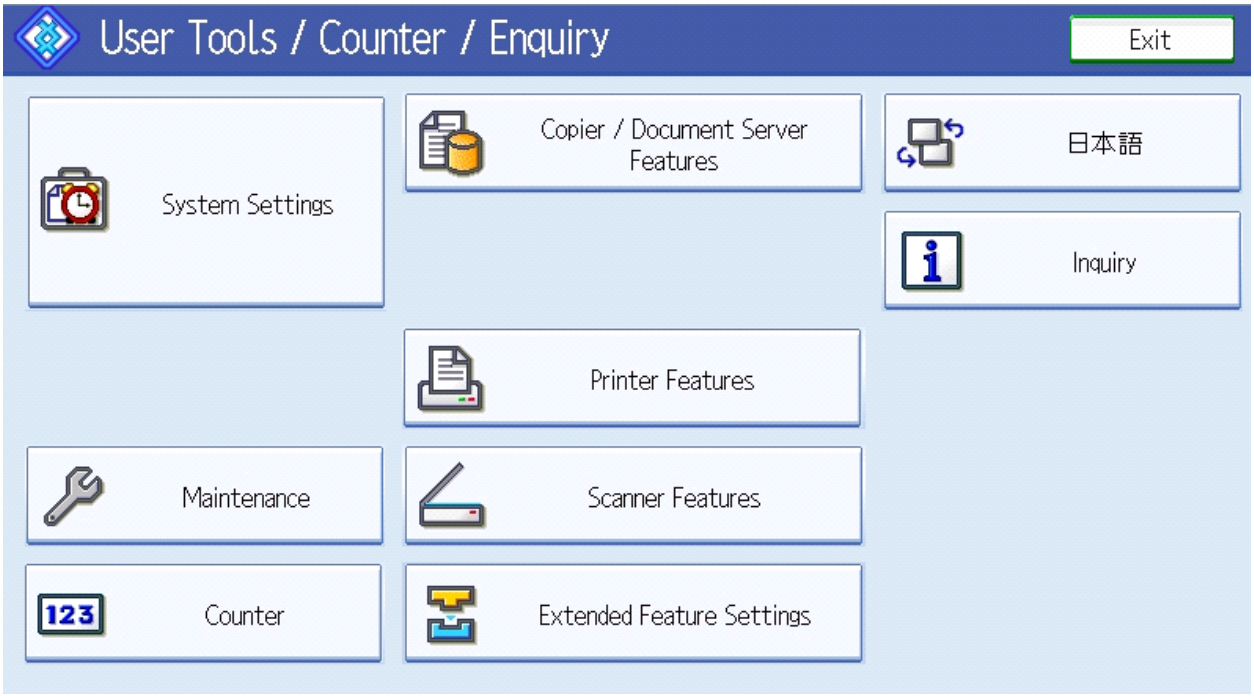
`sdk\dsdk\dist\33960192`

6 Copy all the files from the `XletRepository` directly to the `33960192` folder.

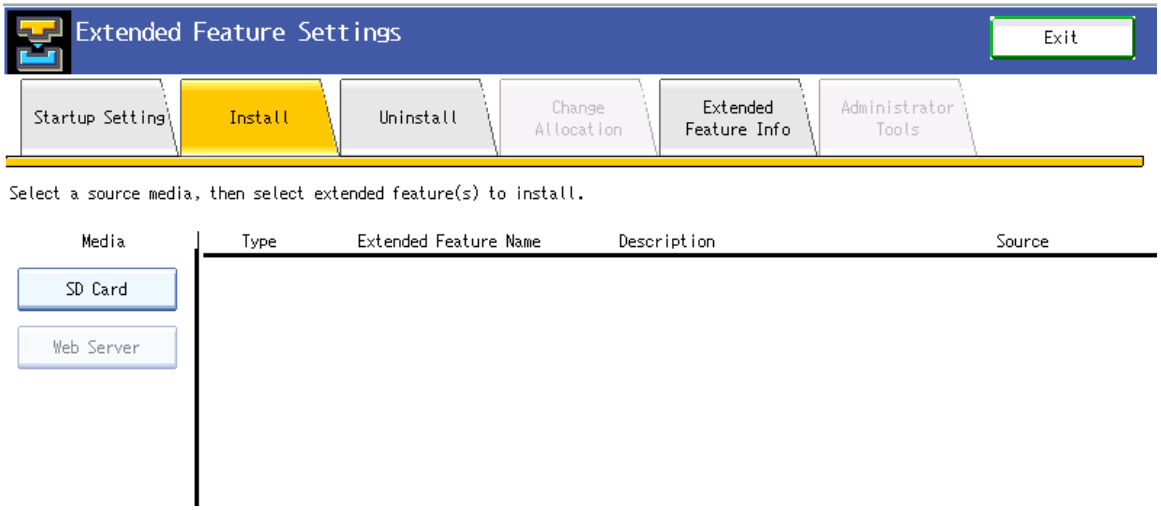
7 Copy the `sdk` directory (and all subdirectories) onto an SD card. Once they are copied, walk up to the device and put the SD card in the available SD card slot.

8 At the device, press the **User Tools/Counter** button. The **User Tools / Counter / Enquiry** screen will appear on the device.

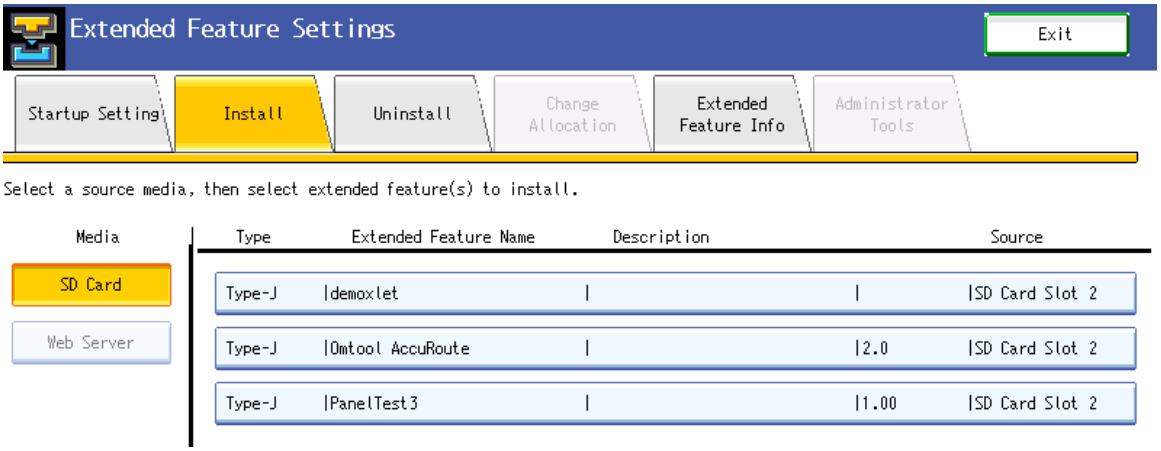
9 Press the **Extended Feature Settings** button.



10 On the **Extended Features Settings** screen, press the **Install** tab.



11 On the **Install** screen, press the **SD Card** button located under the **Media** heading. Locate and press on **Omtool AccuRoute**.

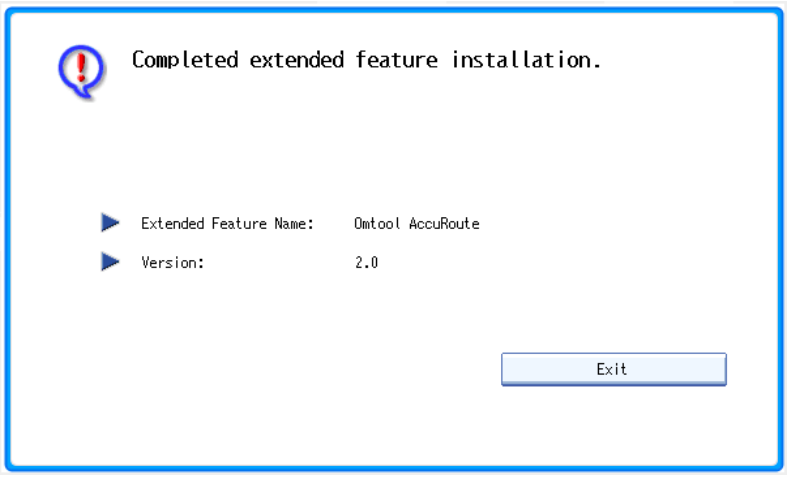


12 On the **Extended Feature Installation** dialog, select the following:

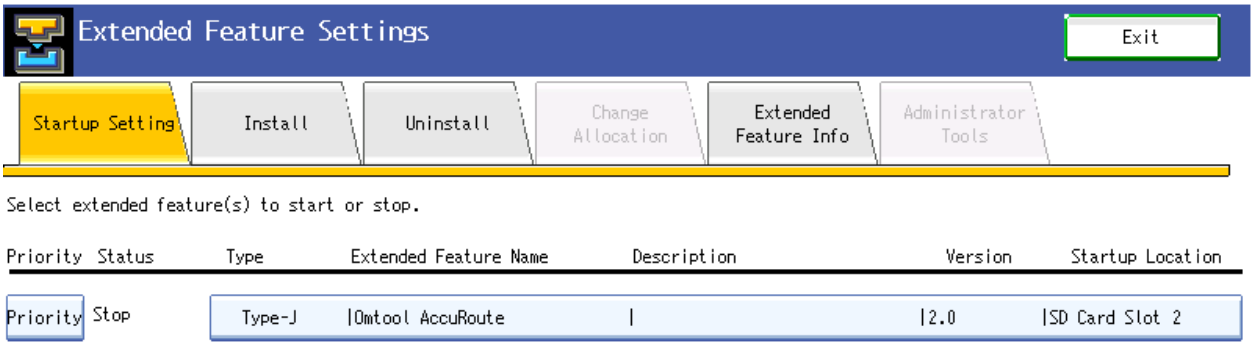
- **Install to** - Select to install the Omtool AccuRoute application to the Machine HDD, SD Card Slot 1, or SD Card Slot 2.
- **Startup Method** - Select to have the Omtool AccuRoute application **Auto Start** (recommended) or **Do not Auto Start**.

13 Once all the installation options are selected, press **Next**. Verify that all the information on the **Ready to Install** dialog is correct. Then, press **OK**.

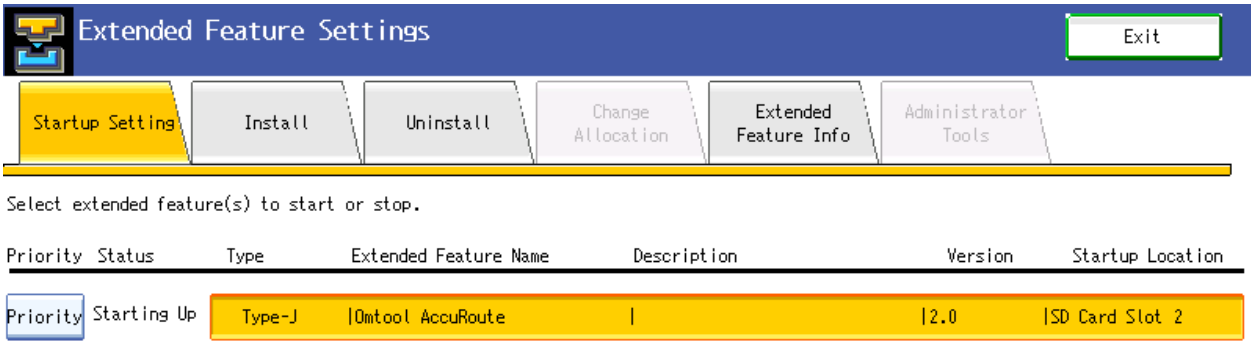
14 When the Omtool AccuRoute application installs correctly, a screen titled **Completed extended feature installation** will appear. Press **Exit**.



15 Verify that the Omtool AccuRoute application is running on the device. If it is not, it will be in the **Stop** state as indicated in the **Status** column (below). To start the application, press the **Extended Feature Name**.

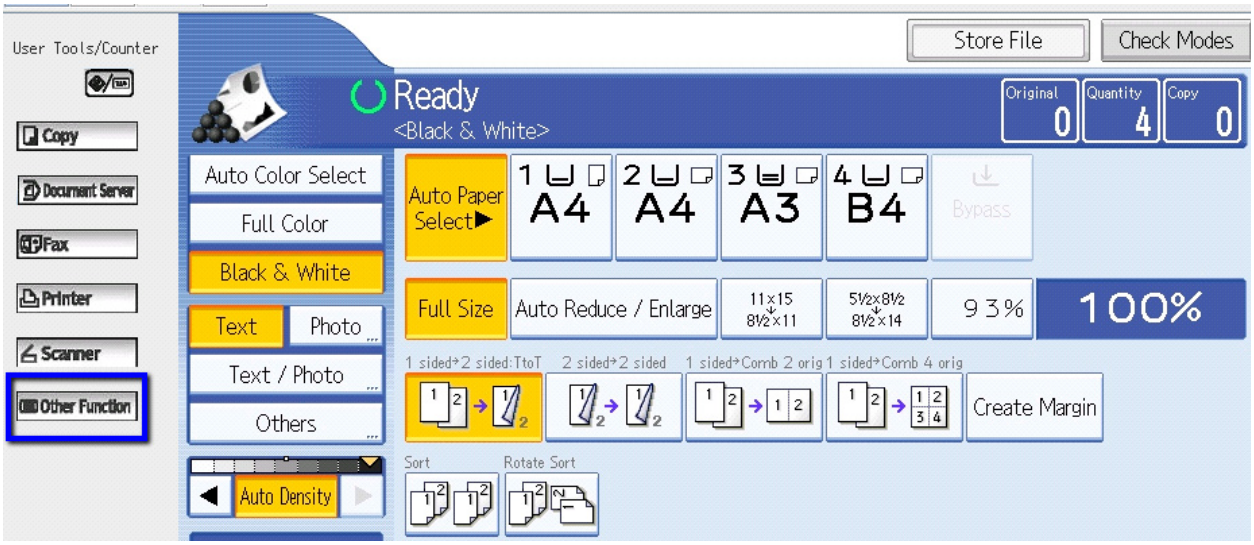


16 Once the Omtool AccuRoute application has started, it will be in the **Starting Up** state as indicated in the **Status** column.

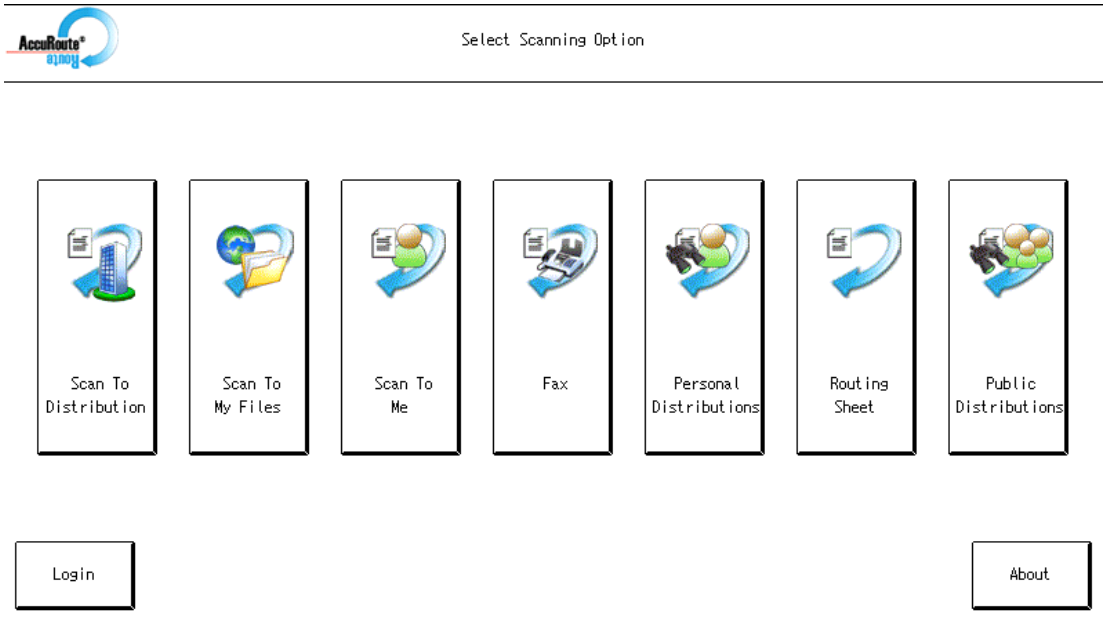


To use the Omtool AccuRoute application on the device, press **Exit** to leave the **Extended Feature Settings** page.

17 On the device panel, press the **Other Function** button. AccuRoute Embedded Device Client for Ricoh ESA v5.0 will launch.



18 If AccuRoute Embedded Device Client for Ricoh ESA v5.0 was properly installed, the AccuRoute Home Screen will appear:



Configuring the server

When a message arrives on the AccuRoute server, the Dispatch component applies rules to the message. The rules determine how the server processes the message. Every message on the server must match a rule associated with an action in order to be processed and distributed to its final destination.

Most of these rules are created by default when you install AccuRoute. You can, if needed, create rules based on customized AccuRoute scanning features available on devices in your environment. For more information on rules and how to create them, consult the Omtool Server Administrator Help accessed through the AccuRoute v5.0 documentation page.

When rules have been created for all AccuRoute scanning features available on devices in your environment, the AccuRoute server is fully configured for the Embedded AccuRoute for Ricoh (ESA) Device Client. You can test the AccuRoute scanning features at this point (Section 6: Testing).