
Embedded AccuRoute[®] for Xerox[®] (EIP) Device Client v2.0 Installation Guide

For AccuRoute v4.0

May 2013



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>

© 2013 by Omtool, Ltd. All rights reserved. Omtool, AccuRoute and the Company logo are trademarks of the Company. Trade names and trademarks of other companies appearing in this document are the property of their respective owners.

Omtool product documentation is provided as part of the licensed product. As such, the documentation is subject to the terms outlined in the End User License Agreement. (You are presented with the End User License Agreement during the product installation. By installing the product, you consent to the terms therein.)

Permission to use the documentation is granted, provided that this copyright notice appears in all copies, use of the documentation is for informational and non-commercial or personal use only and will not be copied or posted on any network computer or broadcast in any media, and no modifications to the documentation are made. Accredited educational institutions may download and reproduce the documentation for distribution in the classroom. Distribution outside the classroom requires express written permission. Use for any other purpose is expressly prohibited by law.

Omtool and/or its suppliers make no guaranties, express or implied, about the information contained in the documentation. Documents and graphics contained therein could include typographical errors and technical inaccuracies. Omtool may make improvements or changes to the documentation and its associated product at any time.

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 1: Introduction

Overview of Embedded AccuRoute for Xerox (EIP) Device Client.....	1-1
Main components of the environment.....	1-3
Installation components.....	1-4
Document workflow	1-4
Workflow for the Fax, Routing Sheet, Scan to Destination, and Scan to Distribution features.....	1-5
Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features.....	1-6
Deploying Embedded AccuRoute for Xerox (EIP) Device Client	1-7
Related documentation.....	1-7

Section 2: Requirements

Supported devices.....	2-1
AccuRoute server requirements	2-2
Device authentication requirements	2-2

Section 3: Installation

Installing Embedded AccuRoute for Xerox (EIP) Device Client v2.0.....	3-1
Installing Embedded AccuRoute for Xerox (EIP) Device Client on a remote system.....	3-2
Uninstalling Embedded AccuRoute for Xerox (EIP) Device Client.....	3-2
Upgrading Embedded AccuRoute for Xerox (EIP) Device Client.....	3-3
Uninstalling AccuRoute Embedded Device Clients	3-3
Installing AccuRoute Embedded Device Clients.....	3-3

Section 4: Configuration for HTTPS Support

Requirements for setting up a CA certificate.....	4-1
Changing the OmtoolXeroxEIP Application pool.....	4-2
Downloading the MakeCert executable.....	4-2
Creating the certificate	4-2
Installing the certificate to Internet Information Services (IIS).....	4-3
Creating an SSL binding	4-3
Requiring SSL for the virtual web sites	4-3
Enabling directory browsing in IIS.....	4-4
Verifying the SSL binding.....	4-4
Verifying HTTPS browsing	4-4
Editing the OmiSAPIU.xml file	4-5
Editing the Bootstrap.xml file	4-5

Section 5: Required Configuration

Entering a license for Embedded AccuRoute for Xerox (EIP) Device Client.....	5-1
Automatic device license activation.....	5-1
Manual license activation.....	5-2
Activating or deactivating multiple clients or a subset of licenses	5-4
Adding devices using AccuRoute Server Administrator	5-4
Creating a group of devices.....	5-4
Configuring Xerox device authentication on the device.....	5-8
Defining Domain Properties	5-12
Defining User Properties	5-13
Defining Password Properties	5-14
Adding a new device.....	5-30
Configuring the server	5-32

Section 6: Optional Configuration

Setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster	6-1
Adding the remote server's name to DCOM	6-2
Configuring a Distribution Rule to appear at the top of the device listing.....	6-2
Configuring scan settings in Distribution Rules.....	6-3
Adding an automatic logout timer.....	6-3
Note about scan settings for compression	6-5

Section 7: Testing

Testing the Routing Sheet feature.....	7-1
Testing the Device Administrator user interface	7-2

Section 8: Troubleshooting

Detecting workflow issues.....	8-2
Troubleshooting the delivery mechanism	8-2
Troubleshooting messages on the AccuRoute server.....	8-3
Troubleshooting the Web server	8-5
Troubleshooting the multifunction device	8-5
Troubleshooting .NET error when installing Embedded AccuRoute for Xerox (EIP) Device Client.....	8-5
Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster	8-6
Troubleshooting issues when the AccuRoute server cannot decipher the	
Distribution Rule instructions in a Routing Sheet	8-6
Troubleshooting issues when configuring the device to Enable Secure HTTP (SSL).....	8-7
Troubleshooting inability to configure a device to Enable HTTP(SSL) and creating a new self-signed certificate.....	8-7

Section I: Introduction

This guide contains instructions on deploying Embedded AccuRoute for Xerox (EIP) Device Client to multifunction devices running Xerox 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 Xerox \(EIP\) Device Client](#) (I-1)

[Main components of the environment](#) (I-3)

[Installation components](#) (I-4)

[Document workflow](#) (I-4)

[Deploying Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (I-7)

[Related documentation](#) (I-7)

Overview of Embedded AccuRoute for Xerox (EIP) Device Client

Embedded AccuRoute for Xerox (EIP) Device Client brings the versatile document routing capabilities of AccuRoute to supported devices running Xerox SDK 2.0 library as well as a limited set of devices running Xerox SDK 1.0 library. These capabilities are founded in Omtool's Distribution Rule technology.

Embedded AccuRoute runs on Xerox EIP (Extensible Interface Platform), an ASP.NET layer sitting between the device and the AccuRoute server. It communicates between the Xerox SDK installed on the device and the AccuRoute server via the Embedded AccuRoute for Intelligent Device Client application.

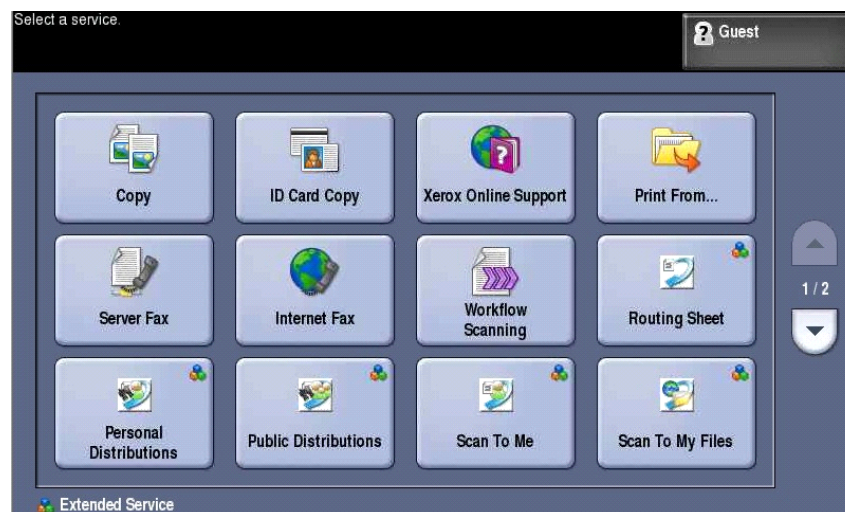


Figure I-1: AccuRoute scanning features on the Xerox device running Embedded AccuRoute for Xerox (EIP) Device Client

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 7: Testing](#), for the complete screen sequence of each feature.)

Table I-1: AccuRoute scanning features in Embedded AccuRoute for Xerox (EIP) 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 in Step 20 (page 5-17) 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 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 .

Table I-1: AccuRoute scanning features in Embedded AccuRoute for Xerox (EIP) Device Client

Feature	Description	Login required	Notes
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 display 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.).	No	

Main components of the environment

The Embedded AccuRoute for Xerox (EIP) Device Client environment consists of the following components.

- **AccuRoute Server** - The main back-end server for processing and routing documents.

Note AccuRoute v4.0 installs the AccuRoute Intelligent Device Client as part of the server installation. No separate installation of this component is required unless the Embedded AccuRoute for Xerox (EIP) Device Client is installed on a remote system, and then the AccuRoute Intelligent Device Client would be installed on the remote system as well.

- **Embedded AccuRoute for Xerox (EIP) Device Client v2.0** - See [Section 3: Installation](#) for installation instructions.

Note AccuRoute v4.0 supports both Xerox (EIP) Device Client v2.0 and Xerox (EIP) Device Client v1.1, but they cannot be installed on the same system. For more information, see [Installing Embedded AccuRoute for Xerox \(EIP\) Device Client on a remote system \(3-2\)](#).

- **Xerox Device** - See [Supported devices \(2-1\)](#) for a list.

Installation components

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

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

Component	Location	Function
Embedded AccuRoute for Xerox (EIP) Device Client Install	...\Omtool\Omtool Server\Clients	The setup contains the setup.exe file for Xerox EIP. Use this file to install the Embedded AccuRoute for Xerox (EIP) Device Client.
Embedded AccuRoute for Xerox (EIP) 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 Xerox (EIP) 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 Xerox (EIP) Device Client integration.

Basic workflow is:

- When a device user scans a document, the device submits the document to Embedded AccuRoute for Xerox (EIP) Device Client via HTTP/HTTPS protocol.
- The Embedded AccuRoute for Xerox (EIP) 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

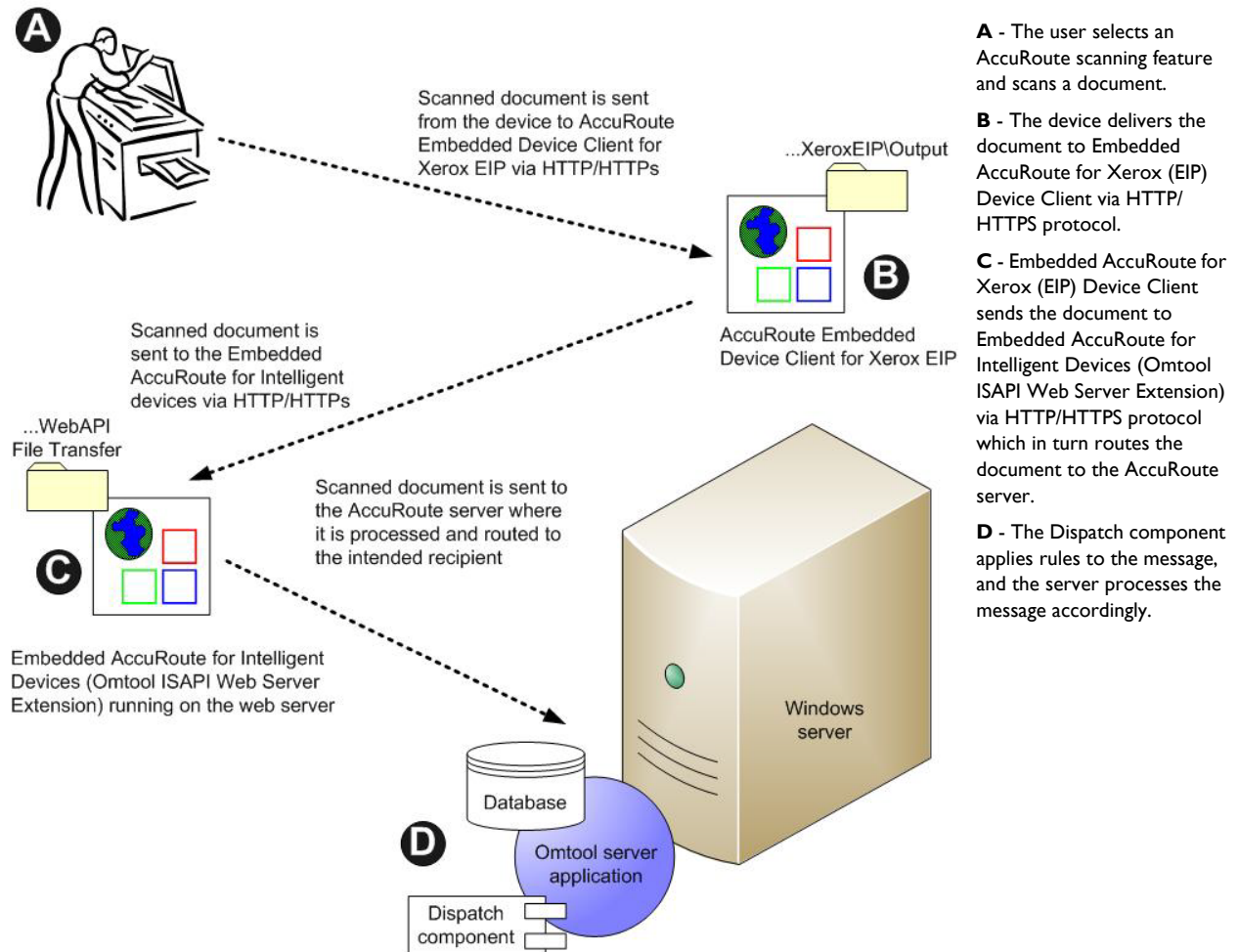


Figure I-2: Workflow for Fax, Routing Sheet, Scan to Destination, and Scan to Distribution

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 Xerox (EIP) Device Client to retrieve Distribution Rules.

Note For Personal Distributions, Scan to Me, and Scan to My Files, the user must authenticate at the device using the configured authentication type. See [Configuring Xerox device authentication on the device \(5-8\)](#).

The Embedded AccuRoute for Xerox (EIP) 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 Xerox (EIP) Device Client. As soon as the Embedded AccuRoute for Xerox (EIP) Device Client returns the data to the device, the workflow resumes.

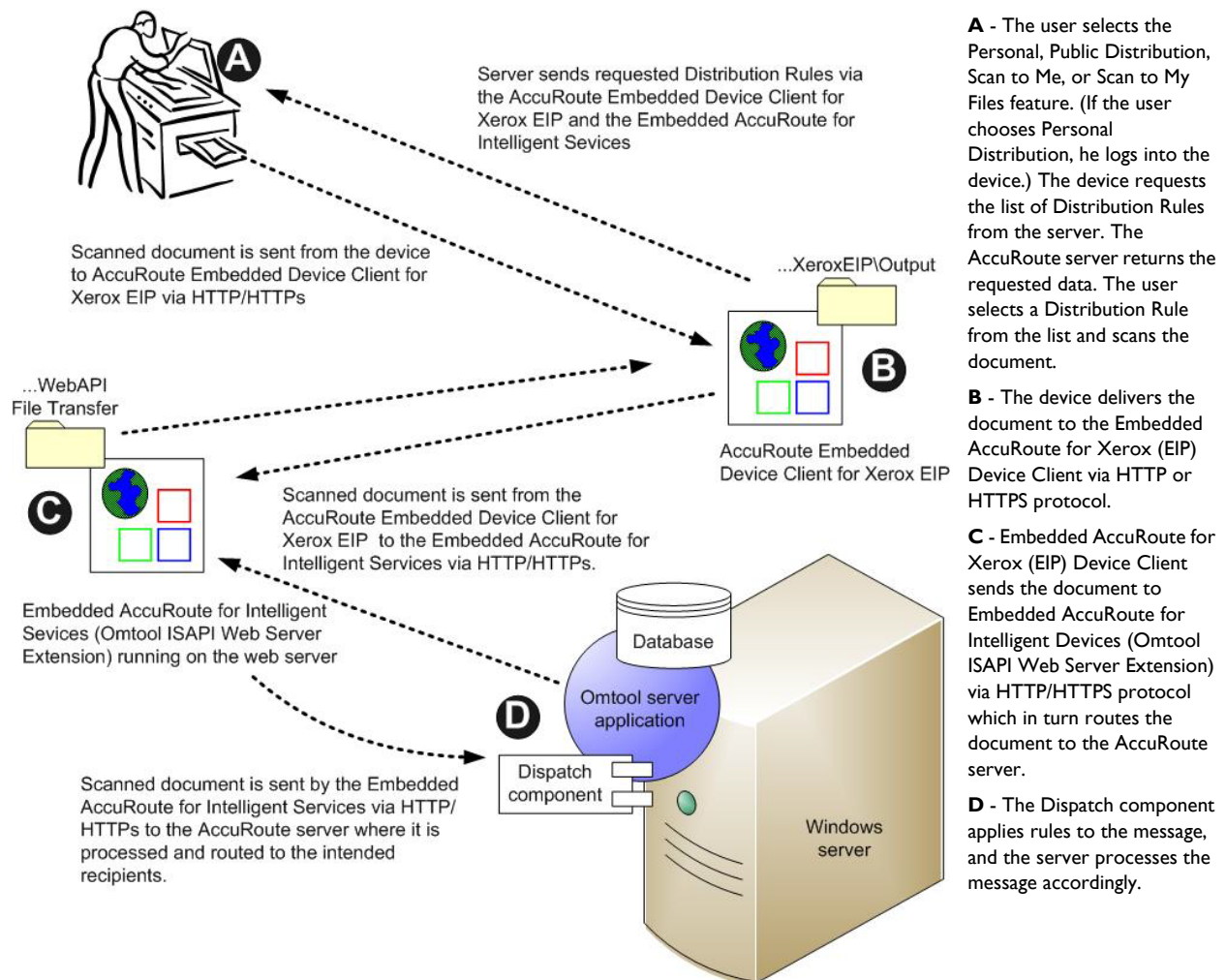


Figure I-3: Workflow for Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files

Deploying Embedded AccuRoute for Xerox (EIP) Device Client

- 1 Complete the installation requirements. ([Section 2: Requirements](#))

Note If you are planning to use HTTPS protocol, you must create a CA certificate before installing Embedded AccuRoute for Xerox (EIP) Device Client. Refer to [Section 4: Configuration for HTTPS Support](#).

- 2 Install Embedded AccuRoute for Xerox (EIP) Device Client on the AccuRoute Intelligent Device Client server. ([Section 3: Installation](#))
- 3 Configure the Embedded Web Server of the device. ([Section 5: Required Configuration](#))
- 4 Configure the AccuRoute server. ([Section 5: Required Server configuration](#))
Refer also to the *AccuRoute[®] Server Installation and Integration Guide*, which is available through <http://www.omtool.com/documentation/accuroute/4.0/documentation.htm>
- 5 Configure optional capabilities. ([Section 6: Optional Configuration](#))
- 6 Test the AccuRoute scanning features on the device. ([Section 7: Testing](#))
- 7 Troubleshoot the setup, if necessary. ([Section 8: Troubleshooting](#))

Related documentation

- [AccuRoute v4.0 Server Installation Guide](#)
- [Omtool Server Administrator Help](#)
- [Xerox EIP 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 v4.0, consult the [AccuRoute v4.0 documentation page](#).

Section 2: Requirements

This section includes:

[Supported devices](#) (2-1)

[AccuRoute server requirements](#) (2-2)

[Device authentication requirements](#) (2-2)

Supported devices

Omtool supports Embedded AccuRoute for Xerox (EIP) Device Client on all devices listed in this section. Consult Xerox to determine compatible firmware versions for supported devices.

Table 2-1: List of devices supported with Embedded AccuRoute for Xerox (EIP) Device Client

Device	Qualified by Omtool	Xerox EIP Version	Software Version
550/560	Color 560	1.5	55.30.61, ESS1.207.3, IOT 64.18.0, IIT 6.16.1, ADF 12.11.0, SJFI3.0.18, SSMII.16.0
ColorQube 87xx	ColorQube 8700S	2	071.160.101.36000, ESS 071.161.32710
ColorQube 92xx	ColorQube 9203	1.5	061.050.222.24401
Phaser 36xxMFP	Xerox Phaser 3635 MFP	1	20.105.11.000 digital signature now cannot go back, supports card reader; 20.105.14.000 supports card reader
WorkCentre 53xx	WorkCentre 5300	1.5	53.20.31, ESS1.205.1, IOT 30.39.0, ADF 7.10.0, SJFI3.0.18, SSMII.16.0
WorkCentre 56xx	WorkCentre 5632 v.1 Multifunction System	1.5	025.054.065.190 supports card reader
WorkCentre 57xx	WorkCentre 5755	2	061.132.222.07901 supports card reader
WorkCentre 64xx	WorkCentre 6400	1	061.070.102.23501, 061.070.100.24201, ESS 061.070.22410
WorkCentre 71xx	WorkCentre 7120	1.5	71.22.52
WorkCentre 72xx	WorkCentre 7242	1	1.207.112
WorkCentre 73xx	WorkCentre 7335	1	ESS PSI.227.169, IOT 3.0.5, IIT 22.13.1, ADF 11.6.5, SJFI3.0.8, SSMII.7.2
WorkCentre 74xx	WorkCentre 7435	1.5	75.13.92, ESS PSI.182.180, IOT 41.1.0, IIT 22.13.1, ADF 20.0.0, SJFI 3.0.12, SSMI 1.11.1
WorkCentre 75xx	WorkCentre 7530	2	061.121.222.32600 supports card reader

Table 2-1: List of devices supported with Embedded AccuRoute for Xerox (EIP) Device Client

Device	Qualified by Omtool	Xerox EIP Version	Software Version
WorkCentre 76xx	WorkCentre 7655 v.1 Multifunction System	1.5	0.40.33.53250, ESS 0.040.033.53250, IOT 08.32.00, UI, BIOS 07.11
WorkCentre Pro 245	WorkCentre Pro 245	1	ESS 0.040.022.50115, IOT 50.4.0, UI 0.12.60.12, BIOS 07.07

Note All Xerox devices must be set to SSL mode within the device's internal Web server. See Xerox for further instructions.

AccuRoute server requirements

Embedded AccuRoute for Xerox (EIP) Device Client requires:

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

Device authentication requirements

Embedded AccuRoute for Xerox (EIP) 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 v4.0 Server Installation Guide* ([AccuRoute v4.0 documentation page](#)).

The types of authentication are:

- **Device** authentication uses the native Xerox LDAP authentication built into the device. This is configurable from the Embedded Web Server.
- **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.

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

This section includes:

[Installing Embedded AccuRoute for Xerox \(EIP\) Device Client v2.0](#) (3-1)

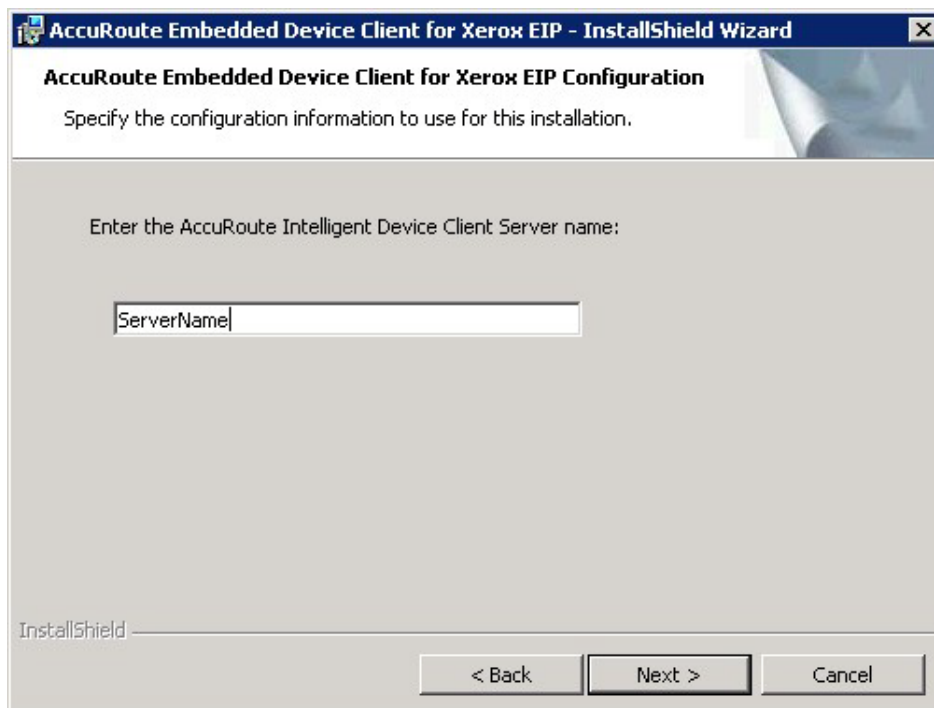
[Installing Embedded AccuRoute for Xerox \(EIP\) Device Client on a remote system](#) (3-2)

[Uninstalling Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (3-2)

[Upgrading Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (3-3)

Installing Embedded AccuRoute for Xerox (EIP) Device Client v2.0

- 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\EIP2.0` and run `setup.exe`. The InstallShield wizard launches with the **Welcome** message.
- 3 Click **Next**. The **AccuRoute Intelligent Device Client Server name** page opens.



- 4 Keep the default name and click **Next**.

- 5 Click **Install** to begin installation. The setup installs Embedded AccuRoute for Xerox (EIP) Device Client. The InstallShield Wizard shows a message indicating when the installation is complete.
- 6 Click **Finish**.
- 7 Continue to [Section 5: Required Configuration](#).

Installing Embedded AccuRoute for Xerox (EIP) Device Client on a remote system

- 1 Log on to the system where you want to install Embedded AccuRoute for Xerox (EIP) Device Client using an account that belongs to the local Administrators group.

Note The system must be running Windows 2008 and must have Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) and AccuRoute v4.0 installed.

- 2 Navigate to the `\\[AccuRoute Server]\Omtool\Omtool Server\Clients\EIP2.0` directory and right-click the **setup.exe** and select **Run as administrator**. The InstallShield wizard launches with the **Welcome** message.
- 3 Click **Next**. The **AccuRoute Intelligent Device Client Server name** page opens.
- 4 Keep the default (this should be the name of the remote IIS system onto which you are currently installing Embedded AccuRoute for Xerox (EIP) Device Client).
- 5 Click **Next**.
- 6 Click **Install** to begin installation. The setup installs Embedded AccuRoute for Xerox (EIP) Device Client. The InstallShield Wizard shows a message indicating when the installation is complete.
- 7 Click **Finish**.
- 8 Continue to [Section 5: Required Configuration](#).

Uninstalling Embedded AccuRoute for Xerox (EIP) Device Client

- 1 Go to the **Control Panel** and, depending on your version of Windows, click **Add or Remove Programs** or **Uninstall a program**.
- 2 Select **Embedded AccuRoute for Xerox (EIP) Device Client**. Right-click and select **Uninstall**. You are prompted to confirm that you want to uninstall the software.
- 3 Click **Yes** to uninstall Embedded AccuRoute for Xerox (EIP) Device Client.

Upgrading Embedded AccuRoute for Xerox (EIP) 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 AccuRoute Embedded Device Clients

- To uninstall existing AccuRoute Embedded Device Clients, refer to the steps in [Uninstalling Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (3-2).

Installing AccuRoute Embedded Device Clients

- To install an Embedded AccuRoute for Xerox (EIP) Device Client, see [Installing Embedded AccuRoute for Xerox \(EIP\) Device Client v2.0](#) (3-1).
- To install an Embedded AccuRoute for Xerox (EIP) Device Client on a remote system, see [Installing Embedded AccuRoute for Xerox \(EIP\) Device Client on a remote system](#) (3-2).

Section 3: Installation

Section 4: Configuration for HTTPS Support

This section describes setting up a CA certificate using Microsoft Certificate Services and enabling Secure Socket Layer (SSL).

Note If you are using HTTP, skip this section and go to [Section 5: Required Configuration](#).

In order to use HTTPS protocol communication when sending documents from the device to the AccuRoute server, follow the instructions in this section to create a CA Certificate using Microsoft Certificate Services and enable SSL.

Note HTTP and HTTPS cannot coexist and configuration for the device communication must be either HTTP or HTTPS for all devices.

If you require HTTPS support, you can follow the instructions in this section to set up a CA certificate with the Microsoft Certificate Services and enable SSL. Otherwise, use a certificate from a trusted certificate authority. The certificate must be installed on the IIS system.

Requirements for setting up a CA certificate

You must meet the following requirements when setting up a CA certificate:

- Web server that meets the requirements for AccuRoute Intelligent Device Client.
- Windows user account that belongs to the Administrators group.

The remainder of this section provides procedures that you should complete in the order they are presented:

[Changing the OmtoolXeroxEIP Application pool](#) (4-2)

[Downloading the MakeCert executable](#) (4-2)

[Creating the certificate](#) (4-2)

[Installing the certificate to Internet Information Services \(IIS\)](#) (4-3)

[Creating an SSL binding](#) (4-3)

[Requiring SSL for the virtual web sites](#) (4-3)

[Enabling directory browsing in IIS](#) (4-4)

[Verifying the SSL binding](#) (4-4)

[Verifying HTTPS browsing](#) (4-4)

[Editing the OmISAPIU.xml file](#) (4-5)

[Editing the Bootstrap.xml file](#) (4-5)

Changing the OmtoolXeroxEIP Application pool

When using HTTPS, the OmtoolXeroxEIP Application pool must be changed to ApplicationPoolIdentity:

- 1 Open Internet Information Services (IIS 7) Manager.
- 2 In the **Connections** pane, highlight **Application Pools**.
- 3 In the **Applications Pool** center window, highlight and right-click **EIPAppPool**.
- 4 Select **Advanced Settings**. Under **Process model/Identity**, click the button to expose the drop-down list.
- 5 Select **ApplicationPoolIdentity** and select **OK**.
- 6 Restart IIS.

Downloading the MakeCert executable

Copy [makecert.exe](#) to your local computer. The MakeCert executable is available as part of the Windows SDK. For instructions on how to download the Windows SDK and the MakeCert executable, see the [Microsoft documentation](#).

When the download is complete, copy the executable to a shared network folder from where you can access it.

Creating the certificate

- 1 Open a command prompt and navigate to the directory where you saved the MakeCert executable ([makecert.exe](#)) on your local computer (typically on the C drive).
- 2 Run the following command (as Administrator):

```
makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server"  
-b 01/01/2006 -e 01/01/2023 -ss my -sr localMachine -sky exchange -sp  
"Microsoft RSA SChannel Cryptographic Provider" -sy 12  
"fully_qualified_domain_name_of_iis_server.cer"
```

fully_qualified_domain_name_of_iis_server should be in this format:
`servername.domain.com`

Note There is a space at the end of the first three lines shown above.

When the command is run properly, the system will display a message indicating that it succeeded.

Installing the certificate to Internet Information Services (IIS)

You must now install the certificate from the root of C.

- 1 Select and right-click the certificate.
- 2 Select **Install Certificate**. The **Certificate Import** wizard is displayed.
- 3 Select **NEXT**.
- 4 Select **Place all certificates in the following store** and select **BROWSE**.
- 5 Select **Trusted Root Certification Authorities** and select **OK**.
- 6 You will be prompted with a security warning:
*You are about to install a certificate from a certification authority (CA) claiming to represent...
Do you want to install this certificate?*
Select **YES**. A message indicating the import was successful should display.

Creating an SSL binding

- 1 Open the IIS Manager.
- 2 Click on the **Default Website** and locate **Bindings** under **Edit Site** (top right corner of the window).
- 3 Click on **Bindings**. The **Site Bindings** dialog opens.
- 4 Click on **HTTPS type** and select **Edit**. The **Edit Site Bindings** dialog opens.
- 5 In the **SSL certificate** drop-down, select the certificate that was created earlier and click **OK**.
- 6 Click **Close** to exit the dialog.

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local machine > Default WebSite** and select **Xerox EIP**.
- 3 Open **SSL Settings** and check **Require SLL**. Under **Client certificates**, select **Ignore**.
- 4 Expand **Local machine > Default WebSite** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**.
- 6 Under **Client certificates**, select **Ignore**.

Enabling directory browsing in IIS

- 1 Open the IIS Manager.
- 2 Expand **Local machine > Default WebSite** and select **Xerox EIP**.
- 3 Double-click on **Directory browsing**.
- 4 In the right **Actions** field, select **ENABLE**.
- 5 Expand **Local Machine > Default Web Site** and select **WebAPI**.
- 6 Double-click on **Directory browsing**.
- 7 In the right **Actions** field, select **ENABLE**.

Verifying the SSL binding

- 1 Open the IIS Manager.
- 2 Expand **Local machine > Default WebSite** and select **WebAPI**.
- 3 Click on **Browse *:443 (HTTPS)** under **Manage Application/Browse Application** (located at the top right corner of the IIS dialog).

You will see this message: *There is a problem with this website's security certificate.*

Note This message is expected and safe to ignore.

- 4 Click the **Continue to this website (not recommended)** option.
- 5 Verify that the **IIS 7** dialog opens.

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **Xerox EIP**.
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed:
`...\\XeroxEIP\\Configuration\\`
- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.

- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:

```
... \WebAPI \
```

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.

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

- 2 In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

```
<FileTransfer>https://fully_qualified_domain_name/WebAPI/FileTransfer/  
</FileTransfer>
```

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path.

```
C:\Program Files (x86)\Omtool\XeroxEIP\Configuration\
```

- 2 In bootstrap.xml, change `http` to `https`.

```
<Server>https://fully_qualified_domain_name/webapi/scripts/omisapiu.dll  
</Server>
```

- 3 Save the file.
- 4 Reset IIS.

Section 4: Configuration for HTTPS Support

Section 5: Required Configuration

This section includes:

- [Entering a license for Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (5-1)
- [Adding devices using AccuRoute Server Administrator](#) (5-4)
- [Configuring the server](#) (5-32)

Entering a license for Embedded AccuRoute for Xerox (EIP) Device Client

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

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

- **Automatically** when you enter a device 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 device activation code.
 - ▶ Create an Export file into which the device activation code is copied.
 - ▶ Create an Import file and use this file for activation from a system that does have internet access.

Automatic device 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 device 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 device 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.

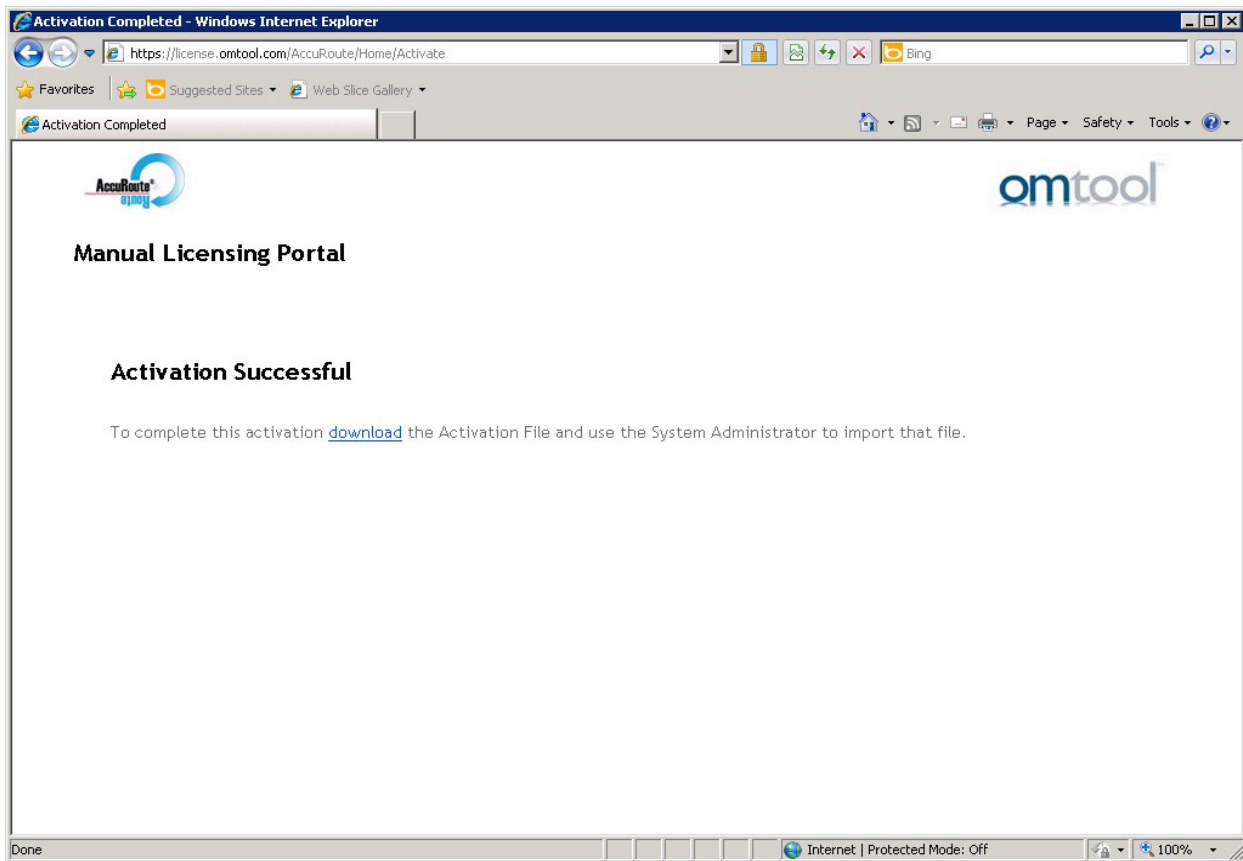


Manual Licensing Portal

Enter your activation code and select the Exported Activation File made using the Server Administrator.	
Activation Code:	<input type="text"/>
	<input checked="" type="radio"/> Activate License <input type="radio"/> Deactivate License
Exported Activation File:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="NEXT >"/>	

- 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, `ManualActivation.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**.

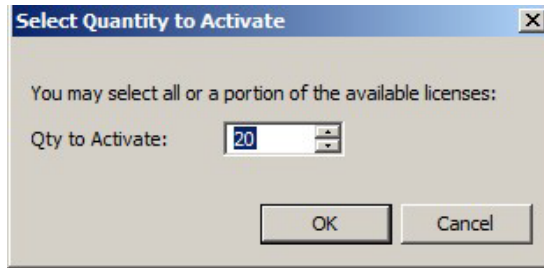
Note You can minimize or close the browser.

- 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 `ManualActivation.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.

Adding devices using AccuRoute Server Administrator

This section describes the procedures for:

[Creating a group of devices](#) (5-4)

[Adding a new device](#) (5-30)

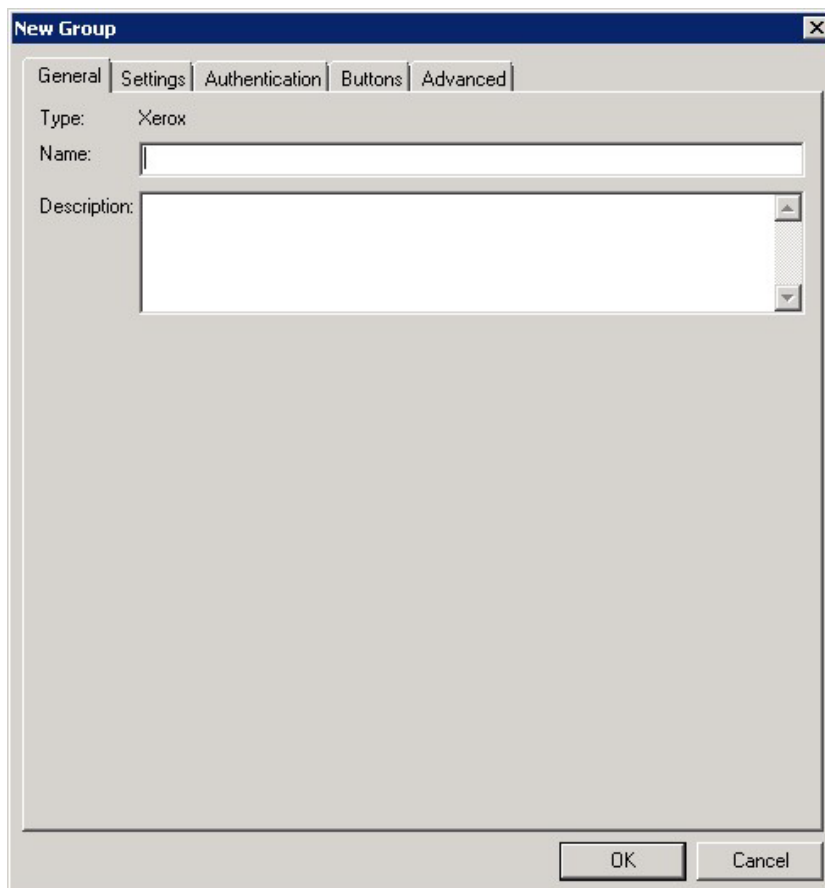
Creating a group of devices

Create a new Group for each group of devices. 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.

- 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 > Xerox group**. The **New Group** page opens.

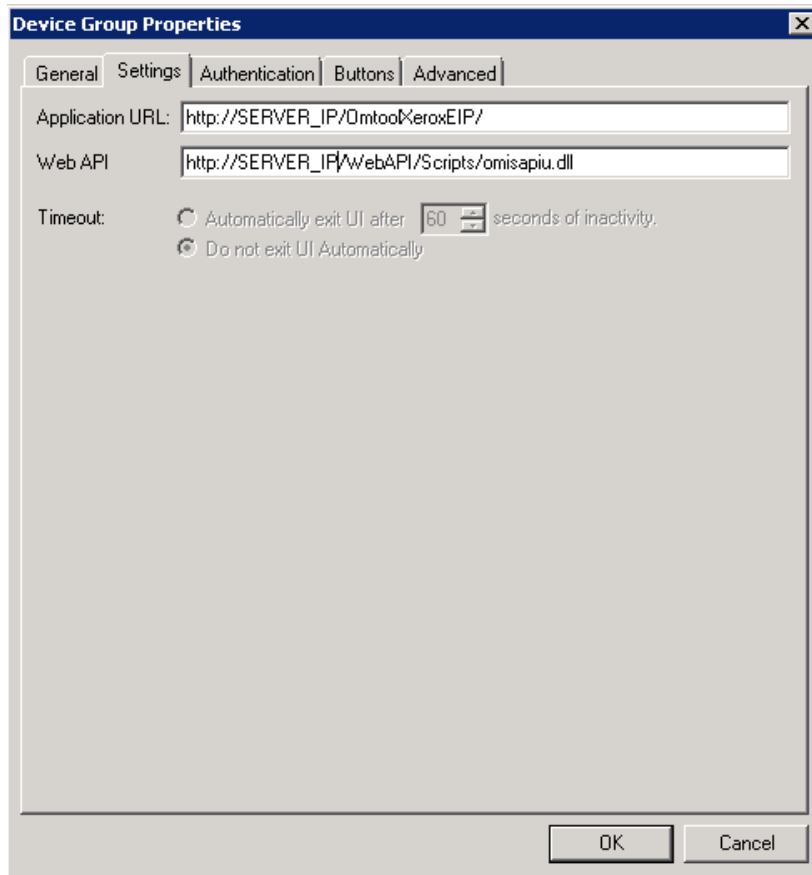


The screenshot shows a 'New Group' dialog box with the following elements:

- Title bar: New Group (with a close button)
- Tabbed interface: General (selected), Settings, Authentication, Buttons, Advanced
- Type: Xerox
- Name: [Empty text box]
- Description: [Empty text box with scrollbars]
- Buttons: OK, Cancel

- 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 settings only if the IIS/Web server is remote or if you are configuring HTTPS.



Note If you are using HTTPS:

1. For the **Application URL**, replace the IP address with the fully qualified domain name. Change http to https. For example:
`https://FullyQualifiedServerName/OmtoolXeroxEIP/`
2. For the **Web API**, replace the IP address with the fully qualified domain name. Change http to https. For example:
`https://FullyQualifiedServerName/WebAPI/Scripts/omisapiu.dll`
3. Click **OK**.

Note If you installed Embedded AccuRoute for Xerox (EIP) Device Client on a remote system, you must manually enter the IP address of that system.

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

The screenshot shows the 'Device Group Properties' dialog box with the 'Authentication' tab selected. The 'Type' dropdown is set to 'Device'. The 'Fields' section shows 'Domain', 'User', and 'Password' with 'User Entered' for each. The 'LDAP Lookup Settings' section includes fields for Server (vmad70.vmad700.com), Port (389), Search Base (DC=vmad700.DC=com), Filter (&{(objectClass=user)[sAMAccountName=[USER_NAME]]}), Username, Password, and Attribute Map (Exchange.default.xml). There are checkboxes for 'Bind using Windows Generic Security Services' and 'Confirm authentication', and buttons for 'Attribute Aliases...' and 'Test LDAP Lookup'.

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

- ▶ **Device** is the default and requires no configuration. In this case, the **Fields** section and **Properties** button are not active. The AccuRoute server verifies only the native DEVICES LDAP query information.
- ▶ 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.

- 9 If you select **Device** as the authentication type, continue with [Configuring Xerox device authentication on the device](#) (5-8).

If you select **Email**, **Login**, or **PIN** as the authentication type, continue with [Defining Domain Properties](#) (5-12).

Configuring Xerox device authentication on the device

The following procedure uses an example configured for a ColorQube 8700S. Other devices will have slight differences in the terminology used within the device's web server.

- a Access the devices Internal Web server and log in.
- b Click the **Properties** tab. Then, select **Connectivity > Protocols** or **Setup** (depending on the OS version) > **LDAP**.
- c Click **Add New**.

- d In the **General Information** or **Server Information** section (depending on the OS version):
 - ▲ Select **IPv4 Address**.
 - ▲ Enter a name in the **Friendly Name** text box.
 - ▲ Select **ADS** in the **LDAP Server** drop-down.
- e In the **Optional Information** section:
 - ▲ Enter the **Search Directory Root** (`DC=DomainName,DC=COM`).
 - ▲ Select **System** for the **Login Credentials to Access LDAP Server**.
 - ▲ Enter the **DomainName** or **Login Name** (depending on the OS version).
 - ▲ Enter the **Password**.
 - ▲ Select the option to **Select to save new password**. (If you return to this window, the login information will display as blank.)

- f Apply SSL and other settings, if necessary. Defaults were used in this example.

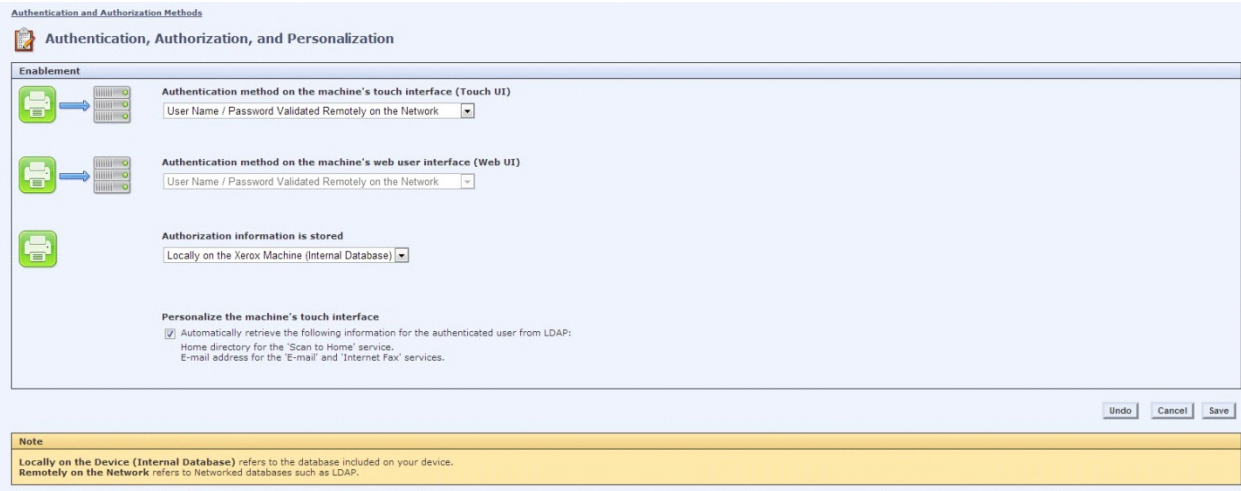
- g Once all information is verified, click the **Apply** button.
- h Click the **Contexts** tab and select defaults.
- i Click the **User Mappings** tab. Verify that all information is correct.
- j In the **Search** section, enter a name to verify LDAP connectivity. (All Imported Heading defaults were used.)
All available attributes will be displayed under the Sample header if the query was successful.
- k In the left menu under **Security > Authentication**, select **Setup** to display the Authentication, Authorization, and Personalization settings.

Configuration Setting	Method (Defined Above)	Required / Optional
Authentication Servers	Authentication (Touch UI & Web UI)	✔ Required; Coi
Machine's User Information Database	Authorization	✔ Required; Coi
Tools and Feature Access (Lock / Unlock)	Authorization	✔ Optional; Con
LDAP Servers	Personalization	✔ Required; Coi
Service Registration	(Convenience Link)	✔ Optional; Con

- l Click the **Authentication Method on the machine's touch user interface (Touch UI)** option. Then, click the **Edit** button.

Section 5: Required Configuration

- m From the drop-down, select **User Name / Password Validated Remotely on the Network** option.



- n Check the **Configuration Settings**:

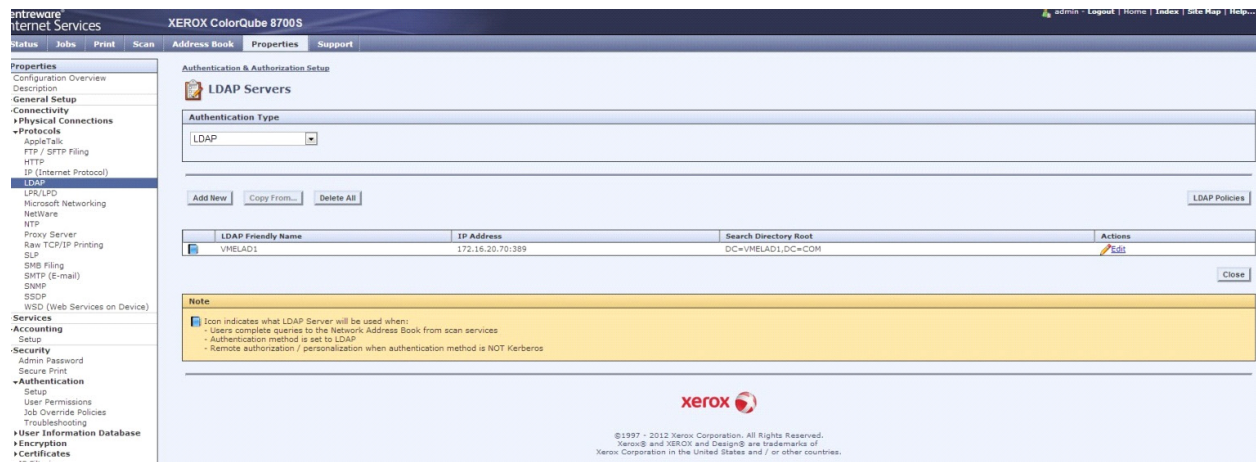
Configuration Setting	Method (Defined Above)	Required / Optional Status	Action
Authentication Servers	Authentication (Touch UI & Web UI)	Required; Configured	Edit...
Machine's User Information Database	Authorization	Required; Configured	Edit...
Tools and Feature Access (Lock / Unlock)	Authorization	Optional; Configured	Edit...
LDAP Servers	Personalization	Required; Configured	Edit...
Service Registration	(Convenience Link)	Optional; Configured	Edit...

Note Under Configuration Settings, if **LDAP Servers > Personalization** shows a red exclamation mark, you need to define which LDAP server to use. (This might not be necessary.) If there is a red exclamation mark, select **LDAP Servers**. Then, click the **Edit** button and choose the LDAP server you have configured.

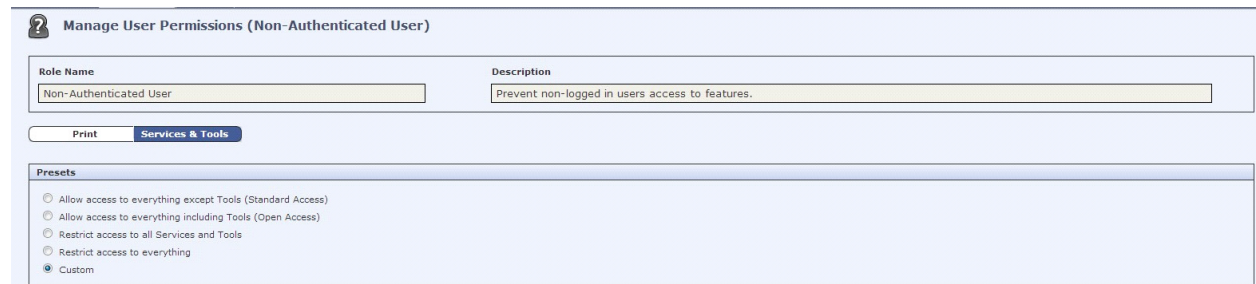
Graphic Key

- Required configuration to enable the Authentication, Authorization, and/or Personalization methods.
- Optional configuration expanding feature offering.
- Minimum configuration using factory defaults.
- Fully configured.

- o Verify the LDAP server you configured is in the device list of LDAP servers. In the left menu under **Protocols**, select **LDAP** to display the LDAP Servers.



- p In the left menu under **Security > Authentication**, select **User Permissions > Non-Authenticated Users > Edit**.
- q Select **Service & Tools**.



Note This example uses custom presets. For more information on presets, see the Xerox Administrator Guide.

- r For the Omtool feature button(s) desired for device authentication login, select **Not Allowed** in the **Role State** column. For example, you might select **Personal Distributions** and **Scan to Me**. The **Not Allowed** option locks those features requiring authentication.



- s Click **Apply**.
- t On the main page of the Device Internal Web server, select **IP (Internet Protocol)** under the **Protocols** heading in the left menu.
- u Click the **DNS** tab and verify that the **Requested Domain Name** and **DNS Server Addresses** match the Omtool DNS server settings. Click **Apply** when finished.
- v Reboot the device.
- w Continue with Step 16 on page 5-16.

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.

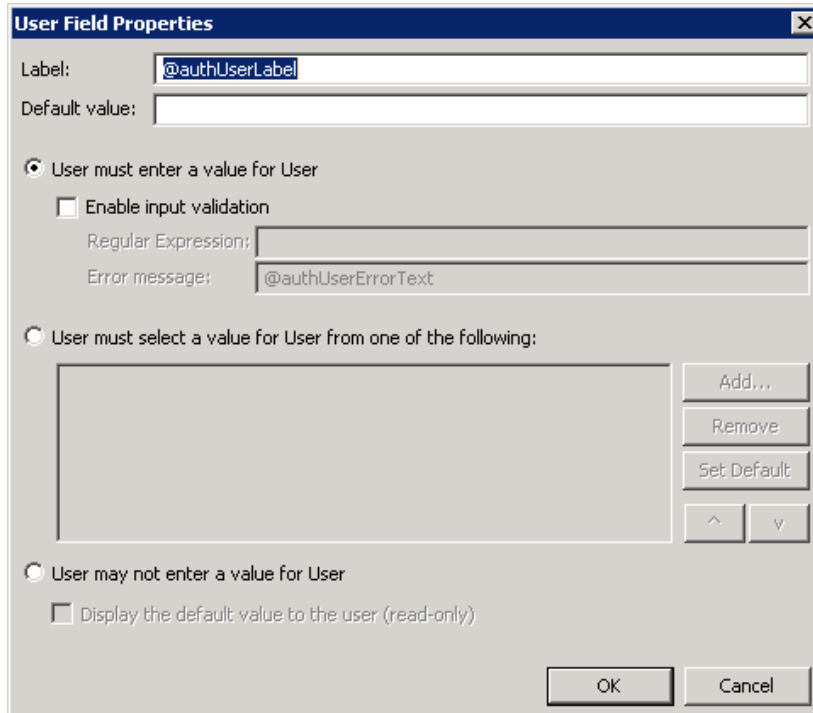
When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **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](#) (5-13).

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:



The **User Field Properties** dialog box is shown with the following fields and options:

- Label:** @authUserLabel
- Default value:** (empty text box)
- User must enter a value for User**
 - Enable input validation**
 - Regular Expression:** (empty text box)
 - Error message:** @authUserErrorText
- User must select a value for User from one of the following:**
 - (Empty list box)
 - Add...** button
 - Remove** button
 - Set Default** button
 - ^** button
 - v** button
- User may not enter a value for User**
 - Display the default value to the user (read-only)**

OK and **Cancel** buttons are at the bottom right.

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](#) (5-14).

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 10 on page 5-15.

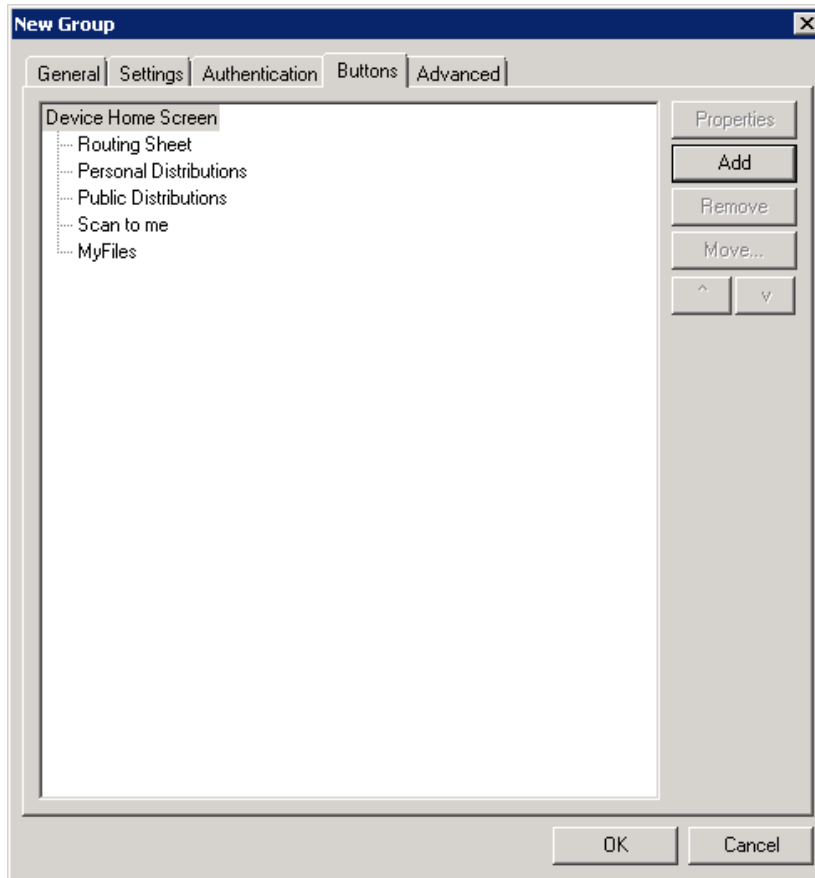
- 10** On the **Device Group Properties** page, keep the defaults for **Server**, **Port**, **Search Base**, and **Filter** (under the **LDAP LookUp Settings** heading).

The screenshot shows the "Device Group Properties" dialog box with the "Settings" tab selected. The "LDAP LookUp Settings" section is expanded, showing the following configuration:

- Type: Device
- Fields: Domain (User Entered), User (User Entered), Password (User Entered)
- Server: VMAD70.vmad700.com
- Port: 389
- Search Base: DC=vmad700.DC=com
- Filter: (&(objectClass=user)[sAMAccountName=[USER_NAME]])
- Username: (empty)
- Password: (empty)
- Attribute Map: Exchange.default.xml
- Bind using Windows Generic Security Services
- Confirm authentication
- Message: @msgConfirmation

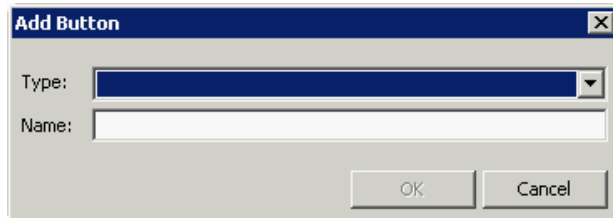
- 11** In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.
- 12** In the **Password** text box, enter the Administrator password.
- 13** If you are working in an Exchange environment, select [Exchange.default.xml](#) (Exchange Attributes) from the **Attribute Map** drop-down.
- 14** In some cases, it is necessary to select **Bind using Windows Generic Security Services**.
- 15** Select the **Confirm authentication** option if you want to display a prompt on the device to verify the user's information when authenticating.

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



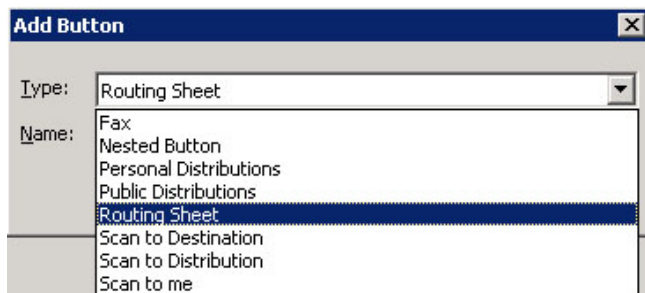
Note It is best to add or remove all previously set buttons before installing to the device. All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Reinstallation is required only if a new button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

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

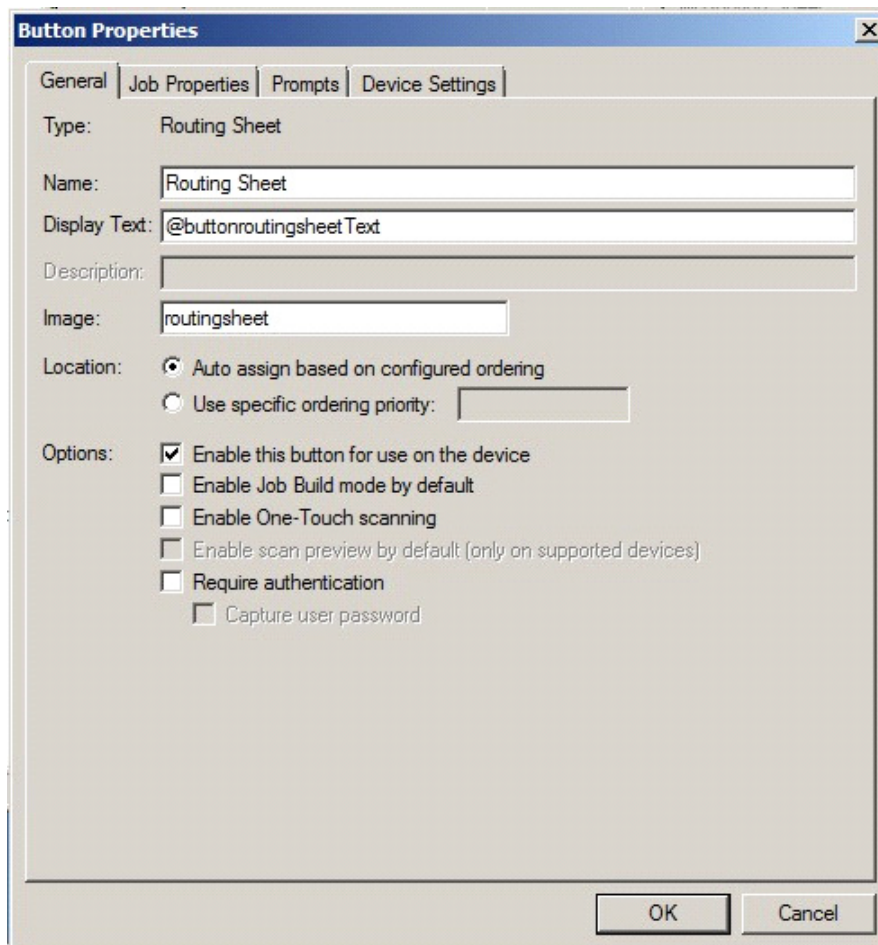


Note If the **Add** button is not active, click on **Device Home Screen**.

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



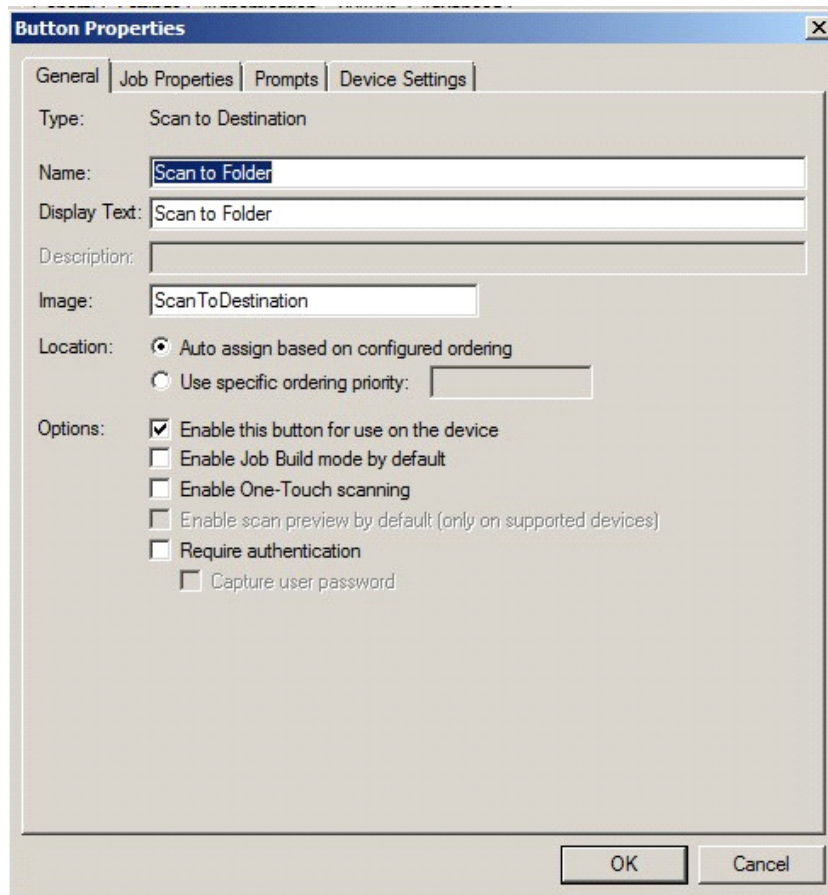
- 19 Enter a **Name** for the button. Then, click **OK**.
- 20 You will need to define properties for the button. With the button highlighted on the list, click **Properties**.



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

Note Do not change Image from the default value.

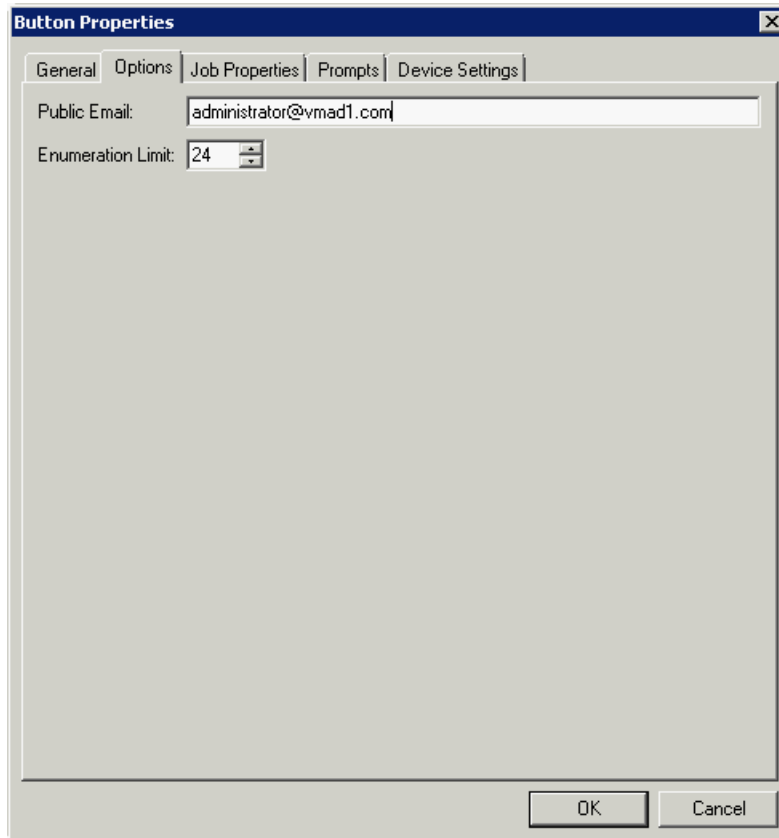
Note To change “Scan to Destination” to “Scan to Folder,” change the **Display Text** and **Description**.



- 21 Specify a location for the button. Select either of these options:
- 22 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.
- 23 Select additional options for the button:
 - ▶ **Enable this button for use on the device** - Self-explanatory.
 - ▶ **Enable Job Build mode by default** - Indicates the device will not send scanned pages until all pages in a job are scanned. For example, if a device can scan a specific number of pages at one time (such as 50 pages), the user can scan additional sets before the job is sent.

- ▶ **Enable One-Touch scanning** - Not a supported option in Xerox EIP v2.0.
- ▶ **Enable scan preview by default** - Not a supported option in Xerox EIP v2.0.
- ▶ **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.

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



Enter a **Public Email** address (if applicable) and set the **Enumeration Limit** for distributions (the maximum number of distributions allowable).

- 25 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.

Select Embedded Directive

Title

Owner e-mail:

Date created: 8/15/2012 to 8/15/2012

Date last used: 8/15/2012 to 8/15/2012

Expired

Single use

Public

Find

Title ▲	Owner	Created	Last Used	Single Use	Expires
---------	-------	---------	-----------	------------	---------

Select

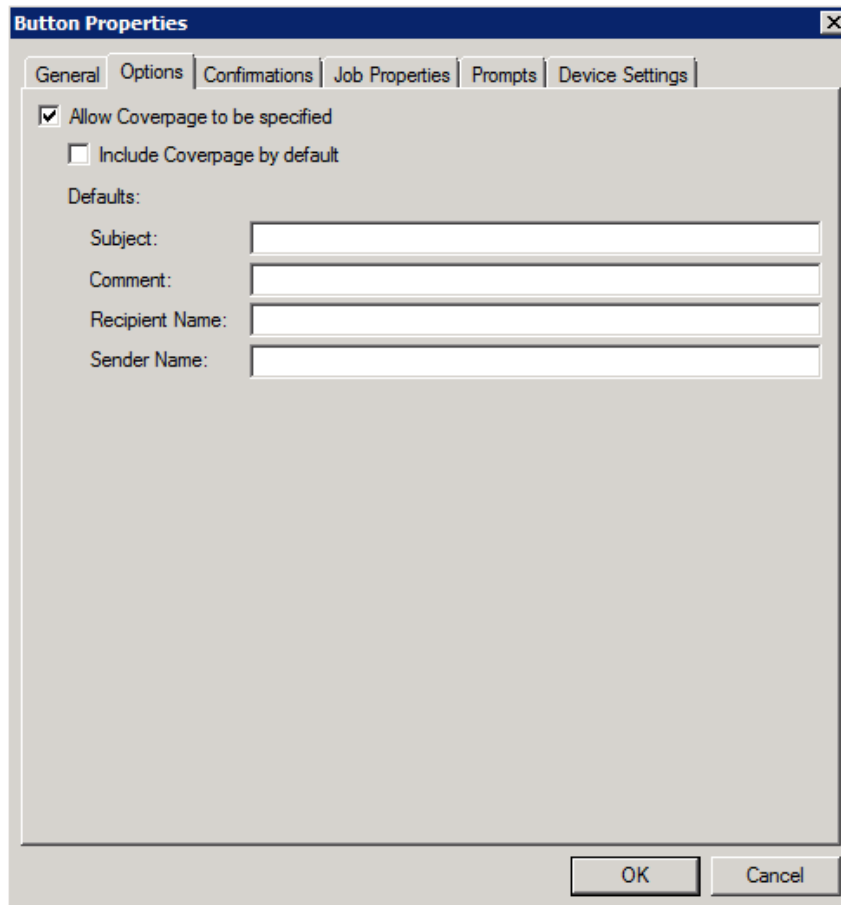
Cancel

Properties...

0 item(s)

- 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.

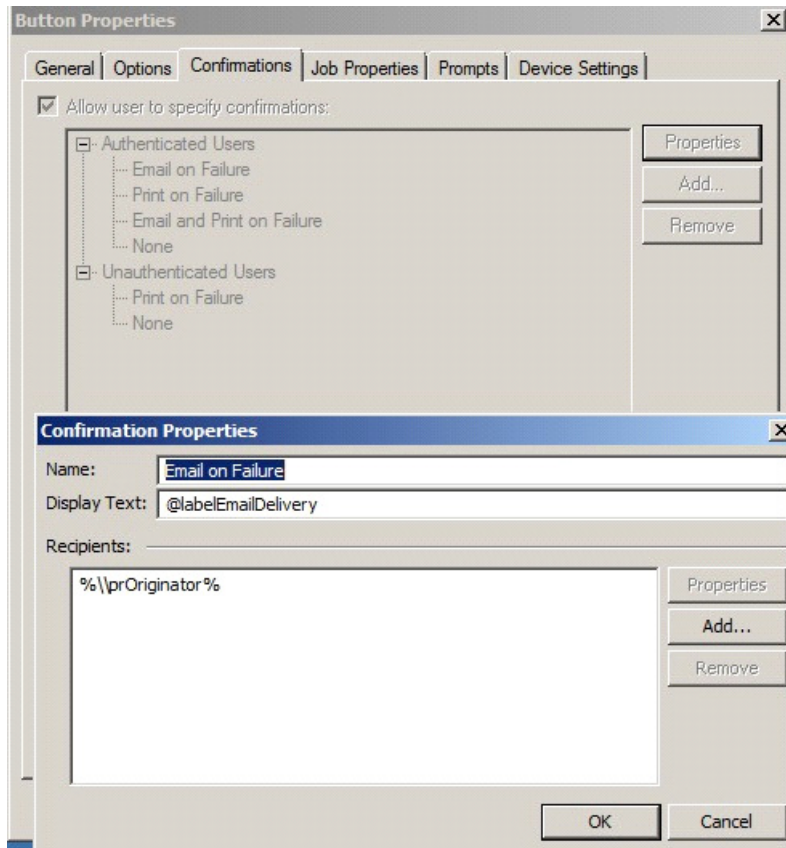
- 26** If you are adding a **Fax** button, click the **Options** tab to configure fax cover pages. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.



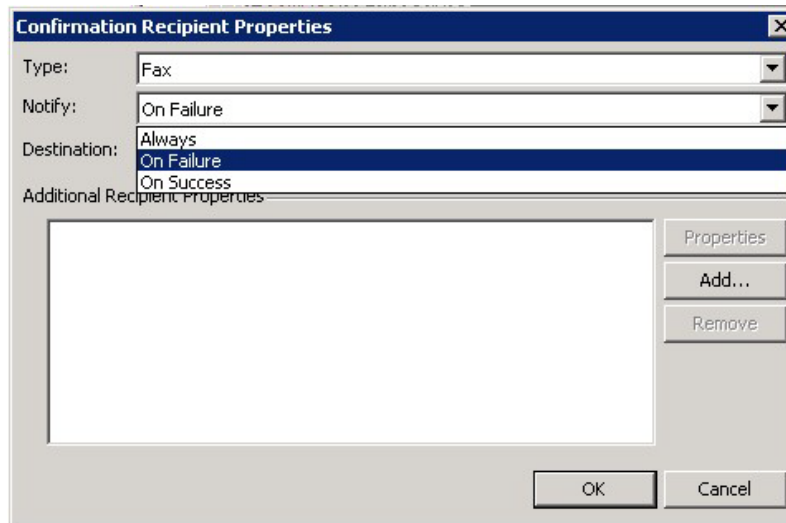
The image shows a screenshot of the "Button Properties" dialog box, specifically the "Options" tab. The dialog box has a title bar with a close button (X) and a tabbed interface with the following tabs: "General", "Options", "Confirmations", "Job Properties", "Prompts", and "Device Settings". The "Options" tab is selected. Inside the dialog, there are two checkboxes: "Allow Coverpage to be specified" (checked) and "Include Coverpage by default" (unchecked). Below these checkboxes, there is a section labeled "Defaults:" with four text input fields: "Subject:", "Comment:", "Recipient Name:", and "Sender Name:". At the bottom right of the dialog, there are "OK" and "Cancel" buttons.

- 27** 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.



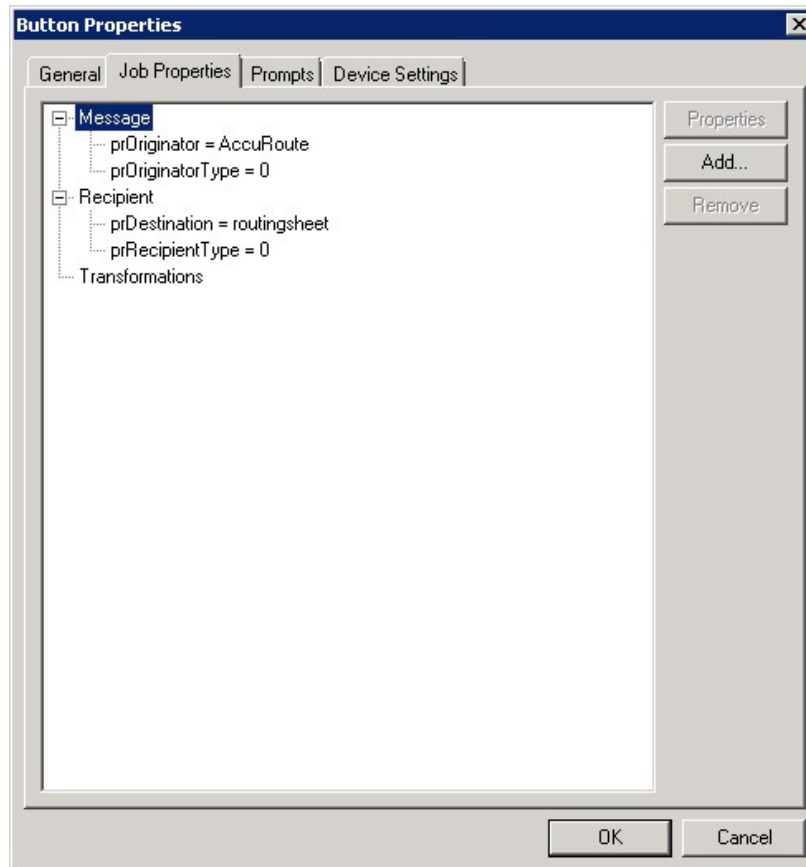
Type. - Leave this as the default.

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.

- 28 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.



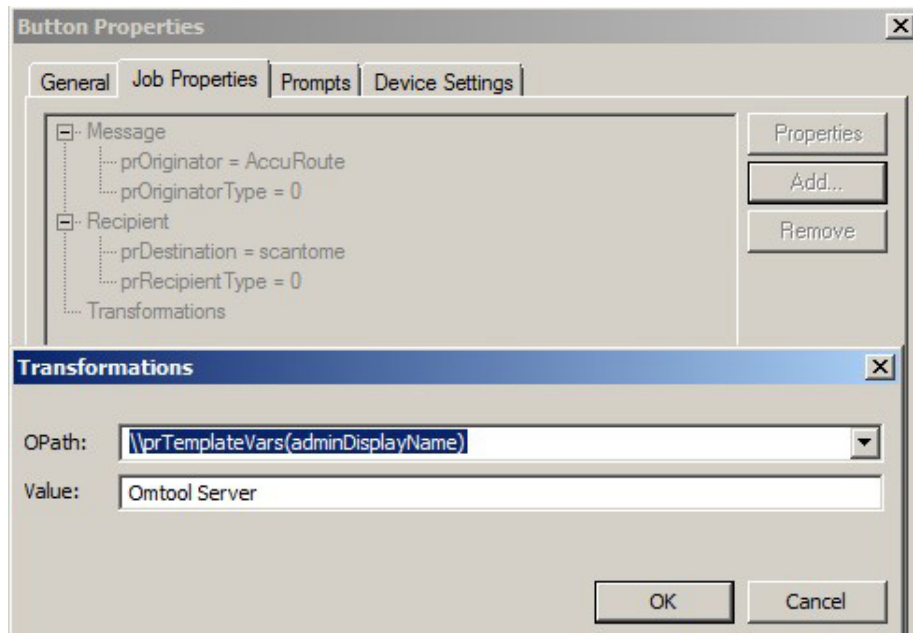
You can add, remove, or change a property. This example shows the property of a **Destination**.



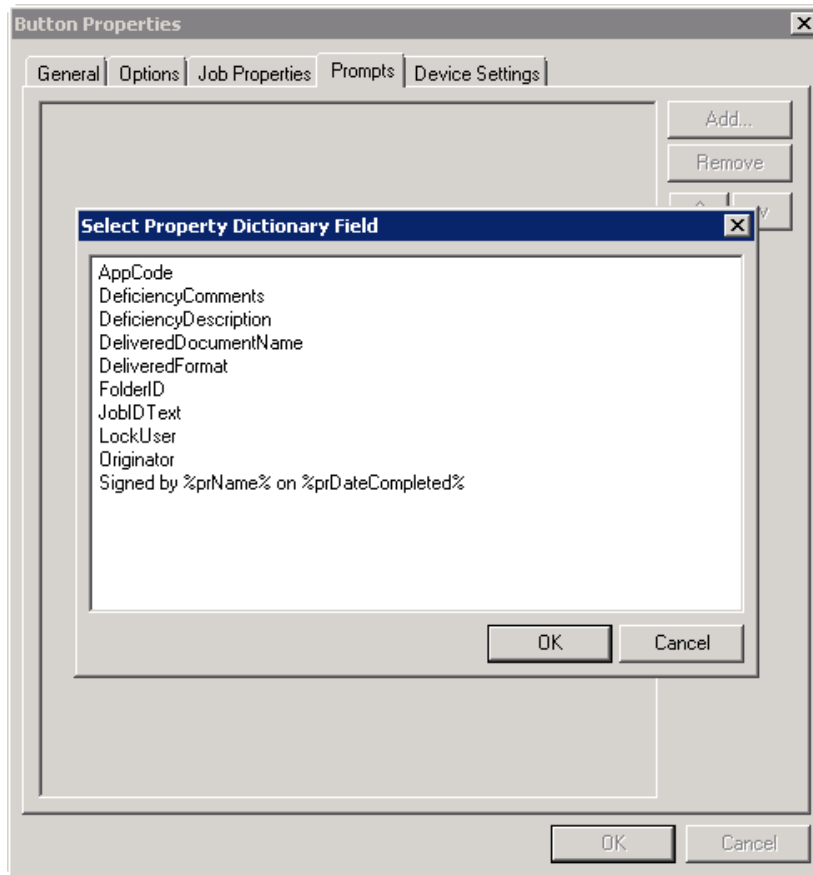
You can change an **Originator**, **Destination**, or **Recipient**. You also can add a **Transformation**, replacing a data value (a message property, recipient property, Embedded Directive (Distribution Rule) property, or template variable) with another value.

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.
- ▶ Transformations can be used to transform, replace, or map any Omtool properties (including attributes from Active Directory) to any other Omtool property value.

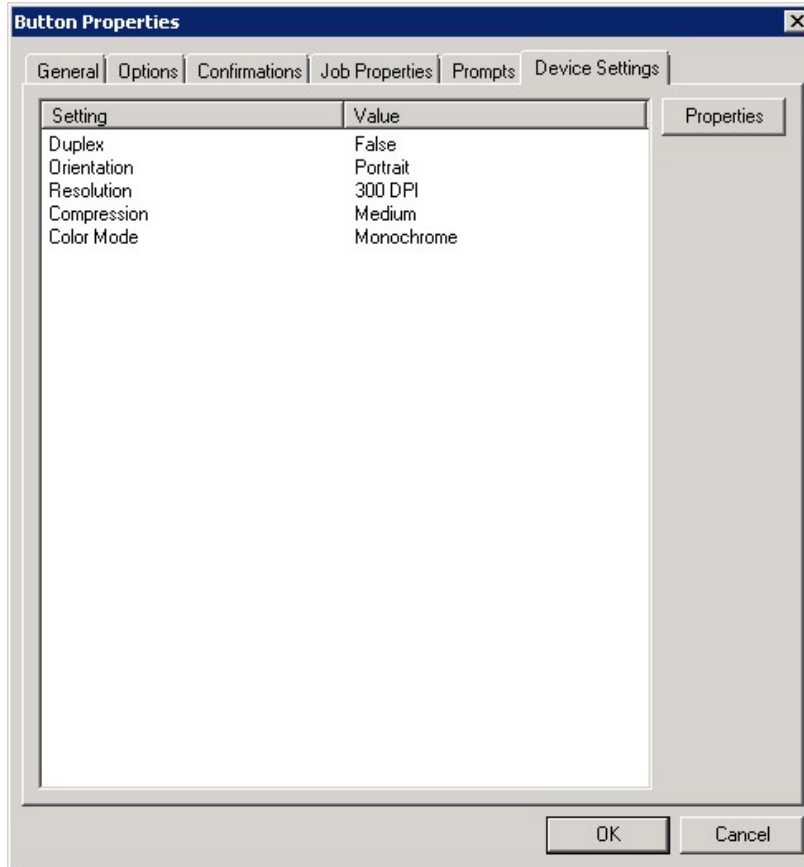


- 29 Click the **Prompts** tab. Click **Add** to select a prompt configured on the AccuRoute server. The **Select Property Dictionary Field** is displayed.

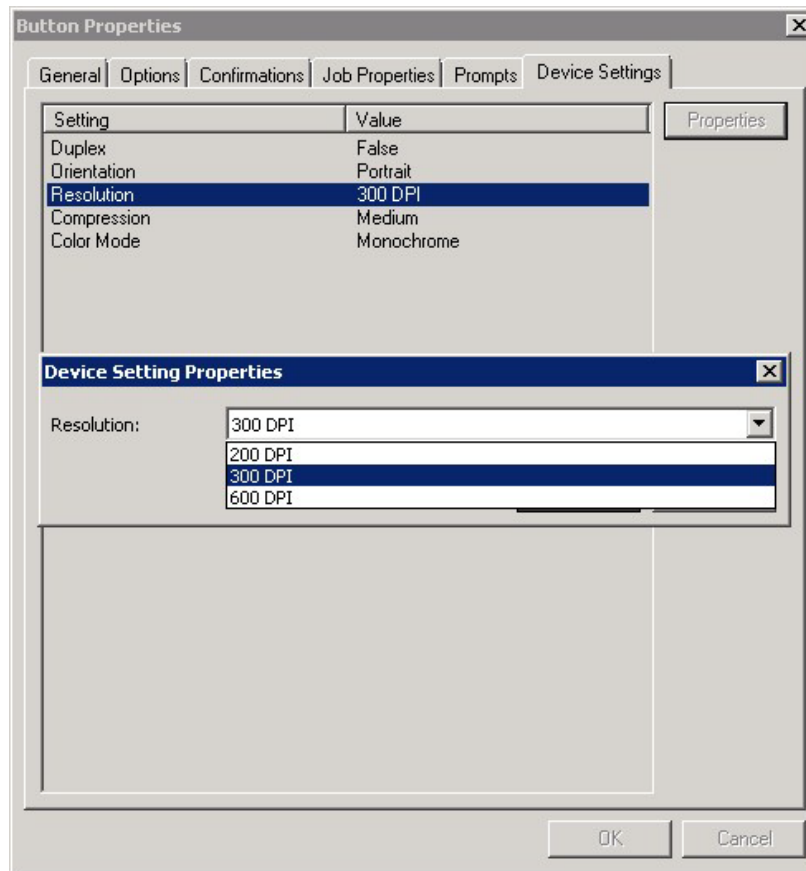


Select a prompt and click **OK**.

- 30** 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.



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

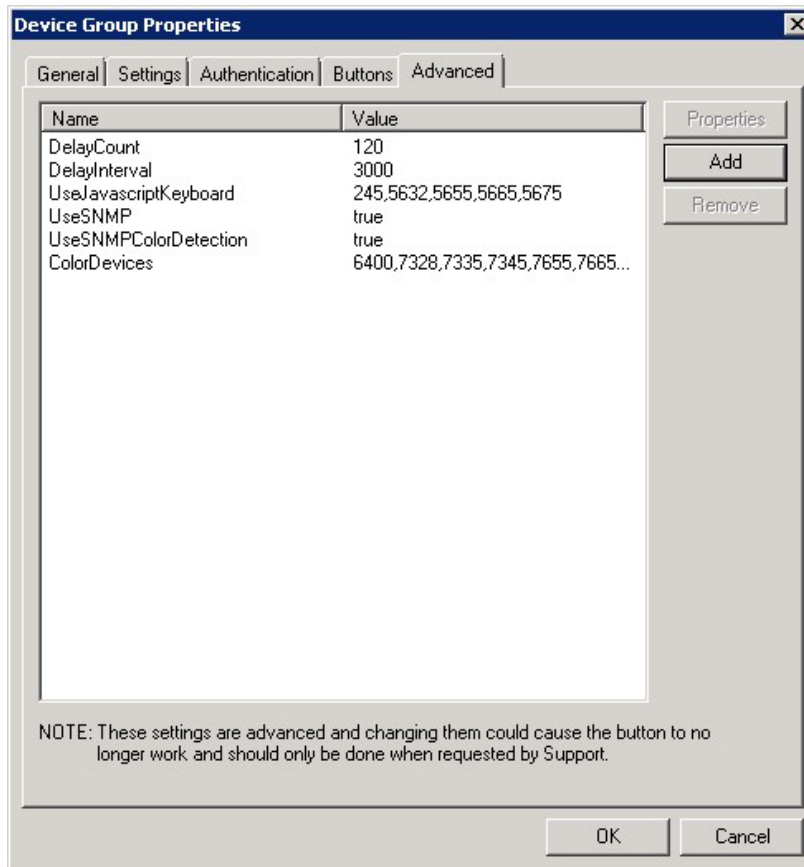


32 Click **OK** to return to the **Device Group Properties**.

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.

- 33** 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.

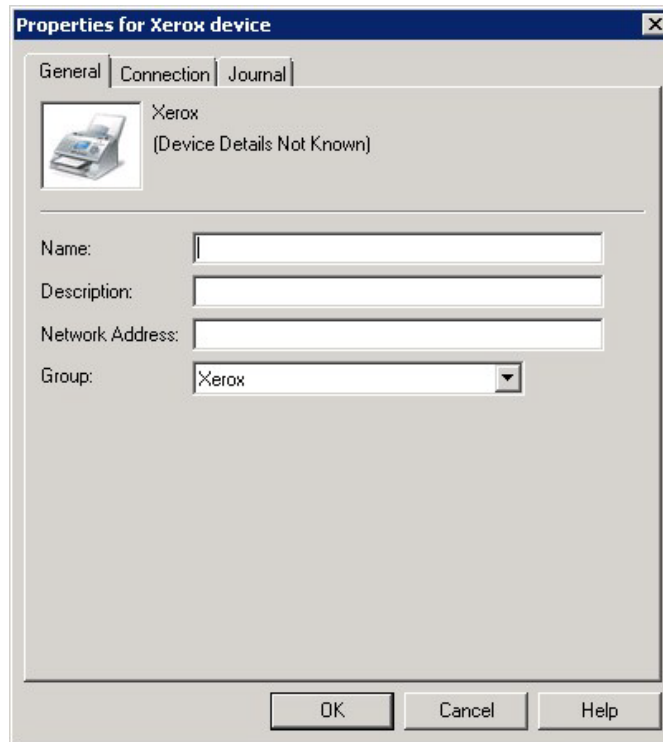


- 34** Click **OK** to end your work with the **Device Group Properties**.

Adding a new device

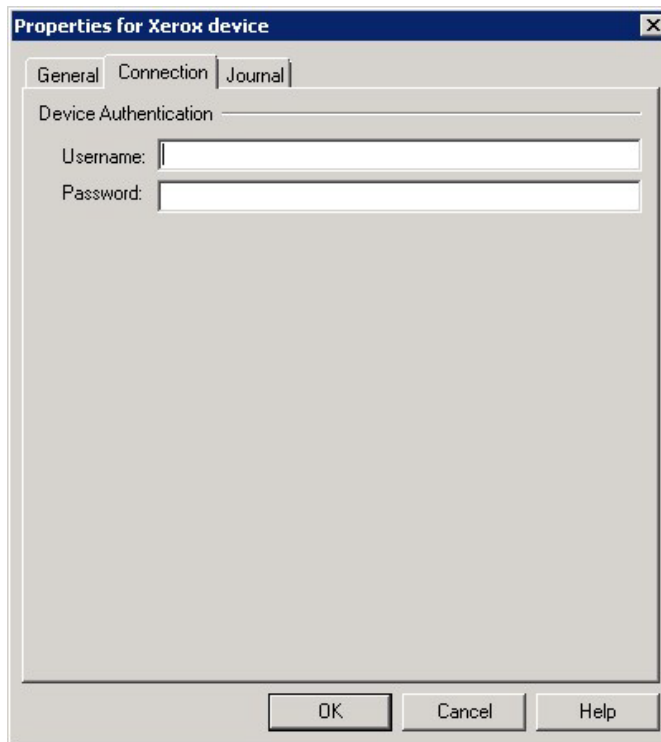
- 1 In the console tree, expand the AccuRoute server and right-click **Devices**.
- 2 Select the group name. Then, right-click and select **New > Device**.

The **Properties for device** page opens.



- 3 In the **Name** text box, enter a name for the device.
- 4 Optionally, in the **Description** text box, enter a device description.
- 5 In the **Network Address** text box, enter the device IP address.

6 Click the **Device Configuration** tab.



The screenshot shows a dialog box titled "Properties for Xerox device" with a close button (X) in the top right corner. The dialog has three tabs: "General", "Connection", and "Journal". The "General" tab is selected. Under the heading "Device Authentication", there are two text input fields: "Username:" and "Password:". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

7 In the **Username** text box, enter the device Administrator name.

8 In the **Password** text box, enter the Administrator password.

9 Click **OK** to add the device.

10 Test by selecting the newly added device. Right-click on the device name and select **Query** from the drop-down options.

Verify that the device is successfully queried from the server (refer to the Status entry, which should indicate "Query - Succeeded").

11 After a successful query, right-click and select **Install**.

12 Verify that the buttons appear on the device.

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 Omttool Server Administrator Help accessed through the [AccuRoute v4.0 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 Xerox (EIP) Device Client. You can test the AccuRoute scanning features at this point ([Section 7: Testing](#)).

Section 6: Optional Configuration

This section includes:

[Setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#) (6-1)

[Adding the remote server's name to DCOM](#) (6-2)

[Configuring a Distribution Rule to appear at the top of the device listing](#) (6-2)

[Configuring scan settings in Distribution Rules](#) (6-3)

[Adding an automatic logout timer](#) (6-3)

[Note about scan settings for compression](#) (6-5)

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`. Press **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 For all three levels - **Launch and activation permissions**, **Access Permissions** and **Configuration Permissions** - click **Edit**.
- 8 Add **Anonymous** to the list of users and assign it full permissions.

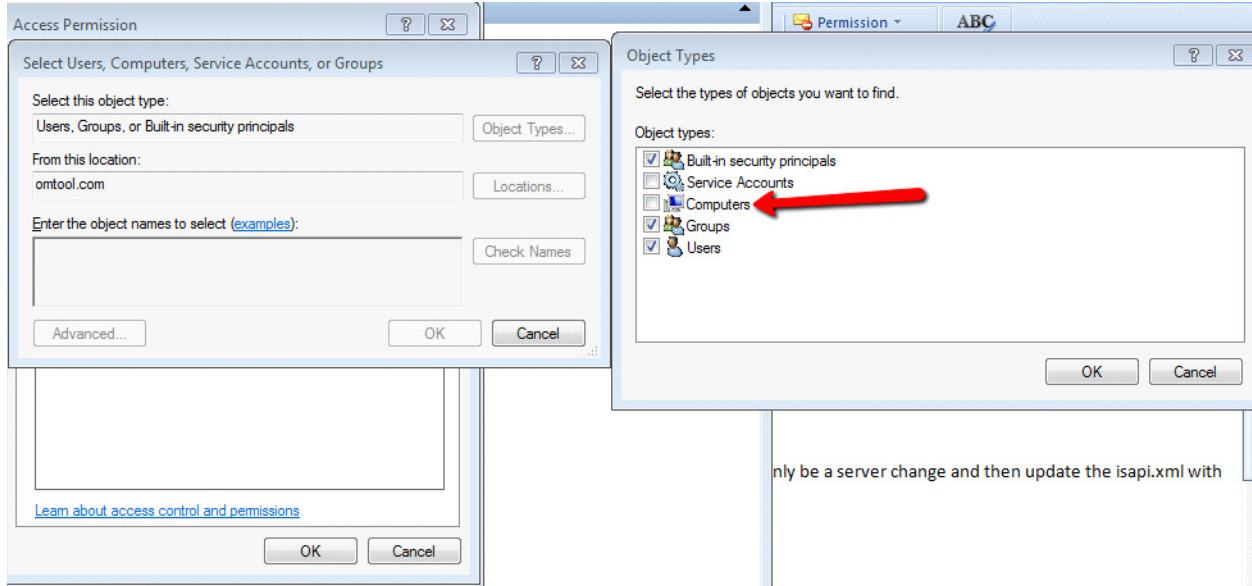
Additional procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the [AccuRoute v4.0 Server Installation Guide](#).

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.

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 see and use the Distribution Rule easily rather than having 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 are shown first in the list, then the Distribution Rules are listed alphabetically. Finally, the rules marked to show at the top of a device are listed.

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 scanned 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 click 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 device and select a Distribution Rule with which to scan a document. The scan settings in the Distribution Rule will override any device scan setting.

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

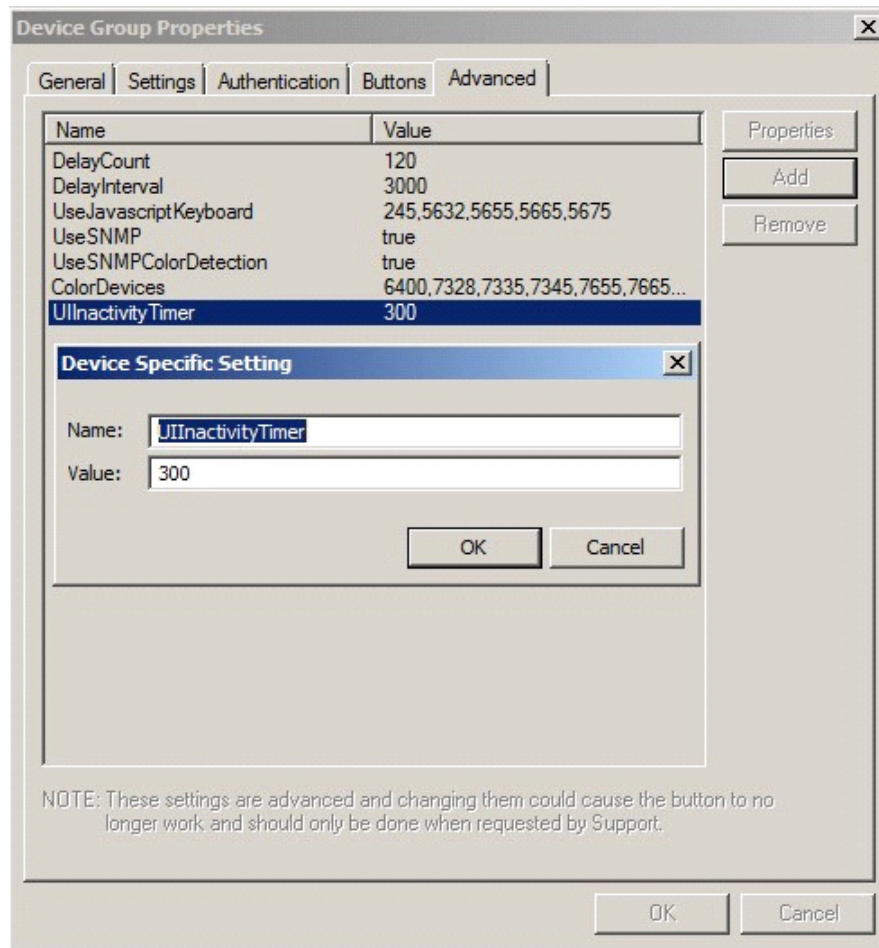
- On the **Tools > Message Options > Scan Settings** tab of the AccuRoute Desktop Client
- On the **Distributions > Options > Scan Settings** tab of the AccuRoute Web Client

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** distribution). 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.

Adding an automatic logout timer

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and open the **Devices** node.
- 3 Right-click the desired device group and select **Properties**.
- 4 Click the **Advanced** tab.

- 5 Click the **Add** button. The **Device Specific Setting** dialog is displayed.



- 6 Enter the following in the **Name** field:
`UIInactivityTimer`
- 7 Enter a value in seconds (for example, `60` = 60 seconds).
- 8 Click **OK** twice.

Note about scan settings for compression

Changing the compression setting in the administrator corresponds with the Quality/File size setting within More Options on the device. The table below outlines the scan setting equivalents (for example, compression set as Low in the AccuRoute Server Administrator is equivalent to Normal Quality/File size on the device).

Table 6-1: Scan settings for compression

Compression setting in the AccuRoute Server Administrator	Compression setting in More Options (Quality/File size) on the device
Low	= Normal on the device
Medium	= Higher on the device
High	= Maximum on the device

Section 7: Testing

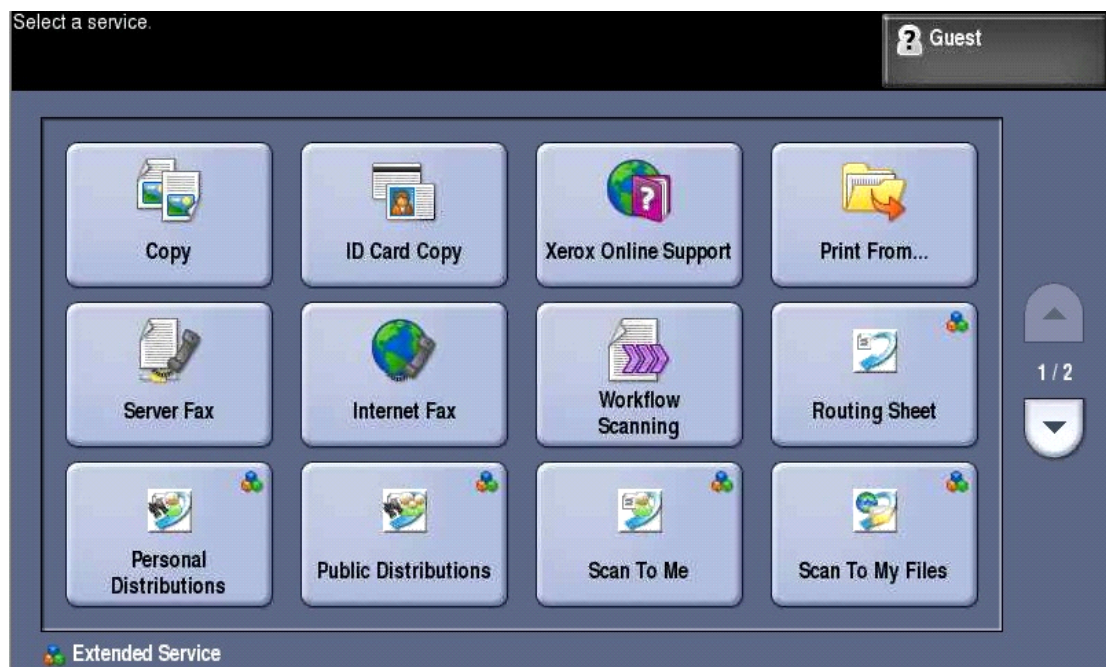
The following section provides a procedure for testing the Routing Sheet feature. This will ensure that your installation is operational. This section includes:

[Testing the Routing Sheet feature \(7-1\)](#)

[Testing the Device Administrator user interface \(7-2\)](#)

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 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**. (If this feature is not visible, use the scroll bar or **More** button to find it.)

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 display screen or on the hard keypad.

Alternately, to change the scan attributes, click **More Options**.

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.

The scan job starts. A progress counter shows the scan job status

To stop the scan job, press **Cancel Job**. 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 8: Troubleshooting](#).

- 7 To scan another document using the Routing Sheet option, click **Back**. To end the session and go back to the main AccuRoute menu, click **OK**.

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 \(8-6\)](#).

Testing the Device Administrator user interface

To test the Device Administrator user interface, complete the procedure for [Creating a group of devices \(5-4\)](#).

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
- Device

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

Section 8: Troubleshooting

This section includes:

[Detecting workflow issues](#) (8-2)

[Troubleshooting the delivery mechanism](#) (8-2)

[Troubleshooting messages on the AccuRoute server](#) (8-3)

[Troubleshooting the Web server](#) (8-5)

[Troubleshooting the multifunction device](#) (8-5)

[Troubleshooting .NET error when installing Embedded AccuRoute for Xerox \(EIP\) Device Client](#) (8-5)

[Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices \(Omttool ISAPI Web Server Extension\) in a cluster](#) (8-6)

[Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet](#) (8-6)

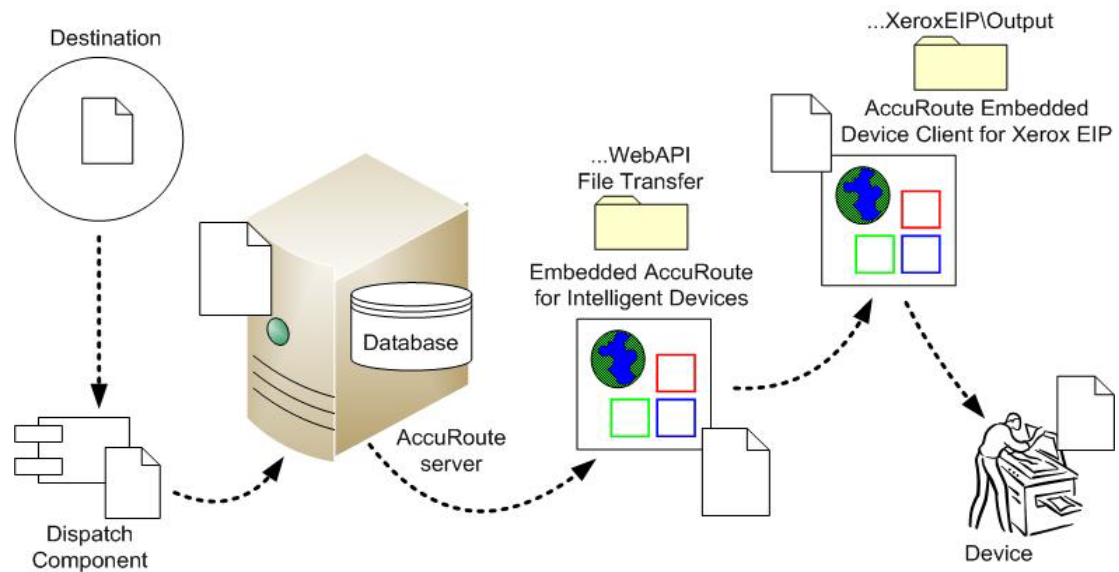
[Troubleshooting issues when configuring the device to Enable Secure HTTP \(SSL\)](#) (8-7)

[Troubleshooting inability to configure a device to Enable HTTP\(SSL\) and creating a new self-signed certificate](#) (8-7)

If you cannot resolve an issue, contact [Omttool 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 Xerox (EIP) Device Client, the Web server, and the device.

Figure 8-1: 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](#).

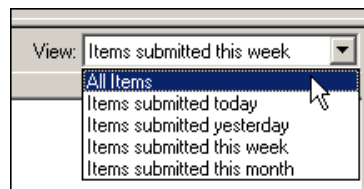
Troubleshooting messages on the AccuRoute server

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

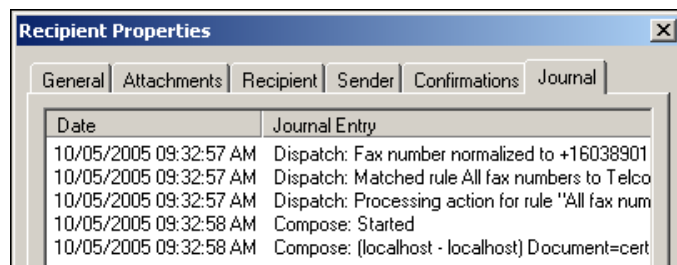
- Was the message submitted to the AccuRoute server?
- Assuming the message was submitted to the AccuRoute server, what caused the delivery failure? The state and status of the message, along with details in the message journal, provide some important clues.

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**.

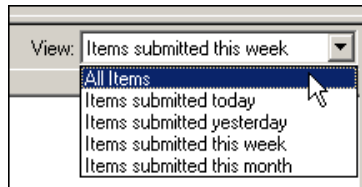


- c Sort all items by the date submitted.
- d Look for the message.
 - ▶ **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If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

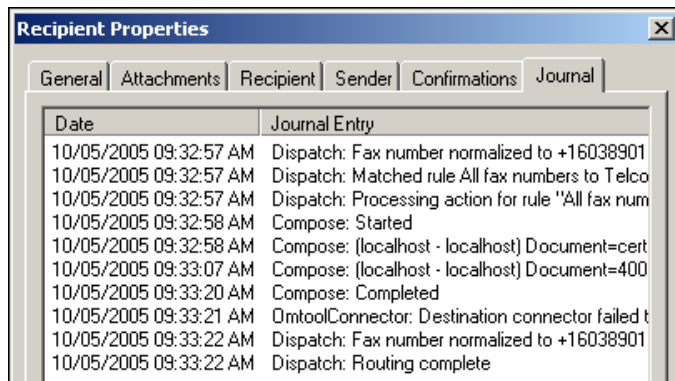


- ▶ **Message not found** - Go to step 4 and look for the message in the History queue.

- 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 v4.0, consult the [AccuRoute v4.0 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 Xerox documentation.

Troubleshooting .NET error when installing Embedded AccuRoute for Xerox (EIP) Device Client

Problem:

When installing Embedded AccuRoute for Xerox (EIP) Device Client v2.0 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 v3.5.1 before proceeding with the Embedded AccuRoute for Xerox (EIP) Device Client 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 v4.0 Server Installation Guide](#).

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

Problem:

When using a Xerox 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 issues when configuring the device to Enable Secure HTTP (SSL)

Problem:

All Xerox devices must be set to HTTPS/SSL mode when using EIP. Sometimes you may not be able to configure the device to Enable Secure HTTP(SSL). If a device's domain controller information changed after the certificate was created, you can resolve the issue by creating a new certificate.

Solution:

Create a new self-signed certificate for Xerox devices. This example shows how to create a self-signed certificate on a Workcentre 6400:

- 1 Open the Device Embedded Web Server and log in.
- 2 From the top menu, select **Properties**.
- 3 In the left menu, select **Machine Digital Certificate > Create new Certificate**.
- 4 Select the default value of **Self Signed Certificate: Establish a Self Signed Certificate on this machine** and select **Continue**.
- 5 Fill out the form and click **Apply**. The device updates at this time.
- 6 Follow steps 1 and 2 again and select **Connectivity > Protocols > HTTP**.
- 7 Select the **Enable Secure HTTP(SSL)** radio button and click **Apply**.

Troubleshooting inability to configure a device to Enable HTTP(SSL) and creating a new self-signed certificate

All Xerox devices must be set to HTTPS/SSL mode when using EIP. If a device's domain controller information changed after the certificate was created, you must create a new one. This action can also resolve the issue of being unable to configure the device to Enable Secure HTTP(SSL).

The following example shows how to create a self-signed certificate on a Workcentre 6400:

- 1 Open the Device Embedded Web Server and log in.
- 2 On the top menu, select **Properties**.
- 3 In the left menu, select **Machine Digital Certificate > Create new Certificate**.
- 4 Accept the default setting **Self Signed Certificate: Establish a Self Signed Certificate on this machine** and select **Continue**.
- 5 Fill out the form and select **Apply**. The device will update at this time.
- 6 Follow steps 1 and 2 again and select **Connectivity > Protocols > HTTP**.
- 7 Select the **Enable Secure HTTP(SSL)** radio button and click **Apply**.

