

---

# Embedded AccuRoute<sup>®</sup> for HP<sup>®</sup> OXPd Device Client 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](mailto:customerservice@omtool.com) or [support@omtool.com](mailto: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](mailto:sales@omtool.com)

# Contents

## Section 1: Introduction

|   |     |
|---|-----|
| Overview of AccuRoute Embedded Device Client for HP OXPd.....   | 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 Fax Release feature .....  | 1-6 |
| Workflow for the Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files features..... | 1-7 |
| Deploying AccuRoute Embedded Device Client for HP OXPd.....   | 1-8 |
| Related documentation.....  | 1-8 |

## Section 2: Requirements

|  |     |
|--|-----|
| Supported devices.....                                       | 2-1 |
| Supporting large color documents.....                        | 2-2 |
| Updating the Deviceloader.xml to add a supported device..... | 2-3 |
| AccuRoute server requirements .....                          | 2-4 |
| Device authentication requirements .....                     | 2-4 |

## Section 3: Installation

|  |     |
|--|-----|
| Installing AccuRoute Embedded Device Client for HP OXPd v1.6 .....                             | 3-1 |
| Installing AccuRoute Embedded Device Client for HP OXPd v1.4 .....                             | 3-2 |
| Installing AccuRoute Embedded Device Client for HP OXPd (v1.6 or v1.4) on a remote system..... | 3-3 |
| Uninstalling AccuRoute Embedded Device Client for HP OXPd.....                                 | 3-4 |
| Upgrading AccuRoute Embedded Device Clients for HP OXPd.....                                   | 3-5 |
| Uninstalling AccuRoute Embedded Device Clients .....   | 3-5 |
| Installing AccuRoute Embedded Device Clients.....  | 3-5 |

## Section 4: Configuration for HTTPS Support

|   |      |
|---|------|
| Setting up a CA certificate and enabling SSL with Windows 2008 R2 .....     | 4-2  |
| Requirements for setting up a CA certificate .....                          | 4-2  |
| Downloading the MakeCert executable.....                                    | 4-2  |
| Creating the certificate.....   | 4-3  |
| Installing the certificate to Internet Information Services (IIS).....      | 4-3  |
| Exporting the certificate to the OXPd v1.6 Device Client directory.....     | 4-3  |
| Creating an SSL binding .....   | 4-4  |
| Requiring SSL for the virtual web sites .....                               | 4-4  |
| Enabling directory browsing in IIS .....                                    | 4-5  |
| Verifying the SSL binding .....   | 4-5  |
| Verifying HTTPS browsing.....   | 4-5  |
| Editing the OmISAPIU.xml file.....  | 4-6  |
| Editing the Bootstrap.xml file.....   | 4-6  |
| Setting up a CA certificate and enabling SSL with Windows 2003 64-bit ..... | 4-7  |
| Requirements for setting up a CA certificate .....                          | 4-7  |
| Downloading the MakeCert executable.....                                    | 4-7  |
| Running the MakeCert executable and creating the certificate.....           | 4-7  |
| Exporting the certificate to the OXPd v1.6 Device Client directory.....     | 4-8  |
| Requiring SSL for web sites .....   | 4-14 |
| Editing the OmISAPIU.xml file.....  | 4-15 |
| Editing the Bootstrap.xml file.....   | 4-16 |

## Section 5: Required Configuration

|   |      |
|---|------|
| Entering a license for AccuRoute Embedded Device Client for HP OXPd ..... | 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  |
| Adding a new device.....  | 5-27 |
| Choosing an authentication method.....                                    | 5-30 |
| Configuring LDAP authentication .....                                     | 5-30 |
| Configuring the server .....  | 5-31 |

## Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices

|                                   |     |
|-----------------------------------|-----|
| Supported Devices.....            | 6-1 |
| Exporting the XML files .....     | 6-2 |
| Installing OXPd v1.6 buttons..... | 6-4 |

## Section 7: Optional Configuration

|  |      |
|--|------|
| Setting up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a cluster ..... | 7-1  |
| Adding the remote server's name to DCOM .....  | 7-2  |
| Configuring a Distribution Rule to appear at the top of the device listing.....                              | 7-2  |
| Configuring scan settings in Distribution Rules.....   | 7-3  |
| Configuring the Universal Input connector for HP OXP file processing.....                                    | 7-3  |
| Requirements for the Universal Input Connector .....   | 7-3  |
| Installing the Universal Input connector license .....   | 7-4  |
| Configuring the Fax Release button.....  | 7-8  |
| Creating the Fax Release property (prDestinationFaxNumber).....  | 7-8  |
| Creating the Administrator view options .....  | 7-9  |
| Creating the DTT Administrator Group for the Web Client .....  | 7-10 |
| Configuring a release calendar .....   | 7-10 |
| Configuring the DTT .....  | 7-11 |

## Section 8: Testing

|   |     |
|---|-----|
| Testing the Routing Sheet feature.....                | 8-1 |
| Testing the Device Administrator user interface ..... | 8-2 |

## Section 9: Troubleshooting

|  |     |
|--|-----|
| Detecting workflow issues.....   | 9-2 |
| Troubleshooting the delivery mechanism .....   | 9-2 |
| Troubleshooting messages on the AccuRoute server.....  | 9-3 |
| Troubleshooting the Web server .....   | 9-5 |
| Troubleshooting the multifunction device .....   | 9-5 |
| Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd.....   | 9-5 |
| Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices<br>(Omtool ISAPI Web Server Extension) in a cluster ..... | 9-6 |
| Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule<br>instructions in a Routing Sheet .....                          | 9-6 |
| Troubleshooting problems associated with applying all additional scan attributes .....   | 9-7 |
| Troubleshooting problems when scanning large documents.....  | 9-7 |
| Troubleshooting problems when scanning 100+ color pages .....  | 9-8 |
| Troubleshooting an SNMP error.....   | 9-9 |



# Section I: Introduction

This guide contains instructions on deploying AccuRoute Embedded Device Client for HP OXPd to multifunction devices running OXP SDK v1.6.x and OXP SDK v1.4.x. 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 AccuRoute Embedded Device Client for HP OXPd](#) (I-1)

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

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

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

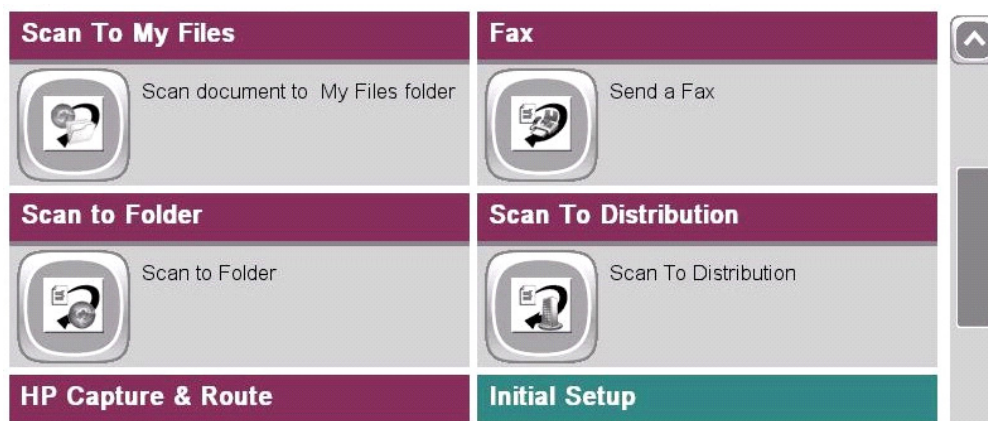
[Deploying AccuRoute Embedded Device Client for HP OXPd](#) (I-8)

[Related documentation](#) (I-8)

## Overview of AccuRoute Embedded Device Client for HP OXPd

AccuRoute Embedded Device Client for HP OXPd brings the versatile document routing capabilities of AccuRoute to supported devices running OXP SDK library v1.6.x as well as a limited set of devices running OXPd SDK library v1.4.x. These capabilities are founded in Omtool's Distribution Rule technology.

AccuRoute Embedded Device Client for HP OXPd runs on OXP (Open Extensibility Platform), an ASP.NET layer sitting between the device and the AccuRoute server. It communicates between the OXP 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 HP device running AccuRoute Embedded Device Client for HP OXPd**

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

**Table I-1: AccuRoute scanning features in AccuRoute Embedded Device Client for HP OXPd**

| 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             |   |
| Fax Release   | The user can hold all jobs to a fax number for an indefinite period of time and then release all jobs using a PIN associated with the fax number. The user creates and uses a “release” calendar to specify times during which all fax jobs will be released.  | Yes            | <a href="#">Configuring the Fax Release button (7-8)</a> involves creating a property (prDestinationFaxNumber) to filter ending jobs for each destination fax number, creating a Destination Translation Table (DTT) Administrator Group, configuring a release calendar to specify release times, and configuring the DTT used to define routing features. |
| 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.<br><br>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<br>(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 5-14) 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.   |                |   |



**Table I-1: AccuRoute scanning features in AccuRoute Embedded Device Client for HP OXPd**

| 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.<br><br>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.<br><br>For more information on this feature, consult <a href="#">Section 2: Requirements</a> . |
| 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 Web Client 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 AccuRoute Embedded Device Client for HP OXPd environment consists of the following components.

- **AccuRoute Server** - The AccuRoute server is 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 AccuRoute Embedded Device Client for HP OXPd is installed on a remote system, and then the AccuRoute Intelligent Device Client would be installed on the remote system as well.

- **AccuRoute Embedded Device Client for HP OXPd v1.4 or OXPd v1.6** - See [Section 3: Installation](#) for installation instructions.
- **HP Device** - See [Supported devices](#) (2-1) for a list.

## Installation components

The AccuRoute Embedded Device Client for HP OXPd setup includes multiple components detailed in this table.

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

| Component  | Location  | Function   |
|--|---|--|
| AccuRoute Embedded Device Client for HP OXPd Install               | ...\Omtool\Omtool Server\Clients                    | The setup contains the setup.exe file for both HP OXPd v1.6 and HP OXPd v1.4. Use this file to install the AccuRoute Embedded Device Client for HP OXPd.   |
| AccuRoute Embedded Device Client for HP OXPd 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.<br><br><b>Note:</b> A device license must be installed in order for the Device Client Configuration manager node to be used. |

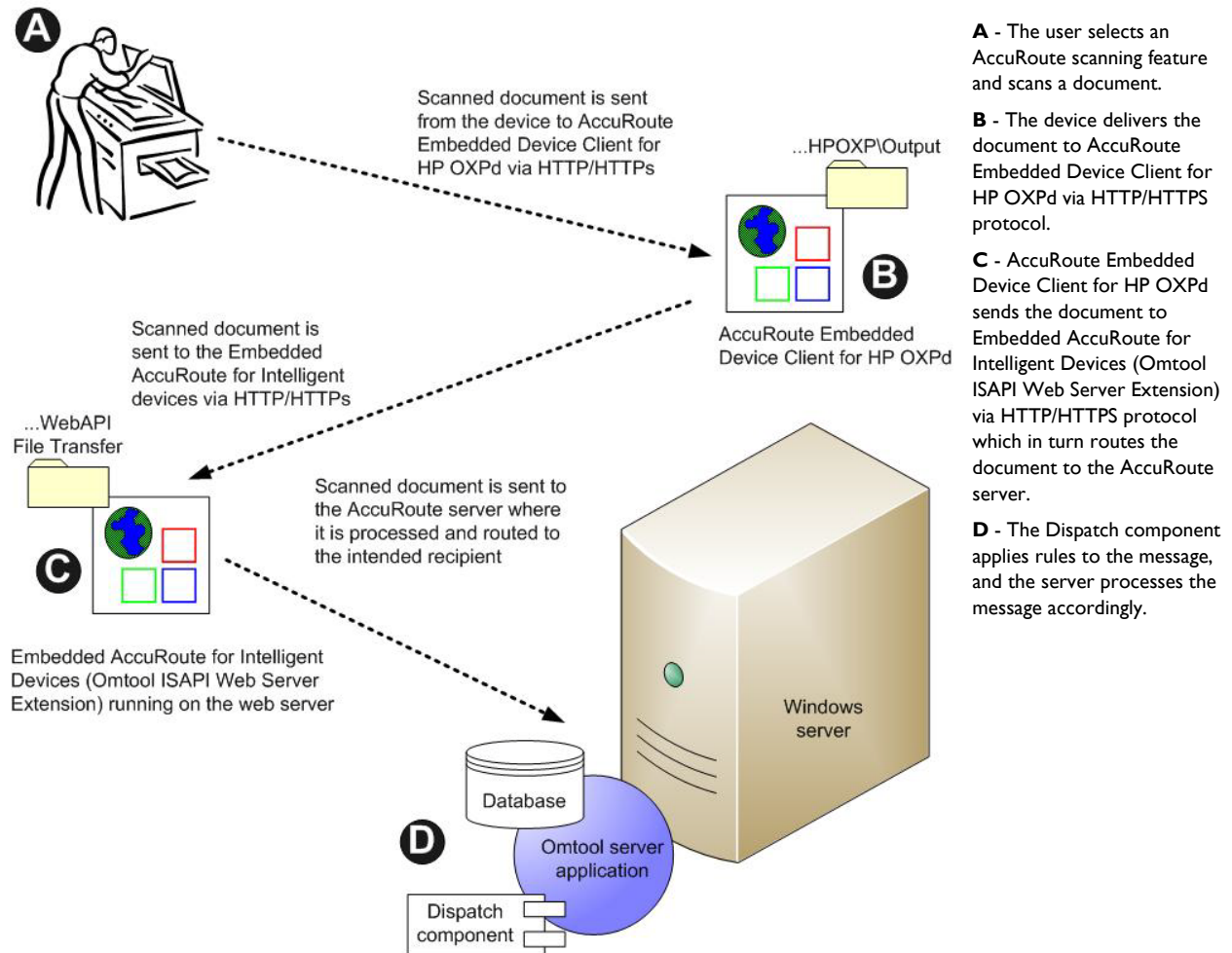
## Document workflow

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

Basic workflow is:

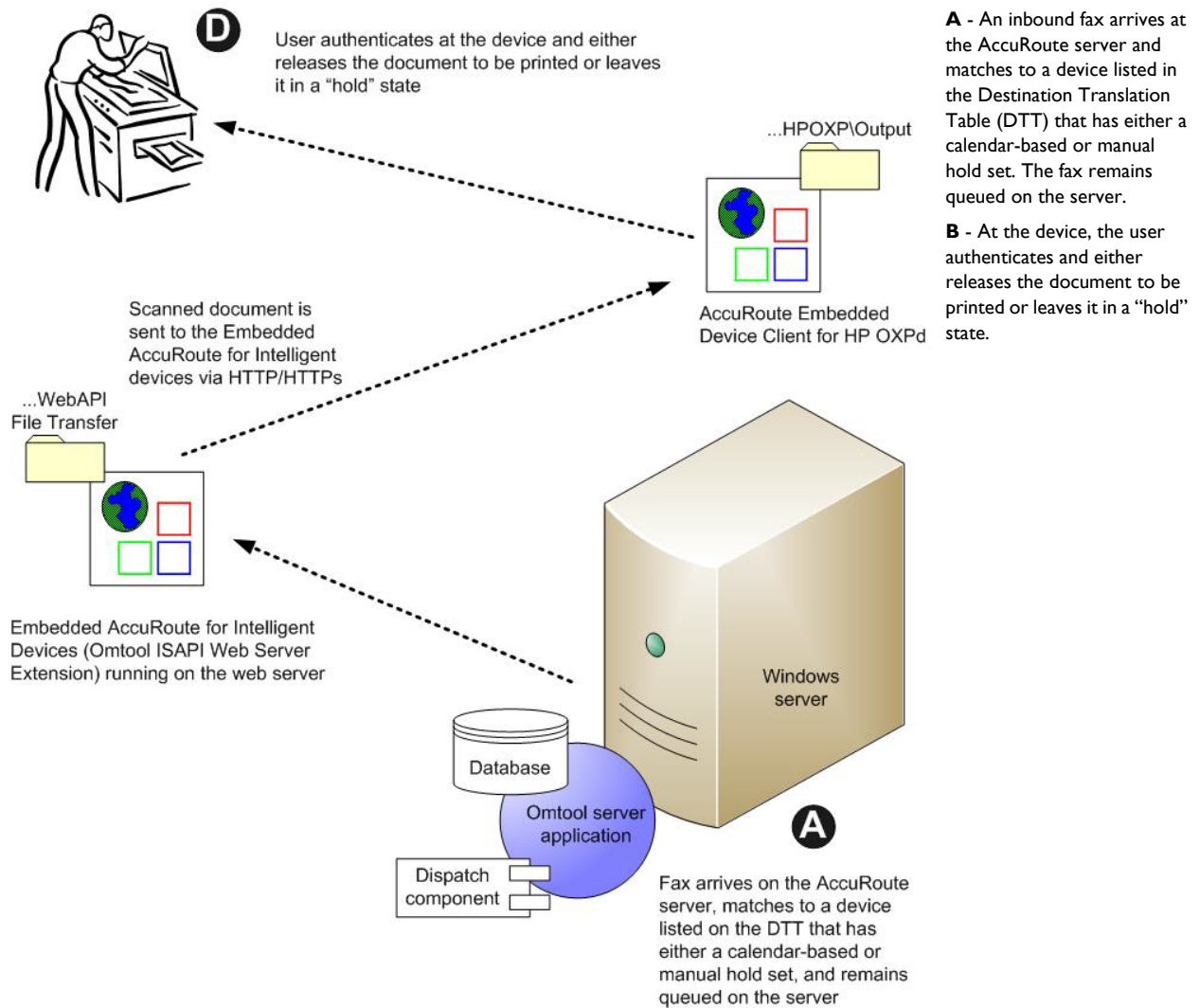
- When a device user scans a document, the device submits the document to AccuRoute Embedded Device Client for HP OXPd via HTTP/HTTPS protocol.
- The AccuRoute Embedded Device Client for HP OXPd then routes the document to the AccuRoute server via HTTP/HTTPS protocol.
- The Dispatch component applies 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 Fax Release feature



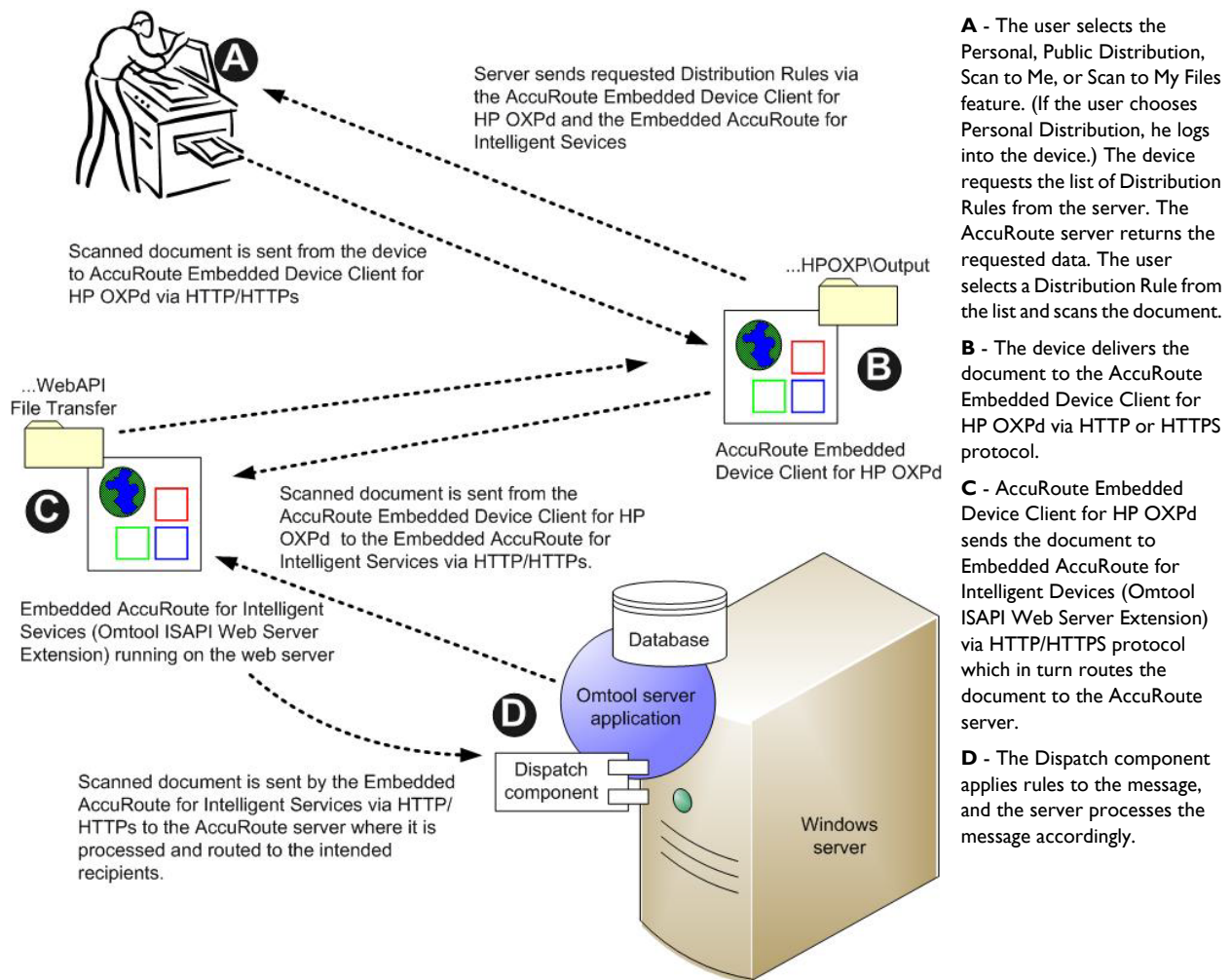
**Figure I-3: Workflow for Fax Release**

## 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 AccuRoute Embedded Device Client for HP OXPd to retrieve Distribution Rules.

**Note** For Personal Distributions, Scan to Me, and Scan to My Files, the device user must authenticate himself at the device using the configured authentication type. See [Choosing an authentication method](#) (5-30).

The AccuRoute Embedded Device Client for HP OXPd 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 AccuRoute Embedded Device Client for HP OXPd. As soon as the AccuRoute Embedded Device Client for HP OXPd returns the data to the device, the workflow resumes.



**Figure I-4: Workflow for Personal Distributions, Public Distributions, Scan to Me, and Scan to My Files**

---

# Deploying AccuRoute Embedded Device Client for HP OXPd

- 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 AccuRoute Embedded Device Client for HP OXPd. Refer to [Setting up a CA certificate and enabling SSL with Windows 2008 R2 \(4-2\)](#) or [Setting up a CA certificate and enabling SSL with Windows 2003 64-bit \(4-7\)](#).

---

- 2 Install AccuRoute Embedded Device Client for HP OXPd 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<sup>®</sup> Server Installation and Integration Guide*, which is available through <http://www.omtool.com/documentation/accuroute/4.0/documentation.htm>
- 5 Configure optional capabilities. ([Section 7: Optional Configuration](#))
- 6 Test the AccuRoute scanning features on the device. ([Section 8: Testing](#))
- 7 Troubleshoot the setup, if necessary. ([Section 9: Troubleshooting](#))

---

## Related documentation

- [AccuRoute v4.0 Server Installation Guide](#)
- [Omttool Server Administrator Help](#)
- [HP OXPd 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](#) (2-4)

[Device authentication requirements](#) (2-4)

### Supported devices

Omtool supports AccuRoute Embedded Device Client for HP OXPd on all devices listed in this section. Consult HP to determine compatible firmware versions for supported devices.

**Table 2-1: List of devices supported with AccuRoute Embedded Device Client for HP OXPd**

| Device                     | Group | Supported firmware      | Minimum Installed RAM | OXPd Version | Web Jetadmin (Operation System) |
|----------------------------|-------|-------------------------|-----------------------|--------------|---------------------------------|
| Color LaserJet CM 4730 MFP | 20    | 50.210.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| Digital Sender 9250c       | 20    | 48.220.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M3035 MFP         | 20    | 48.241.2                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M4345 MFP         | 20    | 48.241.2                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M4349 MFP         | 20    | 48.230.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M5035 MFP         | 20    | 48.230.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M5039 MFP         | 20    | 48.230.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M9040 MFP         | 20    | 51.180.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M9050 MFP         | 20    | 51.180.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| LaserJet M9059 MFP         | 20    | 51.180.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| Color LaserJet CM 6030 MFP | 40    | 51.180.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| Color LaserJet CM 6040 MFP | 40    | 52.191.2                |                       | 1.6.3.2      | Yes (Oz)                        |
| Color LaserJet CM 6049 MFP | 40    | 52.180.5                |                       | 1.6.3.2      | Yes (Oz)                        |
| Color LaserJet CM 3530 MFP | 50    | 53.171.4                |                       | 1.6.3.2      | Yes (Oz)                        |
| Color LaserJet CM 4540 MFP | XX    | 2131305_192065          |                       | 1.6.3.2      | Yes (FutureSmart)               |
| ScanJet Enterprise 8500n   | XX    | 20120113_2131309_192119 |                       | 1.6.3.2      | Yes (FutureSmart)               |
| LaserJet M525              | XX    | 2200643_228344          |                       | 1.6.3.2      | Yes (FutureSmart)               |

**Table 2-1: List of devices supported with AccuRoute Embedded Device Client for HP OXPd**

| Device             | Group | Supported firmware | Minimum Installed RAM | OXPd Version | Web Jetadmin (Operation System) |
|--------------------|-------|--------------------|-----------------------|--------------|---------------------------------|
| LaserJet FLOW M525 | XX    | 2200643_229650     |                       | 1.6.3.2      | Yes (FutureSmart)               |
| LaserJet M575      | XX    | 2200643_228345     |                       | 1.6.3.2      | Yes (FutureSmart)               |
| LaserJet FLOW M575 | XX    | 2200893_229649     |                       | 1.6.3.2      | Yes (FutureSmart)               |
| LaserJet M775      | XX    | 2200890_229591     |                       | 1.6.3.2      | Yes (FutureSmart)               |
| LaserJet M4555 MFP | XX    | 2131305_192067     |                       | 1.6.3.2      | Yes (FutureSmart)               |
| Scanjet 7000n      | XX    | 2131305_192072     |                       | 1.6.3.2      | Yes (FutureSmart)               |

**Note** All LaserJet models listed here are part of the *MFP series*. Other LaserJet models that are part of the *printer series* do not have the scanning capabilities required to support AccuRoute Embedded Device Client for HP OXPd.

**Note** OXPd:SolutionInstaller only supports network-enabled device models. OXPd:SolutionInstaller also requires that the device on which it is running has a writable, non-volatile mass storage partition.

**Note** Only the OXPd 1.4 for Group 10 device model is supported. Other devices will fail to install.

## Supporting large color documents

To support large color documents, an IIS setting (Request Filtering) must be set to the maximum 3000000000. Content length must be modified on the WebAPI site. To increase content length in IIS:

- 1 Open Internet Information Services (IIS 7) Manager.
- 2 Select **WebAPI** under **Sites**.
- 3 Double-click on **Request Filtering**.
- 4 Select **Edit Feature Settings** under the **Actions** menu.
- 5 Increase the value in **Maximum allowed content length**. The default is 30000000 and it must be increased to 3000000000 (adding two more zeroes).
- 6 Reset IIS.



## Updating the Deviceloader.xml to add a supported device

Verify that your device is listed in Table 2-1 to be sure it will be added by default with AccuRoute Embedded Device Client for HP OXPd. If your installation fails, your device may not have been added. In this case, you must add your device to the Deviceloader.xml manually prior to query or installation of the client application.

**Important** If you have multiple devices that are the same model (for example, you have three Aficio MP 3000 devices in your environment), you will 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 entered. In that case, you will not need to add the information.

To modify the Deviceloader.xml:

- 1 Go to the directory:

```
C:\Program Files (x86)\Omtool\RicohESA
```

- 2 Open the `Deviceloader.xml` file for editing purpose.
- 3 Under the Models node add the appropriate information for **HP model** and **Group number X** into a new Model type as follows:

```
<Model type="HPmodel"minimumFirmware="">GroupnumberX</Model>
```

For example:

```
Value for Model node specifies the configuration listed under
- <Models>
  <Model type="Aficio MP C3000" minimumFirmware="">Group2X</Model>
  <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. -->
```

See Table 2-1 for a list of supported devices.

- 4 Save your changes and close the file.

## AccuRoute server requirements

AccuRoute Embedded Device Client for HP OXPd requires:

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

---

## Device authentication requirements

AccuRoute Embedded Device Client for HP OXPd 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 HP 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 AccuRoute Embedded Device Client for HP OXPd v1.6](#) (3-1)

[Installing AccuRoute Embedded Device Client for HP OXPd v1.4](#) (3-2)

[Installing AccuRoute Embedded Device Client for HP OXPd \(v1.6 or v1.4\) on a remote system](#) (3-3)

[Uninstalling AccuRoute Embedded Device Client for HP OXPd](#) (3-4)

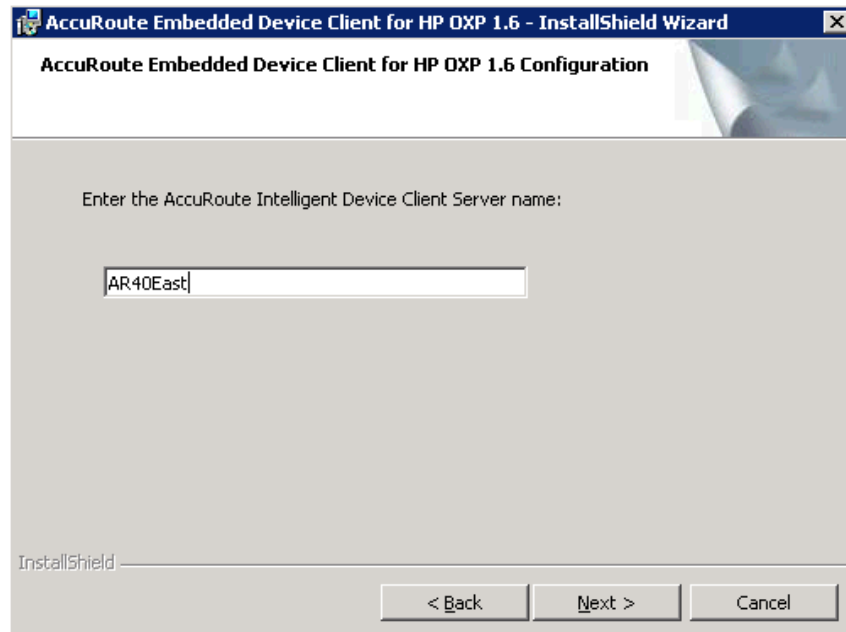
[Upgrading AccuRoute Embedded Device Clients for HP OXPd](#) (3-5)

---

### Installing AccuRoute Embedded Device Client for HP OXPd v1.6

- 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\HPOXP1.6` and run **setup.exe**. The InstallShield wizard launches with the **Welcome** message.
- 3 Click **Next**. The **Destination Folder** page opens.

- 4 Keep the default location and click **Next**. The **AccuRoute Embedded Device Client for HP OXP 1.6 Configuration** page opens.



- 5 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP Address.
- 6 Click **Next**.
- 7 Click **Install** to begin installation. The setup installs AccuRoute Embedded Device Client for HP OXPd. The InstallShield Wizard shows a message indicating when the installation is complete.
- 8 Click **Finish**.
- 9 Continue to [Section 5: Required Configuration](#).

---

## Installing AccuRoute Embedded Device Client for HP OXPd v1.4

- 1 Log on to the system running the AccuRoute server using an account that belongs to the local Administrators group.
- 2 **If you are installing on a default drive:**  
Navigate to the folder `...\Omtool\Omtool Server\Clients\HPOXP1.4` and run `setup.exe`.  
**If you are installing on a non-default drive:**
  - a Open a command prompt window (run as Administrator).
  - b Navigate to the Omtool Clients directory:

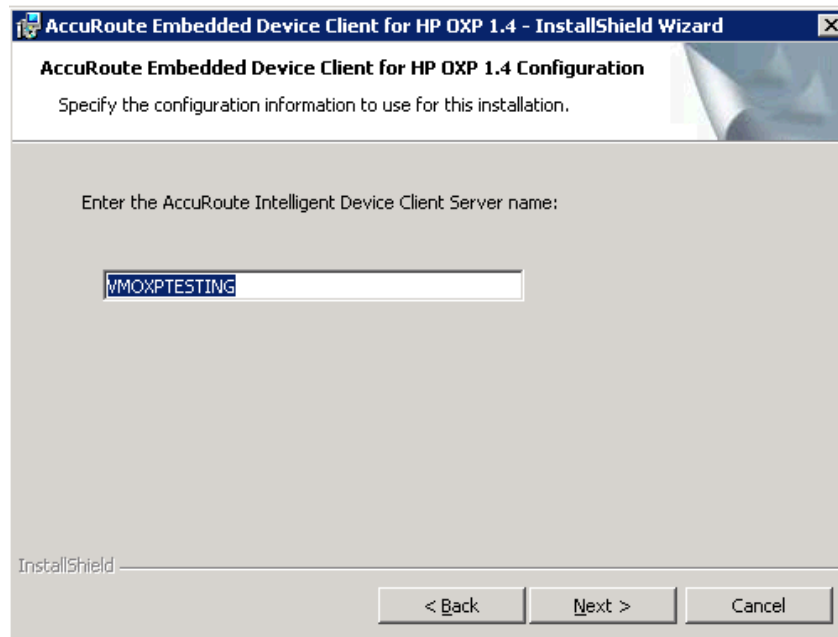
```
...\Omtool\Omtool Server\Clients
```

- c Enter the following command, where `D:\Program Files (x86)\Omtool\HPOXP1.4` is the location to which you want to install the client.

```
setup.exe /s /v"INSTALLDIR="D:\Program Files (x86)\Omtool\HPOXP1.4"
```

The Device Client will be installed on the D drive.

- 3 The InstallShield wizard launches with the **Welcome** message.
- 4 Click **Next**. The **AccuRoute Embedded Device Client for HP OXP 1.4 Configuration** page opens.



- 5 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP Address.
- 6 Click **Next** and you are ready to install the program.
- 7 Click **Install** to begin installation. The setup installs AccuRoute Embedded Device Client for HP OXPd. The InstallShield Wizard shows a message indicating when the installation is complete.
- 8 Click **Finish**.
- 9 Continue to [Section 5: Required Configuration](#).

---

## Installing AccuRoute Embedded Device Client for HP OXPd (v1.6 or v1.4) on a remote system

- I Log on to the system where you want to install AccuRoute Embedded Device Client for HP OXPd using an account that belongs to the local Administrators group.

---

**Note** The system must be running Windows 2008 or 2003 64-bit and must have Embedded AccuRoute for Intelligent Devices (Omttool ISAPI Web Server Extension) and AccuRoute v4.0 installed.

---

- 2 For HP OXPd v1.6:  
Navigate to the `\\Omttool\Omttool Server\Clients\HPOXP1.6` directory and run **setup.exe**.  
For HP OXPd v1.4:  
Navigate to the `\\Omttool\Omttool Server\Clients\HPOXP1.4` directory and run **setup.exe**.  
The InstallShield wizard configures your system for installation and shows the **Welcome** message.
- 3 Click **Next**. The **AccuRoute Embedded Device Client for HP OXP Configuration** page opens.
- 4 In the **AccuRoute Intelligent Device Client Server name** text box, enter the AccuRoute server name or the IP Address.
- 5 Click **Next**.
- 6 Click **Install** to begin installation. The setup installs AccuRoute Embedded Device Client for HP OXPd. The InstallShield Wizard shows a message indicating when the installation is complete.
- 7 Click **Finish**.
- 8 Continue to [Section 5: Required Configuration](#).

---

## Uninstalling AccuRoute Embedded Device Client for HP OXPd

To uninstall AccuRoute Embedded Device Client for HP OXPd:

- 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 HP OXP**. Right-click and select **Uninstall**. You are prompted to confirm that you want to uninstall the software.
- 3 Click **Yes** to uninstall AccuRoute Embedded Device Client for HP OXPd.

---

# Upgrading AccuRoute Embedded Device Clients for HP OXPd

---

**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 AccuRoute Embedded Device Client for HP OXPd](#) (3-4).

## Installing AccuRoute Embedded Device Clients

- To install a Device Client for HP OXPd v1.6, see [Installing AccuRoute Embedded Device Client for HP OXPd v1.6](#) (3-1).
- To install a Device Client for HP OXPd v1.4, see [Installing AccuRoute Embedded Device Client for HP OXPd v1.4](#) (3-2).
- To install Device Clients for either version (1.6 or 1.4) on a remote system, see [Installing AccuRoute Embedded Device Client for HP OXPd \(v1.6 or v1.4\) on a remote system](#) (3-3).





# 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.

---

- The administrator will need to create and export the certificate for the Web server as a file named “WebServer.cer” and copy it to the Certificate folder created during the HP OXPd Device Client install.
- During the registration process for the OXPd application onto the device, WebServer.cer will be installed into the device.

---

**Note** No error will be generated if the file does not exist. It will not be possible to configure the device for HTTPS until that file has been installed onto the device.

---

If you require HTTPS support, follow the instructions in this section to set up a CA certificate with the Microsoft Certificate Services and enable SSL.

[Setting up a CA certificate and enabling SSL with Windows 2008 R2](#) (4-2)

[Setting up a CA certificate and enabling SSL with Windows 2003 64-bit](#) (4-7)

Otherwise, use a certificate from a trusted certificate authority. The certificate must be installed on the IIS system.

---

## Setting up a CA certificate and enabling SSL with Windows 2008 R2

The instructions in this section detail how to set up a CA certificate and enable Secure Socket Layer (SSL). The certificate must be created and installed in the IIS.

---

**Note** If you are setting up a CA certificate with Windows 2003 64-bit, refer to [Setting up a CA certificate and enabling SSL with Windows 2003 64-bit \(4-7\)](#).

---

### 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:

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

[Creating the certificate \(4-3\)](#)

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

[Exporting the certificate to the OXPd v1.6 Device Client directory \(4-3\)](#)

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

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

[Enabling directory browsing in IIS \(4-5\)](#)

[Verifying the SSL binding \(4-5\)](#)

[Verifying HTTPS browsing \(4-5\)](#)

[Editing the OmlSAPIU.xml file \(4-6\)](#)

[Editing the Bootstrap.xml file \(4-6\)](#)

You should complete each procedure in the order in which they are presented.

### 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.

## Exporting the certificate to the OXPd v1.6 Device Client directory

---

**Note** Skip this procedure if you are using only the HP OXPd v1.4 Device Client.

---

- 1 Navigate to the **IIS\Local machine** directory and locate **Server Certificates**.
- 2 Find the newly created certificate. Double-click and open the certificate **Properties** page.
- 3 Click on the **Details** tab.
- 4 Choose the **Copy to File** option. The **Certificate Export Wizard** opens.
- 5 Click **Next**.
- 6 On the **Export Private Key** dialog, select **No, do not export the private key**.

- 7 Click **Next**.
- 8 On the **Export File Format** dialog, select **DER encoded X.509 (.CER)**.
- 9 Click **Next**.
- 10 On the **File to Export** dialog, select **Browse**. The **Save As** dialog opens.
- 11 Browse to the directory:  
`C:\Program Files (x86)\Omtool\OXPl.6\Certificate`
- 12 In the **File Name** text box, enter **WebServer.cer with DER Encoded Bindary X.509 (\*.cer)** as the **Save type**.
- 13 Click **Save** and then **Next**. The **Completing the Certificate Export Wizard** opens.
- 14 Click **Finish**.
- 15 When a message appears stating that the export was successful, click **OK**.

## 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 **OXPI.6** (or **OXPI.4**).
- 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 **OXPI.6** (or **OXPI.4**).
- 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 hand corner of the IIS dialog).

You will see the 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 **IIS 7** dialog opens.

## Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OXP v1.6** (or **OXP v1.4**).
- 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:  
For HP OXPd v1.6:  
`...\OXPI.6\Configuration\`  
For HP OXPd v1.4:  
`...\OXPI.4\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)\Omttool\Omttool 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.

For HP OXPd v1.6:

```
C:\Program Files (x86)\Omttool\OXP1.6\Configuration\
```

For HP OXPd v1.4:

```
C:\Program Files (x86)\Omttool\OXP1.4\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.

---

## Setting up a CA certificate and enabling SSL with Windows 2003 64-bit

The instructions in this section detail how to set up a CA certificate and enable SSL. The certificate must be created and installed in the IIS.

---

**Note** If you are setting up a CA certificate with Windows 2008, refer to [Setting up a CA certificate and enabling SSL with Windows 2008 R2 \(4-2\)](#).

---

### 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:

[Downloading the MakeCert executable \(4-7\)](#)

[Creating the certificate \(4-3\)](#)

[Exporting the certificate to the OXPd v1.6 Device Client directory \(4-3\)](#)

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

[Editing the OmlSAPIU.xml file \(4-15\)](#)

[Editing the Bootstrap.xml file \(4-16\)](#)

### 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.

### Running the MakeCert executable and 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:

```
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.

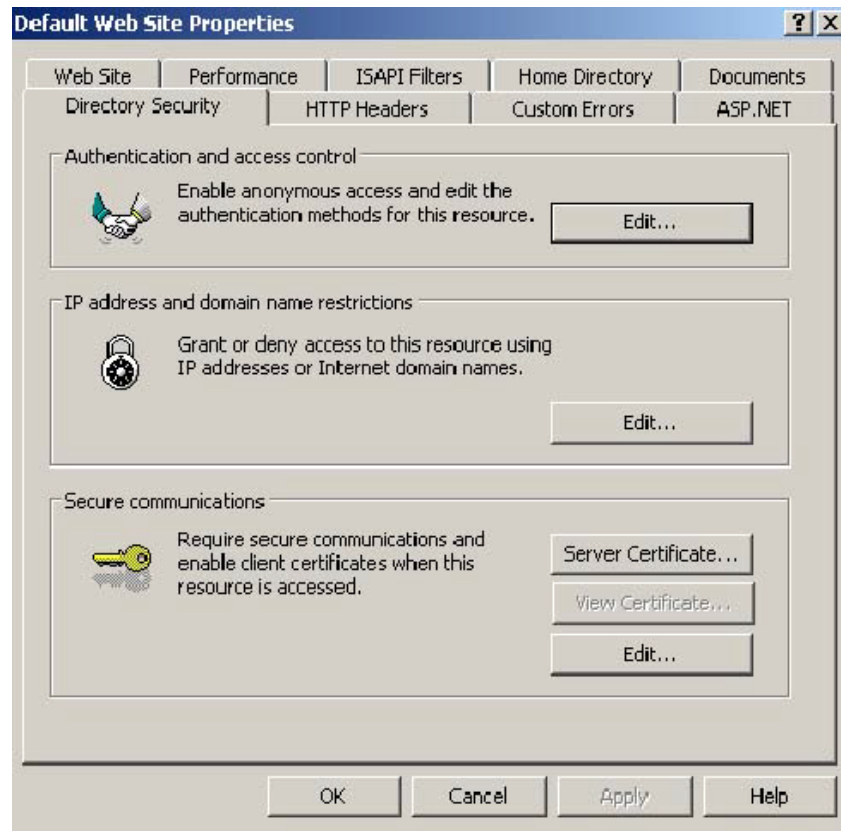
When the command is run properly, the system will display a message indicating that it succeeded.

## Exporting the certificate to the OXPd v1.6 Device Client directory

**Note** Skip this procedure if you are using only the HP OXPd v1.4 Device Client.

Using the Web Server Certification wizard:

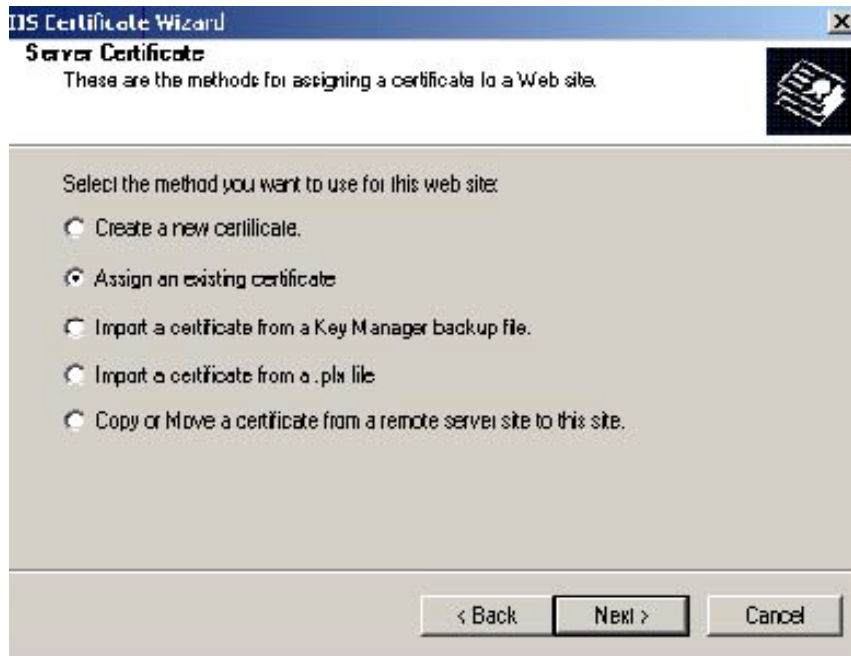
- 1 Open IIS and select **Default Website properties**. The **Directory Security** page is displayed.



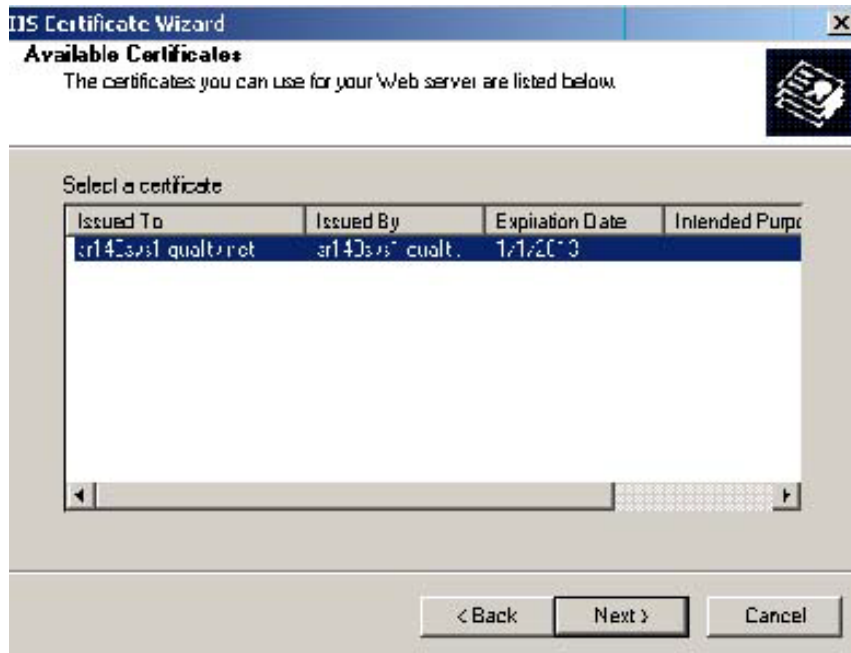
- 2 Click the **Server Certificate** button. The **Welcome to the Web Server Certification Wizard** page is displayed.



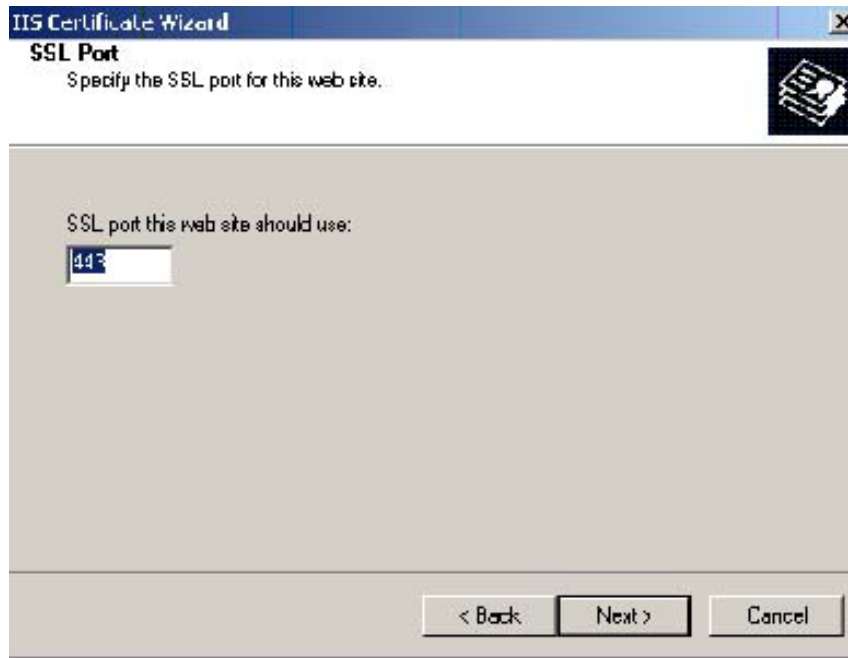
- 3 Click **Next**. The **IIS Certification Wizard** is displayed.



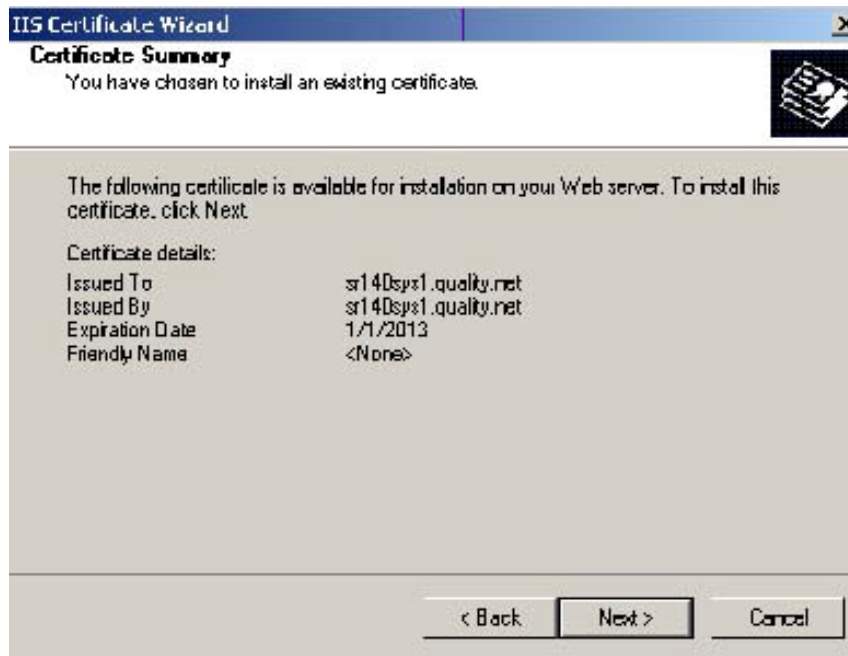
- 4 Select **Assign an existing certificate**. Click **Next**. The certificate created using MakeCert.exe is displayed.



- 5 Click **Next**. A window is displayed prompting for the SSL port.

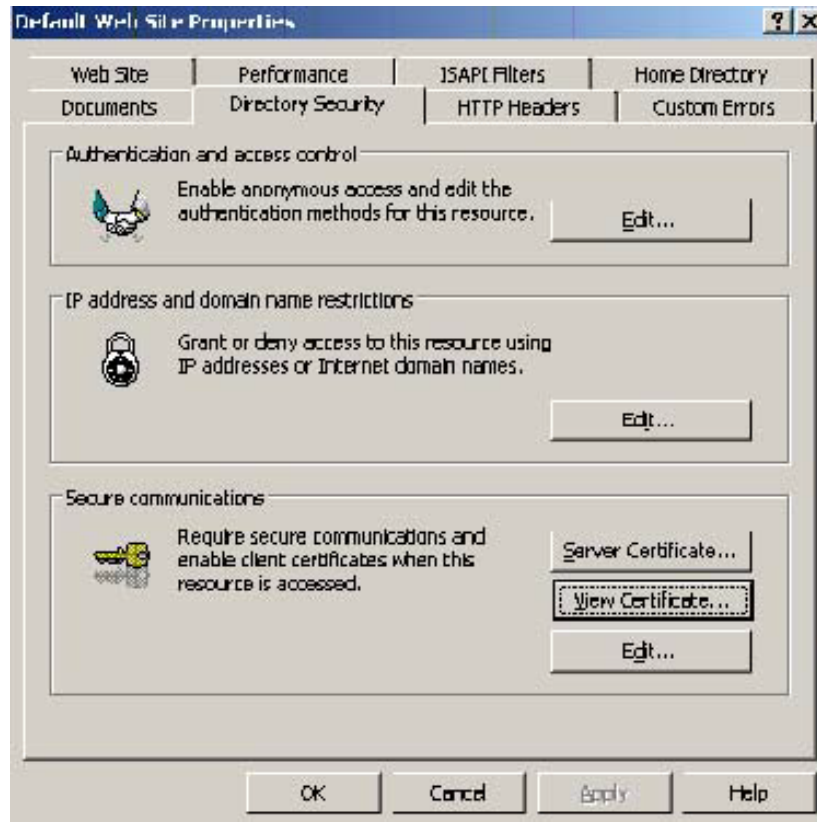


- 6 The port selected should be **443**. Click **Next**. The **Certificate Summary** is displayed.



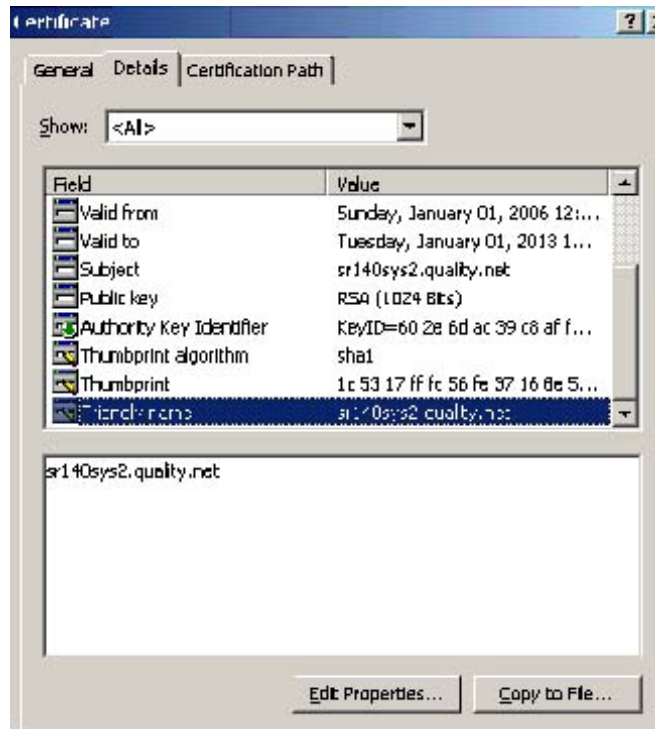
- 7 Click **Next**. A message indicates that the Web Server Certificate wizard is completed.
- 8 Click **Finish**. You are returned to the **Directory Security** page.
- 9 Export the certificate:
  - a Open IIS\local machine and navigate to the **Default Web Site** node.

- b Select website **OXPI.6**.
- c Right-click and select **Properties**.
- d Click the **Directory Security** tab.

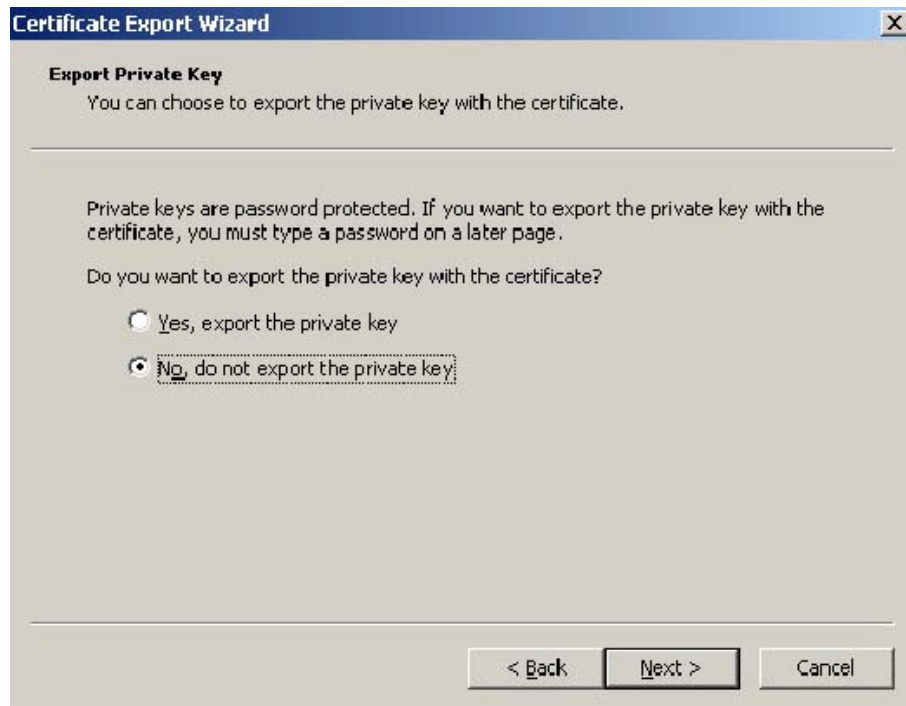


- e In the **Secure communications** section, click the **View Certificate** button.

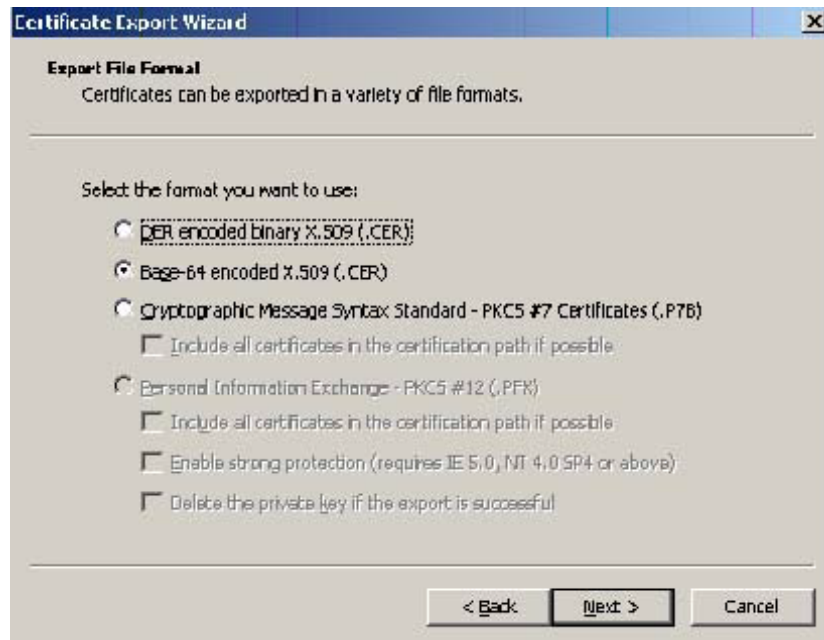
- f Click the **Details** tab. Select the newly created certificate name.



- g Click the **Copy to File** button. The **Welcome to the Certificate Export Wizard** page is displayed.
- h Click **Next**. The **Export Private Key** page is displayed.



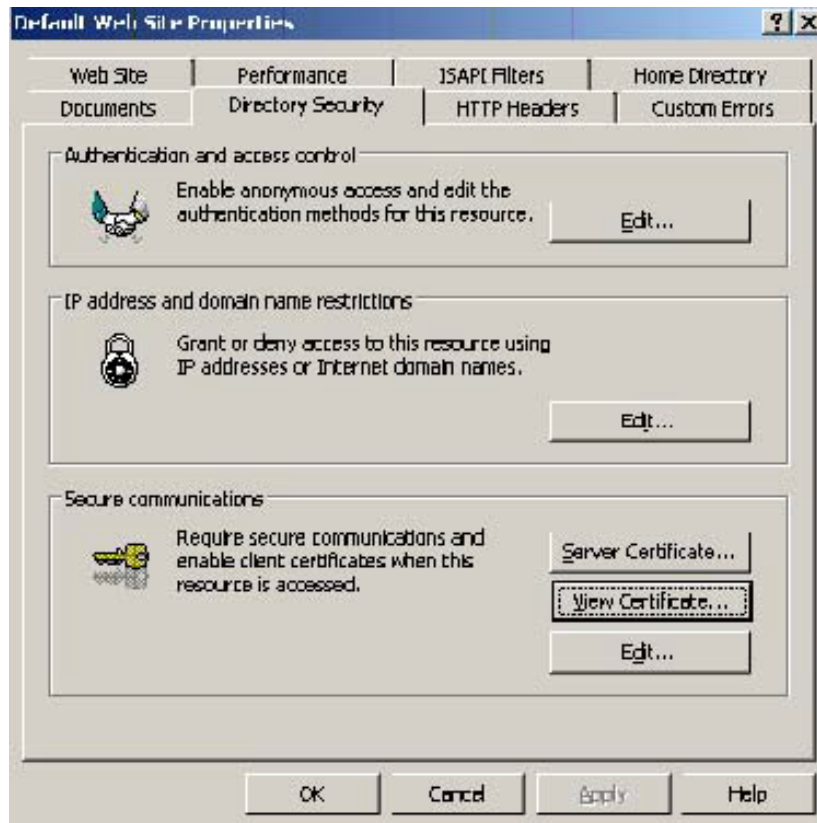
- i Select **No, do not export the private key** and click **Next**. The **Export File Format** page is displayed.



- j Select **Base-64 encoded x.509 (CER)**. Click **Next**.
- k Browse to this location:  
`C:\Program Files (x86)\Omtool\OXP1.6\Certificate`  
Enter the file name as:  
`Webserver.cer`
- l Click **Save**. A message indicates the export was successful. Click **OK**.
- m Click **Finish** to exit the Certificate Export wizard.

## Requiring SSL for web sites

- 1 Open IIS\local machine and navigate to the **Default Web Site** node.
- 2 Select web site **OXPI.6** (or **OXPI.4**).
- 3 Right-click and select **Properties**.
- 4 Click the **Directory Security** tab.



- 5 In the **Secure communications** section, click the **Edit** button. The **Secure Communications** page is displayed.



- 6 Select **Require secure channel (SSL)** and **Require 128-bit encryption**.
- 7 Click **OK** twice.

## Editing the OmISAPIU.xml file

- 1 Navigate to the following path.  
`C:\Program Files (x86)\Omttool\Omttool 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.

For HP OXPd v1.6:

`C:\Program Files (x86)\Omtool\OXP1.6\Configuration`

For HP OXPd v1.4:

`C:\Program Files (x86)\Omtool\OXP1.4\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 5: Required Configuration

This section includes:

[Entering a license for AccuRoute Embedded Device Client for HP OXPd](#) (5-1)

[Adding devices using AccuRoute Server Administrator](#) (5-4)

[Choosing an authentication method](#) (5-30)

[Configuring the server](#) (5-31)

---

## Entering a license for AccuRoute Embedded Device Client for HP OXPd

---

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

---

You can activate the AccuRoute Embedded Device Client for HP OXPd 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 > Omttool > 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.omttool.com/accuroute>  
 The **Manual Licensing Portal** page opens.

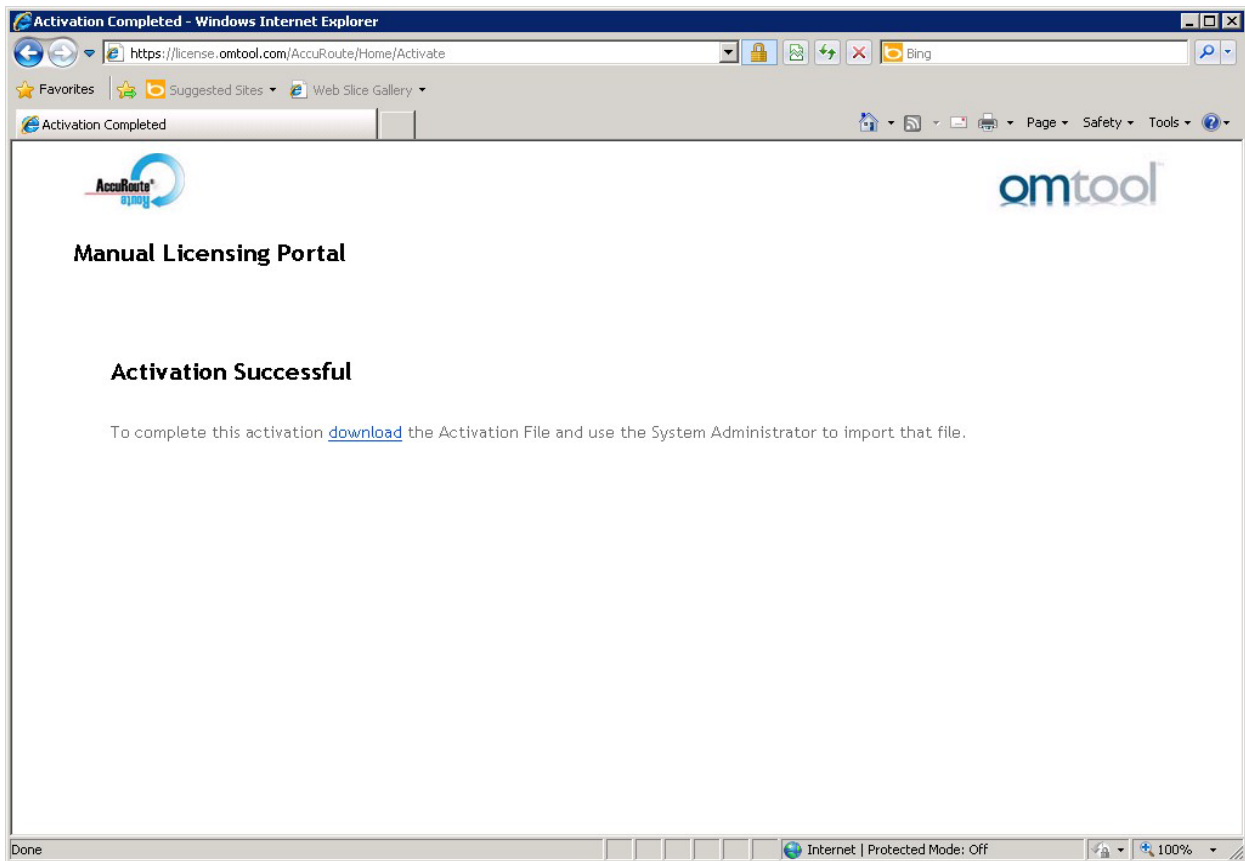


### Manual Licensing Portal

|   |  |
|---|--|
| 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 &gt;"/>  |  |

- 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.

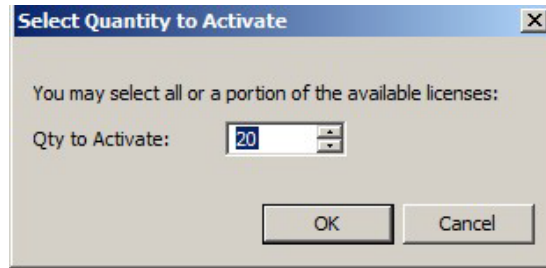
---

- 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](#) (5-27)

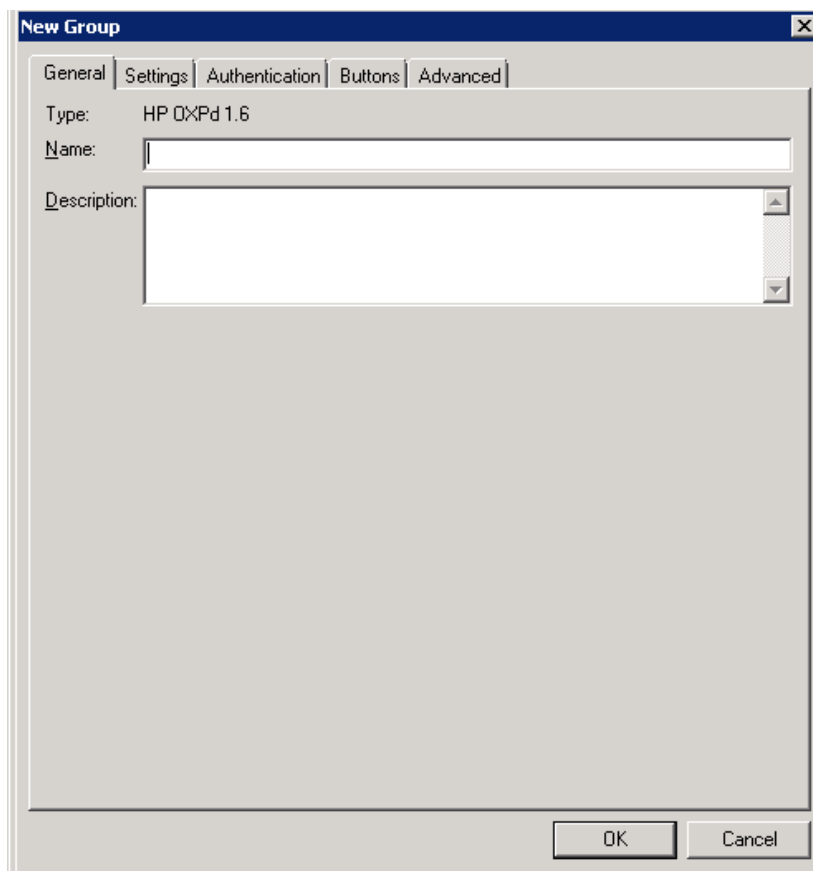
### Creating a group of devices

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 > Omttool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **Devices**.
- 3 Select **New > HP OXPd 1.6 group** (or **HP OXPd 1.4 group**).

The **New Group** page opens.

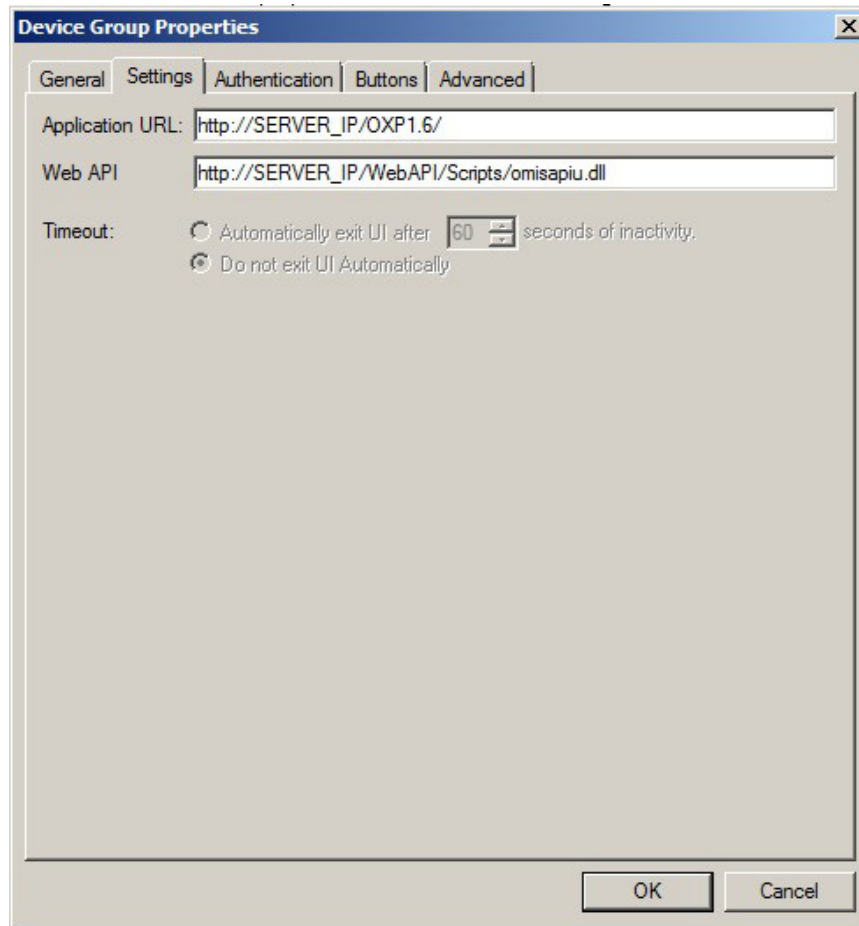


The screenshot shows a 'New Group' dialog box with the following elements:

- Title bar: New Group (with a close button)
- Tabbed interface: General (selected), Settings, Authentication, Buttons, Advanced
- Type: HP OXPd 1.6
- Name: [Empty text box]
- Description: [Empty text area]
- 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/OXP1.6/`
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 AccuRoute Embedded Device Client for HP OXPd 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 contains a table with three rows: 'Domain', 'User', and 'Password', each with a 'User Entered' value and a 'Properties' button. The 'LDAP Lookup Settings' section includes a 'Server' field with 'vmad70.vmad700.com', a 'Port' dropdown set to '389', a 'Search Base' field with 'DC=vmad700.DC=com', a 'Filter' field with '(&{(objectClass=user)[sAMAccountName=[USER\_NAME]])', 'Username' and 'Password' fields, and an 'Attribute Map' dropdown set to 'Exchange.default.xml'. There are 'Attribute Aliases...' and 'Test LDAP Lookup' buttons. The 'Bind using Windows Generic Security Services' checkbox is unchecked. The 'Confirm authentication' checkbox is also unchecked, and the 'Message' field contains '@msgConfirmation'. 'OK' and 'Cancel' buttons are at the bottom.

- 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 HP device authentication on the device](#) (5-8).

If you select **Email**, **Login**, or **PIN** as the authentication type, continue with [Defining Domain Properties](#) (5-9).

## Configuring HP device authentication on the device

- a Open a Web browser and enter the device IP address.
- b Log in to the Embedded Web Server. All options become available.
- c Go the **Settings** tab and click **Authentication Manager**.
- d Locate the following AccuRoute functions:
  - ▲ Scan to My Files
  - ▲ Personal Distributions
  - ▲ Scan to Me

The list shows the options that are installed with AccuRoute Embedded Device Client for HP OXPd, so it can contain all, some, or none of these functions.

- e For each of the features listed above, click on the drop-down menu.
- f Select **LDAP** as the authentication method for each scanning feature that requires user login.

**Authentication Manager**

Set the Device Functions that require users to successfully sign in before use. Each function can require a different Sign In Method.

| Home Screen Access                             | Sign In Method    |
|--|-------------------|
| Sign In At Walk Up                             | None              |
| Device Functions                               | Sign In Method    |
| Copy   | None              |
| Color Copy                                     | None              |
| Send to E-mail                                 | None              |
| Send Fax                                       | None              |
| Send to Folder                                 | None              |
| Job Storage                                    | None              |
| Create Stored Job                              | None              |
| Digital Sending Service (DSS) Secondary E-mail | None              |
| Digital Sending Service (DSS) Workflow         | None              |
| Simplex Copy                                   | None              |
| Public Distributions                           | None              |
| Personal Distributions                         | None              |
| Fax  | None              |
| Routing Sheet                                  | None              |
| Scan To Me                                     | LDAP              |
| Scan To Folder                                 | None              |
| HP AC Express                                  | HPAC - PIC Server |
| Scan To My Files                               | LDAP              |
| Future Installations                           | Sign In Method    |

- g Click **Apply**.
- h Continue with Step 16 on page 5-13.



## 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:

The screenshot shows the "Domain Field Properties" dialog box. It has a title bar with a close button. The "Label:" field contains "@authDomainLabel". The "Default value:" field is empty. The "User must enter a value for Domain" radio button is selected. Under this option, "Enable input validation" is unchecked, "Regular Expression:" is empty, and "Error message:" contains "@authDomainErrorText". The "User must select a value for Domain from one of the following:" radio button is unselected, and its list box is empty. To the right of the list box are buttons for "Add...", "Remove", "Set Default", and up/down arrows. The "User may not enter a value for Domain" radio button is unselected, and "Display the default value to the user (read-only)" is unchecked. "OK" and "Cancel" buttons are at the bottom right.

---

**Note** Domain definition is optional for all authentication types.

---

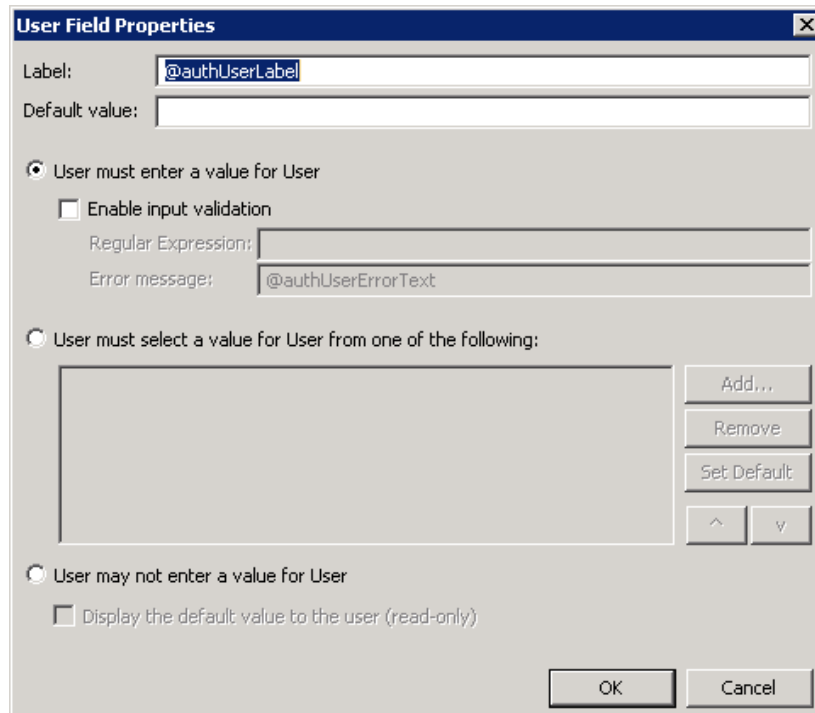
When you define a domain, you can specify a **Default value** (domain) that will be displayed at the device. In addition, you can specify one of the following:

- **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](#) (5-10).

## 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 located 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](#) (5-11).

## 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:

The screenshot shows the "Password Field Properties" dialog box. It has a title bar with a close button. The "Label:" field contains "@authPasswordLabel". The "Default value:" field is empty. The "User must enter a value for Password" radio button is selected. Below it, the "Enable input validation" checkbox is unchecked. The "Regular Expression:" field is empty, and the "Error message:" field contains "@authPasswordErrorText". The "User must select a value for Password from one of the following:" radio button is unselected. Below it is an empty list box with buttons "Add...", "Remove", "Set Default", "^", and "v". The "User may not enter a value for Password" radio button is unselected. Below it, the "Display the default value to the user (read-only)" checkbox is unchecked. At the bottom are "OK" and "Cancel" buttons.

**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 5-12.

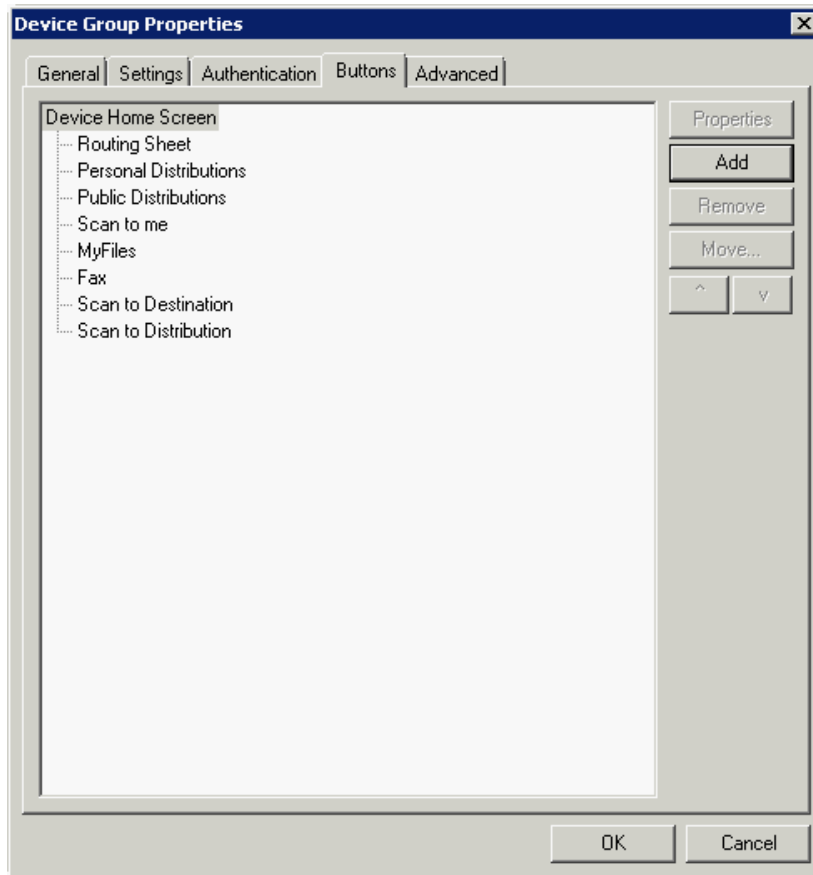
- 10** On the **Device Group Properties** page, keep the defaults for **Server**, **Port**, **Search Base**, and **Filter** (under the **LDAP LookUp Settings** heading).

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

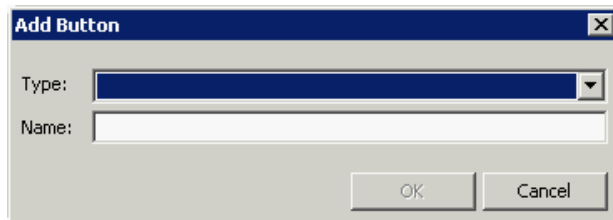
- 11** In the **Username** text box, enter the name of a Windows user who has permissions to query the active directory.
- 12** In the **Password** text box, enter the Administrator password.
- 13** If you are working in an Exchange environment, select Exchange.default.xml (Exchange Attributes) from 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.



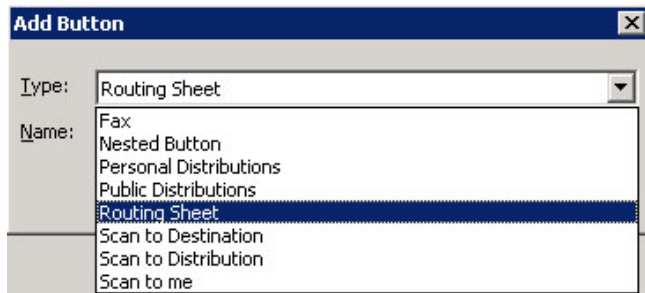
**Note** It is best to add or remove all previously set buttons before installing to the device. All features/settings within each button can be configured after the button has been installed to a device and are updated instantaneously after selecting **OK**. Reinstallation is required only if a new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



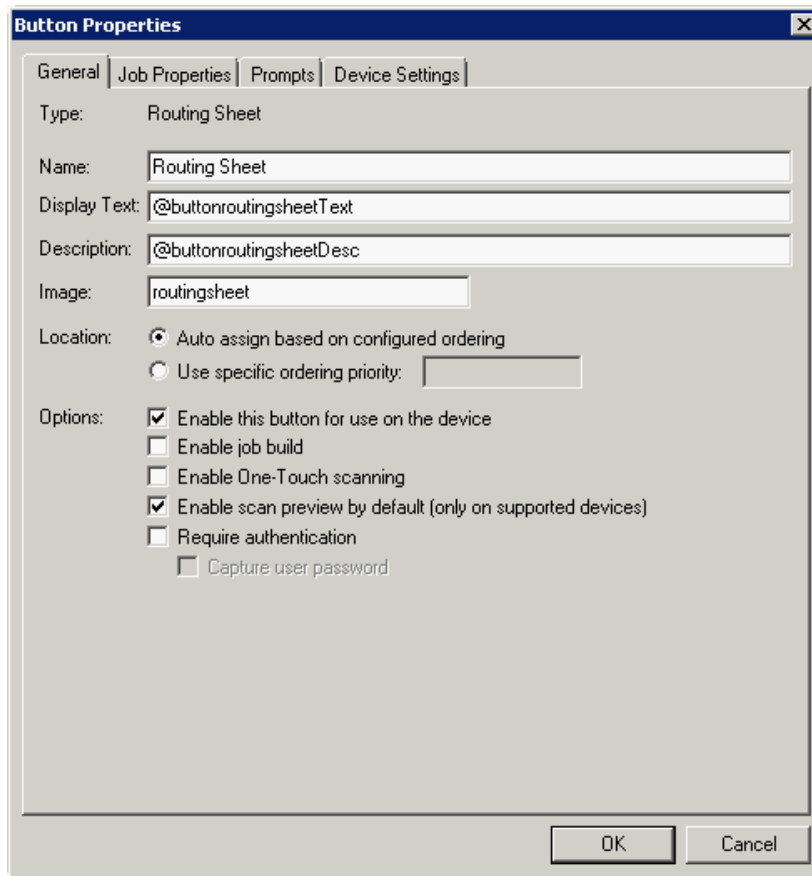
**Note** If the **Add** button is not active, click on **Device Home Screen**.

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**, **Display Text**, and **Description** 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:

- ▶ **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.

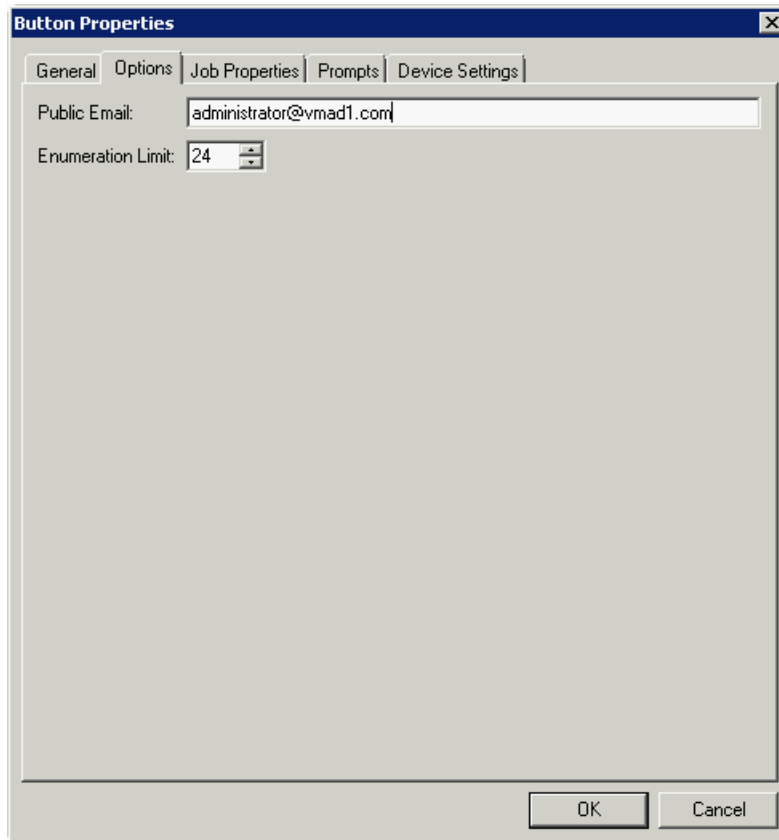
```

**22** Select additional options for the button:

- ▶ **Enable this button for use on the device** - Self-explanatory.
- ▶ **Enable job build** - 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** - Allows the user to select a button with the documents already loaded in the Automatic Document Feeder for one-touch scanning. Typically, this is used with a Distribution that has all scan settings saved.
- ▶ **Enable scan preview by default (only on supported devices)** - Applies to **Futuresmart** devices only.
- ▶ **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.

**23** 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).



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

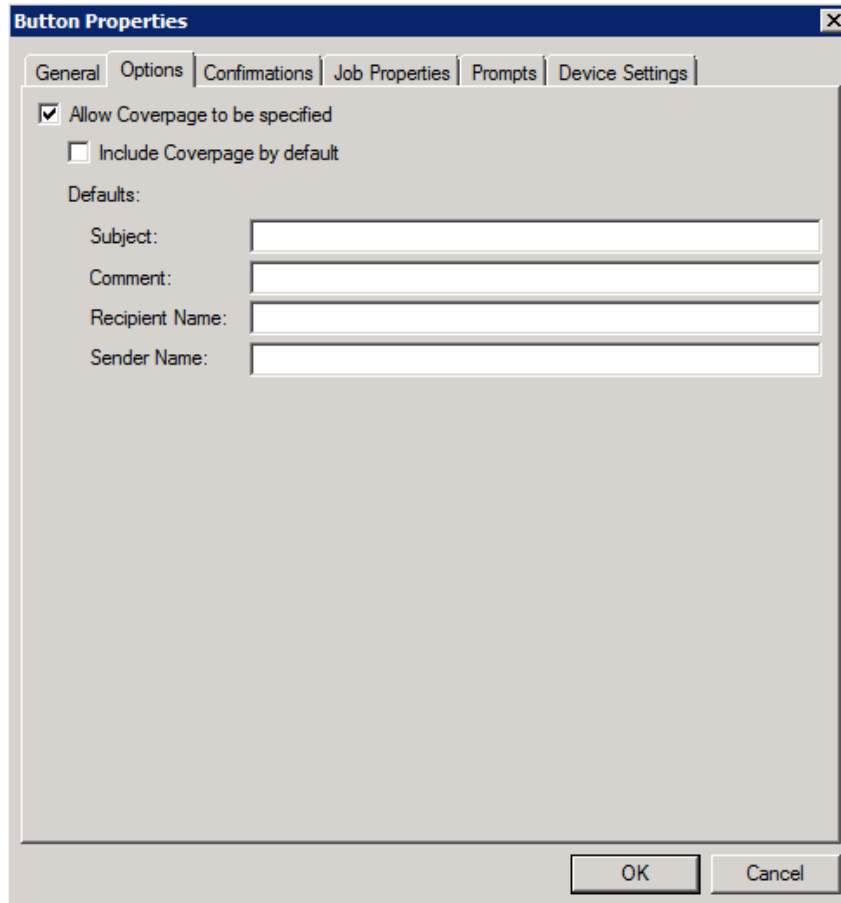


- a Click **Select** and the **Select Embedded Directive** dialog is displayed enabling you to select a Distribution Rule.

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

- 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.

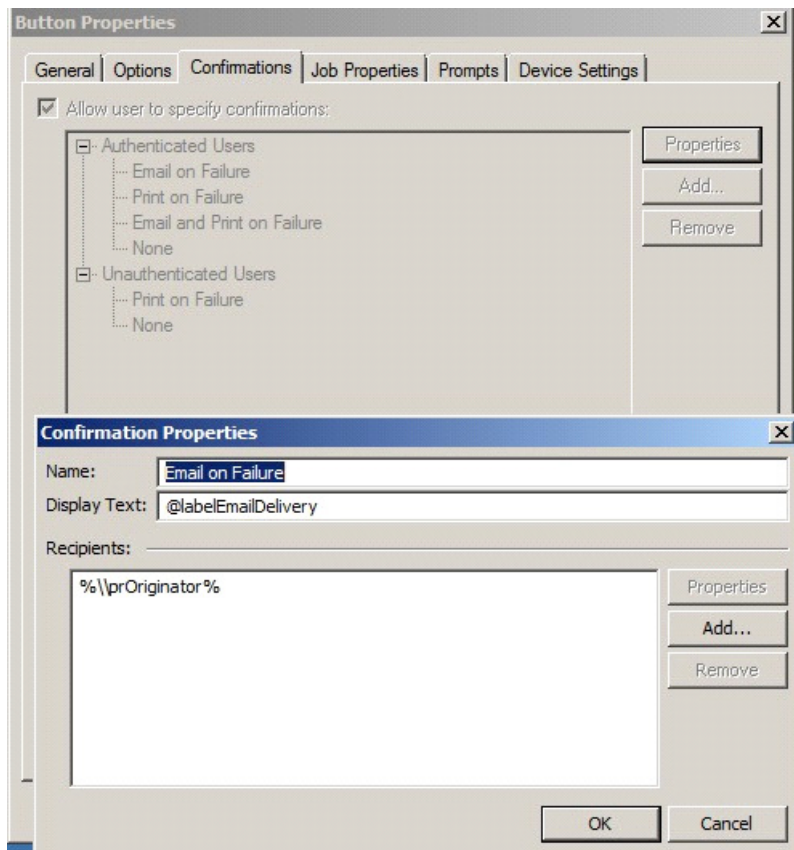
- 25** If you are adding a **Fax** button, click the **Options** tab to configure fax cover pages. Select options to allow a cover page to be specified and include the cover page by default. In addition, you can indicate the information (subject, etc.) that will appear on the cover page.



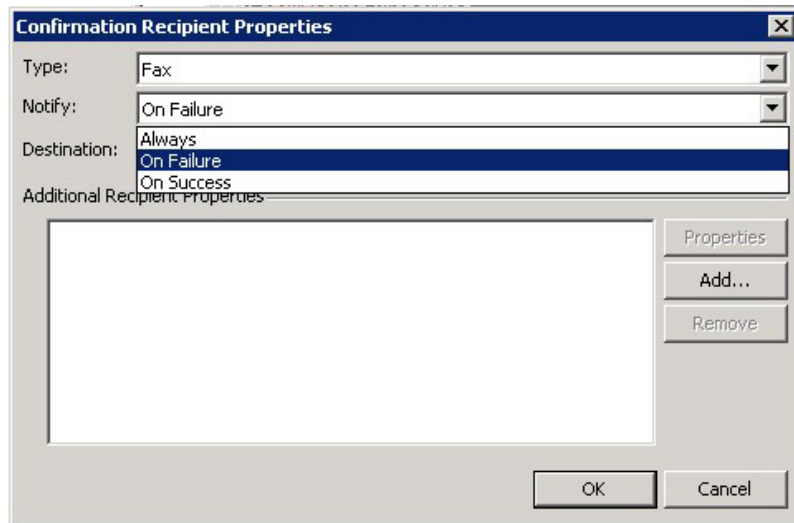
The image shows a screenshot of the "Button Properties" dialog box, specifically the "Options" tab. The dialog box has a title bar with a close button (X) and a tabbed interface with the following tabs: "General", "Options", "Confirmations", "Job Properties", "Prompts", and "Device Settings". The "Options" 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.

- 26** 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 faxed faxes:



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



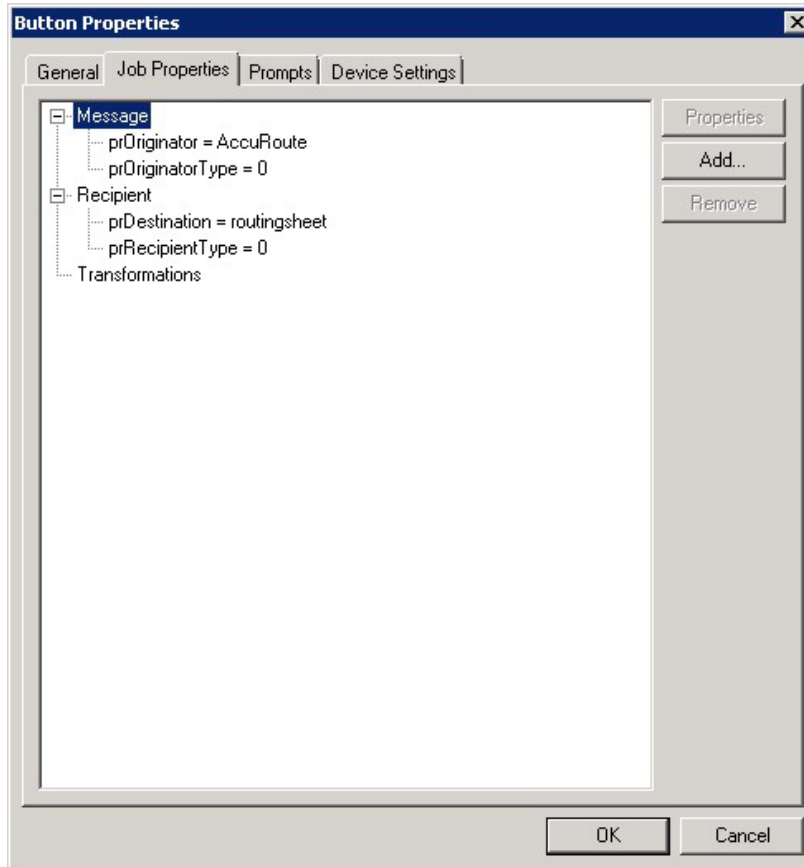
**Type.** - Leave this as the default.

**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.

- 27 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.



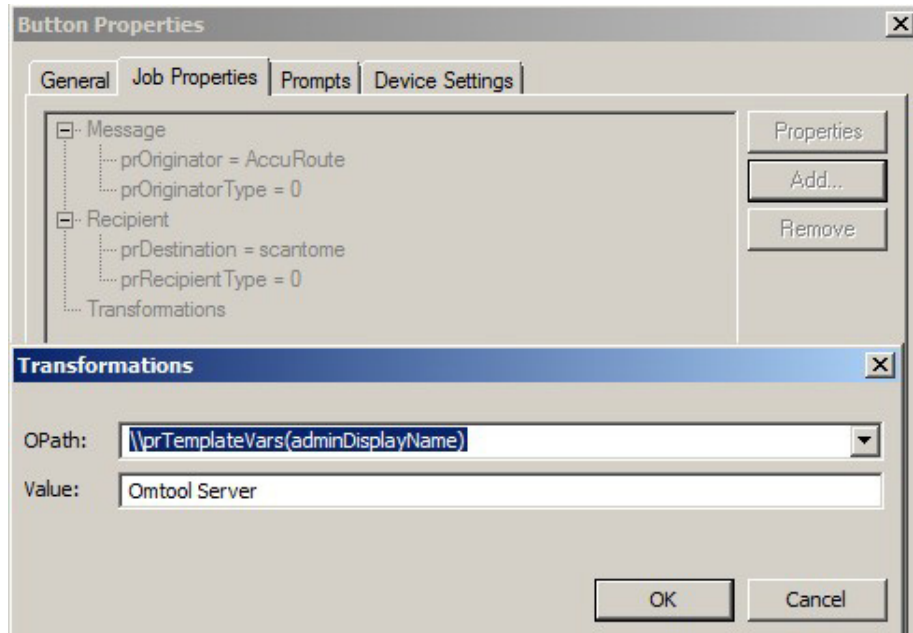
You can add, remove, or change a property. This example shows the property of a **Destination**.



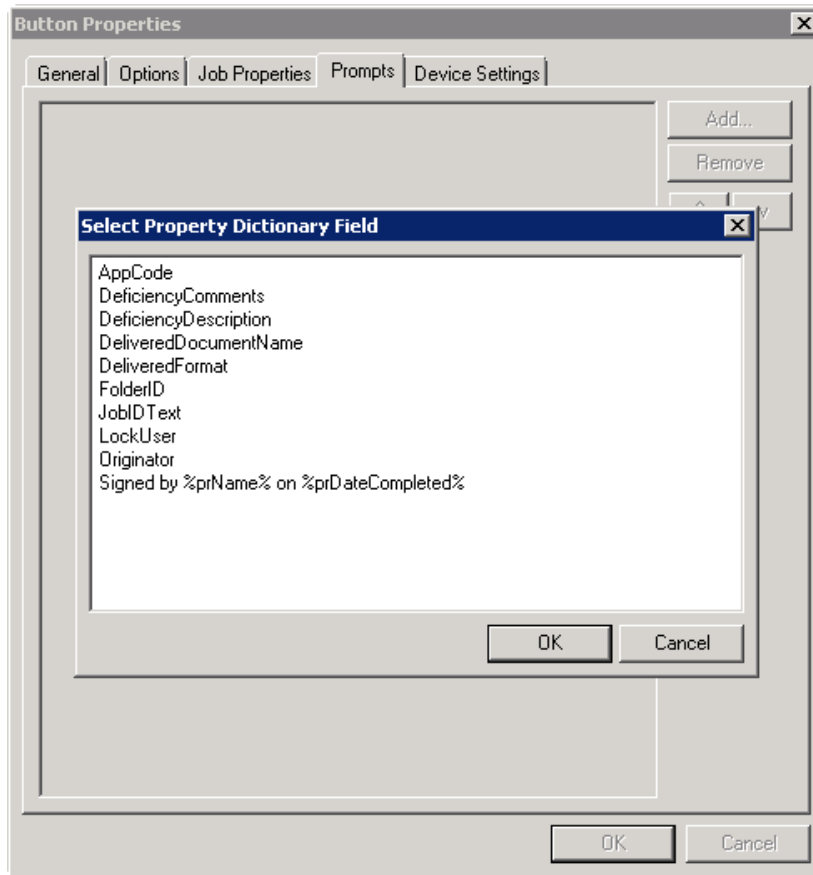
You can change an **Originator, Destination, or Recipient**. You also can add a **Transformation**, replacing a data value (a message property, recipient property, Embedded Directive (Distribution Rule) property, or template variable) with another value.

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 Omttool properties (including attributes from Active Directory) to any other Omttool property value.

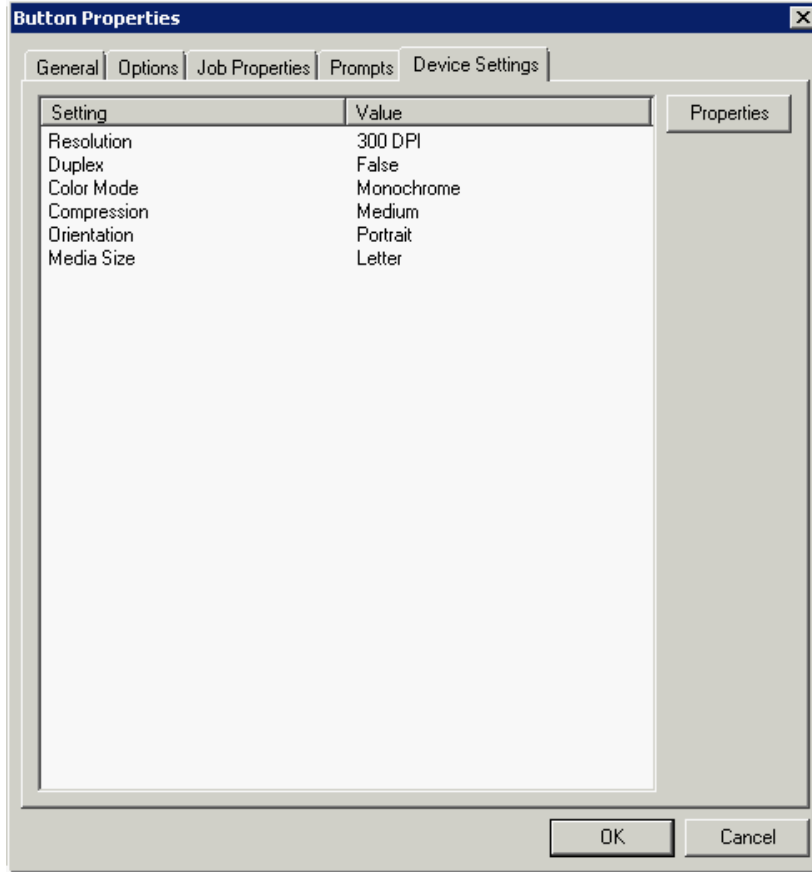


- 28 Click the **Prompts** tab. Click **Add** to select a prompt configured on the AccuRoute server. The **Select Property Dictionary Field** is displayed.



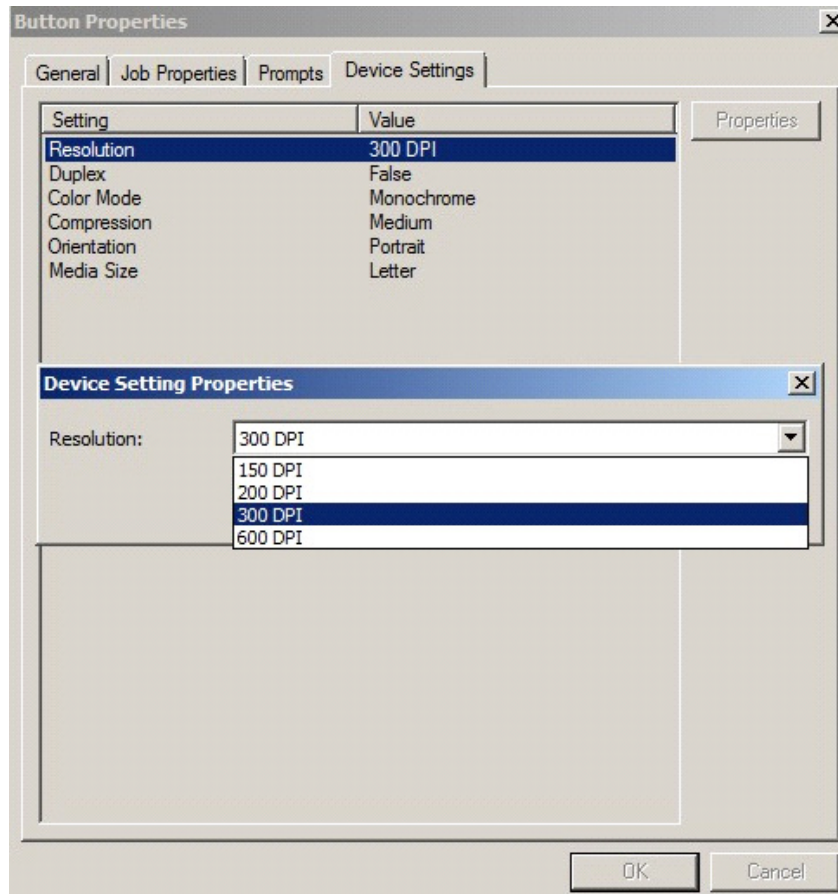
Select a prompt and click **OK**.

- 29 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.





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

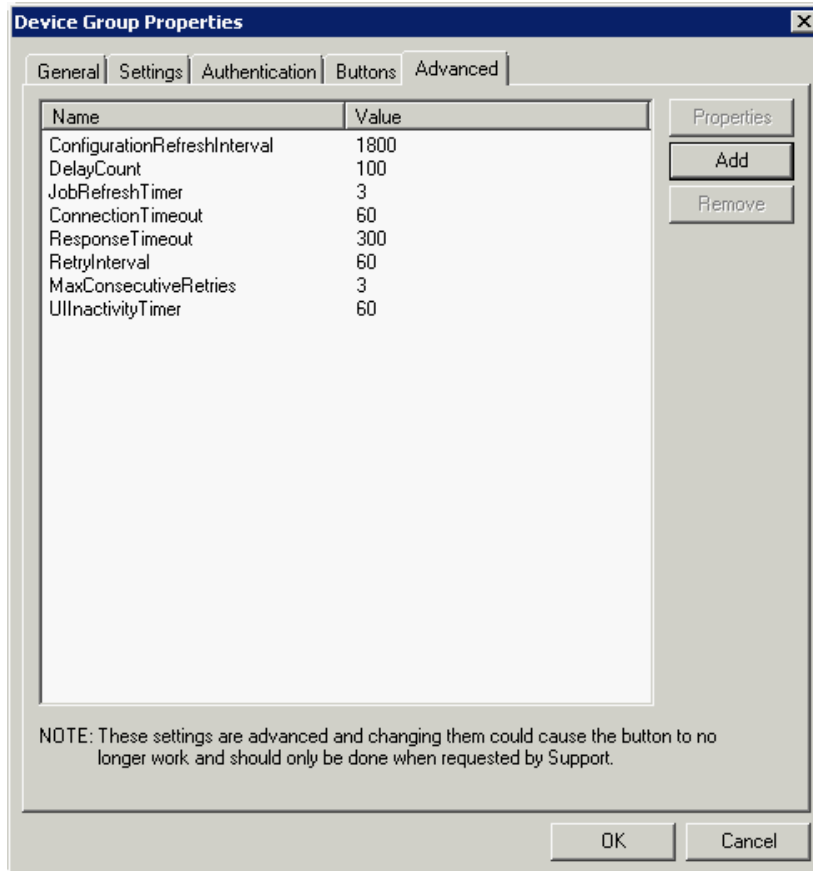


**31** Click **OK** to return to the **Device Group Properties**.

**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.

- 32 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.



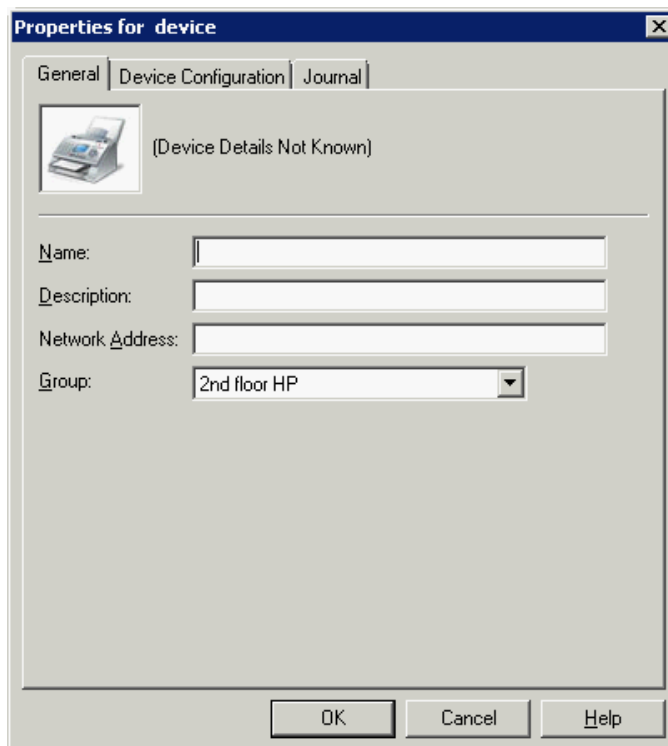
- 33 Click **OK** to end your work with the **Device Group Properties**.
- 34 Once a button configuration is complete, the XML files can be exported for importing into HP's Web Jetadmin server for button deployment.

Go to the **Devices** node and right-click on the group name. Then, select the **Export to Web Jetadmin** option. See [Installing OXPd v1.6 buttons](#) (6-4).

## Adding a new device

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

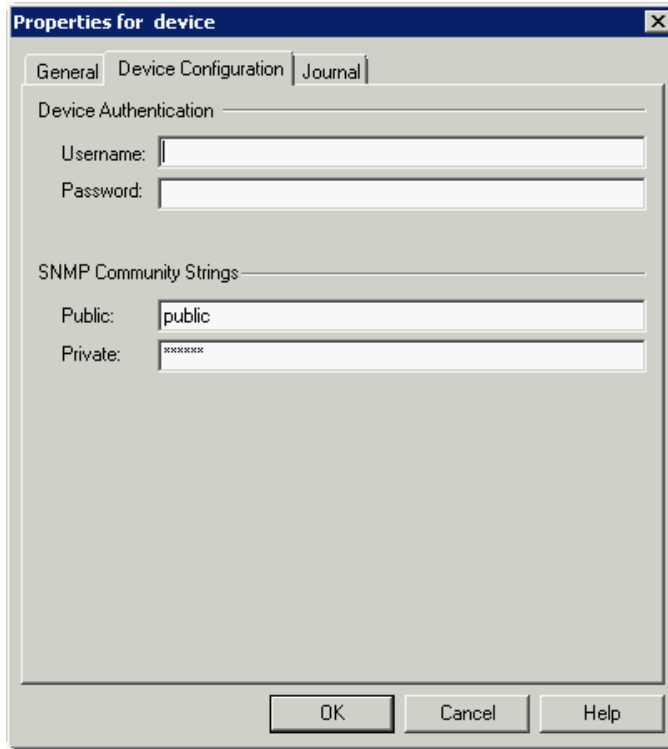
The **Properties for device** page opens.



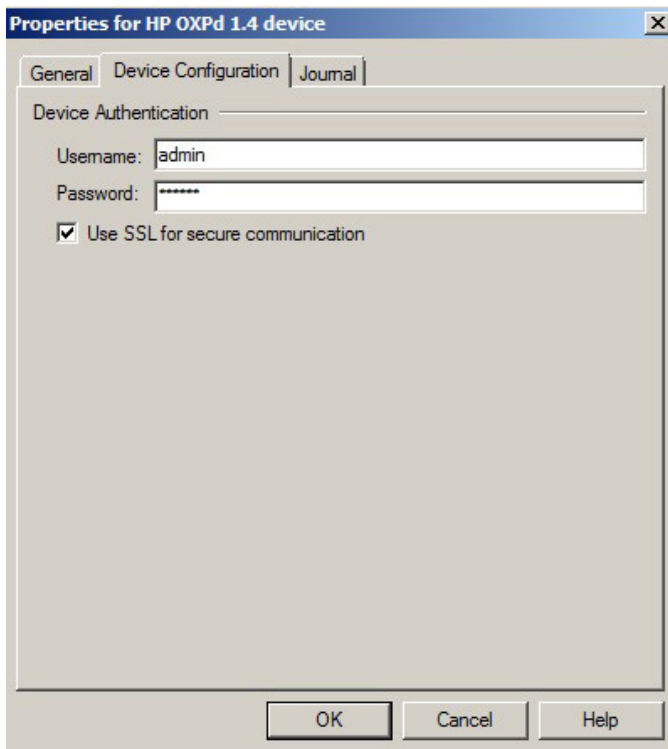
The screenshot shows a dialog box titled "Properties for device" with a close button (X) in the top right corner. It has three tabs: "General", "Device Configuration", and "Journal". The "General" tab is selected. Inside the dialog, there is a printer icon on the left and the text "(Device Details Not Known)" on the right. Below this, there are four input fields: "Name:" (text box), "Description:" (text box), "Network Address:" (text box), and "Group:" (dropdown menu with "2nd floor HP" selected). At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 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 HP device IP address.

- 6 Click the **Device Configuration** tab. The following example is for HP OXPd v1.6 devices:



This example is for HP OXPd v1.4 devices:



- 7 In the **Username** text box, enter the device Administrator name.
- 8 In the **Password** text box, enter the Administrator password.
- 9 If you are using HP OXPd v1.6, configure the **SNMP Community Strings** section (this section will not appear for HP OXPd v1.4).
  - ▶ In the **Public** text box, enter the v1.6 device public community string.
  - ▶ In the **Private** text box, enter the v1.6 device private community string.

The default value is `public` in both the **Public** and **Private** fields.

- 10 If you are installing to an HP OXPd v1.4 device using HTTPS, you must select the **Use SSL for secure communication** option (this section will not appear for HP OXPd v1.6).
- 11 Click **OK** to add the device.
- 12 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”).
- 13 After a successful query, right-click and select **Install**.
- 14 Verify that the buttons appear on the device.

## Choosing an authentication method

The AccuRoute Embedded Device Client for HP OXPd must be able to authenticate the device user when the **Personal Distributions**, **Scan to Me**, or **Scan to My Files** option is used.

You can configure:

- LDAP authentication
- HP authentication at the device

## Configuring LDAP authentication

When you choose LDAP Authentication, the user is prompted to enter an email username and password. The HP Authentication Manager uses the login credentials to initiate a lookup. The lookup validates the user and returns the user's email address. Then the AccuRoute Embedded Device Client for HP OXPd uses the email address to request information from the AccuRoute server, such as a list of the user's Personal Distributions. When the scan is submitted to the AccuRoute server as a message, the email address is used to set the property prOriginator.

Both the email username and password are required to identify the device user, and the credentials are validated via LDAP authentication. This method provides increased security.

The following figure is an example of an LDAP Authentication configuration for Active Directory. (For information on configuring LDAP Authentication, consult [HP documentation](#).)

| Information  | Settings | Digital Sending | Networking |
|--|----------|-----------------|------------|
| <div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <p><b>Configure Device</b></p> <p>E-mail Server</p> <p>Alerts</p> <p>AutoSend</p> <p>Security</p> <p>Authentication Manager</p> <p><b>LDAP Authentication</b></p> <p>Kerberos Authentication</p> <p>PIN Authentication</p> <p>Edit Other Links</p> <p>Device Information</p> <p>Language</p> <p>Date &amp; Time</p> <p>Wake Time</p> </div> <div style="width: 80%; padding-left: 5px;"> <h3 style="margin: 0;">LDAP Authentication</h3> <div style="background-color: #0056b3; color: white; padding: 2px; margin-bottom: 5px;">Accessing the LDAP Server</div> <p>LDAP Server Bind Method: <input type="text" value="Simple"/></p> <p>LDAP Server: <input type="text" value="172.18.30.185"/></p> <p>Port: <input type="text" value="389"/></p> <div style="background-color: #0056b3; color: white; padding: 2px; margin-bottom: 5px;">Credentials</div> <p><input checked="" type="radio"/> Use Device User's Credentials</p> <p>Bind Prefix: <input type="text" value="cn"/></p> <p><input type="radio"/> Use LDAP Administrator's Credentials</p> <p>LDAP Administrator's DN: <input type="text"/></p> <p>Password: <input type="text"/></p> <div style="background-color: #0056b3; color: white; padding: 2px; margin-bottom: 5px;">Searching the Database</div> <p>Bind and search Root: <input type="text" value="ou=engineering,cn=users,dc=hp,dc=com"/></p> <p>Match the name entered with the LDAP attribute of: <input type="text" value="cn"/></p> <p>Retrieve the device user's email address using attribute of: <input type="text" value="mail"/></p> <p>and name using the attribute of: <input type="text" value="displayName"/></p> </div> </div> |          |                 |            |
| <div style="display: flex;"> <div style="width: 20%; border-right: 1px solid #ccc; padding-right: 5px;"> <p><b>Other Links</b></p> <p><a href="#">hp instant support</a></p> <p><a href="#">Order Supplies</a></p> <p><a href="#">Product Support</a></p> </div> </div>  |          |                 |            |

LDAP Authentication binds to the LDAP server with the device user's common name (CN). The search is conducted within the root ou=engineering,cn=users,dc=hp,dc=com using the device user's common name (CN). The return value is the user's email address (mail) and name (displayName).

**Figure 5-1: Example of an LDAP authentication configuration for Active Directory**

---

## 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 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 AccuRoute Embedded Device Client for HP OXPd. You can test the AccuRoute scanning features at this point ([Section 8: Testing](#)).

Section 5: Required Configuration



# Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices

The information in this section will allow you to administrate and install HP OXPd embedded buttons onto HP devices using the Web Jetadmin application. This section includes:

[Supported Devices](#) (6-1)

[Exporting the XML files](#) (6-2)

[Installing OXPd v1.6 buttons](#) (6-4)

## Supported Devices

The following devices are supported:

**Table 6-1: HP Device Series Matrix**

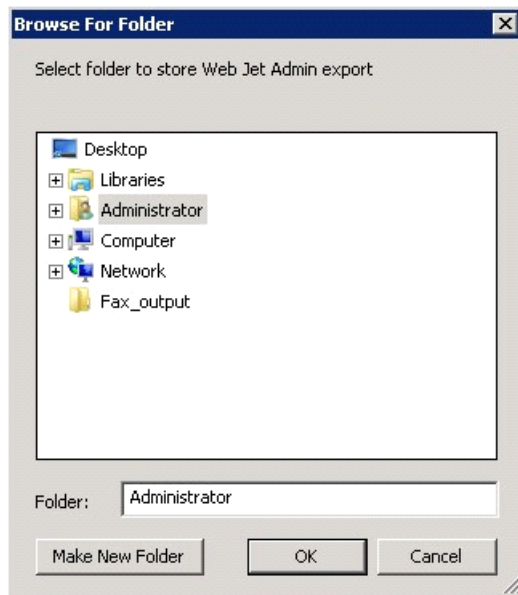
| Device                     | Operating System | Device                     | Operating System |
|----------------------------|------------------|----------------------------|------------------|
| Color LaserJet 4730 MFP    |                  | LaserJet M9050 MFP         | Oz               |
| Digital Sender 9200c       |                  | LaserJet M9059 MFP         | Oz               |
| LaserJet 4345 MFP          |                  | Color LaserJet CM 6030 MFP | Oz               |
| LaserJet 9040 MFP          |                  | Color LaserJet CM 6040 MFP | Oz               |
| LaserJet 9050 MFP          |                  | Color LaserJet CM 6049 MFP | Oz               |
| LaserJet 9500 MFP          |                  | Color LaserJet CM 3530 MFP | Oz               |
| Color LaserJet CM 4730 MFP | Oz               | Color LaserJet CM 4540 MFP | FutureSmart      |
| Digital Sender 9250c       | Oz               | ScanJet 7000n              | FutureSmart      |
| LaserJet M3035 MFP         | Oz               | ScanJet 8500               | FutureSmart      |
| LaserJet M4345 MFP         | Oz               | LaserJet Flow M525 MXP     | FutureSmart      |
| LaserJet M4349 MFP         | Oz               | LaserJet Flow M575 MXP     | FutureSmart      |
| LaserJet M5035 MFP         | Oz               | LaserJet M775 MFP          | FutureSmart      |
| LaserJet M5039 MFP         | Oz               | LaserJet M4555 MFP         | FutureSmart      |
| LaserJet M9040 MFP         | Oz               |                            |                  |

## Exporting the XML files

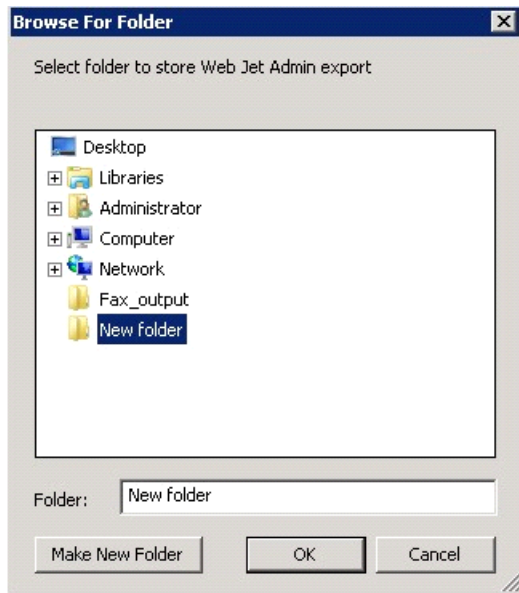
Complete the following procedure for AccuRoute to configure the HP OXP Device Client with the desired settings.

- 1 Once the configuration is complete (as described in [Section 3: Installation](#) and [Section 5: Required Configuration](#)), right-click the **Devices** group to which you intend to deploy buttons. Select **Export to Web Jet Admin**.
- 2 You can now store the XML files by browsing to a network folder or creating a new folder destination.

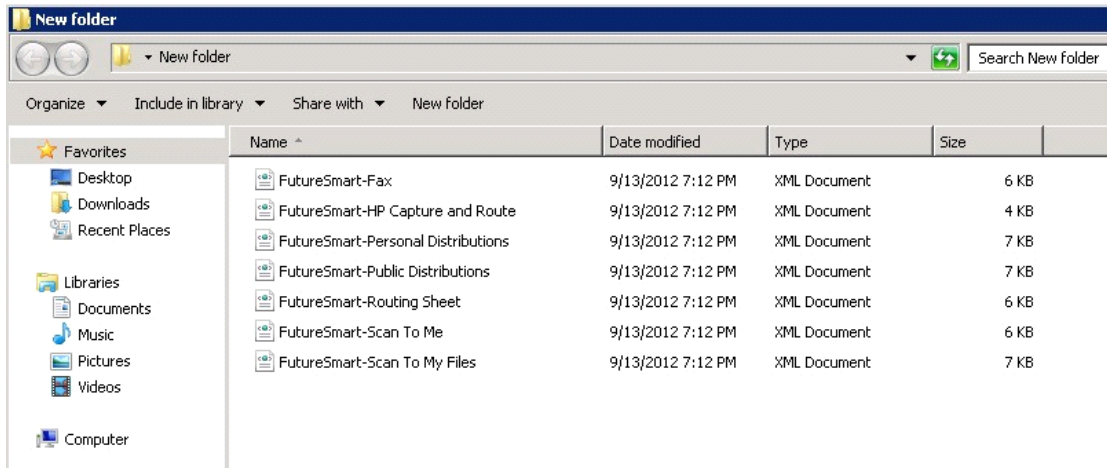
### Browse:



### Make New Folder:



- 3 Click **OK** and verify the correct buttons are represented in XML format.

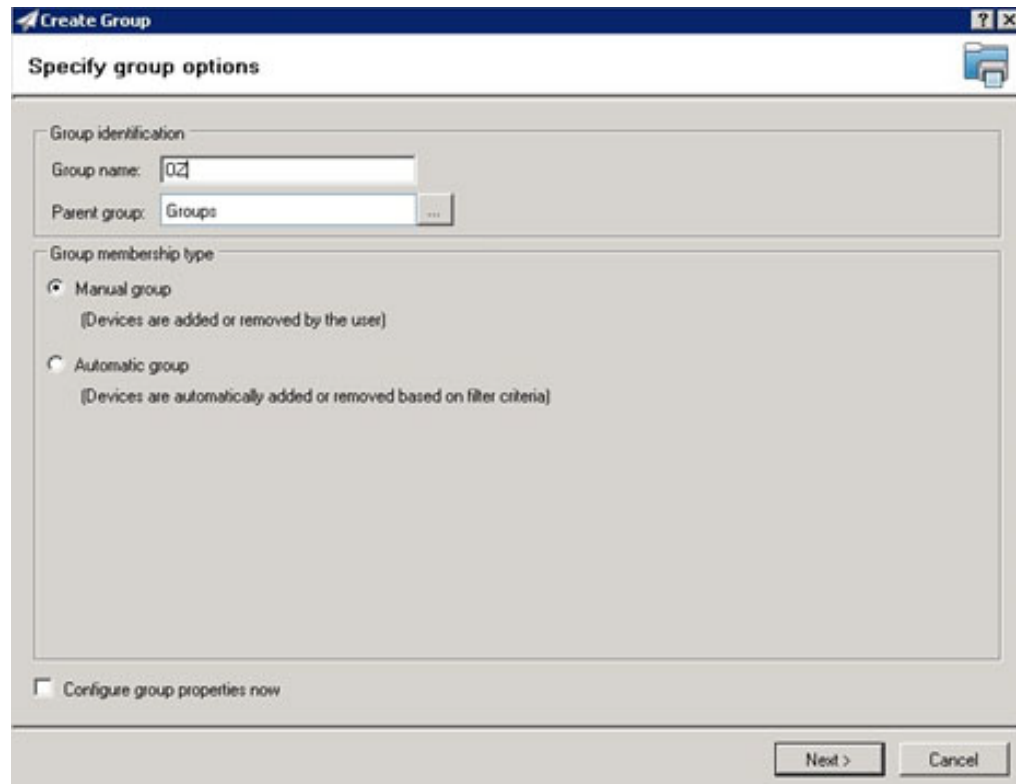


## Installing OXPd v1.6 buttons

Once the XML files have been edited and you are able to discover devices using the Web Jetadmin application, you can install HP OXPd buttons using the Web Jetadmin application.

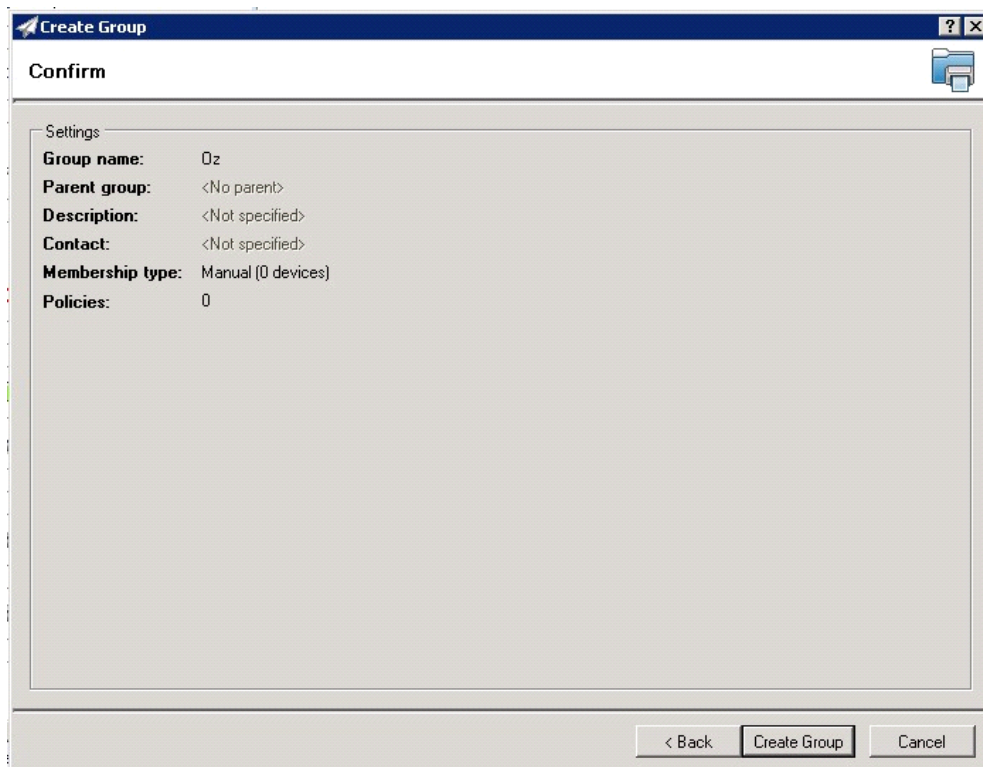
- 1 Right-click the **Group** node and select **New group**.

The **Specify group options** page is displayed.

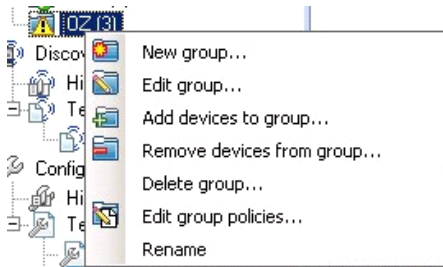


- 2 Enter the name of the new group that you will use to group similar devices for HP OXPd button installation. (Preferably, this is a device group name that will allow the administrator to easily configure similar firmware or button functionality installations such as Jedi, Oz, etc.)

- 3 Click **Next** and verify the group name is correct. The **Confirm** page is displayed, showing the settings for the group.

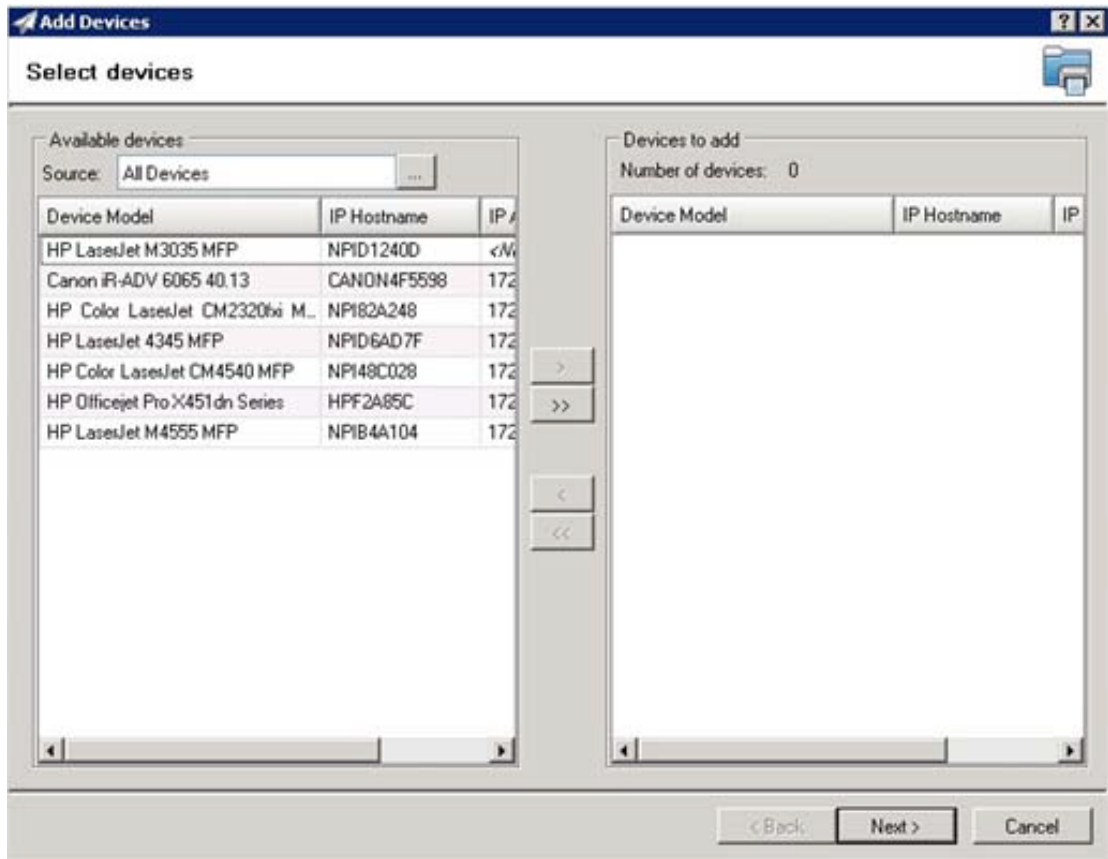


- 4 Click **Create Group** and then **Done**.
- 5 Right-click the newly created group and select **Add devices to your group**.

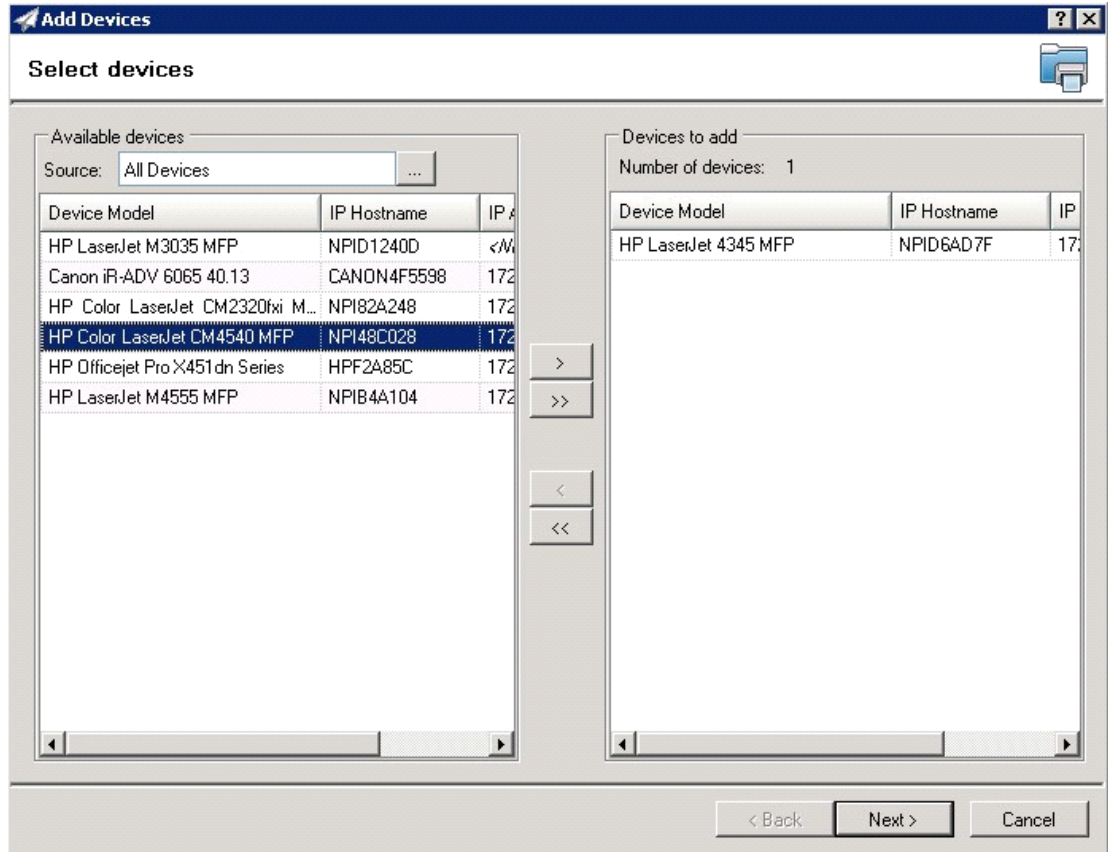


**Note** For more options in using the Web Jetadmin device filters to find or add devices, consult HP's Web Jetadmin team for a complete Web Jetadmin installation guide.

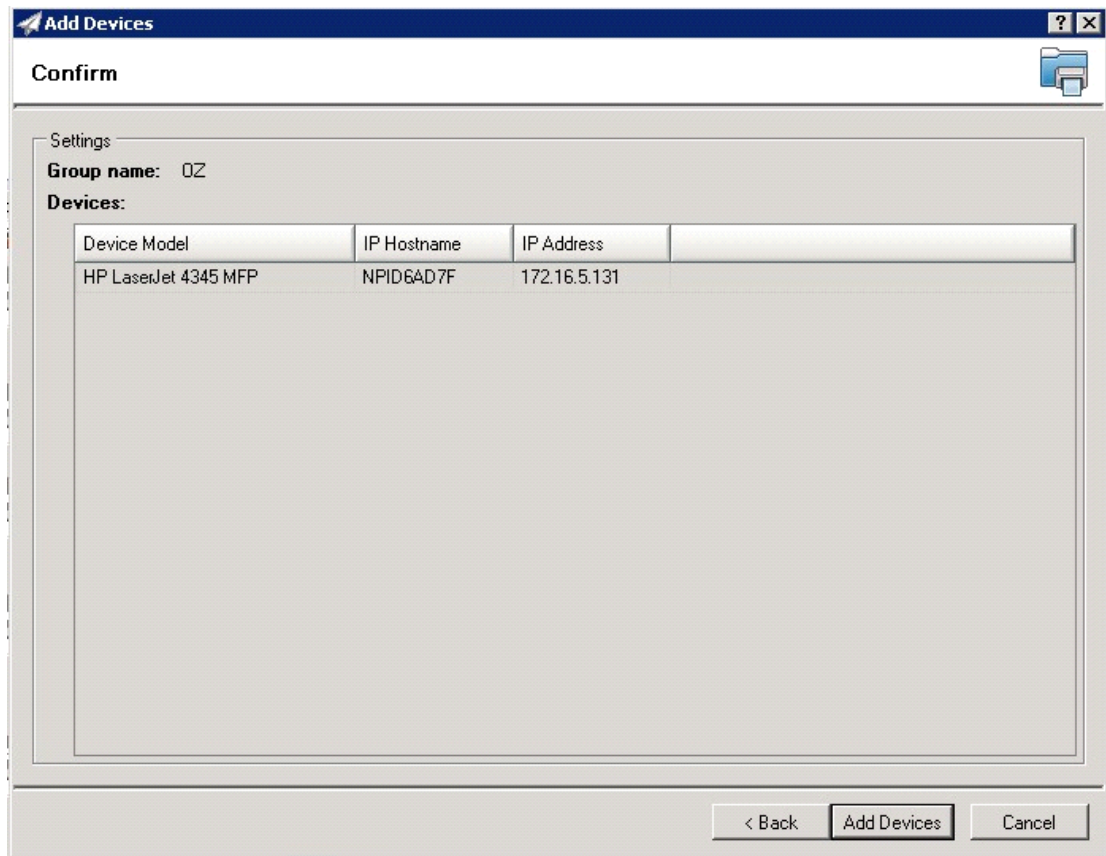
The **Select Devices** page is displayed.



- In the **Available devices** list (on the left), highlight the device(s) to be added to the group. Then click the **>** (add) button. The selected device(s) will be added to the **Devices to add** list (on the right).



- 7 Click **Next**. The **Confirm** page is displayed.



Settings

Group name: OZ

Devices:

| Device Model         | IP Hostname | IP Address   |
|----------------------|-------------|--------------|
| HP LaserJet 4345 MFP | NPID6AD7F   | 172.16.5.131 |

< Back   Add Devices   Cancel

- 8 Click the **Add Devices** button. You should see the devices added to your new group in the **Group** window.



**9** Highlight the device(s) to which you want to install buttons.

OZ (1 of 3 Selected)

| Device Model                 | IP Address   | IP Hostname | Port (Any) | Severity | Hardware Address |
|------------------------------|--------------|-------------|------------|----------|------------------|
| HP LaserJet M4345 MFP        | 172.16.5.208 | NPI822592   | 1          |          | 001708822592     |
| HP Color LaserJet 4730 MFP   | 172.16.5.130 | NPI58DA67   | 1          |          | 00143858DA67     |
| HP Color LaserJet CM6040 MFP | 172.16.5.117 | NPI1CB481   | 1          |          | 001B781CB481     |

My Settings | Device

- Alternative Letterhead Mo...
- Asset Number
- Auto Cleaning Page
- Auto Continue
- Browser
- Clearable Warnings
- Company Name
- Contact Person
- Control Panel Display
- Control Panel Language
- Date and Time
- Date/Time Format
- Daylight Savings Time
- Default Media Size
- Default Media Type
- Default Print Density
- Default Printer Copies
- Device Certificates
- Device Location
- Device Name
- Duplex Binding
- Duplex Blank Pages
- Duplex Impressions

Alternative Letterhead Mode

On  
 Off

Asset Number

Auto Cleaning Page

Auto cleaning frequency: 2000  
Cleaning page size: Letter (8.5x11 in)

Auto Continue

On  
 Off

Browser

Connection timeout: 60 seconds  
Response timeout: 300 seconds  
Trusted sites:

**10** Click the **Config** tab and scroll to the **OXPd Device Functions** subset (as shown below) and check the box in the upper left corner of the center window. The title bar of that area will display: *OXPd Device Functions (Changes Pending - Click 'Apply' to continue).*

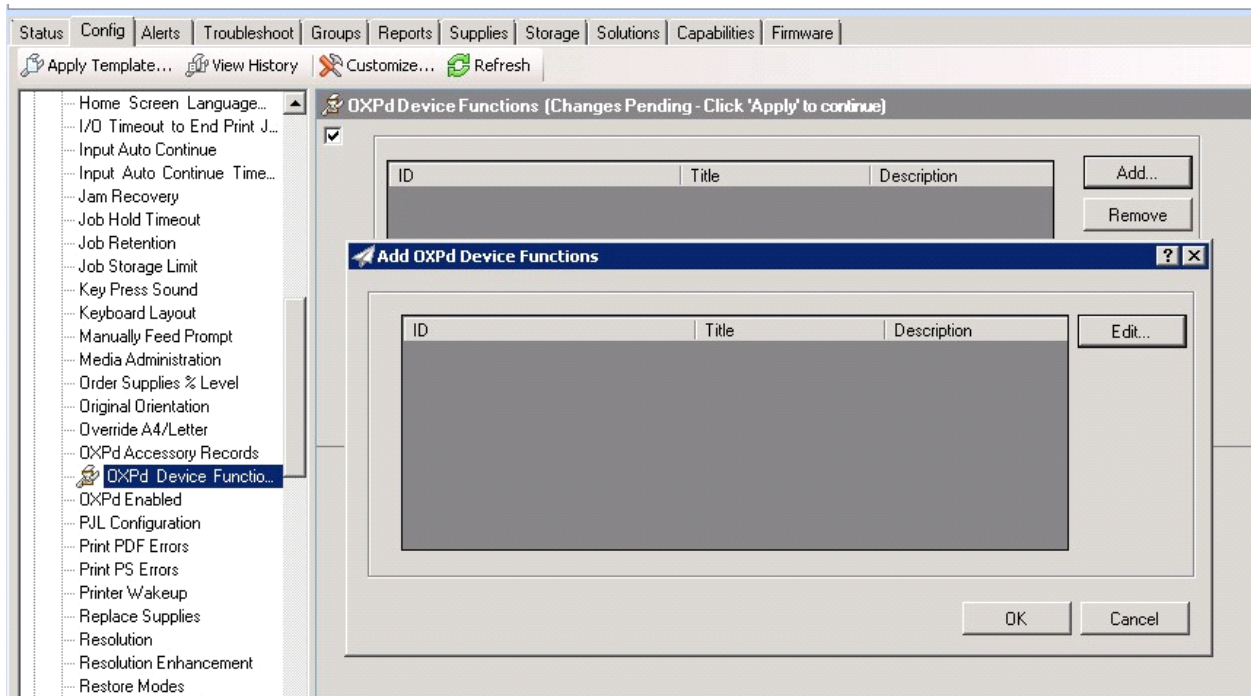
OXPd Device Functions (Changes Pending - Click 'Apply' to continue)

| ID | Title | Description |
|----|-------|-------------|
|    |       |             |

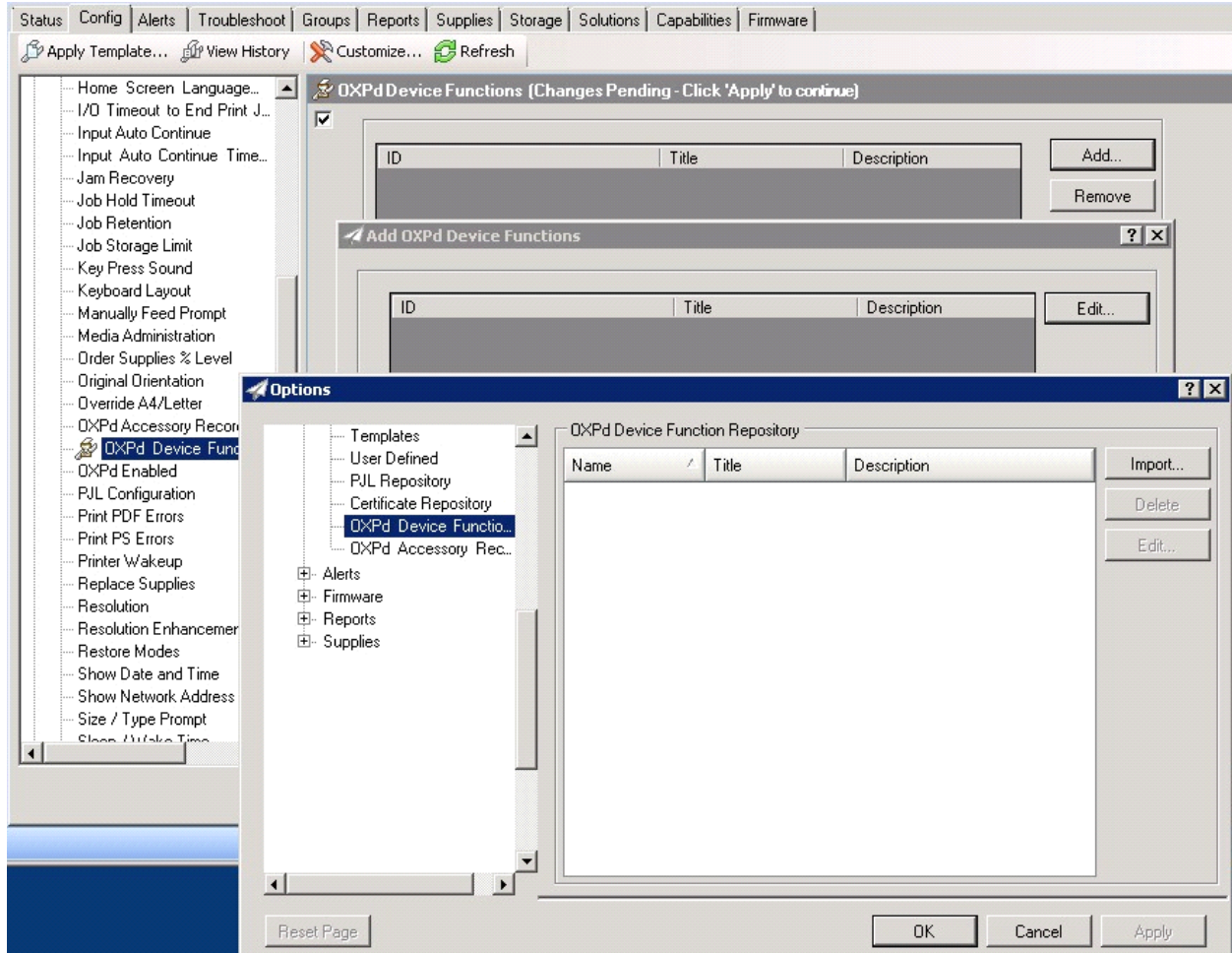
Add...  
Remove

Save as Template... Schedule... Apply...

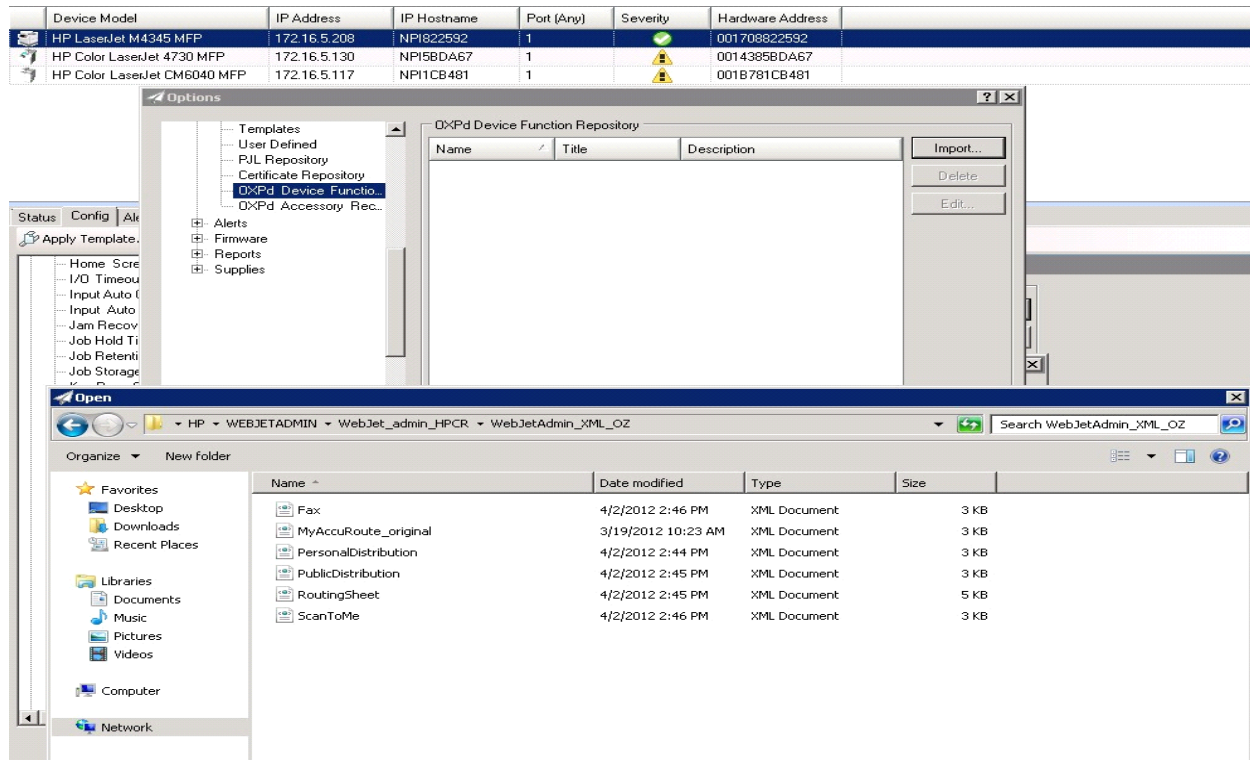
**II Click the Add button. The Add OXPd Device Functions windows is displayed.**



- 12 Click the **Edit** button. The **OXPd Device Function Repository** window is displayed and will enable you to import the edited HP OXPd solutions XML files (from [Exporting the XML files](#) on page 6-2).

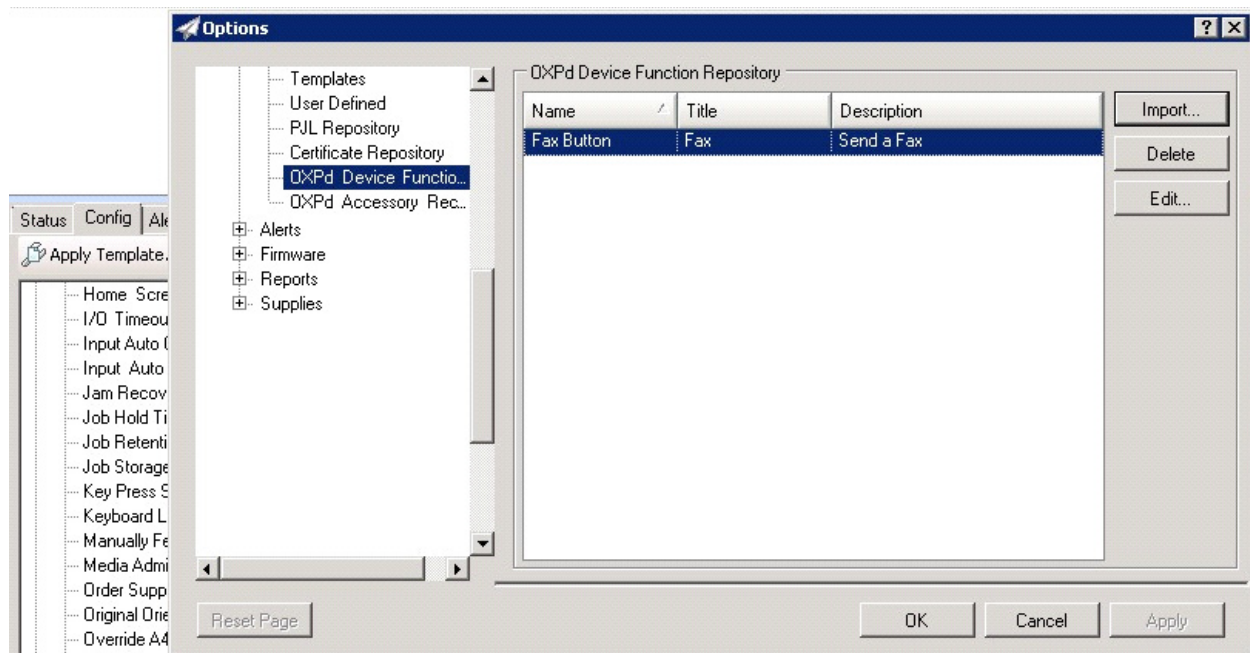


## Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices

**13 Click Import.** In the **Open** window, search for your XML files.

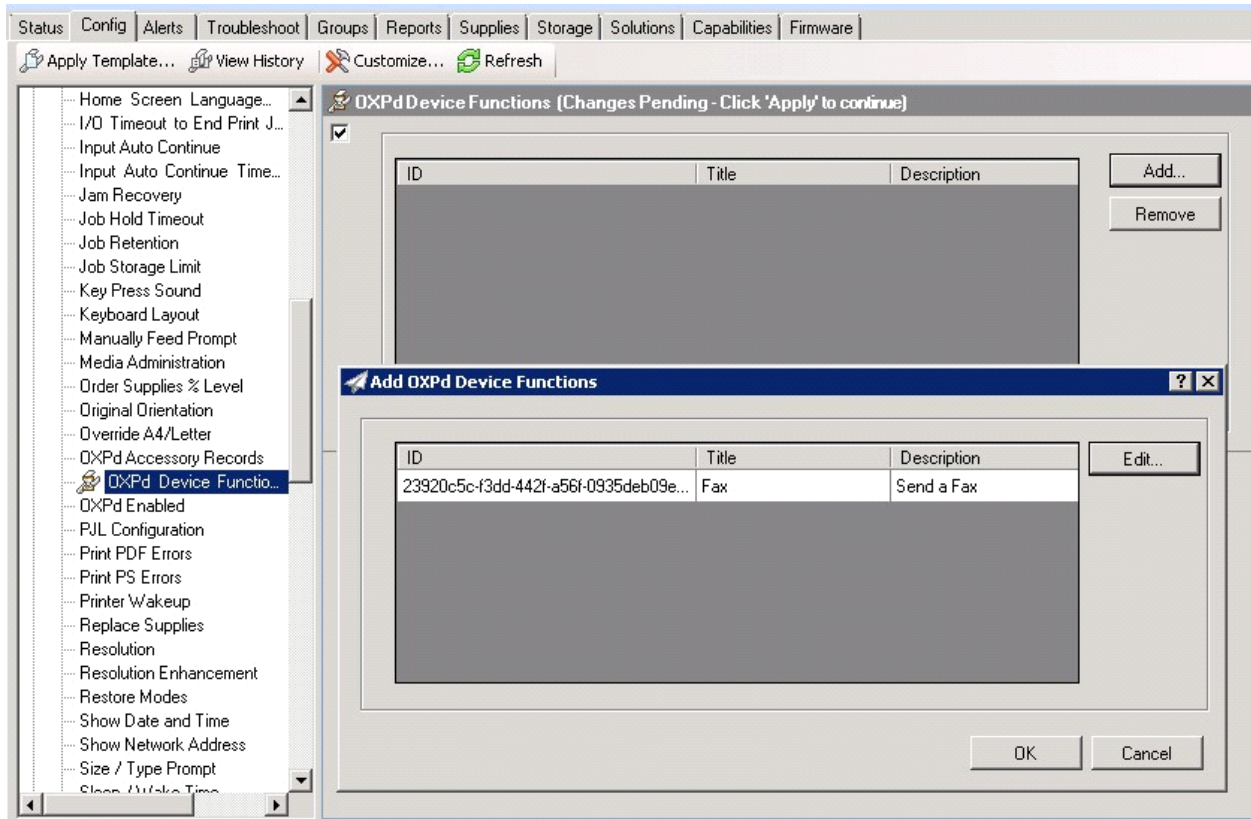
**14** Select to highlight the file and then click **Open** to add the file. (You can import only one file at a time in the **Open** window.)

**15** Verify that the selected feature XML file is reflected in the **OXPd Device Function Repository** window.





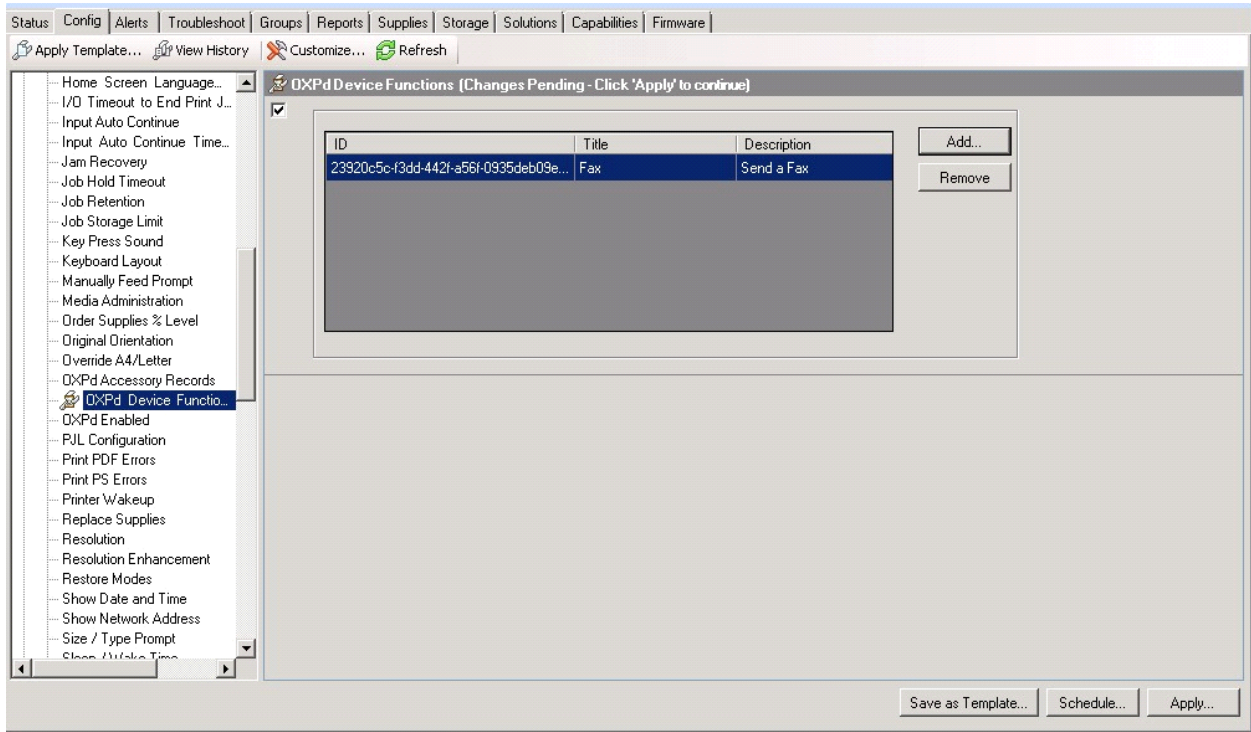
**16** Click **OK**. The **Add OXPd Device Functions** window is displayed.



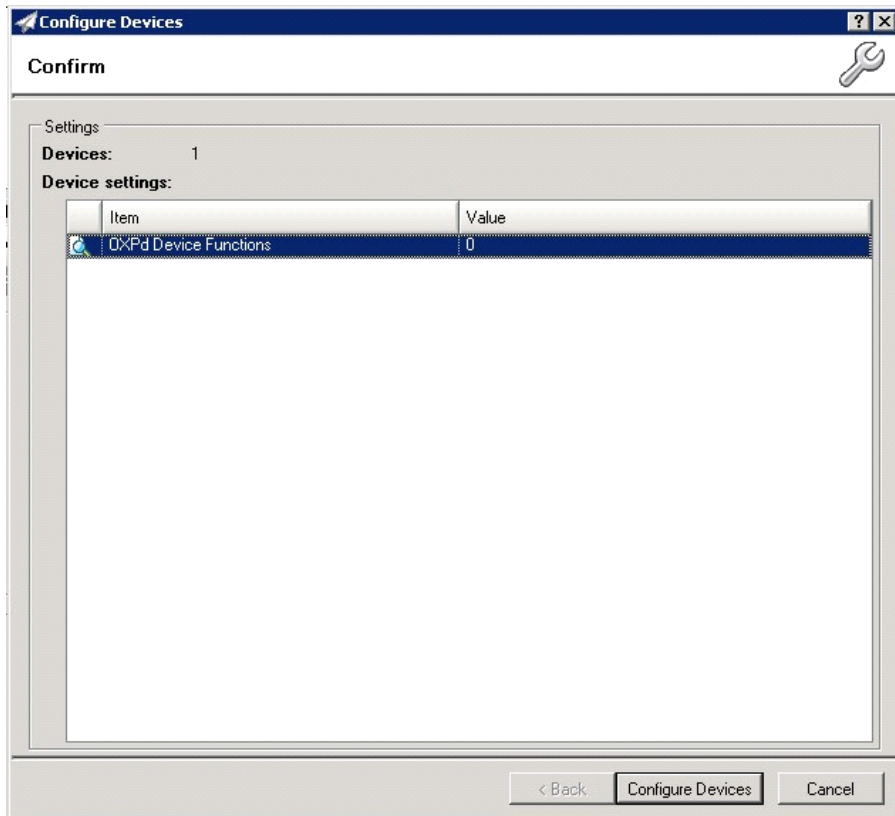
**17** You should see the file referring to the feature(s) or button(s) you are about to install onto the device. Click **OK** to close the **Add OXPd Device Functions** window and return to the **OXPd Device Functions** window.

At this point, you can continue to add another feature or button (repeating Steps 11 through 16).

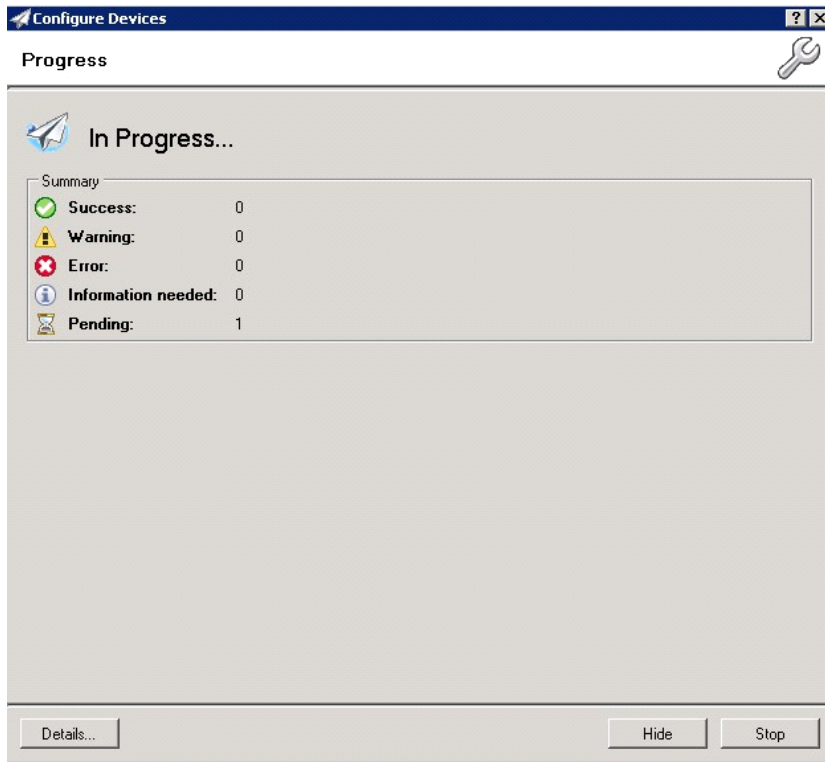
Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices



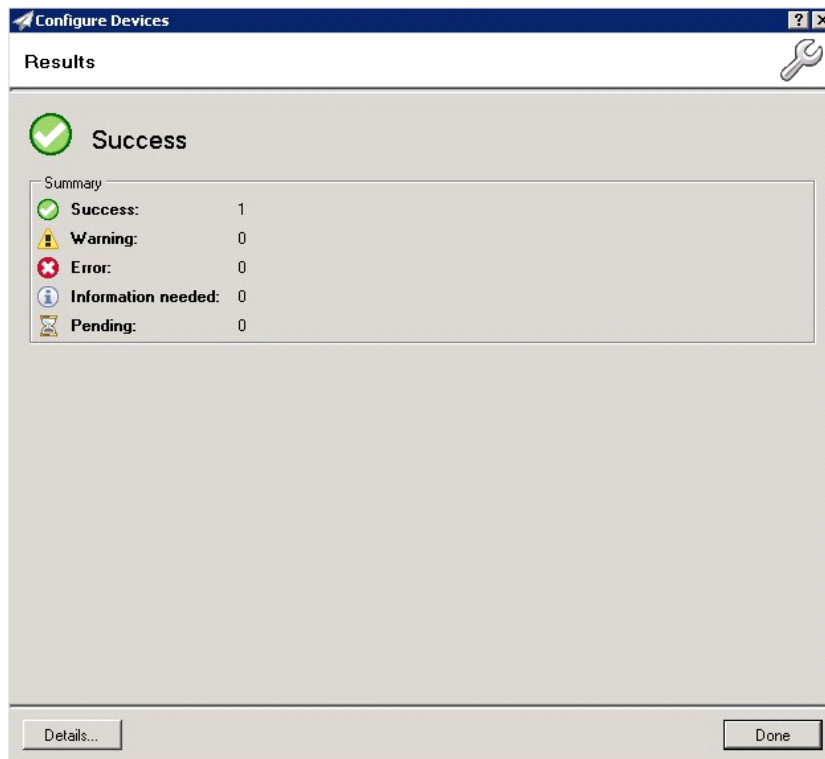
18 After you have added and confirmed all of the desired features/buttons, click **Apply**. **Confirm** page is displayed.



19 Click the **Configure Devices** button. The **In Progress** window is displayed.



The **Results** screen will then indicate if the installation was successful or if an error was received.



Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices

**Note** You can click the **Details** button to show additional notes if an error has occurred.

**20** Click **Done** to return to the main **Group** window, which defaults to the **Device** subset node.

The screenshot displays the HP Web Jetadmin interface. At the top, a blue header bar shows 'OZ (1 of 3 Selected)'. Below this is a table with columns: Device Model, IP Address, IP Hostname, Port (Any), Severity, and Hardware Address. The table contains three rows of device information.

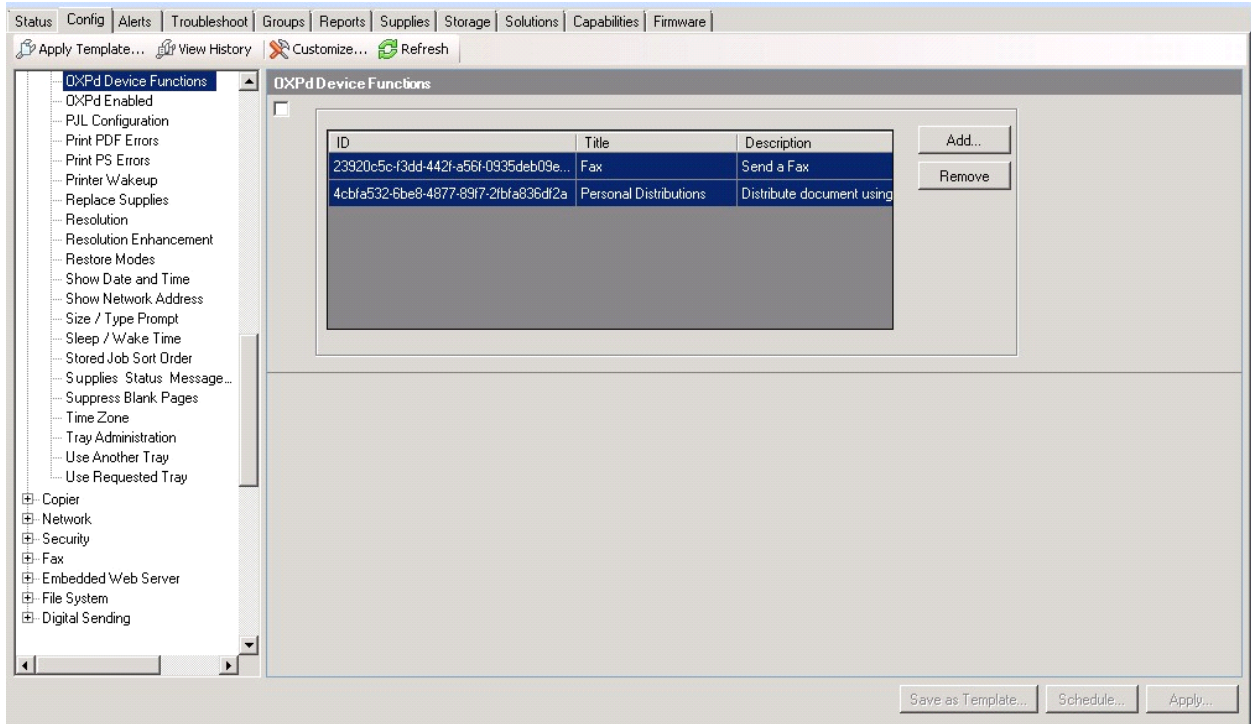
| Device Model                 | IP Address   | IP Hostname | Port (Any) | Severity | Hardware Address |
|------------------------------|--------------|-------------|------------|----------|------------------|
| HP LaserJet M4345 MFP        | 172.16.5.208 | NPI822592   | 1          |          | 001708922592     |
| HP Color LaserJet 4730 MFP   | 172.16.5.130 | NPI5BDA67   | 1          |          | 0014385BDA67     |
| HP Color LaserJet CM6040 MFP | 172.16.5.117 | NPI1CB481   | 1          |          | 001B781CB481     |

Below the table is a navigation menu with options: Status, Config, Alerts, Troubleshoot, Groups, Reports, Supplies, Storage, Solutions, Capabilities, Firmware. Below the menu are buttons: Apply Template..., View History, Customize..., Refresh.

The main area shows a configuration window for 'Device' settings. The left sidebar lists various settings categories. The right pane shows the configuration for 'Alternative Letterhead Mode' (radio buttons for On/Off), 'Asset Number' (text field), 'Auto Cleaning Page' (checkbox, Auto cleaning frequency: 2000, Cleaning page size: Letter (8.5x11 in)), 'Auto Continue' (radio buttons for On/Off), and 'Browser' (checkbox, Connection timeout: 60 seconds, Response timeout: 300 seconds, Trusted sites: text area). At the bottom right are buttons: Save as Template..., Schedule..., Apply...



**21** Scroll down to the **OXPd Device Functions** subset and you should see the feature buttons that have been successfully added to the HP device.



**22** Test the buttons on the device panel to verify all functionality.

---

Section 6: Using HP's Web Jetadmin Application to Install Omtool OXPd v1.6 Buttons on HP Devices

# Section 7: Optional Configuration

This section includes:

[Setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#) (7-1)

[Adding the remote server's name to DCOM](#) (7-2)

[Configuring a Distribution Rule to appear at the top of the device listing](#) (7-2)

[Configuring scan settings in Distribution Rules](#) (7-3)

[Configuring the Universal Input connector for HP OXP file processing](#) (7-3)

[Configuring the Fax Release button](#) (7-8)

---

## 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 give him full permissions.

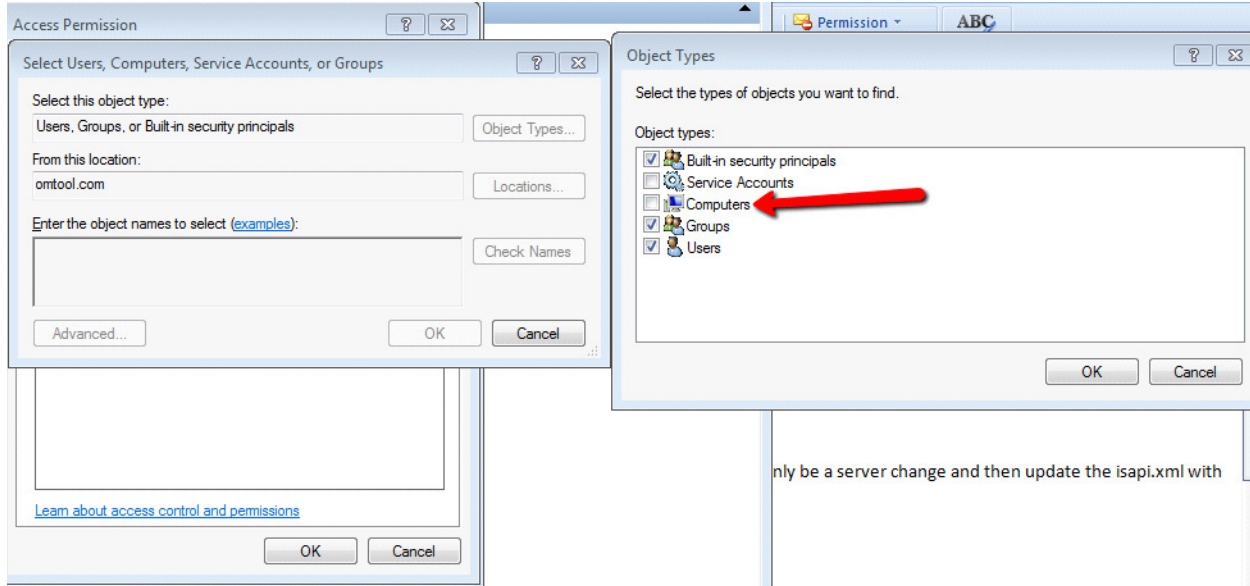
Additional procedures for setting up Embedded AccuRoute for Intelligent Devices in a cluster are provided in the appendix titled, *Setting up an AccuRoute server cluster*, in the [AccuRoute v4.0 Server Installation Guide](#).

## 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.

---

## Configuring the Universal Input connector for HP OXP file processing

AccuRoute Universal Input connector is a connector that can pick up and process orphaned OXP 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 OXP application fails to route scanned files to the AccuRoute server, this new connector will be able to pick up and process the OXP files for processing on the AccuRoute server.

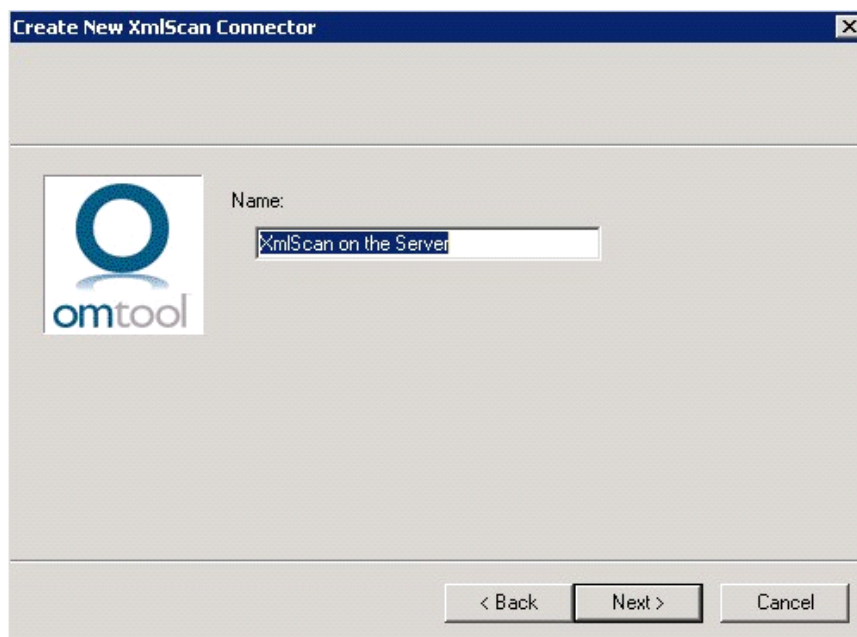
## Requirements for the Universal Input Connector

- AccuRoute 4.0

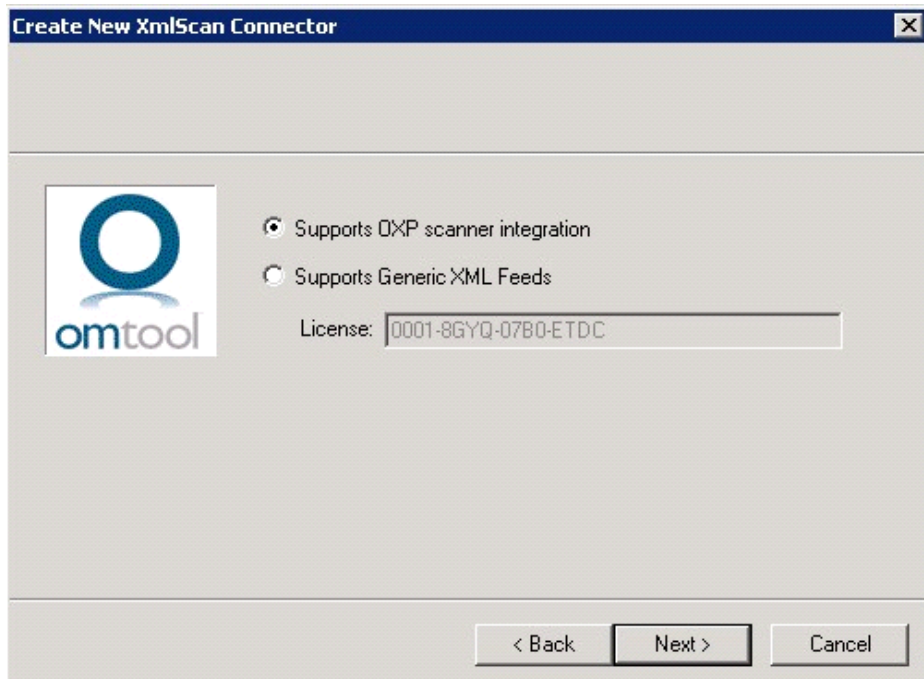
- AccuRoute Embedded Device Client for HP OXPd 1.6.4

## Installing the Universal Input connector license

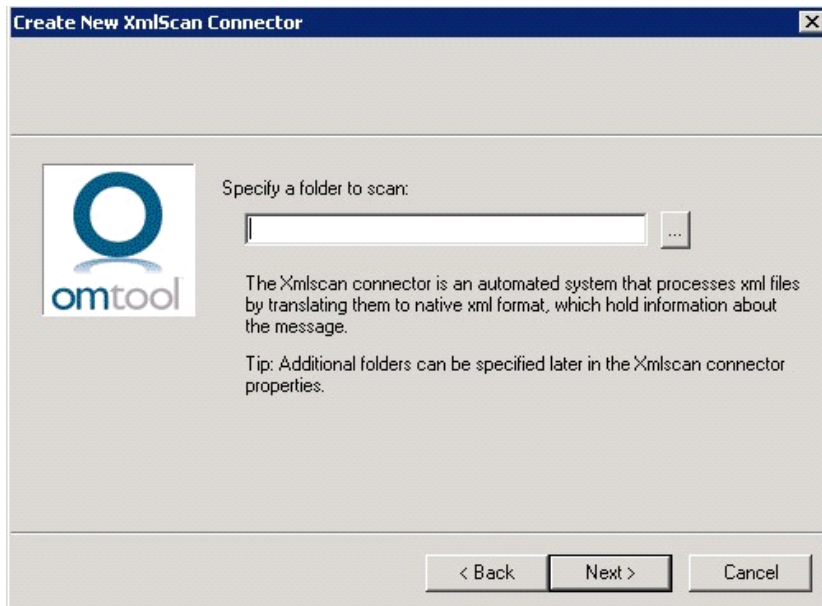
- 1 Log in to the AccuRoute v4.0 server using an account that belongs to the AccuRoute Administrators group.
- 2 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 3 In the console tree, expand the AccuRoute Server Administrator and right-click **Connectors**. Select **New AccuRoute connector for > Universal Input**.
- 4 Enter a name for the connector or keep the default name. Click **Next**.



- 5 Be sure the default setting, **Supports OXP scanner integration**, is selected. Click **Next**.



- 6 Browse to the folder from which the XmlScan connector will be processing files. Click **Next**.

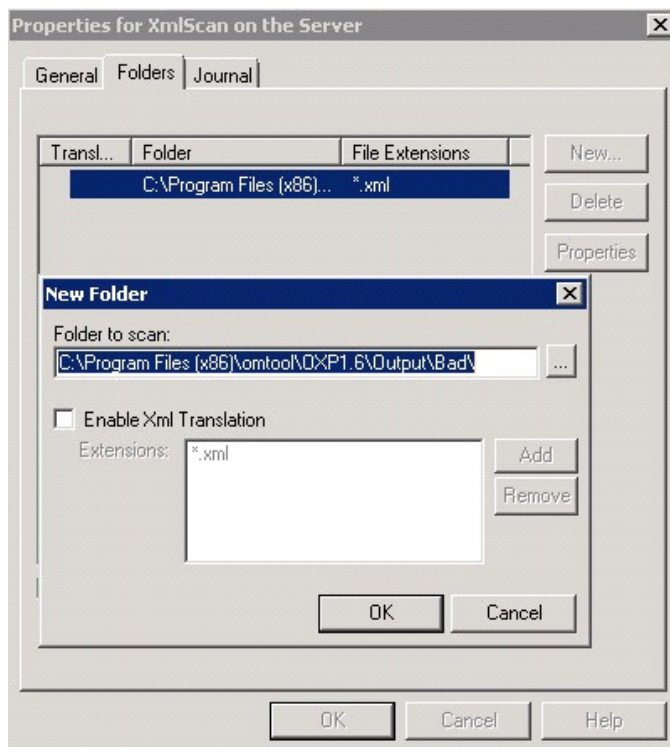


- a If the OXP application already had a processing failure and has automatically created a **Bad** folder structure, browse to that folder in this location:

X:\Program Files (x86)\omtool\OXP1.6\Output\Bad



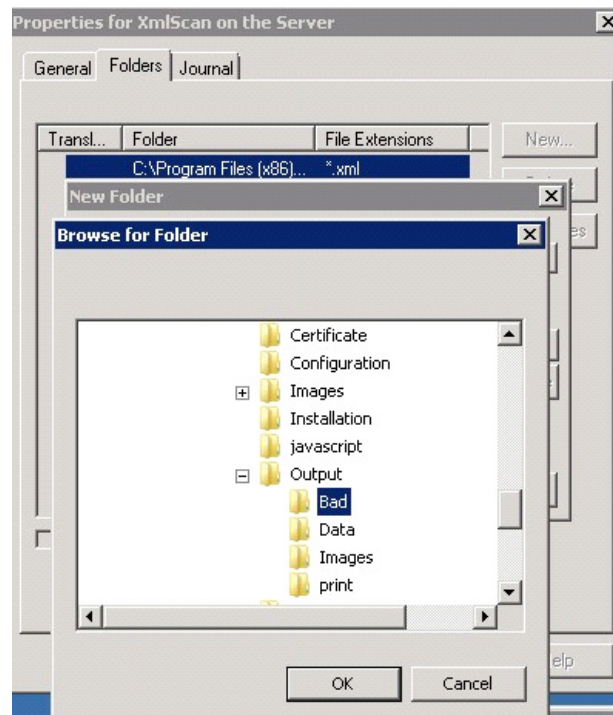
- Click **OK** and verify on the **Folders** tab that the **Bad** folder has **Enable Xml Translation** unchecked. Click **OK** twice to save the connector configuration.



- b If you are setting up the XmlScan connector prior to any processing failures, create a folder named **Bad** inside the **Output** folder in this location:



X:\Program Files (x86)\omtool\OXPl.6\Output\Bad  
Click **OK**.



For example, If the AccuRoute Web application fails to process the OXP (data and image) files and those files are left in these folders structures:

X:\Program Files (x86)\omtool\OXPl.6\Output\Data

X:\Program Files (x86)\omtool\OXPl.6\Output\Images

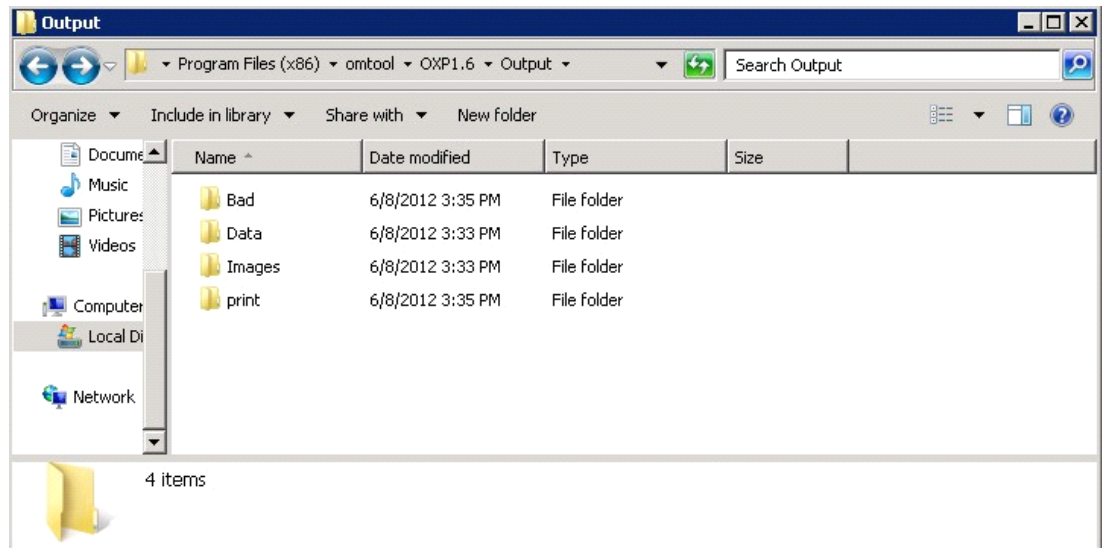
Two new folders will be created automatically when a scan fails to route to the Omtool Web application:

X:\Program Files (x86)\omtool\OXPl.6\Output\Bad ...

This folder will be the new pickup folder for the XmlScan Connector. Files will automatically be moved to this folder by the OXP application.

X:\Program Files (x86)\omtool\OXPl.6\Output\print ...

This folder processes the print back to device “Failed to process document” notification.



- 7 Once the folder is selected, leave the **Enable Xml Translation** box unchecked.
- 8 Select **OK** twice to save the connector configuration.

## Configuring the Fax Release button

In order to support the Fax Release button for AccuRoute Embedded Device Client for HP OXPd v1.6.4, a new property dictionary item must be created to filter the pending jobs for each destination fax number as it is listed in the Destination Translation Table (DTT). This configuration involves:

- [Creating the Fax Release property \(prDestinationFaxNumber\)](#) (7-8) dictionary item to filter the pending jobs for each destination fax number as it is listed in the DTT.
- [Creating the DTT Administrator Group for the Web Client](#) (7-10), which is required to use the Fax Release button.
- [Configuring a release calendar](#) (7-10) to specify times during which all fax jobs will be released.
- [Configuring the DTT](#) (7-11), which is used to define routing features for a specific device.

## Creating the Fax Release property (prDestinationFaxNumber)

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 1 In the console tree, expand the AccuRoute Server Administrator and click **Configuration**.
- 2 Right-click **Properties** and select **New > Property Dictionary**. The **Property Dictionary Item** page opens.
- 3 In the **Name** text box, enter the metadata field name.
- 4 In the **Label** text box, enter a suitable label.

- 5 In the **Instructions** text box, enter any needed instructions.
- 6 Verify that the **Type** is set to **Text**.
- 7 In the **Mappings** section, click **New** to open the **Property Definition** page.
- 8 Select **Property Name** option and enter: `prDestinationFaxNumber`
- 9 Click **OK**. The following will be displayed in the **Mappings** section: `\\prDestinationFaxNumber`
- 10 Click **OK** again to create the property.
- 11 Now you will configure the Active volume list. On the AccuRoute Server Administrator console tree, click **Volume Lists**.
- 12 Double-click the **Active** to open the **Active** properties page.
- 13 Click the **Indexing** tab.
- 14 In the **Properties to Index** section, click **Add**. The **Index Properties** page opens.
- 15 Select from the **Property** drop-box the `prDestinationFaxNumber` property.
- 16 Click **OK** to close the **Index Properties** page.
- 17 In the **Property Search Groups** section, click **Add**. In the **Name** text box, enter:  
`prDestinationFaxNumber`
- 18 Select **Add**, then select `prDestinationFaxNumber` from the list of indexed properties. Click **OK** and then **OK** again.
- 19 Click **OK** to close the **Active** page.

## Creating the Administrator view options

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 1 In the console tree, expand the AccuRoute Server Administrator and click **Configuration > Web Client Views**.
- 2 Select **View.admin.xml**. Then, select **Properties**.
- 3 On the **Folders** tab, select the **Administration** node.
- 4 Click the **Properties** button.
- 5 On the **General** tab, enable **Display this folder**.
- 6 Optionally, if this should be the first screen viewed when launching the web client, enable **This is the default folder to display**.
- 7 Click **OK**. Click **OK** again to save the changes.

## Creating the DTT Administrator Group for the Web Client

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 1 In the console tree, expand the AccuRoute Server Administrator and click **Configuration**.
- 2 Right-click **Groups** and select **New > Group**. The **Group** page opens.
- 3 In the **Name** text box, enter a name for the group, such as **DTT Administrator Group**.
- 4 In the **Description** text box, enter a brief description.
- 5 Click **Members** tab and then click **Add**. The **Add Group** page opens.
- 6 Enter a pre-defined Active Directory group and click **Check Names**.
- 7 Select the group from the list returned and click **Finish** to close the **Add Group** page.
- 8 Click the **Clients** tab.
- 9 Select (check) the **Enable members of this group as users** option.
- 10 In the **Allow group to Route to** section, select **Fax, Printer, and E-mail** options.
- 11 Click the **Web Client** tab.
- 12 Select the **Enable members of this group to use the following web view** option. Then, select **View.admin.xml** from the **Web View** drop-down.
- 13 Click **OK** to save the configuration changes and close the **Group** page.

By configuring user permissions, you are allowing the user to view Administrator options for DTT in the AccuRoute Web Client.

## Configuring a release calendar

Release calendars are used when defining a routing destination. (You will assign the device to the calendar when [Configuring the DTT](#)). Times specified on a calendar indicate when faxes are released. For example, if the calendar is set as Monday through Friday, starting in the morning at 8:00 and ending in the afternoon at 5:00 (17:00), faxes will be released only during that time period.

- 1 In the AccuRoute Web Client, click the **Administration** tab. Then, click **Calendars**.
- 2 Click **New**.
- 3 Enter a name for the calendar in the **Name** text box.
- 4 Select start and end times for Monday through Friday.
- 5 Optionally, select **Saturday** and enter start and end times. (If this option is not selected, Saturday is not included in the calendar.)
- 6 Optionally, select **Sunday** and enter start and end times. (If this option is not selected, Sunday is not included in the calendar.)
- 7 Click **OK**.

## Configuring the DTT

- 1 In the AccuRoute Web Client, click the **Administration** button. Then click **New**. The **New Routing Destination** page opens.

The screenshot shows the 'New Routing Destination' page in the AccuRoute web client. The page has a navigation menu on the left with options: Messages, Distributions, My Files, Archive, Preferences, Administration (highlighted), and Help. The main content area contains the following fields and options:

- Fax number:** A text input field.
- Device Serial Number:** A text input field.
- Manual Hold:** A checkbox labeled 'Hold all jobs'. Below it is a 'Pin' text input field.
- Fax Release Calendar:** A checkbox labeled 'Enabled'. Below it is a dropdown menu for 'Calendar' (showing 'Afghanistan Standard Time') and another dropdown menu for 'Time Zone'.
- Destination:** A radio button labeled 'Print on Device'. Below it are three checkboxes: 'Printer:' (with a text input field), 'Print on specific Media' (with a dropdown menu showing 'Letter'), and 'Apply Document Stamp' (with a dropdown menu showing 'Header').
- A radio button labeled 'Route via RightFax' with two dropdown menus.
- At the bottom are 'OK' and 'Cancel' buttons.

- 2 Enter the following information:
  - ▶ **Fax Number** - Enter the fully normalized fax number (for example: +10005551234).
  - ▶ **Device Serial Number** - Enter the serial number for the device. This enables you to match the fax to a specific device printer.
  - ▶ **Manual Hold** - Select the **Hold all jobs** option if all jobs to this device number are to be held indefinitely. If you select this option, enter in the **PIN** text box the PIN value to be used to enable or disable the Manual Hold feature.
 

If there are multiple fax numbers associated with a device, each fax number needs a separate PIN.

If a device is manually put on hold, it will not release jobs until this feature is disabled (the option is not selected). You must enter the applicable PIN to deselect the option.
  - ▶ **Fax Release Calendar** - Select the **Enabled** option if you want to specify a date on which all fax jobs will be released. Select the **Calendar** and **Time Zone** from the drop-downs.
  - ▶ **Destination** - Select either of these options (to print on a device printer or route via RightFax).

- ▲ **Print on Device Printer** - Enter the device IP address or the UNC path to the device. (You can match the fax number to an IP address to reduce the cost of fax-to-fax transmission.)

You can select the **Print on specific Media** option to choose the paper tray used to print incoming faxes. An inbound fax message is queued for a matched device or printer and then printed using a specified paper tray during the time specified with the release calendar.

You also can select the **Apply Document Stamp** option to include a “top line” on an internal fax.

- ▲ **Route via RightFax** - Select the AccuRoute Connector for RightFax from the first drop-down menu and then select the server address of the RightFax server from the second drop-down menu.

### 3 Click **OK**.

To verify that a device was added properly:

- 1 In the AccuRoute Web Client, click the **Administration** tab.
- 2 From the **Find** drop-down on the Routing page, select **Fax Number**. (Optionally, you can select the **Device Serial Number**.)
- 3 Enter the fax number and click **Go**.
- 4 Verify that the DTT entry shows up. For example:

The screenshot shows the AccuRoute Web Client interface. The top navigation bar includes the AccuRoute logo, the omtool logo, and an email address: administrator@vmad100.omtool.com. The main content area is titled "Routing" and features a search bar with a dropdown menu set to "Fax Number" and a search input field containing "+1234567890". Below the search bar is a table with the following data:

| Fax number  | Device Serial Number | Manual Hold Status | Hold Calendar |         |
|-------------|----------------------|--------------------|---------------|---------|
| +1234567890 | 123                  | Off                |               | Release |

Below the table, it indicates "1 Item". The left sidebar contains navigation options: Messages, Distributions, My Files, Archive, Preferences, Administration (with sub-options for Routing and Calendars), and Help.

- 5 Click on the fax number in the table (or the device serial number). The **Routing Destination Properties** page is displayed. Verify the properties for the DTT entry.
- 6 Click **OK**.
- 7 Send a fax (within the release time if a calendar is specified). Verify that the fax is received and printed.

# Section 8: Testing

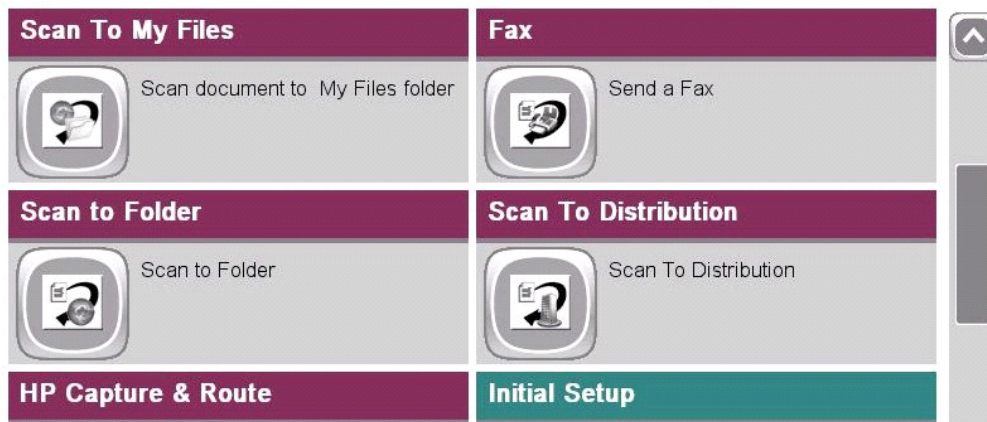
The following section provides a procedure for testing the Routing Sheet feature. This will ensure that your installation is operational. This section includes:

[Testing the Routing Sheet feature \(8-1\)](#)

[Testing the Device Administrator user interface \(8-2\)](#)

## 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 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 indicator 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 9: 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  or the **OK** button.

---

**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 \(9-6\)](#)

---

## 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 9: Troubleshooting

This section includes:

[Detecting workflow issues](#) (9-2)

[Troubleshooting the delivery mechanism](#) (9-2)

[Troubleshooting messages on the AccuRoute server](#) (9-3)

[Troubleshooting the Web server](#) (9-5)

[Troubleshooting the multifunction device](#) (9-5)

[Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd](#) (9-5)

[Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#) (9-6)

[Troubleshooting issues when the AccuRoute server cannot decipher the Distribution Rule instructions in a Routing Sheet](#) (9-6)

[Troubleshooting problems associated with applying all additional scan attributes](#) (9-7)

[Troubleshooting problems when scanning large documents](#) (9-7)

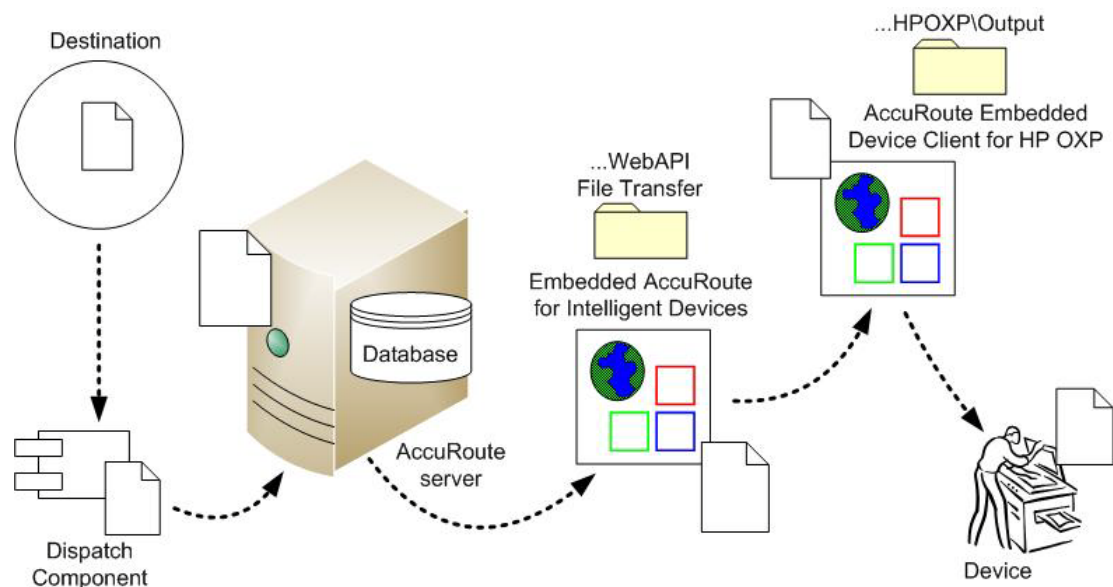
[Troubleshooting problems when scanning 100+ color pages](#) (9-8)

[Troubleshooting an SNMP error](#) (9-9)

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. Omttool 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 AccuRoute Embedded Device Client for HP OXP, the Web server, and the device.

**Figure 9-1: 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](#).

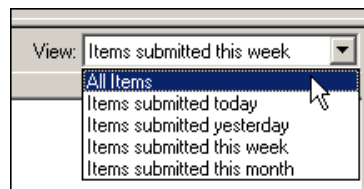
## Troubleshooting messages on the AccuRoute server

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

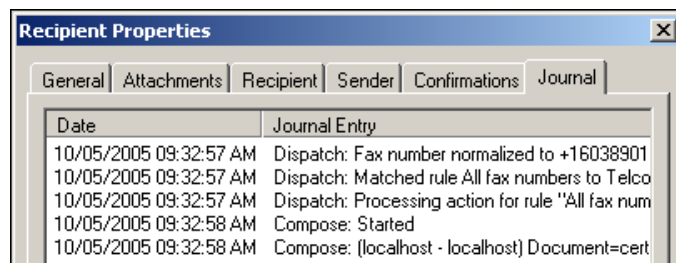
- Was the message submitted to the AccuRoute server?
- Assuming the message was submitted to the AccuRoute server, what caused the delivery failure? The state and status of the message, along with details in the message journal, provide some important clues.

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**.



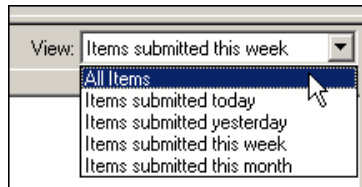
- c Sort all items by the date submitted.
- d Look for the message.
  - ▶ **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the AccuRoute server. If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



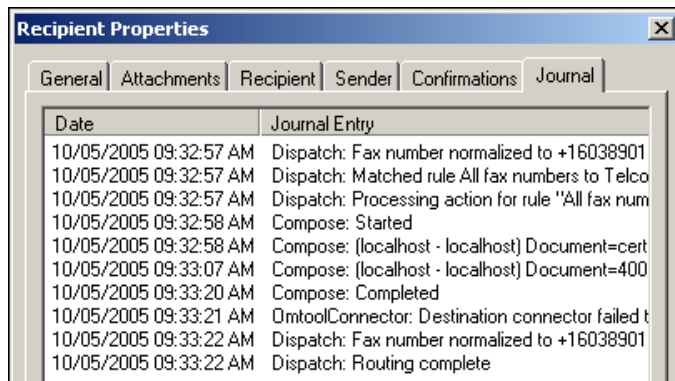
- ▶ **Message not found** - Go to step 4 and look for the message in the History queue.

#### 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 HP documentation.

---

## Troubleshooting .NET error when installing AccuRoute Embedded Device Client for HP OXPd

### **Problem:**

When installing AccuRoute Embedded Device Client for HP OXPd v1.6 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 AccuRoute Embedded Device Client for HP OXPd v1.6 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 an HP 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 problems associated with applying all additional scan attributes

### Problem:

All additional scan attributes are configured together (Darkness, back ground cleanup, contrast, sharpness, Heavy originals), and the following message appears when attempting to scan a document at the HP device:

```
The action cannot be performed because options specified in the configuration file are not supported by this device. Try again on a different device.
```

### Solution:

This message is displayed because the scan options are not supported by the device. Consult your HP manual or with your Administrator and find out which scan options are supported for your device model. The list of scan options commented in the configuration file are not supported by all the devices. Only those options that are supported by a particular device model should be un-commented and used.

---

## Troubleshooting problems when scanning large documents

### Problem:

After a document is scanned, the message indicating scan completion with delivery information is missing. However, the document is routed to the AccuRoute server for processing.

### Solution:

Configure the following:

- Increase the sleep schedule from 10 minutes to the maximum, which is 4 hours
- Increase the inactivity timeout in the device Embedded Web Server to 300 seconds
- Increase the Content length in Internet Information Service Manager (IIS)

To increase the sleep schedule:

- 1 Log in to the Embedded Web Server.
- 2 Select the **General** tab.
- 3 In the left pane, locate **Sleep Schedule**.
- 4 Increase the Sleep Delay to the maximum allowable time: **120** minutes. Click **Apply**.

To increase the inactivity timeout in the device Embedded Web Server:

- 1 Log in to the Embedded Web Server.
- 2 Select the **General** tab.
- 3 In the left pane, locate **Control Panel Administration Menu**.
- 4 In the center pane, expand **Administration**.

- 5 Click on **Display Settings**.
- 6 Locate **Inactivity Timeout** and increase the value to **300** seconds.

To increase content length in IIS:

---

**Note** The content length must be modified on both the **OmtoolDXPWebApp1.6** and the **OmtoolWebAPI** sites.

---

- 1 Go to the Internet Information Services manager and select **OXPI.6** under **Sites**.
- 2 Double-click on **Request Filtering**.
- 3 Select **Edit Feature Settings** under the **Actions** menu.
- 4 Increase the value in **Maximum allowed content length**. The default value is **30000000**. Modify the value to **300000000**.
- 5 Select **WebAPI** under **Sites**.
- 6 Double-click on **Request Filtering**.
- 7 Select **Edit Feature Settings** under the **Actions** menu.
- 8 Increase the value in **Maximum allowed content length**. The default value is **30000000**. Modify the value to **300000000**.
- 9 Reset IIS.

---

## Troubleshooting problems when scanning 100+ color pages

### Problem:

When scanning more than 100 color pages, it takes additional time for the scans to arrive on the AccuRoute server.

### Solution:

To improve performance.

- 1 Go to the Internet Information Services (IIS) manager configured for AccuRoute 4.0.
- 2 Open the following file for editing (such as with Notepad):  
`C:\Program Files (x86)\Omtool\OXPI.6`
- 3 Locate `<httpRuntime maxRequestLength="500000" executionTimeout=1800>`.  
Change the executionTimeout to 5400:  
`<httpRuntime maxRequestLength="500000" executionTimeout=5400>`
- 4 Save the file and restart IIS.



---

## Troubleshooting an SNMP error

### Problem:

When you perform an nvram full init, the Set Community string and the Get Community string are both set to public. However, when you set the admin password, it sets the Set Community string to the admin password. The networking tab of the Embedded Web Server of the device does not display the value if it is set. Instead it shows asterisks (\*\*). The best practice is to set the value to blank, as it will assume public for both and display the value as "Not Set (default to public)."

### Solution:

To display the value.

- 1 Log in to the Embedded Web Server.
- 2 Select the **Networking** tab.
- 3 Choose settings under security.
- 4 Under **SNMPc1/2** on the **Status** tab, there are two fields: **Get Community Name** and **Set Community Name**.

Change the community name values by setting the values as blank for **Get Community Name** and **Set Community Name**.

- 5 Click **Apply** to remove any value. Now, no values are set for the two fields.

