
HP[®] OXPd Device Client Installation and Integration Guide

For HP OXPd Device Client v1.4

March 9, 2010



Omttool, Ltd.

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

Omttool Europe

25 Southampton Buildings
London
WC2A 1AL
United Kingdom
Phone: +44(0) 203 043 8580
Toll-free in the UK: +44(0) 800 011 2981
Fax: +44(0) 203 043 8581

Web: <http://www.omttool.com>

© 2010, Omtool, Ltd. All Rights Reserved.

AccuRoute®, Genifax™, Image-In™, ObjectArchive™, Omtool™, Swiftwriter® 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 Website 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:** 888-303-8098 (toll-free in the US)
- **Fax:** 978-659-1301
- **E-mail:** Customerservice@omtool.com or Support@omtool.com

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

Sales, consulting services, licenses, and training

Contact Omtool Sales using any of the following methods:

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

Contents

Section 1: Introduction

HP OXPd Device Client.....	1-1
Main components of the environment.....	1-3
Installation components.....	1-3
Document workflows.....	1-4
Deployment summary.....	1-6
Custom configuration.....	1-7
Modifying the default configuration.....	1-7
Customizing HP OXPd Device Client.....	1-7
Related documentation.....	1-7

Section 2: Requirements

Supported devices.....	2-1
Server requirements.....	2-3
Installation requirements.....	2-3
Requirements for HTTPs protocol communication.....	2-3
Deployment requirements.....	2-4

Section 3: Installation

Downloading HP OXPd Device Client v1.4 update.....	3-1
Installing HP OXPd Device Client v1.4 update.....	3-1
Installing HP OXPd Device Client v1.4.....	3-3
Installing HP OXPd Device Client on a remote system.....	3-6
Required DCOM permissions.....	3-7
Uninstalling HP OXPd Device Client.....	3-8

Section 4: Required configuration

Enabling ASP.NET.....	4-1
Installing HP OXPd Device Client on the device.....	4-1
Adding device using Omtool Server Administrator.....	4-1
Pushing HP OXPd Device Client on the device using the Omtool Server Administrator.....	4-4
Configuring authentication.....	4-4
Choosing an authentication method.....	4-4
Configuring LDAP Authentication.....	4-5
Configuring authentication on the device.....	4-6
Configuring authentication for when AccuRoute Intelligent Device Client is remote.....	4-8

Section 5: Required configuration on the server

Creating a rule for Scan to Folder feature.....	5-2
-------------------------------------------------	-----

Section 6: Testing

Testing the Routing Sheet feature.....	6-1
Testing the Public Distributions feature.....	6-3
Testing the Personal Distribution feature.....	6-5
Testing the MyAccuRoute feature.....	6-7
Testing the Fax feature.....	6-9
Testing the Scan to Folder feature.....	6-13

Section 7: Troubleshooting

Detecting workflow issues.....	7-1
Troubleshooting the delivery mechanism.....	7-2
Troubleshooting the message on the Omtool Server.....	7-2
Troubleshooting the HP OXPd Device Client.....	7-4
Troubleshooting the Web server.....	7-4
Troubleshooting the multifunction device.....	7-4
Troubleshooting changes to the configuration.xml file.....	7-5
Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices (Omttool ISAPI Web Server Extension) in a cluster environment.....	7-5
Troubleshooting issues where the AccuRoute Server cannot decipher the Embedded Directive instructions in a Routing Sheet.....	7-6
Troubleshooting problems associated with applying all additional scan attributes.....	7-6

Appendix: Optional configuration

Enabling one touch scan capability.....	8-1
Enabling one touch scan.....	8-2
Setting the priority order of the AccuRoute buttons.....	8-3
Configuring the default scan properties.....	8-5
Overriding recipient properties using wizard pages.....	8-7
Override delivery format in the AccuRoute Server.....	8-7
Setting up Embedded AccuRoute for Intelligent Devices (Omttool ISAPI Web Server Extension) in a cluster.....	8-8
Enabling Batch Scanning.....	8-8
Configuring use of AddressBook service for LDAP lookups.....	8-9
Configuring prompts.....	8-10
Configuring multiple domains.....	8-12
Configuring multiple search nodes.....	8-13
Configuring User PIN.....	8-14
Configuring PIN with Password (for any Active Directory field other than employeeID).....	8-15
Configuring server side validation.....	8-16
Configuring an Embedded Directive to appear in top of device listing.....	8-17
Configuring scan settings in Embedded Directives.....	8-17
Configuring device print back feature.....	8-18
Configuring Property Transformations.....	8-18
Configuring device to use Secure Socket Layer (SSL) for communication.....	8-19
Changing the label of print status message.....	8-21

Appendix: Setting up a CA Certificate using Microsoft Certificate Services and enable SSL

Requirements for setting up a CA certificate.....	9-1
Installing the Certificate Services component.....	9-2
Creating a CA certificate request.....	9-5
Requesting the CA certificate.....	9-10

Installing the CA certificate on the Default Web Site.....	9-13
Enabling SSL on OmtoolDXPWebApp and OmtoolWebAPI.....	9-16
Instructions for setting the device to use SSL.....	9-17

Section I: Introduction

This guide contains instructions on deploying HP OXPd Device Client to multifunction devices running OXP SDK v1.4.8.0. It is written for systems administrators with detailed knowledge of the AccuRoute® Server and the HP device.

This section includes:

[HP OXPd Device Client](#) (I-1)

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

[Installation components](#) (I-3)

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

[Deployment summary](#) (I-6)

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

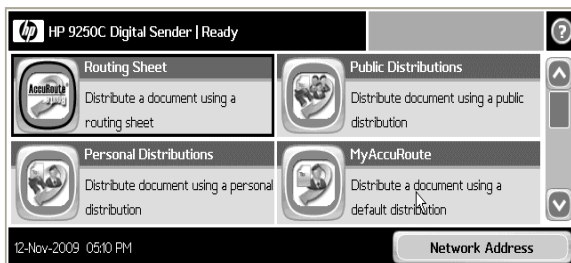
HP OXPd Device Client

HP OXPd Device Client brings the versatile document routing capabilities of AccuRoute to supported HP devices running OXP SDK library v1.4.x. These capabilities are founded on Omtool's Embedded Directive technology.

HP OXPd Device Client runs on OXP (Open Extensibility platform), an ASP.NET layer sitting between the HP device and the AccuRoute Server. It communicates between the OXP SDK installed on the HP device and the AccuRoute Server via the Embedded AccuRoute for Intelligent devices application.

In the main menu, HP OXPd Device Client presents the device user with several AccuRoute scanning features.

Figure I-A AccuRoute scanning features on the HP device running HP OXPd Device Client



The display panel on the HP device shows AccuRoute scanning features.

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

Table I-A AccuRoute scanning features in HP OXPd Device Client

Feature	Description	Login required	Notes
Public Distributions	The user selects Public Distributions and then selects a public distribution option, or Embedded Directive. The device scans and delivers the document to the AccuRoute Server via HTTP / HTTPs protocol. The server decodes the Embedded Directives 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.
Personal Distributions	The user selects Personal Distributions, logs in to the device, and selects a personal distribution option, or Embedded Directive. The device scans and delivers the document to the AccuRoute Server via HTTP / HTTPs protocol. The server decodes the Embedded Directives and distributes the document to the intended recipient.	Yes	
MyAccuRoute	The user selects MyAccuRoute 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 using the device user's personal MyAccuRoute directive and distributed to the intended recipients. Or the scanned document is emailed to the sender (the default).	Yes	MyAccuRoute is an advanced feature of AccuRoute Desktop/AccuRoute Web Client. It enables the server to process all AccuRoute messages from the same user with the same Embedded Directive. For more information on this feature, consult the AccuRoute Desktop installation guide. Go to Related documentation on I-7.
Routing Sheet	The user selects Routing Sheet. The device scans and delivers the document to the AccuRoute Server via HTTP / HTTPs protocol. The AccuRoute Server then decodes the Embedded Directive and distributes the document to the intended recipients.	No	
Scan to Folder	The device scans and delivers the document to the AccuRoute folder via HTTP / HTTPs protocol. The AccuRoute Server picks up the scanned document from the network folder, processes it and delivers it to the intended folder.	No	
Fax	This option allows the user to do 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	

Main components of the environment

The HP OXPd Device Client environment consists of the following components listed below.

- **AccuRoute Server** - AccuRoute v3.01
The AccuRoute Server is the main back end server for processing and routing documents. For instructions on installing AccuRoute Server, consult the Installation guide.
-
- Note* AccuRoute v3.01 installs the AccuRoute Intelligent Device Client v2.1.1 as part of the server install. No separate installation of this component is required.
-
- **HP OXPd Device Client**- The instructions for installing HP OXPd Device Client are in this guide.
 - **HP Device** - For a list of supported devices with minimum firmware requirements, go to [Supported devices](#) (2-1)

Installation components

The HP OXPd Device Client setup includes multiple components that are detailed in the following table.

Table I-B Description of installation components with locations and functions

Component	Location	Function
HP OXPd Device Client	network folder where you downloaded the setup files.	The setup contains the setup.exe file. Use this file to install the HP OXPd Device Client v1/4.
HP OXPd Device Client Configuration file	...\Program Files\omtool\HPOXP\Configuration\configuration.xml	This XML file is installed in system running the HP OXPd Device Client. This file supplies the configuration data to the device. It is configured automatically by the setup.

Document workflows

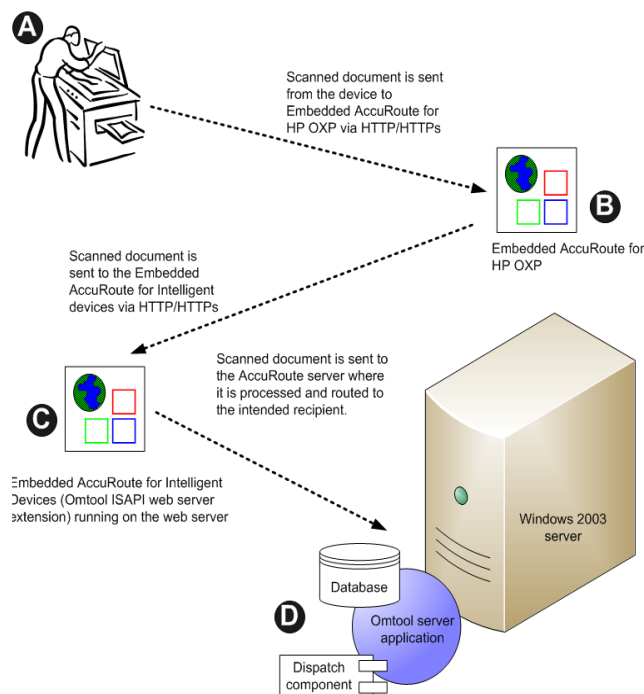
The workflow that moves a document from the device to its final destination involves the user, the device, the HP OXPd Device Client, Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension), and the Omtool Server. An understanding of this workflow can be helpful in troubleshooting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

In its most basic workflow, when a device user scans a document, the device submits the document to HP OXPd Device Client via HTTP / HTTPS protocol. The HP OXPd Device Client then routes the document to the AccuRoute Server via HTTP / HTTPS protocol. The Dispatch component applies rules to the message and AccuRoute Server processes the message and routes them to the intended recipients.

The following workflow applies to the features Fax, Routing Sheet, Routing Sheet with Scan More, Scan to Folder, Scan to Folder with Scan More, MyAccuRoute and MyAccuRoute with Scan More.

Important For MyAccuRoute and MyAccuRoute with Scan More features, the device user must authenticate himself at the device using the configured authentication type. See [Configuring authentication \(4-4\)](#) for more information on authentication.

Figure I-B Workflow for Fax, Routing Sheet, Routing Sheet with Scan More, Scan to Folder, Scan to Folder with Scan More, MyAccuRoute and MyAccuRoute with Scan More



A- The user selects an AccuRoute scanning feature and scans a document. **B-** The device delivers the document to HP OXPd Device Client via HTTP/HTTPS protocol. **C-** HP OXPd Device Client sends the document to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension)

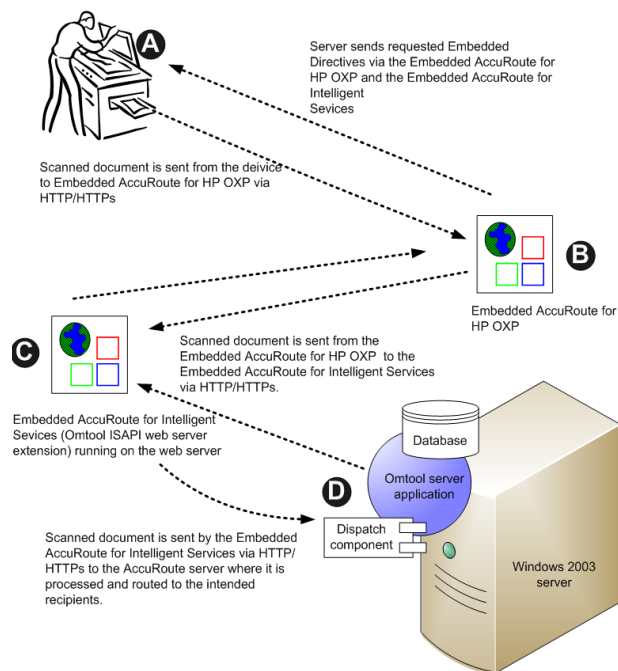
via HTTP/HTTPs protocol which in turn routes the document to the AccuRoute Server. **D** - The Dispatch component applies rules to the message, and the server processes the message accordingly.

For Public and Personal Distributions when a user begins a scan session, the device requests the HP OXPd Device Client to retrieve Embedded Directives.

Note For Personal Distributions, the device user must authenticate himself at the device using the configured authentication type. See [Configuring authentication \(4-4\)](#) for more information on authentication.

The HP OXPd Device Client then submits a request to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) which retrieves the data from the Omtool Server and supplies it to the HP OXPd Device Client. As soon as the HP OXPd Device Client returns the data to the device, the basic workflow resumes.

Figure I-C Workflow for Personal Distributions and Public Distributions



A- The user selects Personal or Public Distribution feature. (If the user chooses Personal Distribution, he logs into the device.) The device requests the list of Embedded Directives from the server. The AccuRoute Server returns the requested data. User selects an Embedded Directive from the list and scans document. **B** - Device delivers the document to the HP OXPd Device Client via HTTP or HTTPs protocol. **C**- HP OXPd Device Client sends the document to Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) via HTTP/HTTPs protocol which in turn routes the document to the AccuRoute Server. **D** - The Dispatch component applies rules to the message, and the server processes the message accordingly.

Deployment summary

To deploy HP OXPd Device Client:

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

Note If you are planning to use HTTPs protocol, you must create a CA certificate before installing HP OXPd Device Client.

- 2 Install HP OXPd Device Client on the Web server. ([Section 3: Installation](#))
- 3 Configure the embedded Web server of the device. ([Section 4: Required configuration](#))
- 4 Configure the Omtool Server. ([Section 5: Required configuration on the server](#))
- 5 Configure optional capabilities. [Appendix: Optional configuration](#)
- 6 Test the AccuRoute scanning features on the device. ([Section 6: Testing](#))
- 7 Troubleshoot the setup if necessary. ([Section 7: Troubleshooting](#))

Custom configuration

By default, HP OXPd Device Client supports one HP OXPd Device Client configuration. You can modify or customize it to support multiple configurations.

Modifying the default configuration

The default configuration is created by the HP OXPd Device Client setup.

- To change the default configuration after HP OXPd Device Client has been deployed, reinstall HP OXPd Device Client:**
- 1 Remove HP OXPd Device Client from the Web server. (Go to [Uninstalling HP OXPd Device Client](#) on 3-8.)
 - 2 Run the HP OXPd Device Client setup again using the desired values. (Go to [Section 3: Installation](#).)
 - 3 Configure the device. (Go to [Section 4: Required configuration](#).)

Customizing HP OXPd Device Client

HP OXPd Device Client can be customized to:

- Run a unique configuration on each device or groups of devices.
Groups can be set up with assistance from Omttool consulting services. To set up groups, contact [Omttool Sales](#).
- Use custom values for button names and icons, the number of Embedded Directives displayed on the device.
- Override native settings on the device.

For information and ideas on how you can customize HP OXPd Device Client, contact [Omttool Sales](#).

Related documentation

- HP OXPd Device Client Quick Start Guides - <http://www.omttool.com/documentation/AccuRouteDeviceIntegration/HPOXP/EmbeddedAccuRouteforHPOXPV1.4QuickStartGuide.pdf>.
- AccuRoute v 3.01 documentation - A complete list of related documentation is available online at: <http://www.omttool.com/documentation/accuroute/v3.01/documentation.htm>.

Section 2: Requirements

This section includes:

- [Supported devices](#) (2-1)
- [Server requirements](#) (2-3)
- [Installation requirements](#) (2-3)
- [Requirements for HTTPs protocol communication](#) (2-3)
- [Deployment requirements](#) (2-4)

Supported devices

Omtool qualified HP OXPd Device Client in the following configurations.

Table 2-A List of devices supported with HP OXPd Device Client v1.4

Device model	Supported firmware version	Supported minimum installed RAM
LJ P3005 series	02.043.1	80 MB
LJ P3015 series	02.043.1	128 MB
LJ M3035mfp series	48.101.4	256 MB
LJ CP3505	03.022.1	384 MB
CLJ CP3525	05.059.3	256 MB
CLJ CM3530	53.031.4	512 MB
LJ P4014	04.049.3	128 MB
LJ P4015	04.049.3	128 MB
LJ 4345mfp series	09.151.3	256 MB
LJ M4345mfp	48.101.4	256 MB
LJ M4349mfp	48.101.4	256 MB
LJ P4515	04.049.3	128 MB
CLJ 4730mfp series	46.231.3	256 MB
CLJ CM4730mfp series	50.081.3	384 MB
LJ M5035mfp series	48.101.4	256 MB
LJ CP6015 series	04.046.1	512 MB
CLJ CM6030mfp series	52.051.3	512 MB

Table 2-A List of devices supported with HP OXPd Device Client v1.4

Device model	Supported firmware version	Supported minimum installed RAM
CLJ CM6040mfp series	52.051.3	512 MB
CLJ CM6049mfp series	52.051.3	512 MB
LJ 9040mfp series	08.141.3	256 MB
LJ 9050mfp series	08.141.3	256 MB
LJ M9040mfp series	51.051.4	384 MB
LJ M9050mfp series	51.051.4	384 MB
LJ M9059mfp series	51.051.4	384 MB
DS 9200c	09.151.3	256 MB
DS 9250C	48.091.3	256 MB
CLJ 9500mfp series	08.141.3	512 MB

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.

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

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 HP OXPd Device Client.

The following table lists the HP devices that were tested in the Omtool laboratory to qualify HP OXPd Device Client v1.4. For each device, the device firmware versions used are listed as well.

Table 2-B HP OXPd Device Client v1.4 for OXP SDK v1.4.8.0 device firmware matrix

Device group	Device model	Firmware version
Group 10	HP LaserJet 4730 mfp	46.231.3
Group 20	HP LaserJet M4345	48.101.4
Group 30	HP Color LaserJet CM8060	75.020.0
Group 40	HP Color LaserJet CM6040	52.051.3
Group 50	HP Color LaserJet CM3530	53.031.4

Server requirements

HP OXPd Device Client requires:

- AccuRoute v3.01 (must be fax-enabled to support fax-based features)
- ASP.NET 3.0
- Microsoft Visual C++ 2005 redistributable package available in <http://www.microsoft.com/Downloads/details.aspx?FamilyID=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en>

Installation requirements

The installation procedure requires:

- Unique e-mail address for the Public Distributions feature

Note When HP OXPd Device Client is installed without the Public Distributions option, this requirement does not apply.

- Filescan connector for the Scan to Folder feature

Note When HP OXPd Device Client is installed without the Scan to Folder option, this requirement does not apply.

Requirements for HTTPs protocol communication

In order to use HTTPs protocol communication when sending documents from the device to the Accuroute server, you must create a CA Certificate using Microsoft Certificate Services and enable SSL. You must create this certificate before installing HP OXPd Device Client . For instructions on how to create the certificate and enable SSL, see [Setting up a CA Certificate using Microsoft Certificate Services and enable SSL \(9-1\)](#)

Deployment requirements

Additional requirements for deployment:

- Public Distributions feature** - The user account associated with this feature must be able to create Embedded Directives. This requires access to AccuRoute Desktop or to AccuRoute Web Client (where the user can create the Embedded Directives and Routing Sheets).
- Personal Distributions feature** - The device user must be able to create Embedded Directives. This requires access to AccuRoute Desktop or to AccuRoute Web Client (where the user can create the Embedded Directives and Routing Sheets).
- MyAccuRoute feature** - This requires access to AccuRoute Desktop or to AccuRoute Web Client (where the user can create the Embedded Directives and Routing Sheets).

Additionally, MyAccuRoute must be configured in the AccuRoute Desktop / AccuRoute Web Client and on the server. To access the AccuRoute Desktop documentation, consult the [AccuRoute v3.01 documentation page](#) and find the relevant sections in that page.

- Routing Sheet feature** - The device user must be able to generate Routing Sheets. This requires access to AccuRoute Desktop or to AccuRoute Web Client (where the user can create the Routing Sheets).
- Scan to Folder feature** - There are no special deployment requirements for this feature.
- Fax features** - There are no special deployment requirements for this feature.

Section 3: Installation

This section includes:

[Downloading HP OXPd Device Client v1.4 update](#) (3-1)

[Installing HP OXPd Device Client v1.4 update](#) (3-1)

[Installing HP OXPd Device Client on a remote system](#) (3-6)

[Uninstalling HP OXPd Device Client](#) (3-8)

Complete these procedures in the order they appear.

Downloading HP OXPd Device Client v1.4 update

Before you can download the setup kit, contact Customer Service and obtain a special login code to download the update.

Note Customer Service at Omtool will issue you the special login code after verifying that purchase is complete.

To download HP OXPd Device Client setup

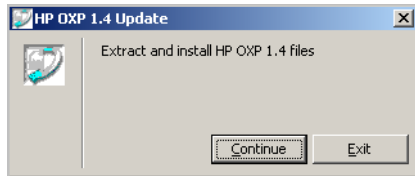
- 1 Go to <http://www.omtool.com/support>.
- 2 Log in using the special login code you obtained from Customer Service.
- 3 Locate the module in the **DOWNLOADS & DOCS** section.
- 4 Download the module and save it to a local drive.
- 5 Extract the files to a location on your AccuRoute Server.
- 6 Continue to [Installing HP OXPd Device Client v1.4 update](#).

Installing HP OXPd Device Client v1.4 update

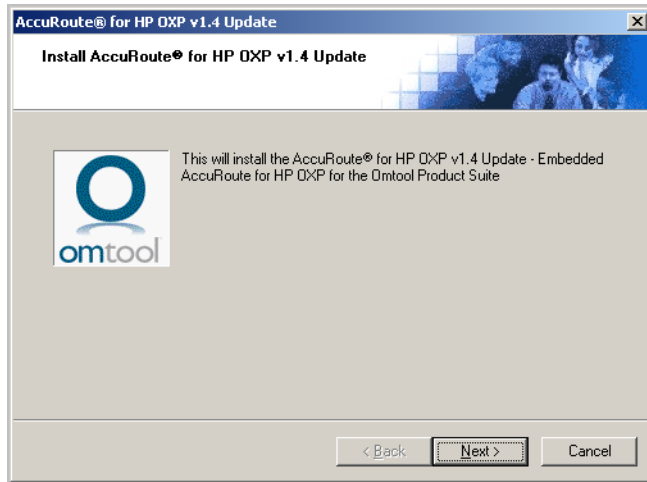
To install HP OXPd Device Client v1.4 update:

- 1 Logon to the system running the AccuRoute Server using an account that belongs to the local Administrators group.
- 2 Navigate to the folder where you saved the module and run **OMARSHPOXPI.4.EXE**.

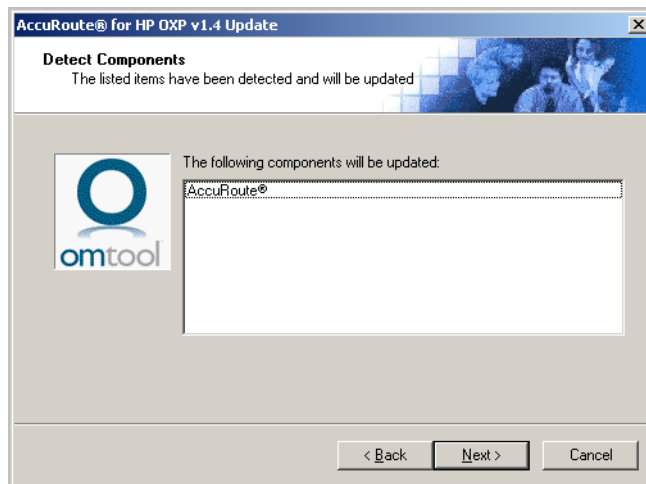
The InstallShield wizard opens the HP OXP 1.4 Update page prompting you to extract and install the files.



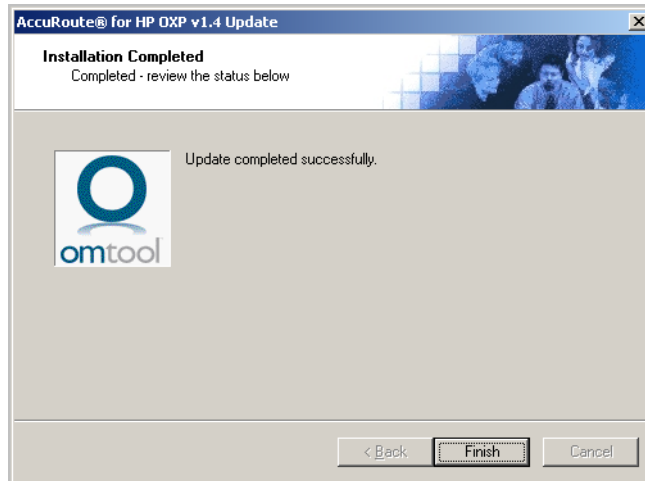
- 3 Click **CONTINUE**. The InstallShield wizard extracts the files and shows the Welcome message.



- 4 Click **NEXT**. The **Detect Components** page lists the components that will be updated.



- 5 Click **NEXT** to apply the update. When complete, you will see the **Installation Completed** message.



- 6 Click **FINISH** to close the wizard.

Installing HP OXPd Device Client v1.4

To install HP OXPd Device Client v1.4:

- 1 Logon to the system running the AccuRoute Server using an account that belongs to the local Administrators group.
- 2 Navigate to the folder **C:\PROGRAM FILES\OMTOOL\OMTOOL SERVER\CLIENTS\HPOXP** and run **SETUP.EXE**.

The InstallShield wizard configures your system for installation and shows the **Welcome** message.



3 Click **NEXT**. The **HP OXP Configuration** page opens.

4 In the **ACCURROUTE** text box, enter the AccuRoute Server name or the IP Address.

5 In the **AUTHENTICATION** text box, enter the Active Directory server name or its IP Address.

6 In the **DEFAULT DOMAIN** text box, enter domain to which the system belongs.

7 In the **Authentication Type** section, select the method by which device users should authenticate themselves. The device displays a login page depends on the type of authentication you select.

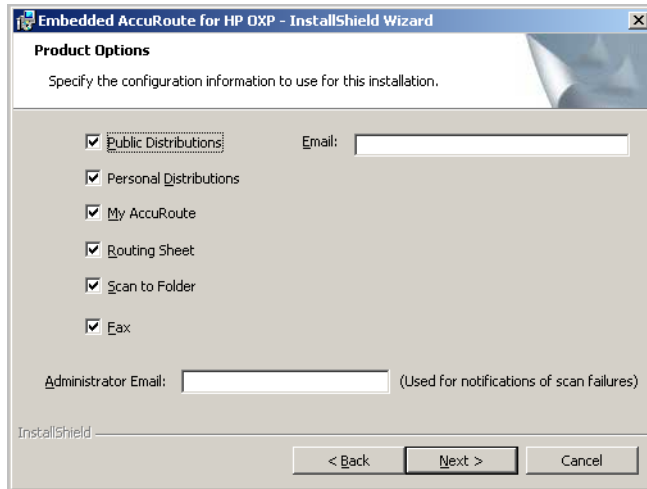
- If you choose **NON-AUTHENTICATED EMAIL**, the device displays an email textbox. To login, enter a valid email address that was created in Active Directory.
- If you choose **PIN**, the device displays a PIN text box to login to use AccuRoute features.

Note PIN refers an attribute of the Active Directory and it can be changed to point to any other Active Directory field by modifying the configuration.xml file.

- If you choose **PIN WITH PASSWORD**, the device displays the **PIN** and the **PASSWORD** text boxes. Device users have to enter a PIN and the corresponding password as defined in Active Directory.
- If you choose **LOGIN WITH PASSWORD**, the device displays text boxes for a username and password as defined in the Active Directory.

8 In the Filing Protocol section, select from **HTTP** (the default) or **HTTPS**.

9 Click **Next**. The **Product Options** page opens.



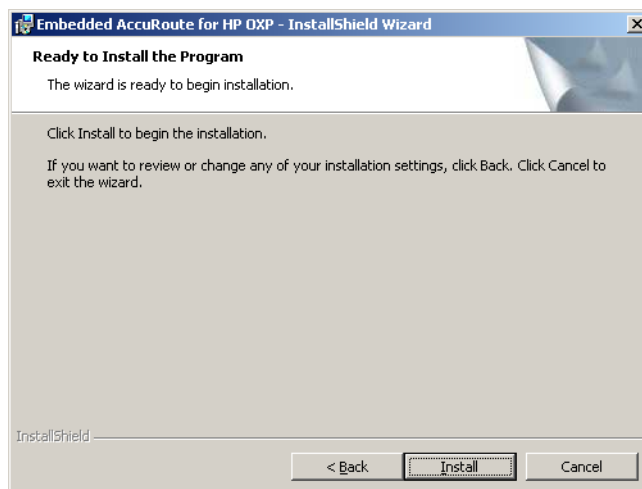
All the product options are selected by default.

10 If you do not want to install any option, un-check the check box beside that option.

If you select the **Public Distributions** option, you must specify an email address. All Embedded Directives for this user are listed under Public Distribution options. If you do not specify the email address, InstallShield Wizard will not let you progress with the installation.

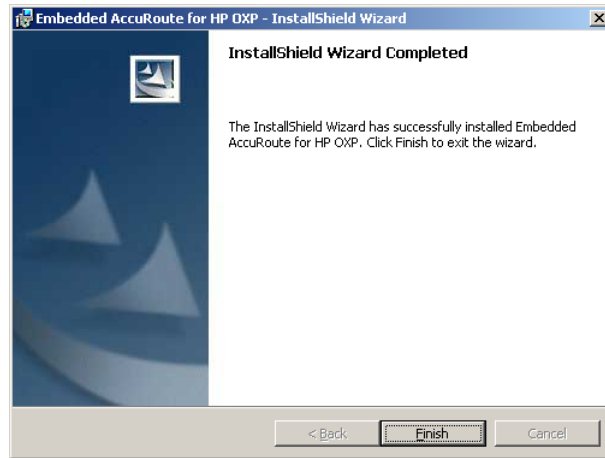
11 In the **ADMINISTRATOR EMAIL** text box, enter the email address of the person who should be notified in case the documents scanned do not get delivered or fail for some reason.

12 Click **NEXT**. The **Ready to Install the Program** page opens.



13 Click **INSTALL** to begin installation. The setup installs HP OXPd Device Client.

When installation is complete, the InstallShield Wizard shows a message indicating that the installation is complete.



- 14 Click **FINISH**.
- 15 Continue to [Required configuration \(4-1\)](#).

Installing HP OXPd Device Client on a remote system

To install HP OXPd Device Client on a remote system:

- 1 Logon to the system where you want to install HP OXPd Device Client using an account that belongs to the local Administrators group.

Note The system must be running Windows 2008, 2003 64 bit and must have Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) installed.

- 2 Navigate to the \\[**ACCURROUTE SERVER**]\GENIFAX\CLIENTS\HPOXP directory and run **SETUP.EXE**.

The InstallShield wizard opens and configures your system for installation and shows the **Welcome** message.



- 3 Follow the instructions in [Installing HP OXPd Device Client v1.4 update](#) (3-1) to complete the remote installation.
- 4 Continue to [Required DCOM permissions](#) (3-7)

Required DCOM permissions

When you install HP OXPd Device Client on a remote system, you must configure the following DCOM permissions on the AccuRoute Server. Without this configuration, the AccuRoute Server cannot communicate with the remote clients.

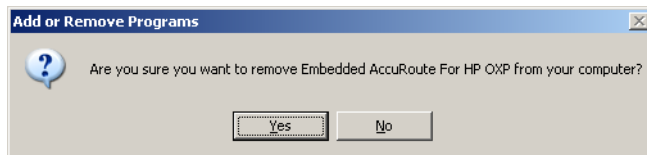
To configure DCOM permissions:

- 1 Logon to the AccuRoute Server using an account that belongs to the local Administrators group.
- 1 Click **START > RUN**.
- 2 Enter `dcomcnfg`. Press **OK**.
The **Component Services** console opens.
- 3 Expand **COMPONENT SERVICES > COMPUTERS > MYCOMPUTER**.
- 4 Select **PROPERTIES** to open the **Properties** page.
- 5 Click **COM SECURITY**.
- 6 Under **Access Permissions**, click **EDIT DEFAULT**.
- 7 Add **Anonymous_Logon** to the list of users and give him full permissions.
- 8 Click **OK** twice to close open dialogs.
- 9 In the left pane, expand **DCOM CONFIG**.
- 10 Browse down to find the application **OmGFAPIServer**.
- 11 Right click the application and select **PROPERTIES** from the drop down menu.

- The **Properties** page opens.
- 12 Click **SECURITY** to open the **Security** page.
 - 13 For all three levels **Launch and activation permissions**, **Access Permissions** and **Configuration Permissions**, click **EDIT**.
 - 14 Add **Anonymous_Logon** to the list of users and give him full permissions.

Uninstalling HP OXPd Device Client

- To uninstall HP OXPd Device Client:**
- 1 Go to the **CONTROL PANEL** and start **ADD OR REMOVE PROGRAMS**.
 - 2 Select **EMBEDDED ACCURROUTE FOR HP OXP** and click **REMOVE**.
You are prompted to confirm that you want to uninstall the software.



- 3 Click **YES**.
HP OXPd Device Client is uninstalled from your system. A progress indicator shows the status of the uninstallation.

Section 4: Required configuration

This section includes:

[Enabling ASP.NET](#) (4-1)

[Installing HP OXPd Device Client on the device](#) (4-1)

[Adding device using Omtool Server Administrator](#) (4-1)

[Pushing HP OXPd Device Client on the device using the Omtool Server Administrator](#) (4-4)

[Configuring authentication](#) (4-4)

Enabling ASP.NET

You must allow ASP.NET in order to view “.asp” pages. By default, the ASP.NET is prohibited.

To allow ASP.NET

- 1 Click **START > ADMINISTRATIVE TOOLS > INTERNET INFORMATION SERVICES (IIS) MANAGER**
- 2 In the left pane of the IIS Manager, expand the local computer and click on **Web Service Extensions**.
The Web Service Extensions page opens listing all Web service extensions, including ASP.NET.
- 3 Select **ASP.NET**.
- 4 Click **ALLOW**.

Installing HP OXPd Device Client on the device

This section includes:

[Adding device using Omtool Server Administrator](#) (4-1)

[Pushing HP OXPd Device Client on the device using the Omtool Server Administrator](#) (4-4)

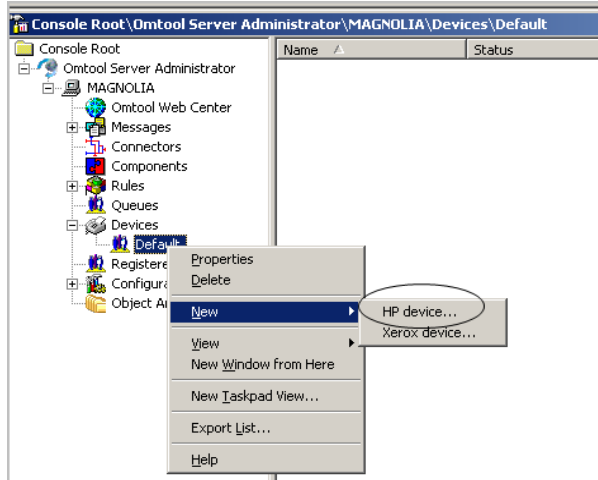
Adding device using Omtool Server Administrator

To add a device using Omtool Server Administrator:

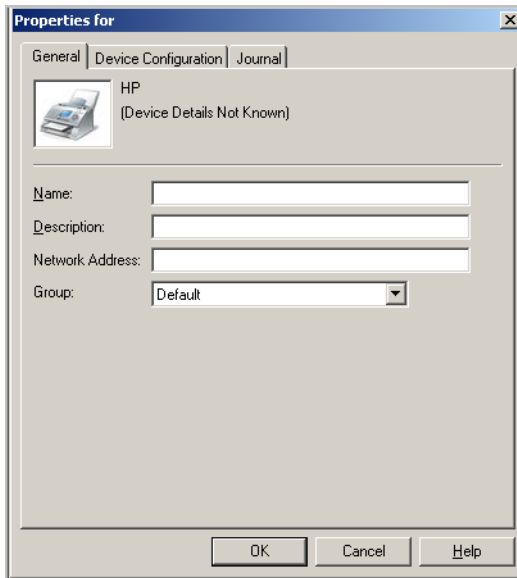
- 1 Click **START > ALL PROGRAMS > OMTPOOL > OMTPOOL SERVER ADMINISTRATOR**.

Section 4: Required configuration

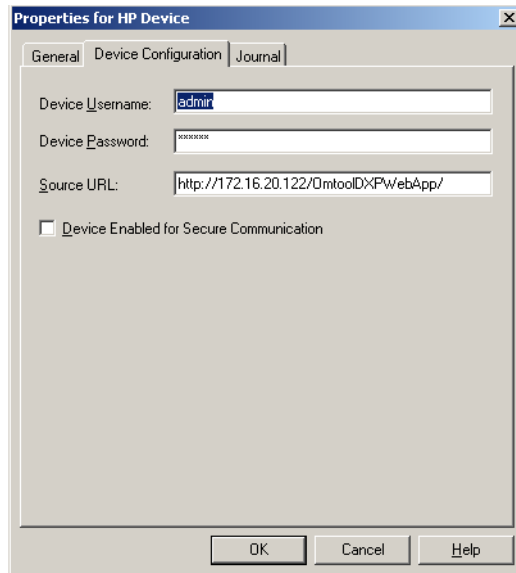
- 2 In the console tree, expand the Omtool Server.
- 3 Go to the **Devices** node.
- 4 Click **DEFAULT > NEW > HP DEVICE**.



The **Properties** for the device page opens.



- 5 In the **NAME** text box, enter a name for the device.
- 6 In the **NETWORK ADDRESS** text box, enter the IP address of the HP device.
- 7 Optionally, in the **DESCRIPTION** text box, enter a description of the device.

8 Click the **Device Configuration** tab.

The screenshot shows a dialog box titled "Properties for HP Device" with three tabs: "General", "Device Configuration", and "Journal". The "Device Configuration" tab is selected. It contains the following fields and options:

- Device Username:** A text box containing the text "admin".
- Device Password:** A text box containing a series of asterisks "*****".
- Source URL:** A text box containing the URL "http://172.16.20.122/OmtoolDXPWebApp/".
- Device Enabled for Secure Communication:** A checkbox that is currently unchecked.

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

9 In the **DEVICE USERNAME** text box, enter the name of the device Administrator. In the **DEVICE PASSWORD** text box, enter password of the Administrator.

The **SOURCE URL** text box is filled in automatically. If you installed HP OXPd Device Client on a remote system, the IP address of that system must be entered manually.

Note If you selected HTTPs protocol (during HP OXPd Device Client installation), edit the source URL and replace http with **https**.

If the device Web server is configured to use HTTPS, check the box beside **DEVICE ENABLED FOR SECURE COMMUNICATION** option. See also, [Configuring device to use Secure Socket Layer \(SSL\) for communication \(8-19\)](#).

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

Pushing HP OXPd Device Client on the device using the Omtool Server Administrator

To install HP OXPd Device Client on the device:

- 1 Click **START > ALL PROGRAMS > OMTOOL > OMTOOL SERVER ADMINISTRATOR**.
- 2 In the console tree, expand the Omtool Server.
- 3 Go to the **Devices** node.
- 4 In the details pane, select the device on which you want to install HP OXPd Device Client.
- 5 Right click and select **INSTALL** from the drop down options.
- 6 The AccuRoute features and configurations are installed on the device. When installation is complete, walk up to the device and verify that the AccuRoute buttons are visible on the screen.

Configuring authentication

This section includes:

[Choosing an authentication method](#) (4-4)

[Configuring LDAP Authentication](#) (4-5)

[Configuring authentication on the device](#) (4-6)

[Configuring authentication for when AccuRoute Intelligent Device Client is remote](#) (4-8)

Choosing an authentication method

The HP OXPd Device Client must be able to authenticate the device user when any of the following features are used:

- Personal Distributions
- MyAccuRoute

You can configure:

- LDAP authentication
- Authentication at the device

Configuring LDAP Authentication

When you choose LDAP Authentication, the user is prompted to enter an e-mail 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 e-mail address. Then the HP OXPd Device Client uses the e-mail address to request information from the Omtool Server, such as a list of the user's personal distributions. When the scan is submitted to the Omtool Server as a message, the e-mail address is used to set the property prOriginator.

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

For information on configuring LDAP Authentication, consult HP documentation: http://ftp.hp.com/pub/printers/mfps/ews_help/help/en/help_LdapAuth2.html

The following figures represent an example of an LDAP Authentication configuration for Active Directory (Go to [Figure 4-A Example of an LDAP Authentication configuration for Active Directory](#) on 4-5.) and the LDAP Authentication settings qualified with Lotus Notes (Go to [Figure 4-B LDAP Authentication configuration qualified with Lotus Notes](#) on 4-5.).

Figure 4-A Example of an LDAP Authentication configuration for Active Directory

The screenshot shows the 'Settings' tab in the HP OXPd Device Client interface, specifically the 'LDAP Authentication' section. The interface is divided into several sections:

- Accessing the LDAP Server:**
 - LDAP Server Bind Method: Simple (dropdown menu)
 - LDAP Server: 172.16.0.185 (text field)
 - Port: 389 (text field)
- Credentials:**
 - Use Device User's Credentials
 - Bind Prefix: cn (text field)
 - Use LDAP Administrator's Credentials
 - LDAP Administrator's DN: (text field)
 - Password: (text field)
- Searching the Database:**
 - Bind and search Root: ou=engineering,cn=users,dc=hp,dc=com (text field)
 - Match the name entered with the LDAP attribute of: cn (text field)
 - Retrieve the device user's email address using attribute of: mail (text field)
 - and name using the attribute of: displayName (text field)

On the left side, there is a navigation menu with options like 'Configure Device', 'E-mail Server', 'Alerts', 'AutoSend', 'Security', 'Authentication Manager', 'LDAP Authentication', 'Kerberos Authentication', 'PIN Authentication', 'Edit Other Links', 'Device Information', 'Language', 'Date & Time', 'Wake Time', and 'Other Links'.

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 e-mail address (mail) and name (displayName).

Figure 4-B LDAP Authentication configuration qualified with Lotus Notes

Section 4: Required configuration

The screenshot shows the 'LDAP Authentication' configuration page. The page is divided into several sections:

- Accessing the LDAP Server:**
 - LDAP Server Bind Method: Simple
 - LDAP Server: 192.168.1.105
 - Port: 389
- Credentials:**
 - Use Device User's Credentials
 - Use LDAP Administrator's Credentials
 - LDAP Administrator's DN: cn=admin
 - Password: [masked]
- Searching the Database:**
 - Bind and search Root: [empty]
 - Match the name entered with the LDAP attribute of: cn
 - Retrieve the device user's email address using attribute of: mail
 - and name using the attribute of: cn

On the left side, there is a navigation menu with options like 'Configure Device', 'E-mail Server', 'Alerts', 'AutoSend', 'Security', 'Authentication Manager', 'LDAP Authentication', 'Kerberos Authentication', 'PIN Authentication', 'Edit Other Links', 'Device Information', 'Language', 'Date & Time', and 'Wake Time'. Below this menu is an 'Other Links' section with links for 'Instant Support', 'Order Supplies', and 'Product Support'.

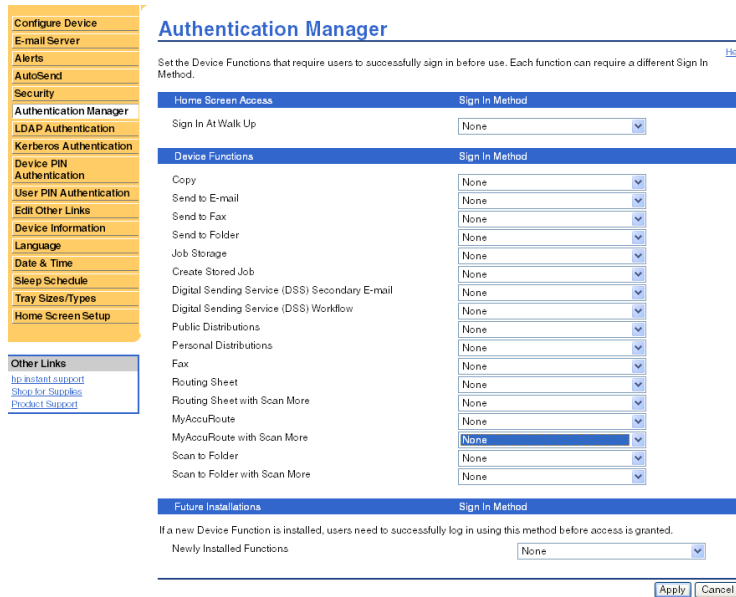
LDAP Authentication binds to the LDAP server with an administrator's common name (CN) and password. The search is conducted using the specified administrator's credentials. The return value is the user's e-mail address (mail) and name (CN).

Configuring authentication on the device

To configure authentication on the device:

- 1 Open a Web browser and enter the IP address of the device.
- 2 Log in to the Embedded Web Server. All options become available.

3 Go the SETTINGS tab and click AUTHENTICATION MANAGER.



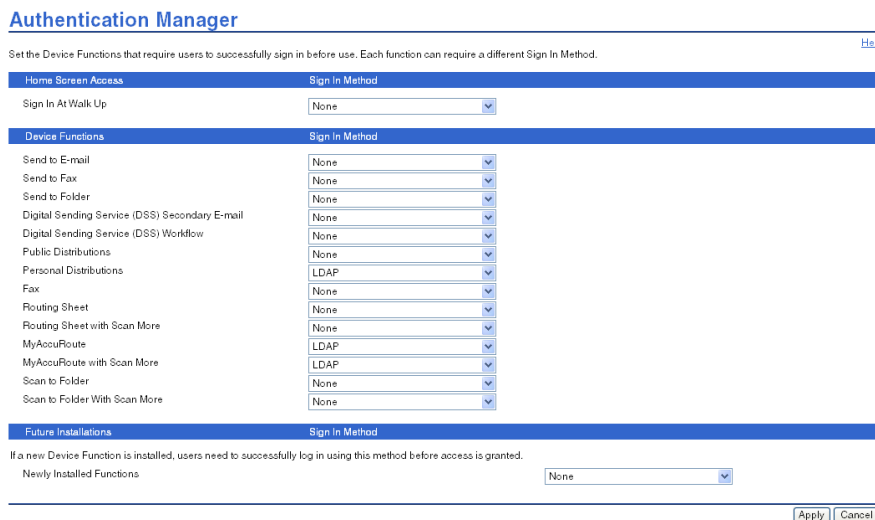
4 Locate the following AccuRoute functions:

- Personal Distributions
- MyAccuRoute
- MyAccuRoute with Scan More

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

5 For each of the features listed above, click on the drop down menu.

6 Select LDAP as the authentication method for each scanning feature that requires user login.



7 Click APPLY.

Configuring authentication for when AccuRoute Intelligent Device Client is remote

For situations when the AccuRoute Intelligent Device Client is remote, configure the UseABService node in the Configuration.xml file so that the HP OXPd Client talks directly to the Active Directory.

This is necessary for both HTTP and HTTPS and for all type of authentication - that is PIN, PIN with password, non-authentication e-mail and Login with password.

To configure authentication for when AccuRoute Intelligent Device Client is remote:

- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Search for the `<Search UseABService` node.
- 4 Verify the value is set as `false`.
- 5 Save your changes to the configuration file.
- 6 Open a command prompt and click **START > RUN**.
- 7 Enter `cmd` and then perform an **iisreset**.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.
- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now, during authentication, HP OXPd Client talks directly to the Active Directory.

Section 5: Required configuration on the server

This section includes:

[Creating a rule for Scan to Folder feature](#) (5-2)

When a message arrives on the Omtool 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. The additional configuration in this section ensures that rules exist for AccuRoute scanning features.

Several AccuRoute scanning features require special rules on the Omtool Server. Most of these rules (are created by default when you install AccuRoute v3.01).

You can if needed create rules based on the AccuRoute scanning features available on devices in your environment. For more information on rules and how to creating them, consult the [Omtool Server Administrator help](#).

When rules have been created for all AccuRoute scanning features available on devices in your environment, the Omtool Server is fully configured for HP OXPd Device Client. Now you are ready to test the AccuRoute scanning features. Go to [Section 6: Testing](#).

Creating a rule for Scan to Folder feature

Note You will need to create this rule only if you are planning to use the Scan to Folder feature.

When a device user selects the Scan to Folder or Scan to Folder with Scan More feature, and scans a document, the HP OXPd Device Client associates the destination e-mail address “FileScan” with the scanned document. This is the unique characteristic you must use to create a rule for this feature.

The routing rule you create must route all outbound messages with the destination e-mail address “FileScan” to a network folder. Other custom actions can be added to the rule.

Note The Scan to Folder feature requires the Filescan connector. The Filescan connector must be added to the Omtool Server before the rule can be created. For more information on the Filescan connector, consult the Administrator help. Go to [Related documentation](#) on I-7.

The device user is able to use Scan to Folder feature only if you create an outbound rule in the AccuRoute Server:

To create a rule for scans using Scan to Folder:

- 1 Start the Administrator.
 - 2 Expand **RULES**, right-click **OUTBOUND** and select **NEW > RULE**. The Create New Rule wizard appears.
 - 3 Set the criteria for this rule:
 - a Click **ADD**, select **DESTINATION IS AN E-MAIL ADDRESS**, and click **NEXT**.
 - b Select **IS**, type [FileScan](#) in the text box. Click **ADD**.
 - c Click **FINISH**. The Create New Rule wizard adds the criteria to the rule.
-
- Note** The value FileScan is not case-sensitive.
-
- d Click **NEXT**.
 - 4 Create the action for this rule:
 - a Click **ADD**, select **ROUTE TO CONNECTOR**. Click **NEXT**.
 - b Select the Filescan connector in the **ROUTE TO CONNECTOR** menu, select a file format for delivered messages in the **DOCUMENT DELIVERY FORMAT** menu.
 - c Go to the override section and select **DESTINATION**. Then enter the location of the destination folder.

UNC format must be used for any folder that is not on the Omtool Server. For example:
\\FileServer\ShareA

A relative path to a local drive is valid if the drive is installed on the Omtool Server. For example:
c:\ScanToFolder
 - d Click **FINISH**. The Create New Rule wizard adds the action to the rule.

This action routes messages to the destination folder in the specified delivery format. Additional actions can be added to achieve a custom routing behavior but none are required.

e Click **NEXT**.

5 Add a failover action if necessary. Click **NEXT**.

The failover action is executed if the primary action fails. For example, the primary action routes messages to a destination folder on FileServer A and the secondary action routes messages to a destination folder on FileServer B. A routing failure can occur if a network issue prevents communication between the Omtool Server and the file server or if the file server is offline.

6 Verify that **STOP PROCESSING OTHER RULES** is selected. Click **FINISH**.

The new outbound rule appears in the details pane.

Section 5: Required configuration on the server

Section 6: Testing

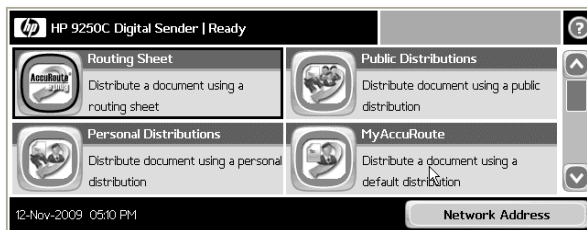
This section includes:

- [Testing the Routing Sheet feature \(6-1\)](#)
- [Testing the Public Distributions feature \(6-3\)](#)
- [Testing the Personal Distribution feature \(6-5\)](#)
- [Testing the MyAccuRoute feature \(6-7\)](#)
- [Testing the Fax feature \(6-9\)](#)
- [Testing the Scan to Folder feature \(6-13\)](#)

Testing the Routing Sheet feature

To test the Routing Sheet feature:

- 1 Create at least one Embedded Directive 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 very front of the document or at the back and go to the device. The main screen looks like this:





- 4 Load the document into the document feeder or place it on the exposure glass. (Use the exposure glass for single page documents only.)
- 5 Press **ROUTING SHEET**. (If this feature is not visible, use the scroll bar to find it.)

The device shows the **Ready to Scan** page.

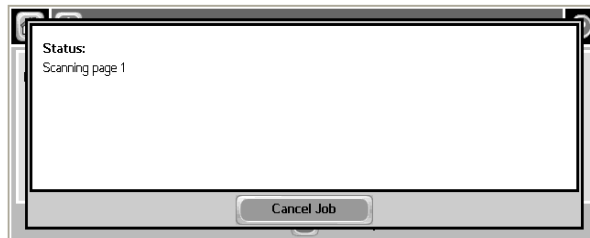


You can do the following:

- a To start the scan job, press  or press **START** on the hard keypad.
 - b 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.
- 6** To begin scanning, press  or press **START** on the hard keypad.

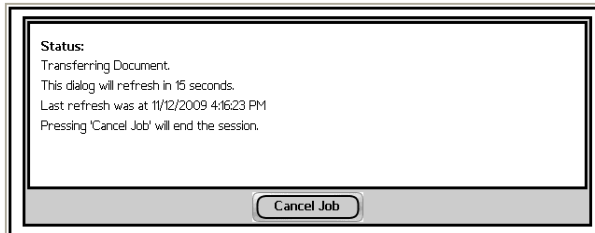
Note If you configure prompts, the **START** hard key pad is not active. For information on configuring prompts, see [Configuring prompts \(8-10\)](#).

The scan job starts. A progress indicator shows the status of the scan job.



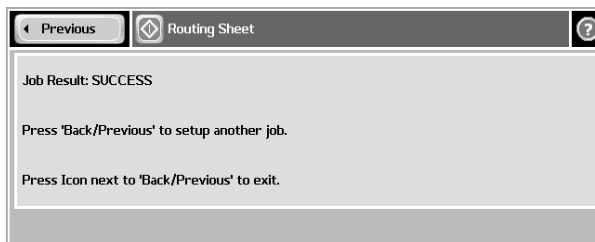
- 7** To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.

The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.



- 8** To scan another document using the Routing Sheet option, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click .

Important If you see that the AccuRoute Server cannot decipher or interpret the Embedded Directive instructions in the Routing Sheet, you must change the device setting from **mixed** to **text**. For instructions, see [Troubleshooting issues where the AccuRoute Server cannot decipher the Embedded Directive instructions in a Routing Sheet \(7-6\)](#)

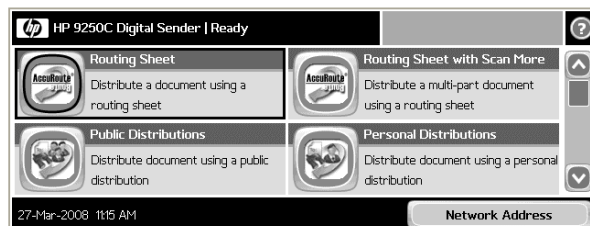
Testing the Public Distributions feature

To test the Public Distributions feature:

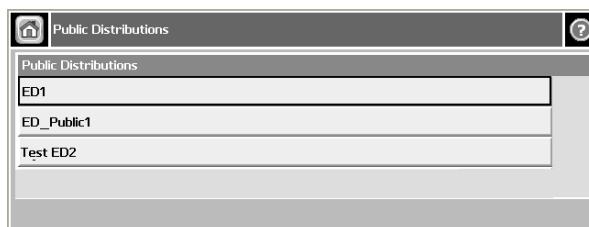
- 1 Create at least one Embedded Directive with the user account that is associated with the Public Distributions feature.

Note The Embedded Directive must allow multiple use. Applications that can create Embedded Directives are AccuRoute Desktop and AccuRoute Web Client applications.

- 2 Assemble a test document and walk up to the device. The main screen looks like this:





- 3 Load the document into the document feeder or place the document on the exposure glass. (Use the exposure glass for single page documents only.)
- 4 Press **PUBLIC DISTRIBUTIONS**. (If this feature is not visible, use the scroll bar to find it.) The device shows public distribution options.



- 5 Press and select a distribution. The device shows the selected distribution.

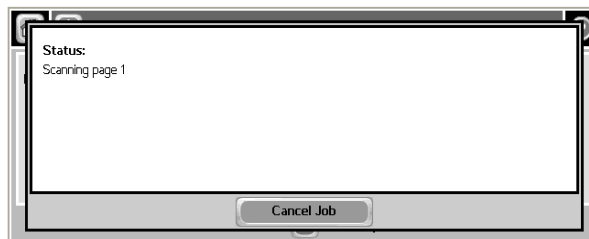


You can do the following:

- a To start the scan job, click press  or press **START** on the hard keypad.
 - b To update the scan settings, click **MORE OPTIONS**. For example, you can specify the page size for the scanned document. The default page size is Letter.
- 6 Click press  or press **START** on the hard keypad.

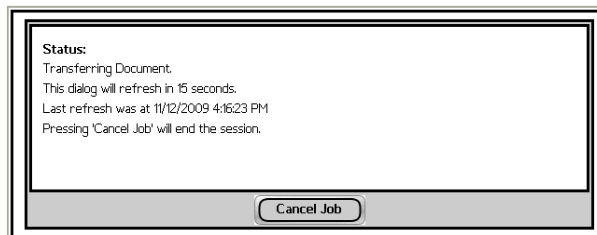
Note If you configure prompts, the **START** hard key pad is not active.

The scan job starts. A progress indicator shows the status of the scan job.



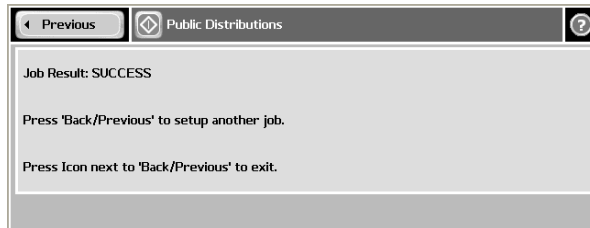
- 7 To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.

The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.



- 8 To scan another document using the Public Distribution option, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click 

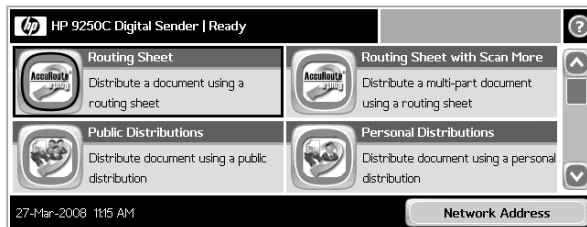
Testing the Personal Distribution feature

To test the Personal Distribution feature:

- 1 Create at least one Embedded Directive with your user account.

Note Applications that can create Embedded Directives are the AccuRoute Desktop and the AccuRoute Web Client application.

- 2 Assemble a test document and go to the device. The main screen looks this:



- 3 Load the document into the document feeder or place the document on the exposure glass. (Use the exposure glass for single page documents only.)
- 4 Press **PERSONAL DISTRIBUTION**. (If this feature is not visible, use the scroll bar to find it.)

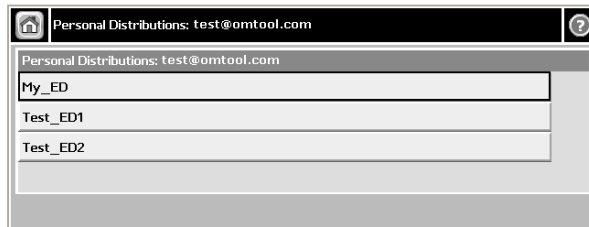
The device prompts you to log in.



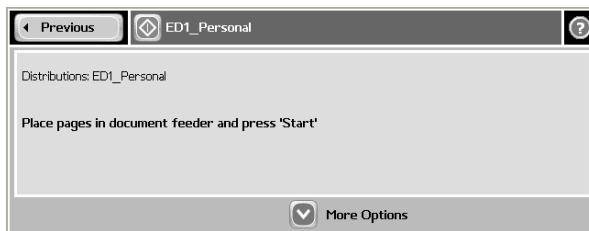
- 5 Login using your LDAP credentials.
 - a Press **USERNAME**. Enter your user name using the keypad that opens. Press **OK** to close the keypad.
 - b Press **PASSWORD**. Enter your password using the keypad that opens. Press **OK** to close the keypad.
 - c Press **OK** to login to the device.

The device shows your personal distribution and subscribed distribution options.



Note Subscribed distributions are Public Distributions of another AccuRoute user to which you are subscribed.



- 6 Press and select a distribution. The device shows the **Ready to Scan** page.



You can do the following:

- a To start the scan job, click press  or press **START** on the hard keypad.
 - b To update the scan settings, click **MORE OPTIONS**. For example, you can specify the page size for the scanned document. The default page size is Letter.
- 7 Press  or press **START** on the hard keypad.

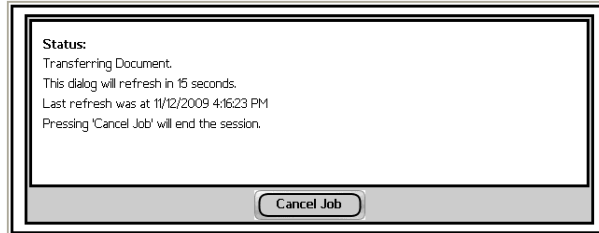
Note If you configure prompts, the **START** hard key pad is not active. For information on configuring prompts, see [Configuring prompts \(8-10\)](#).

The scan job starts. A progress indicator shows the status of the scan job.



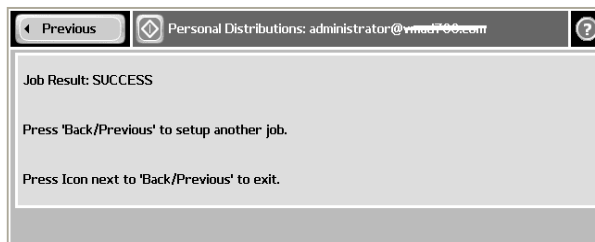
- 8 To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.


The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.

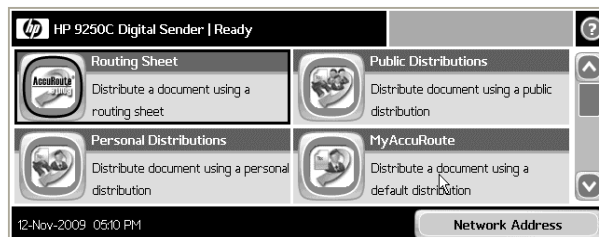


- 9 To scan another document using the Personal Distribution feature, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click 

Testing the MyAccuRoute feature

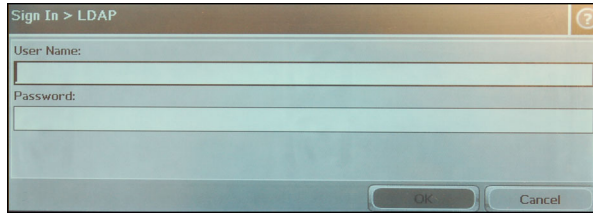
To test the MyAccuRoute feature:

- 1 Verify that MyAccuRoute has been configured for your user account. For more information, consult the AccuRoute Desktop documentation. Go to [Related documentation](#) on I-7.
- 2 Assemble a test document and go to the device. The main screen looks like this:

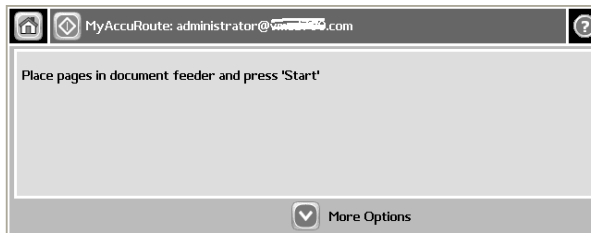


- 3 Load the document into the document feeder or place it on the exposure glass. (Use the exposure glass for single page documents only.)



- 4 Press **MYACCURROUTE**. (If this feature is not visible, use the scroll bar to find it.) The device prompts you to log in.



- 5 Login using your LDAP credentials.
- Press **USERNAME**. Enter your user name using the keypad that opens. Press **OK** to close the keypad.
 - Press **PASSWORD**. Enter your password using the keypad that opens. Press **OK** to close the keypad.
 - Press **OK** to login to the device. The device shows the **Ready to Scan** page.



You can do the following:

- To start the scan job, click press  or press **START** on the hard keypad.
 - To update the scan attributes, click **MORE OPTIONS**. For example, you can specify the page size for the scanned document. The default page size is Letter.
- 6 To begin scanning, press  or press **START** on the hard keypad.

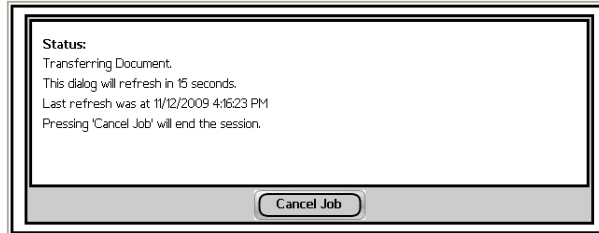
Note If you configure prompts, the **START** hard key pad is not active. For information on configuring prompts, see [Configuring prompts \(8-10\)](#).

The scan job starts. A progress indicator shows the status of the scan job.



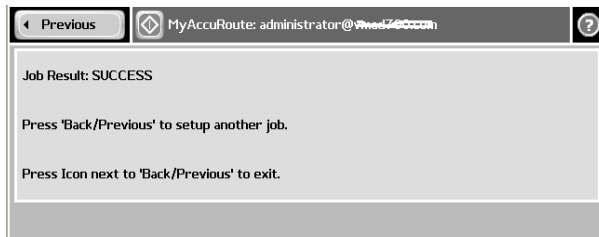
- 7 To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.


The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.

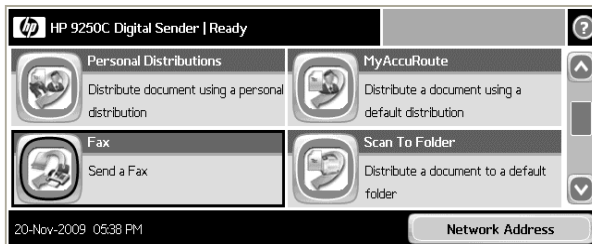


- 8 To scan another document using the MyAccuRoute, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click 

Testing the Fax feature

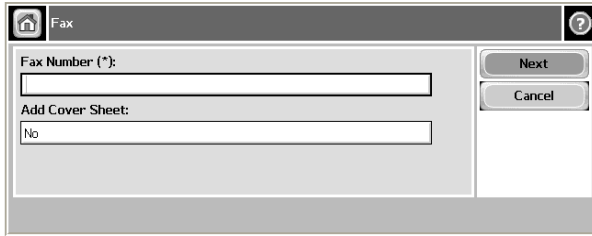
To test the Fax feature:

- 1 Assemble a test document and walk up to the device. The main screen looks like this:



- 2 Load the document into the document feeder or place the document on the exposure glass. (Use the exposure glass for single page documents only.)

- 3 Press **FAX**. (If this feature is not visible, use the scroll bar to find it.) The device prompts you to enter the details about the fax.

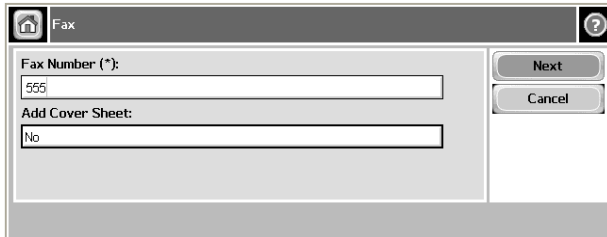


- 4 Press **FAX NUMBER** and enter the fax number from the keypad that opens.

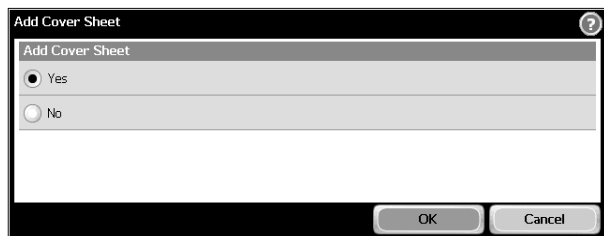


- 5 If you do not want to add the cover page, click **NEXT**. The device shows the **Ready to Scan** message. Go to step 6

If you want to add a cover page press the text box below **ADD COVER SHEET**.The default option is **NO**.



The **Add Cover Sheet** page opens.



Note The cover page information is pulled from the Fax feature button information section in the configuration.xml file.

- a Press **YES** in the **Add Cover Sheet** page. Press **OK** to go back to the **Fax** page.

The screenshot shows a window titled 'Fax'. It has a home icon on the left and a help icon on the right. The main area contains two text input fields: 'Fax Number (*)' with the value '555' and 'Add Cover Sheet:' with the value 'Yes'. To the right of these fields are two buttons: 'Next' and 'Cancel'.

The **Cover Sheet** page opens.

The screenshot shows a window titled 'Cover Sheet'. It has a 'Previous' button on the left and a help icon on the right. The main area contains three text input fields: 'Subject:', 'Sender Name:', and 'Recipient Name:'. To the right of these fields are two buttons: 'Next' and 'Cancel'.

- b Enter the relevant information for Subject, sender and recipient information.

The screenshot shows the 'Cover Sheet' window with the following text entered in the input fields: 'Subject:' contains 'Fax', 'Sender Name:' contains 'Jane Doe', and 'Recipient Name:' contains 'John'. The 'Next' and 'Cancel' buttons are still visible on the right.

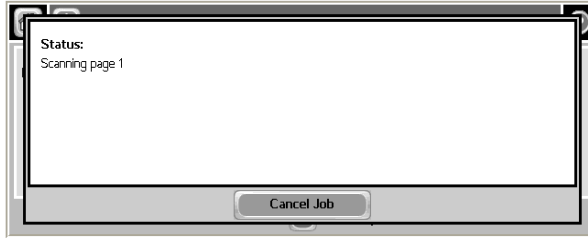
- c Click **NEXT**.

The screenshot shows the 'Fax' window. The 'Fax Number' is now '555'. Below the input fields, there is a text instruction: 'Place pages in document feeder and press 'Start''. At the bottom of the window, there is a 'More Options' button with a downward arrow icon.

- 6 You can do the following:
- a To start the scan job, click press  or press **START** on the hard keypad.
 - b To update the scan attributes, click **MORE OPTIONS**.

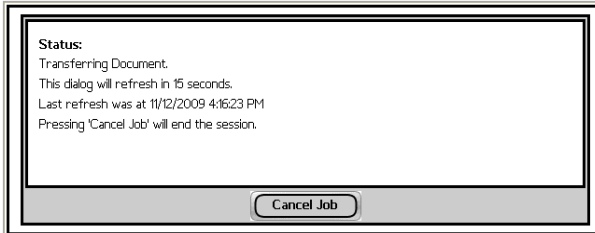
Note If you configure prompts, the **START** hard key pad is not active. For information on configuring prompts, see [Configuring prompts \(8-10\)](#).

The scan job starts. A progress indicator shows the status of the scan job.



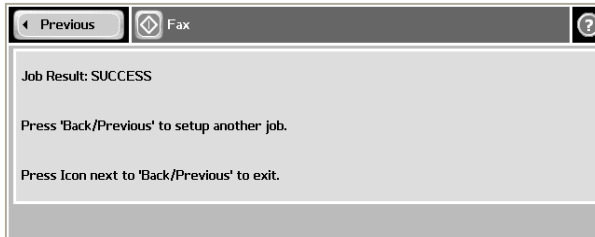
- 7** To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.


The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.

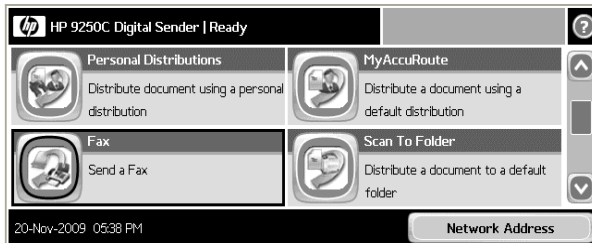


- 8** To scan another document using the Fax feature, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click 

Testing the Scan to Folder feature

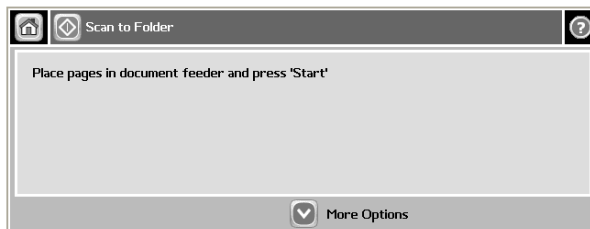
To test the Scan to Folder feature:

- 1 Assemble a test document and go to the device. The main screen looks like this:





- 2 Load the document into the document feeder or place the first page on the exposure glass. (Use the exposure glass for single page documents only.)
- 3 Press **SCAN TO FOLDER**. (If this feature is not visible, use the scroll bar to find it.)

The device shows the **Ready to Scan** page.

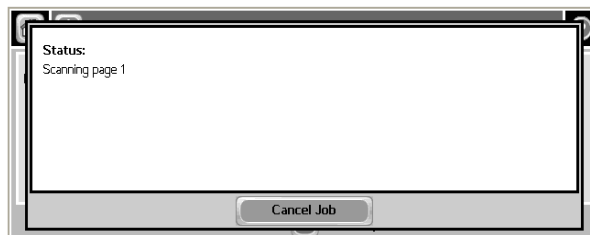


You can do the following:

- a To start the scan job, click press  or press **START** on the hard keypad.
 - b To update the scan attributes, click **MORE OPTIONS**. For example, you can specify the page size for the scanned document. The default page size is Letter.
- 4 Click press  or press **START** on the hard keypad.

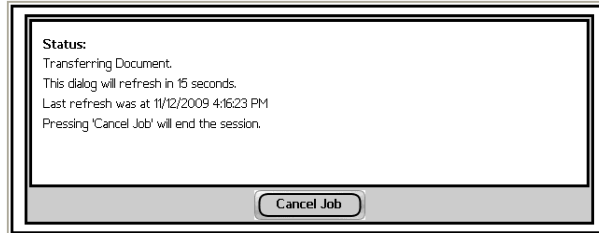
Note If you configure prompts, the **START** hard key pad is not active. For information on configuring prompts, see [Configuring prompts \(8-10\)](#).

The scan job starts. A progress indicator shows the status of the scan job.



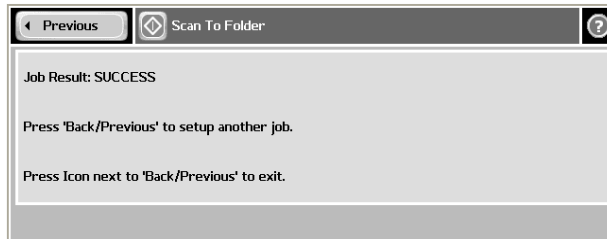
- 5 To stop the scan job, press **CANCEL JOB**. Otherwise wait for the job to finish.

The device shows the message that it is transferring the job to the server.



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

When transfer is complete, you will see the following message. It will tell you if the job was successfully delivered to the Accuroute server or if it failed.



- 6 To scan another document using the Scan to Folder, click **PREVIOUS**. To end the session and go back to the main Accuroute menu, click 

Section 7: Troubleshooting

This section includes:

[Detecting workflow issues \(7-1\)](#)

[Troubleshooting the delivery mechanism \(7-2\)](#)

[Troubleshooting the message on the Omtool Server \(7-2\)](#)

[Troubleshooting the HP OXPd Device Client \(7-4\)](#)

[Troubleshooting the Web server \(7-4\)](#)

[Troubleshooting the multifunction device \(7-4\)](#)

[Troubleshooting changes to the configuration.xml file \(7-5\)](#)

[Troubleshooting permission problems when setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster environment \(7-5\)](#)

[Troubleshooting issues where the AccuRoute Server cannot decipher the Embedded Directive instructions in a Routing Sheet \(7-6\)](#)

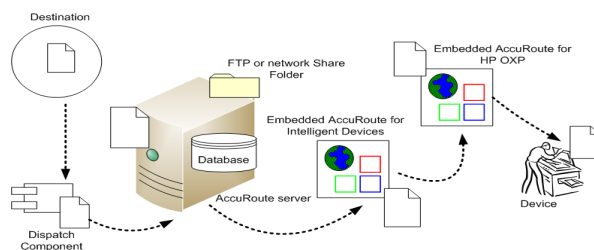
[Troubleshooting problems associated with applying all additional scan attributes \(7-6\)](#)

Complete these procedures in the order they appear. If you cannot resolve the issue, contact [Omtool support](#).

Detecting workflow issues

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

Figure 7-A Troubleshooting the workflow in reverse order



The easiest way to troubleshoot a workflow issue is to follow the document through the workflow in reverse order. 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 HP OXPd Device Client, the Web server, and the device.

To begin troubleshooting, go to [Troubleshooting the delivery mechanism](#) (7-2).

Troubleshooting the delivery mechanism

When the Omtool 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 Omtool Server. Continue to [Troubleshooting the message on the Omtool Server](#).

Troubleshooting the message on the Omtool Server

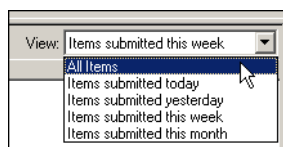
There are two important questions that can be resolved when troubleshooting a message on the Omtool Server:

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

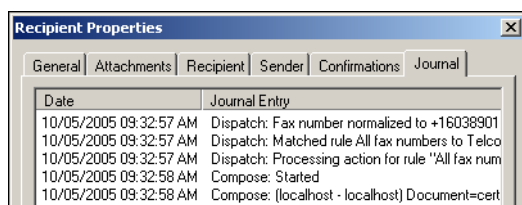
Start troubleshooting by trying to locate the message on the Omtool Server.

To locate the message on the Omtool Server:

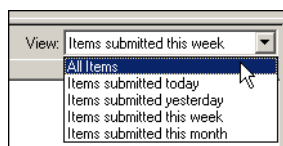
- 1 Start the Administrator.
- 2 Go to **OMTOOL SERVER ADMINISTRATOR > [SERVERNAME] > MESSAGES**.
- 3 Look for the message in the In Process queue:
 - a Click **IN PROCESS**.
 - b View **ALL ITEMS**.



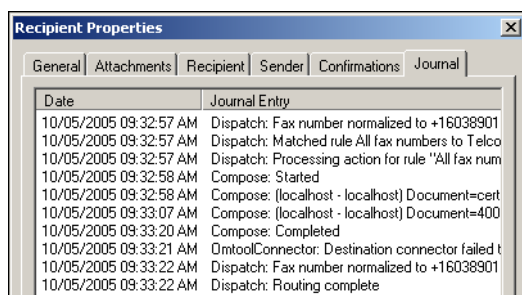
- c Sort all items by the date submitted.
- d Look for the message.
 - **Message found** - View the message journal to determine the current state and status of the message. Then monitor the components and confirm that the message is moving through the processing queues on the Omtool Server. If the Omtool 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 Omtool Server delivered the message but it still has not arrived at its destination, this indicates that the Omtool 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** - Continue to [Troubleshooting the HP OXPd Device Client](#).

Troubleshooting the HP OXPd Device Client

To troubleshoot the HP OXPd Device Client, enable logging.

To enable logging:

- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Go to the <Diagnostics> node pertaining to the device group.

```
<Diagnostics>  
    <!-- Defines whether logging is on or off (0 = off, non-zero =  
on) -->  
    <prDebugLevel>0</prDebugLevel>  
    <prFolderName></prFolderName>  
</Diagnostics>
```
- 4 Change the value from 0 to 1.
- 5 In the <prFolderName> node, enter the path to the debug folder followed by a “\”. (For example, `C:\LogFolder\`)
- 6 Save your changes.
- 7 Restart the World Wide Web Publishing services.
- 8 Go to the embedded Web server settings and load the AccuRoute buttons using the force update option.

Troubleshooting the Web server

The Embedded AccuRoute for Intelligent Devices installation guide has instructions on troubleshooting the Web server. Go to [Related documentation](#) on I-7.

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 changes to the configuration.xml file

Problem:

I made changes to the `configuration.xml` file. But I do not see my changes.

Solution:

When you make any changes to the xml file, you must always do the following so that the changes you make take effect.

- Open `configuration.xml` in a Web browser (for example in Internet Explorer) to validate the xml format.
- Restart the World Wide Web Publishing service so that the changes you make take effect.
- Load the AccuRoute buttons on the device using the force update option. For instructions, see below.
- Enable authentication for the Personal, MyAccuRoute and MyAccuRoute with Scan More features.

Loading the AccuRoute buttons using force update option

If you need to load the AccuRoute buttons immediately, use the **Force Update Now** option.

To load the AccuRoute buttons using the Force Update Now option:

- 1 Open a Web browser and enter the IP address of the device.
- 2 Click **LOGIN** and login to the device using the device administrator name and password.
- 3 Open the **Digital Sending** page.
- 4 Select **OXPD:WORKFLOW** to open the **OXPd:Workflow** page.
- 5 Under the **Force Update** section, click **FORCE UPDATE NOW**.

The device connects to the HP OXPd Device Client and retrieves the configuration data. The OXPd .jar file processes the data and loads the AccuRoute buttons.

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

Problem:

I am having permissions related issues 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. For instructions, see [Setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#)

Troubleshooting issues where the AccuRoute Server cannot decipher the Embedded Directive instructions in a Routing Sheet

Problem:

I am using an HP device to scan a document with a Routing Sheet. The AccuRoute Server cannot decipher the instructions in the Routing Sheet and process the document.

Solution:

You must change the device setting from scanning a Mixed document to scanning a Text document.

To change the device settings in the Embedded Web Server

- 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:

I configured all additional scan attributes together (Darkness, back ground cleanup, contrast, sharpness, Heavy originals). Now when I try to scan a document at the HP device, I get the following message:

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:

You see this message 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.

Appendix A: Optional configuration

This section includes:

- [Enabling one touch scan capability](#) (8-1)
- [Setting the priority order of the AccuRoute buttons](#) (8-3)
- [Configuring the default scan properties](#) (8-5)
- [Overriding recipient properties using wizard pages](#) (8-7)
- [Setting up Embedded AccuRoute for Intelligent Devices \(Omtool ISAPI Web Server Extension\) in a cluster](#) (8-8)
- [Enabling Batch Scanning](#) (8-8)
- [Configuring use of AddressBook service for LDAP lookups](#) (8-9)
- [Configuring prompts](#) (8-10)
- [Configuring multiple domains](#) (8-12)
- [Configuring multiple search nodes](#) (8-13)
- [Configuring User PIN](#) (8-14)
- [Configuring PIN with Password \(for any Active Directory field other than employeeID\)](#) (8-15)
- [Configuring server side validation](#) (8-16)
- [Configuring an Embedded Directive to appear in top of device listing](#) (8-17)
- [Configuring scan settings in Embedded Directives](#) (8-17)
- [Configuring device print back feature](#) (8-18)
- [Configuring Property Transformations](#) (8-18)
- [Changing the label of print status message](#) (8-21)

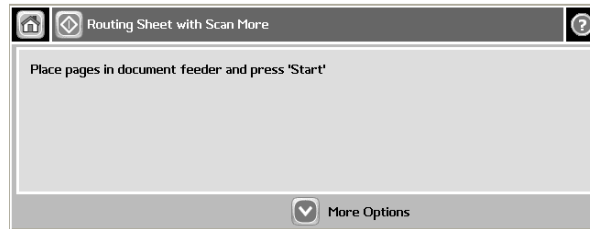
Enabling one touch scan capability

The one touch scan feature allows you to configure the HP OXPd Device Client in such a way that device users who use the Routing Sheet (with Scan More) and Scan to Folder (with Scan More) can start scanning their document as soon as they select the AccuRoute scanning feature.

Note If one touch scan is enabled, the device user is not prompted to start the scan job. This capability is disabled by default.

If one touch scan capability is disabled, you are prompted to begin the scan job.

Appendix:



Note If one touch scan capability is disabled, the device user can configure certain scan attributes using **MORE OPTIONS**. Any changes made to a scan attribute are valid only for the current job.

The device user can make the following attribute changes:

- ▶ **Original Sides** - Allows device users to enable or disable duplex mode.
- ▶ **Resolution** - Allows setting the resolution of the output page.
- ▶ **Color/Black** - Allows the device user to set the preference for generating color or black and white images.
- ▶ **Content Orientation** - Allows device user to set the orientation of the output page.
- ▶ **Original Size** - Allows the device user to set the output page size.
- ▶ **Job Build** - Switch **ON/OFF** the job build mode. If job build mode is **ON**, it allows the user to append more documents.

Enabling one touch scan

If you enable one touch scan, the device user is not prompted to begin the scan job. The job starts automatically.

To enable one touch scan capability:

- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Locate your device group. For example, if you have a Group 20 device, go to the `<Group20>` node.
- 4 Under the `<FeatureSpecific>` node for each feature you want to modify, go to the `<OneTouchEnabled>` node.
- 5 Change the value from `false` to `true`.
- 6 Save the file.
- 7 Restart the World Wide Web Publishing services.

- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Setting the priority order of the AccuRoute buttons

If your environment demands that you change the default order in which the AccuRoute buttons are listed on the device, you can change the priority order of the AccuRoute buttons relative to native HP buttons and other AccuRoute buttons.

To change the priority order:

- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Locate your device group. For example, if you have a Group 20 device, go to the `<Group20>` node.
- 4 Under the `<FeatureSpecific>` node for each feature you want to modify, go to the `<priority>` node.
- 5 Change the priority value. The value must be greater than or equal to zero. Use the information in the tables below to specify an appropriate value for the AccuRoute buttons.

Important An AccuRoute button with lower priority value relative to native HP buttons or other AccuRoute buttons is listed first followed by higher priority AccuRoute buttons.

Table 8-A Homescreen button priorities of HP OXP Group 20, 40 and 50 devices

Homescreen button	Priority value
Copy	10000
Fax	20000
E-mail	30000
Network Folder	50000
Job storage	60000
Supplies status	80000
Administration	90000

Appendix:

Table 8-B Homescreen button priorities of HP OXP Group 10 devices

Homescreen button	Priority value
Copy	10000
Fax	30000
E-mail	20000
Network Folder	50000
Job storage	60000
Supplies status	80000
Administration	90000

Table 8-C Homescreen button priorities of HP OXP Group 30 (Condor) devices

Homescreen button	Priority value
Copy	50
Fax	100
E-mail	150
Network Folder	200
default value	200
Job status	250
Job storage	300
Supplies status	400
Administration	500
Service	1000

- 6** Save the file.
- 7** Restart the World Wide Web Publishing services.

- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Configuring the default scan properties

To configure the default scan properties:

- 1 Log on to the Web server and go to
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Towards the end of the file, search for `<DeviceScanSettings>` and `</DeviceScanSettings>` node.
- 4 Edit the scan properties so they are appropriate for all or most device users. Use the guidelines in [Guidelines on modifying the default scan properties](#) (8-6)
- 5 Save your changes and close the file.
- 6 Restart the World Wide Web Publishing service.

Appendix:

7 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option \(7-5\).T](#)

Table 8-D Guidelines on modifying the default scan properties

Property	Impact	Syntax
JobBuildMode	Determines whether the device user can append scans	Use one of the following values: <ul style="list-style-type: none"> • true to allow the user to append scans • false to prevent the user from appending scans <p>Users must be able to append scans if using “Scan More” features. (These features accommodate documents that are larger than the capacity of the document feeder.)</p>
DuplexMode	Determines whether duplex mode is enabled.	Use one of the following values: <ul style="list-style-type: none"> • true to enable duplex mode • false to disable duplex mode
ResolutionMode	Determines the scanning resolution.	Use one of the following values: <ul style="list-style-type: none"> • 10 for 75dpi • 9 for 150 dpi • 8 for 200dpi • 7 for 300dpi • 6 for 400dpi • 5 for 600dpi
Optimize	Optimizes the scan based on the document composition.	Use one of the following values: <ul style="list-style-type: none"> • 1 for Mixed_0 • 2 for Mixed_1 • 3 for Mixed_2 • 4 for Mixed_3 • 5 for Mixed_4 • 6 for Graphic
ColorMode	Determines whether the scan is saved in color or black and white.	Use of the following values: <ul style="list-style-type: none"> • 1 for black and white (grayscale) • 2 for color
QualityMode	Determines the file size.	Use one of the following values: <ul style="list-style-type: none"> • 0 for small • 1 for standard • 2 for large
Orientation	Determines the page orientation of the output file.	Use one of the following values: <ul style="list-style-type: none"> • 0 for portrait • 1 for landscape

Table 8-D Guidelines on modifying the default scan properties

Property	Impact	Syntax
MediaSize	Describes the size of the media being scanned.	Use one of the following values: <ul style="list-style-type: none"> • 0 for letter (default) • 1 for legal • 13 for B5 • 16 for A5 • 22 for Eight_Point_Five_By_Thirteen • 23 for statement
FileType	Determines the format of the output file.	Use 1 for PDF format.

Overriding recipient properties using wizard pages

The override recipient property feature allows the device administrator to configure properties defined in the `configuration.xml` file which overrides the original recipient properties set on the Accuroute Server. Additionally, it allows the user to provide the template tags either as an overriding property or by itself.

For example, when scanning a document, if the user wants to override the delivered document format, the user can select an alternate document format and send this information to the Accuroute server which in turn overrides the specified document format in the server.

Note The following procedure can only be performed by the Omtool Server Administrator.

Override delivery format in the AccuRoute Server

To enable the sender to override the delivery format

- 1 Go to the Omtool Server and navigate to outbound rules.
- 2 Find all rules that routes message to a connector.
- 3 For each of the rule that routes message to a connector, update the **ALLOW SENDER TO OVERRIDE THE DELIVERY FORMAT** field.
 - a Select the rule, right click and select **PROPERTIES** from the menu.
The **Create New Rule** page opens.
 - b Click **NEXT**. Under **Specify the Actions to take for this Rule**, select the action item.
 - c Click **PROPERTIES**. The **Route to Connector** wizard opens.
 - d Select the check box beside **ALLOW SENDER TO OVERRIDE THE DELIVERY FORMAT**.
 - e Click **FINISH**.

Appendix:

- 4 Click **NEXT**, **NEXT** and then **FINISH** to complete your changes.

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.

- To set up Embedded AccuRoute for Intelligent Devices (Omtool ISAPI Web Server Extension) in a 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.

Enabling Batch Scanning

- To enable batch scanning:**
- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
 - 2 Open `configuration.xml` for editing.
 - 3 Locate your device group. For example, if you have a Group 20 device, go to the `<Group20>` node.

- 4 In that group, find the line that begins with `<Feature id="RoutingSheet"...>`

```
<Feature id="RoutingSheet" type="RoutingSheet" enabled="true"
  toplevel="true">
    .....
      <Recipient>
        <prRecipientType>0</prRecipientType>
        <prDestination>RoutingSheet</prDestination>
      </Recipient>
```
- 5 Add the property `<prAccuRouteBatchScan>` after the property `<prDestination>` and set it to true:

```
<Feature id="RoutingSheet" type="RoutingSheet" enabled="true"
  toplevel="true">
    .....
      <Recipient>
        <prRecipientType>0</prRecipientType>
        <prDestination>RoutingSheet</prDestination>
        <prAccuRouteBatchScan>true</prAccuRouteBatchScan>
      </Recipient>
```
- 6 Save your changes and close the file.
- 7 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Configuring use of AddressBook service for LDAP lookups

To configure use of AddressBook service:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Search for the `<Search UseABService` node.
- 4 Verify the value is set as `true`.
- 5 Save your changes to the configuration file.
- 6 Open a command prompt and click **START > RUN**.
- 7 Enter `cmd` and then perform an `iisreset`.

Appendix:

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.

- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now, during authentication, authentication is done by the AddressBook service.

Configuring prompts

You can configure prompts for Personal and Public Distributions, Routing Sheet, Fax and MyAccuRoute features using the configuration.xml file. For the Public and Personal Distributions features, prompts can be configured in the xml file or on the Omtool Server. The prompts that are configured on the server are also known as Embedded Directive Prompts. For more information, see [Embedded Directive Prompts](#).

HP OXPd Device Client supports user-specified values for the following properties:

- file name
- file type

To configure prompts:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Search for the `<Prompts>` node.
- 4 Enter the following code using the following example as a guideline. In this example, the `DMSDocumentName` prompt is being set up.

```
<Prompts>
<DMSDocumentName>
<Display>Settings</Display>
<Label>DMS Document Name:</Label>
<Type MinLength="5" MaxLength="15">Text</Type>
<Instructions>Enter the dms document name</Instructions>
<Values>
<Value internal="" default="true">dmsdocument</Value>
</Values>
<Properties>
<Property override="true">prDMSDocName</Property>
</Properties>
</DMSDocumentName>
```

- 5 Search for the AccuRoute feature that should use this prompt. Only the Routing Sheet, Fax and MyAccuRoute features can use prompts configured in the xml file.
- 6 Go to the <Prompts> node under the feature node.
- 7 Enter the following code:


```
<Prompts>
<Prompt>DMSDocumentName</Prompt>
</Prompts>
```
- 8 Save your changes.
- 9 Open a command prompt and click Start > Run.
- 10 Enter `cmd` and then perform an `iisreset`.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.
- 11 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now when a user goes to the device and scans a document using the AccuRoute feature for which the prompt was configured, a Wizard opens asking for the DMS Document Name. Configuring prompts is useful in environments with multiple child domains under one parent where you need to configure both the child domains by configuring multiple domains and multiple search nodes.

Table 8-A Guidelines on creating prompts

Property	Impact	Syntax
Prompt Name	Determines the value of the prompt	string
Display	Determines whether the overriding property would be displayed in a separate Wizard page.	Use the following value: Wizard
Label	Determines the title to be displayed for Wizard screen.	[Name of the label]
Instructions	Determines the instructions that is displayed in the wizard screen.	[description]
Type	Determines the data type of the prompts. The attributes MinLength and MaxLength determine the minimum and maximum text data entry length respectively. If the default text value in the configuration.xml file exceeds the MaxLength, then it chops off the length before displaying it. Note: These attributes are not applicable for GenericList data type.	Use one of the following values: <ul style="list-style-type: none"> • Text • GenericList
Value	Determines the value to be displayed or selected on the Wizard screen based on the data type. The attribute internal stores the corresponding internal code used within the Accuroute server.	[Value] [code value]

Appendix:

Table 8-A Guidelines on creating prompts

Property	Impact	Syntax
	The attribute default denotes that the corresponding value is the default. For GenericList data type, the value is selected by default on the screen. For Text data type, the corresponding value is displayed in the text box.	Use one of the following values: <ul style="list-style-type: none"> • true • false
Property	Determines the property name that is used within the Accuroute server. The override attribute denotes that this is an overriding property.	[Property name] Use one of the following values <ul style="list-style-type: none"> • true • false

Configuring multiple domains

To configure multiple domains:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Search for the `<Domain>` node.
- 4 Enter the following code:

```
<Values>
<Value>domain1.yourcompany.com</Value>
<Value>domain2.yourcompany.com</Value>
<Value>domain3.yourcompany.com</Value>
<Value>domain4.yourcompany.com</Value>
</Values>
```
- 5 Save your changes to the configuration file.
- 6 Open a command prompt and click **START > RUN**.
- 7 Enter `cmd` and then perform an **iisreset**.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to `configuration.xml` are not reflected.
- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

During authentication, the device displays the "Select Domain" button. When the user clicks the button, the user is directed to the Domain list page. Once the user selects a domain, authentication proceeds.

Configuring multiple search nodes

To configure multiple search nodes:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Search for the `<Search UseABService>` node.
- 4 Enter the following code just below the line `<Search UseABService>`

```
<Server>[IP Address]</Server>
<Port>389</Port>
<SearchBase/>
<Filter/>
<Username>jsmith@yourcompany.com
</Username>
<Password>[password value]</Password>
<Attributes></Attributes>
<AttributeName></AttributeName>
</Search>
<Search UseABService="false">
<Server>[IP Address]</Server>
<Port>389</Port>
<SearchBase/>
<Filter/>
<Username>jsmith1@yourcompany.com
</Username>
<Password>[password value]</Password>
<Attributes></Attributes>
<AttributeName></AttributeName>
</Search>
<Search UseABService="false">
<Server>[IP Address]</Server>
<Port>389</Port>
<SearchBase/>
<Filter/>
<Username>jsmith2@yourcompany.com
</Username>
```

Appendix:

```
<Password>[password value]</Password>
<Attributes></Attributes>
<AttributeName></AttributeName>
</Search>
```

5 Configure the values of `<Server>`, `<Username>`, and `<Password>` nodes.

6 Save your changes to the configuration file.

7 Open a command prompt and click **START > RUN**.

8 Enter `cmd` and then perform an **iisreset**.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.

9 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now authentication is done by the search nodes that were defined. Authentication is done as soon as the first match is found.

Configuring User PIN

To configure user PIN:

1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.

2 Open `Configuration.xml` for editing.

3 Go to the `<Filter>` node under `<Search UseABService="false">` node.

4 Change the value of the `<Filter>` node as needed. For example:

```
<Filter>facsimileTelephoneNumber</Filter>
<Username>administrator@domain.net</Username>
<Password>qsg@2006</Password>
<Attributes></Attributes>
```

Note The `<username>` and `<password>` are optional. They are required only if the user needs to authenticate against the LDAP server. If the `UseABService` value is set to true (`<Search UseABService="true">`), they are not needed.

5 Save your changes.

6 Now go to the `<Type>` node.

7 Change the value of the node to **PIN**:

```
<Type>PIN</Type>
```

- 8 Go to the `<User>` node and change the value of the `<Label>` node to `PIN:`
`<Label>PIN:</Label>`
- 9 Save your changes.
- 10 Open a command prompt and click **START > RUN**.
- 11 Enter `cmd` and then perform an **iisreset**.
This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.
- 12 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

During authentication, the user is prompted to provide the PIN id.

Configuring PIN with Password (for any Active Directory field other than employeeID)

By default, the PIN authentication is validated against the employeeID in Active Directory. To configure validation against any other Active Directory field, follow the instructions in the procedure below.

To configure Pin with Password (for any Active Directory field other than employeeID):

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Go to the `<Filter>` node under `<Search UseABService="false">` node.
- 4 Change the value of the `<Filter>` node as needed. For example:
`<Filter>facsimileTelephoneNumber</Filter>`
`<Username>administrator@domain.net</Username>`
`<Password>qsg@2006</Password>`
`<Attributes></Attributes>`

Note The username should be a fully qualified domain name.

- 5 Save your changes.
- 6 Now go to the `<Type>` node.
- 7 Change the value of the node to `PIN:`
`<Type>PIN</Type>`

Appendix:

- 8 Go to the `<User>` node and change the value of the `<Label>` node to `PIN:`
`<Label>PIN:</Label>`
- 9 Go to the `<Password>` node and change the value of the `<Label>` node to `Password:`
`<Label>Password:</Label>`
- 10 Save your changes.
- 11 Open a command prompt and click **START > RUN**.
- 12 Enter `cmd` and then perform an `iisreset`.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to `configuration.xml` are not reflected.

After configuring Pin with password in this fashion, login to AccuRoute feature on the device by specifying `facsimileTelephoneNumber` for `Usr-I` (set in Active directory) instead of the email address.

Configuring server side validation

This feature supports Server side validation for prompts and is enabled by setting a `ValidationID` attribute in `<Type>` node inside the `<Prompt>` node.

To configure server side validation:

- 1 Configure ADO validator on the server following instructions in the [Release Notes](#).
- 2 In the Omtool Server Administrator, enable Prompts for the group of users who will use the prompts:
 - a Open the **Group Properties** page, then click **PROMPTS** tab.
 - b Check the box beside **ENABLE MEMBERS OF THIS GROUP TO PROMPT FOR THE FOLLOWING PROPERTIES**.
 - c Select the properties and save your changes.
- 3 Now open AccuRoute Desktop or AccuRoute Web Client and create Embedded Directives. The prompts enabled in the server are available under **OPTIONS > PROMPTS** menu.
- 4 Select the prompts that should be used and enable them in the **OPTIONS** page of your AccuRoute Desktop or AccuRoute Web Client application.
- 5 Login to the HP device and select **Personal** or **Public** Distribution option. The EDs with prompts are listed in the list of available Embedded Directives.
- 6 Select an Embedded Directive. The prompts display in the order in which they are selected in AccuRoute Desktop or AccuRoute Web Client application.
- 7 Enter required prompt values. The values are validated against values set in the AccuRoute Server.

Configuring an Embedded Directive to appear in top of device listing

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

To configure Embedded Directives to appear on top of device listings:

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

Configuring scan settings in Embedded Directives

You can configure scan settings in the Embedded Directives you create. Now when a user goes to an HP device and scans a document using an Embedded Directive 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 Embedded Directive:

- 1 In the Omtool Server Administrator, enable Scan settings for the group of users who will use the scan settings:
 - a Open the **Group Properties** page, then click **SCAN SETTINGS** tab.
 - b Check the box beside **ENABLE MEMBERS OF THIS GROUP TO USE THE SELECTED SCAN SETTINGS**.
 - c Select the settings and save your changes.
- 2 Now open AccuRoute Desktop or AccuRoute Web Client and create Embedded Directives. The scan settings enabled in the server are available under **OPTIONS > SCAN SETTINGS** menu.
- 3 Select the scan settings for the Embedded Directive.
- 4 Login to the HP device and select an Embedded Directive to scan a document with. The scan settings in the Embedded Directive will override any device scan setting.

For example: Say "Mono" is selected as color mode in server, Mono option will be available in Options > Scan settings tab in ARD/AWC. To create and save an ED with Mono scan setting and then select that ED on device (under Public/Personal distribution). You can verify the Color mode in More options screen for the ED. The Color mode set for that ED will be "Black and white"

Configuring device print back feature

The device print back feature allows the user to print a scan confirmation once the job is completed. When enabled, it displays additional button in the job status dialog.

To configure device print back feature:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Go to the Group node to which your device belongs to.
- 4 Enable the `<PrintConfirmation>` node:

```
<PrintConfirmation>
<Enabled>true</Enabled>
<Template>PrintConfirmation</Template>
<Name>Print Status</Name>
</PrintConfirmation>
```
- 5 Save your changes.
- 6 Open a command prompt and click **START > RUN**.
- 7 Enter `cmd` and then perform an **iisreset**.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to `configuration.xml` are not reflected.
- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now when you scan a document, when the job is successfully complete, you will see a Print Status button on the Scan confirmation dialog. On selecting "Print status" button, the scan confirmation receipt is printed back to the device.

Configuring Property Transformations

This feature allows you to translate any property retrieved from the device to any other property or template variables you need.

For example, to translate property `SENDER_DEVICE_AUTH_NAME` to `SSOID` or `SENDER_DEVICE_NAME` to `DEV_NAME`, add the following code to the transformation node to a specific AccuRoute feature node for your device group:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Go to the Group node to which your device belongs to.

- 4 In the <Transformations> node, insert the following code:

```
<Transformations>
  <Transform>
    <Set>\\prTemplateVars (SSOID) </Set>
    <Value>%\\prDeviceMetaData (SENDER_DEVICE_AUTH_NAME) %</Value>
  </Transform>
  <Transform> <Set>\\prTemplateVars (DEV_NAME) </
Set><Value>%\\prDeviceMetaData (SENDER_DEVICE_NAME) %</Value> </
Transform>
</Transformations>
```

- 5 Save your changes.
- 6 Open a command prompt and click **START > RUN**.
- 7 Enter `cmd` and then perform an **iisreset**.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.

- 8 Load the AccuRoute buttons using the force update option. For instructions, see [Loading the AccuRoute buttons using force update option](#) (7-5).

Now, the properties `SENDER_DEVICE_AUTH_NAME` and `SENDER_DEVICE_NAME` are transformed to `SSOID` and `DEV_NAME`.

Configuring device to use Secure Socket Layer (SSL) for communication

In case your environment demands that you use SSL for communication, you need to make the following modifications:

- Edit the configuration.xml file and change all instances of HTTP to HTTPS
- While adding the device through the Omtool Server Administrator, change the Source URL path to HTTPS and check the **DEVICE ENABLED FOR SECURE COMMUNICATION** option.

Editing the configuration.xml file

To edit the configuration.xml file:

- 1 Navigate to **C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION** directory.
- 2 Open `Configuration.xml` for editing.
- 3 Find all instances of HTTP and replace them with HTTPS.
- 4 Save your changes.

Appendix:

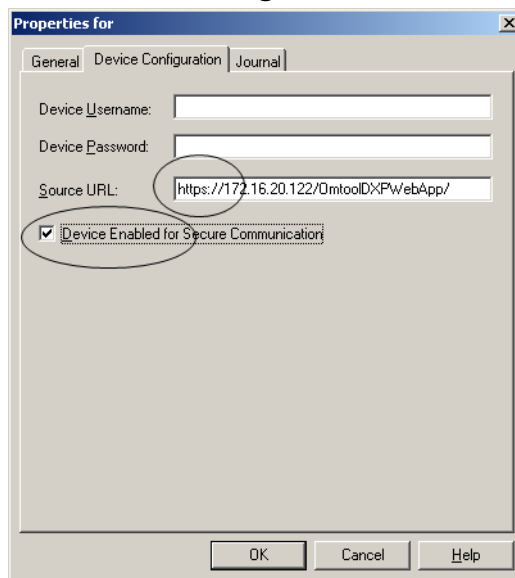
- 5 Open a command prompt and click **START > RUN**.
- 6 Enter `cmd` and then perform an `iisreset`.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to configuration.xml are not reflected.

Adding device using Omtool Server Administrator

To add a device using Omtool Server Administrator:

- 1 Click **START > ALL PROGRAMS > OMTOL > OMTOL SERVER ADMINISTRATOR**.
- 2 In the console tree, expand the Omtool Server.
- 3 Go to the **Devices** node.
- 4 Click **DEFAULT > NEW > HP DEVICE**. The **Properties** for the device page opens.
- 5 In the **NAME** text box, enter a name for the device.
- 6 In the **NETWORK ADDRESS** text box, enter the IP address of the HP device.
- 7 Optionally, in the **DESCRIPTION** text box, enter a description of the device.
- 8 Click the **Device Configuration** tab.



- 9 In the **DEVICE USERNAME** text box, enter the name of the device Administrator. In the **DEVICE PASSWORD** text box, enter password of the Administrator.
The **SOURCE URL** text box is filled in automatically.
- 10 Edit the source URL and replace **http** with **https**.
- 11 Check the box beside **DEVICE ENABLED FOR SECURE COMMUNICATION** option.
- 12 Click **OK** to add the device.

Changing the label of print status message

To change the label of a print status message:

- 1 Navigate to:
C:\PROGRAM FILES\OMTOOL\HPOXP\CONFIGURATION
- 2 Open `configuration.xml` for editing.
- 3 Locate your device group. For example, if you have a Group 20 device, go to the `<Group20>` node.
- 4 Locate the `<PrintConfirmation>` node.
- 5 Change the `<Name>` parameter under the `<PrintConfirmation>` node with new label.

```
<PrintConfirmation>  
    <Enabled>>false</Enabled>  
    <Template>PrintConfirmation</Template>  
    <Name>Print Status</Name>  
</PrintConfirmation>
```

- 6 Save your changes.
- 7 Open a command prompt and click **START > RUN**.
- 8 Enter `cmd` and then perform an `iisreset`.

This is necessary to stop all the Website and application pools and restart them. Without this reset, the changes to `configuration.xml` are not reflected.

Appendix:

Appendix B: Setting up a CA Certificate using Microsoft Certificate Services and enable SSL

If you selected HTTPs support, you must follow the instructions in this section and set up a CA Certificate and enable SSL. The certificate must be created and installed in the IIS.

This section includes:

- [Requirements for setting up a CA certificate](#) (9-1)
- [Installing the Certificate Services component](#) (9-2)
- [Creating a CA certificate request](#) (9-5)
- [Requesting the CA certificate](#) (9-10)
- [Installing the CA certificate on the Default Web Site](#) (9-13)
- [Enabling SSL on OmtoolDXPWebApp and OmtoolWebAPI](#) (9-16)
- [Instructions for setting the device to use SSL](#) (9-17)

Requirements for setting up a CA certificate

The following requirements must be met when a CA certificate is being set up:

- Web server that meets the requirements for AccuRoute Intelligent Device Client. Go to [Installing HP OXPd Device Client on a remote system](#) (3-6)
- Windows user account that belongs to the Administrators group
- Windows installation CD

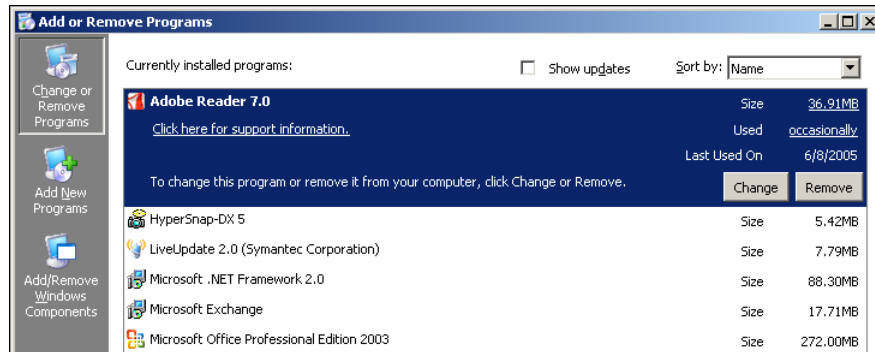
Appendix:

Installing the Certificate Services component

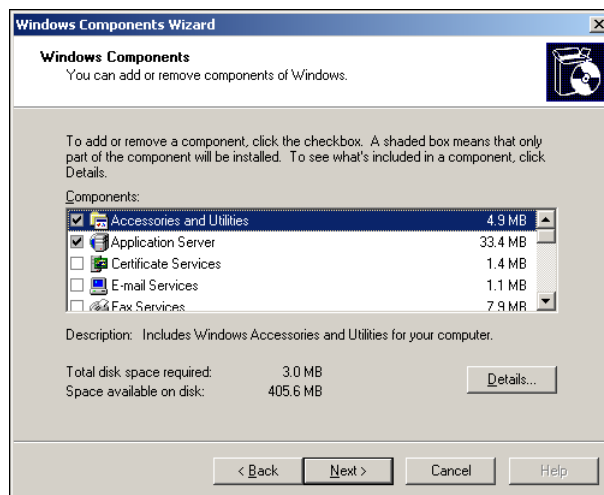
This Windows Components Wizard temporarily stops IIS. Plan the installation accordingly.

To install the Certificate Services component:

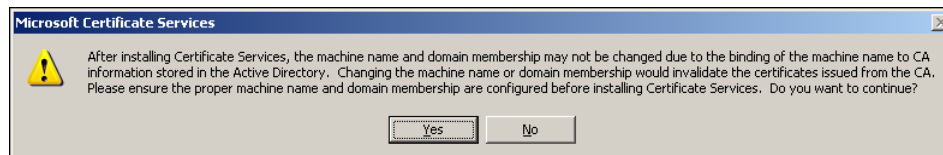
- 1 Go to Control Panel and start **ADD OR REMOVE PROGRAMS**.



- 2 Click **ADD/REMOVE WINDOWS COMPONENTS**. The Windows Components Wizards starts.

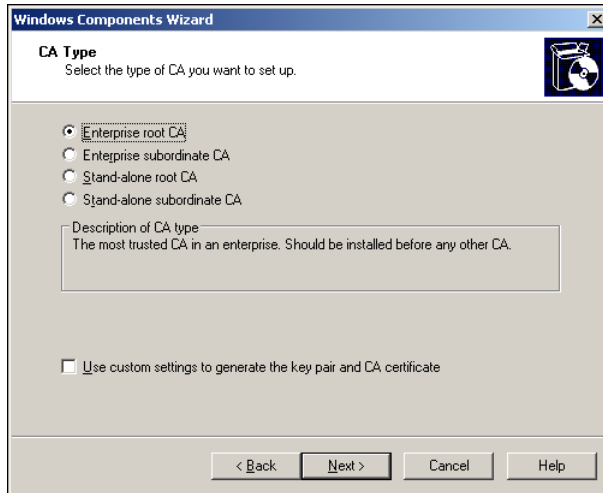


- 3 Select **CERTIFICATE SERVICES**. A message box opens.

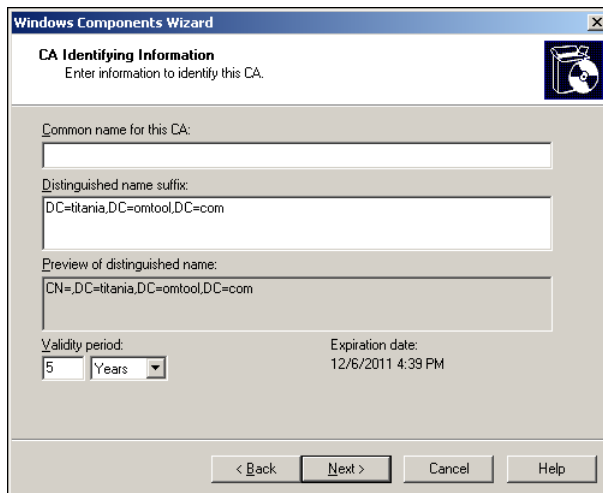


- 4 Read the message and click **YES**.

- 5 Click **NEXT**. The **CA Type** page shows the CA options.



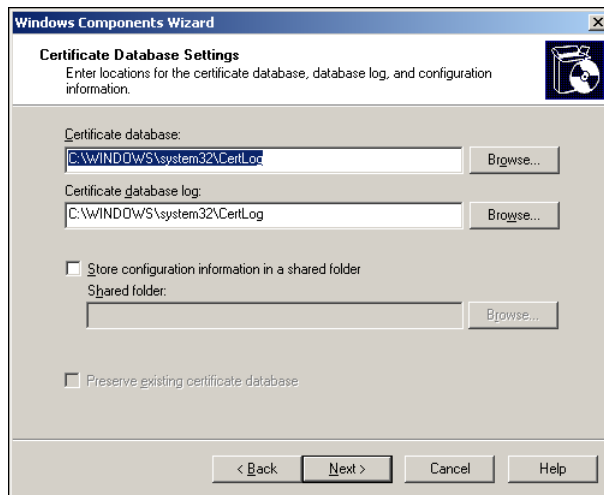
- 6 Verify **ENTERPRISE ROOT CA** is selected and click **NEXT**. The **CA Identifying Information** page shows details about the CA.



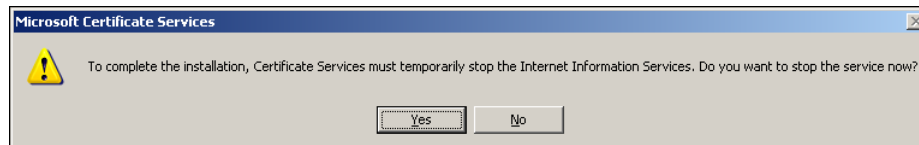
- 7 Enter the Common Name for the CA. This should be the IP address of the system where the certificate is being installed.

Appendix:

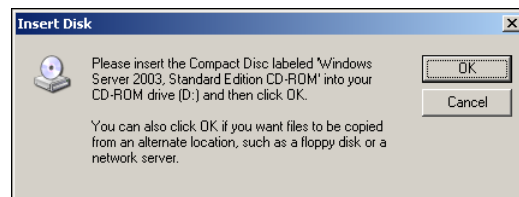
- 8 Click **NEXT**. The **Certificate Database Settings** page shows default locations for the certificate database and certificate database log.



- 9 Click **NEXT**. A message indicating that the installation stops IIS temporarily opens.



- 10 Click **YES**. A message indicating that the Windows CD or network access to the setup files is required opens.



- 11 Click **OK** and locate the files that are required to complete the installation.

The Windows Components Wizard shows a message indicating that the component is installed successfully.



- 12 Click **FINISH**.

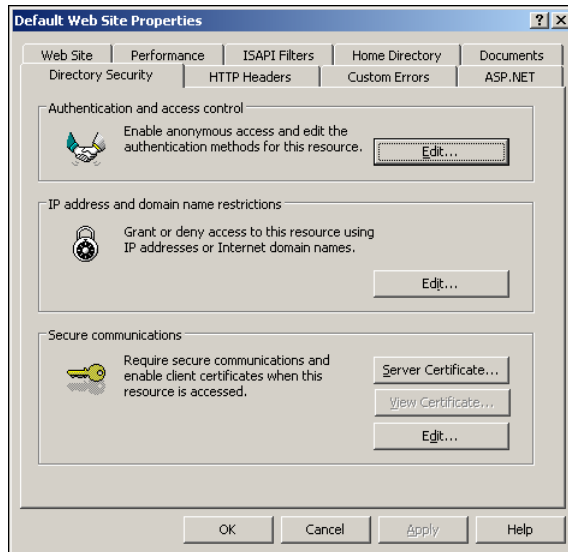
Creating a CA certificate request

To request a CA certificate:

- 1 Start IIS. Locate and expand **DEFAULT WEB SITE** in the console tree
- 2 Configure **Default Web Site** using the instructions below:
 - a Right click **DEFAULT WEB SITE** and select **PROPERTIES** from the drop down menu.
The **Properties** page opens.

Appendix:

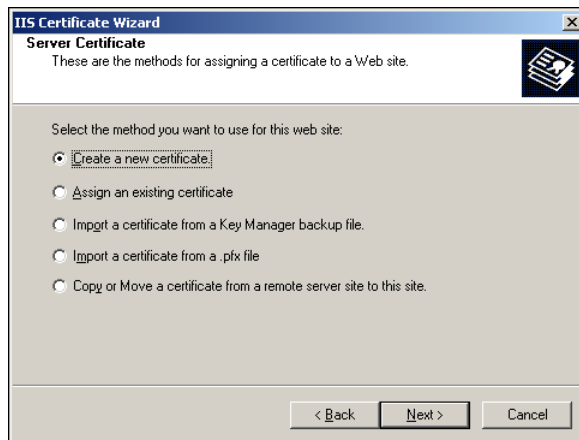
b Click the **DIRECTORY SECURITY** option.



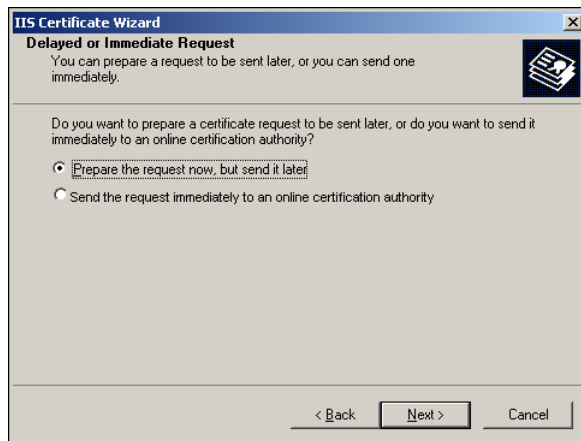
c In the **Secure communications** section, click **SERVER CERTIFICATE**. The certificate wizard shows a welcome message.



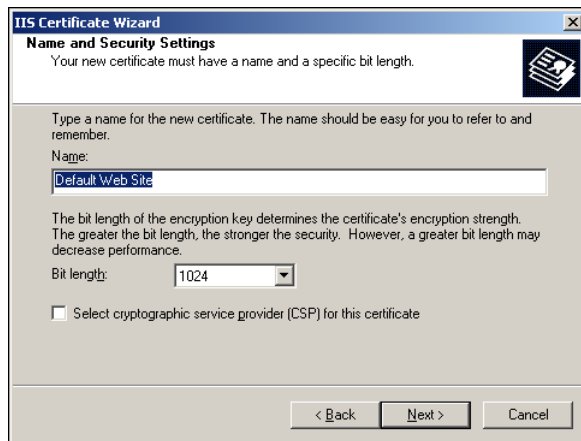
3 Click **NEXT**. The **Server Certificate** page opens.



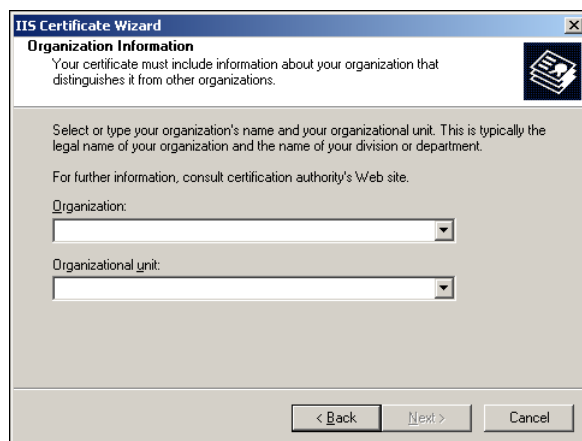
- 4 Verify that **CREATE A NEW CERTIFICATE** is selected and click **NEXT**. The **Delayed or Immediate Request** page opens.



- 5 Click **NEXT**. The **Name and Security Settings** page opens.

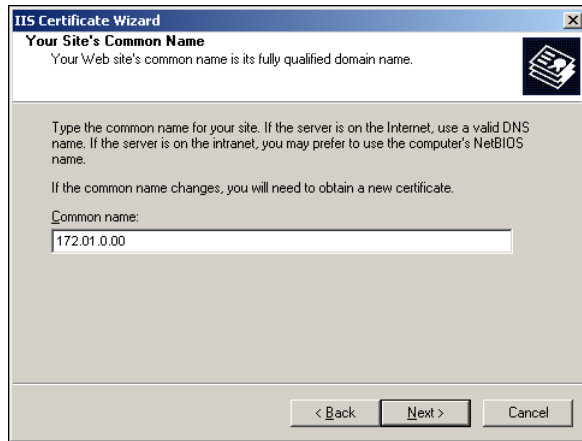


- 6 Enter a friendly name for the certificate and click **NEXT**. The **Organization Information** page opens.



Appendix:

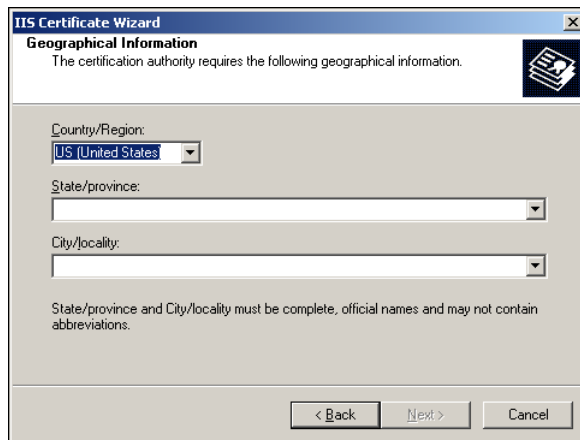
- 7 Enter the organization name and organizational unit name and click **NEXT**. The Your Site's Common Name page opens.



The screenshot shows the 'IIS Certificate Wizard' dialog box with the title 'Your Site's Common Name'. The text inside reads: 'Your Web site's common name is its fully qualified domain name.' Below this, there is a paragraph: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.' A text box labeled 'Common name:' contains the value '172.01.0.00'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

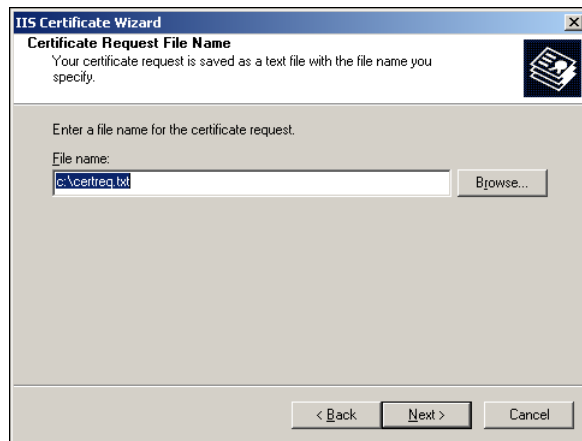
Note In the **Common Name** text box, you must enter the IP address of the system and not the name of the host.

- 8 Enter the IP address CA server and click **NEXT**. The **Geographical Information** page opens.

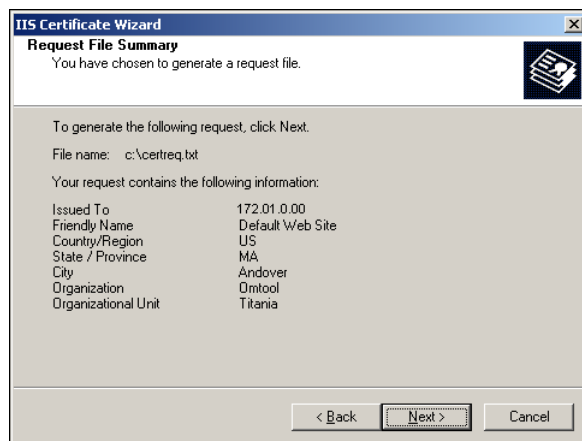


The screenshot shows the 'IIS Certificate Wizard' dialog box with the title 'Geographical Information'. The text inside reads: 'The certification authority requires the following geographical information.' Below this, there are three dropdown menus: 'Country/Region:' with 'US (United States)' selected, 'State/province:', and 'City/locality:'. A note at the bottom states: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 9 Select the country/region, state/province, and city/locality, and click **NEXT**. The **Certificate Request File Name** page opens.

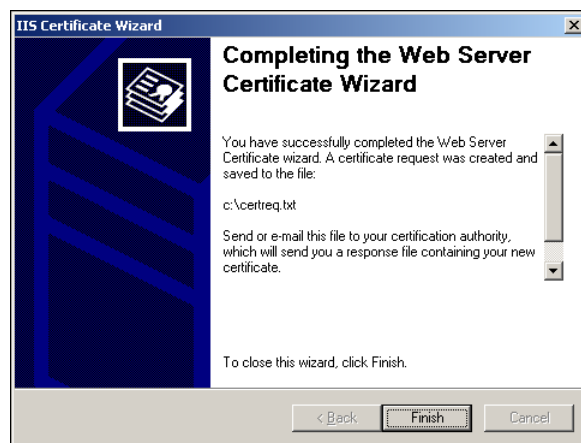


- 10 Change the location and file name for the certificate request if necessary, and then click **NEXT**. The **Request Summary** page opens.



- 11 Review the request details and click **NEXT**.

When the certificate request is created, you see the following message:



- 12 Click **FINISH** and then click **OK** to close the **Default Web Site Properties** page.

The certificate request is saved to a file.

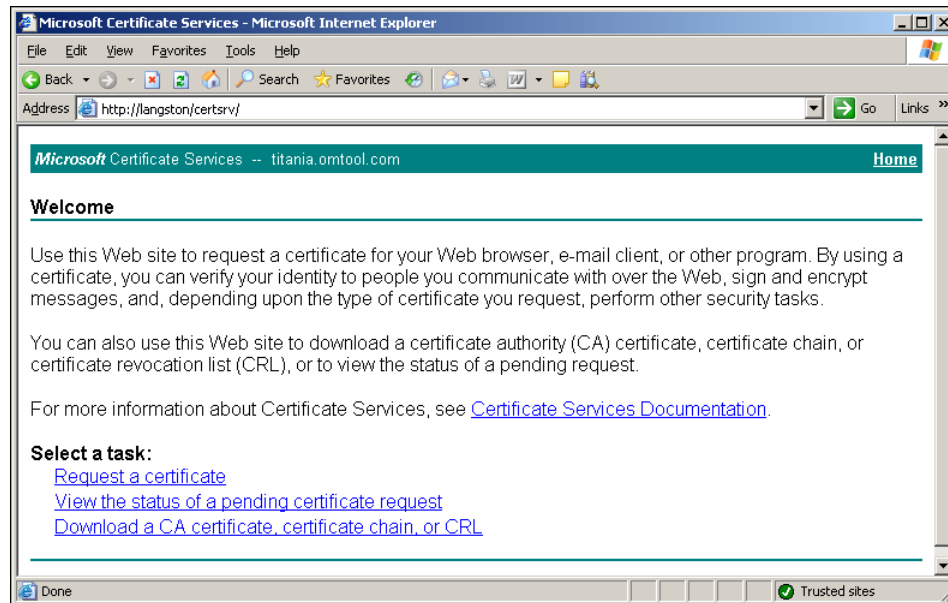
Requesting the CA certificate

To request the CA certificate:

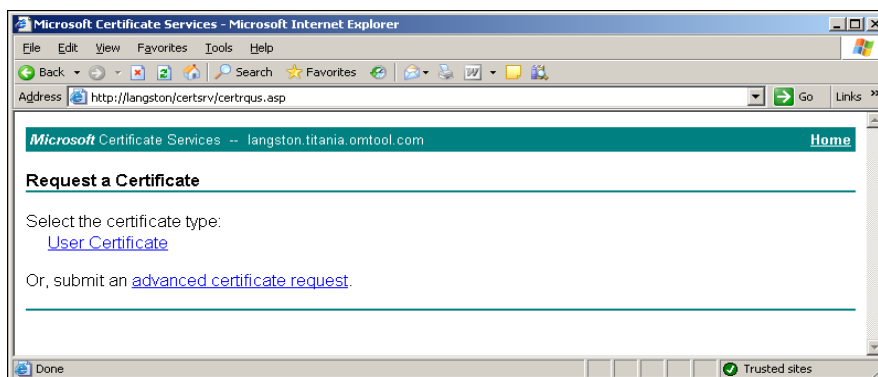
- 1 Start the browser and go to [http://\[Web server\]/certsrv](http://[Web server]/certsrv)

If prompted for login credentials, enter the username and password of an account that belongs to the local Administrators group on the Web server.

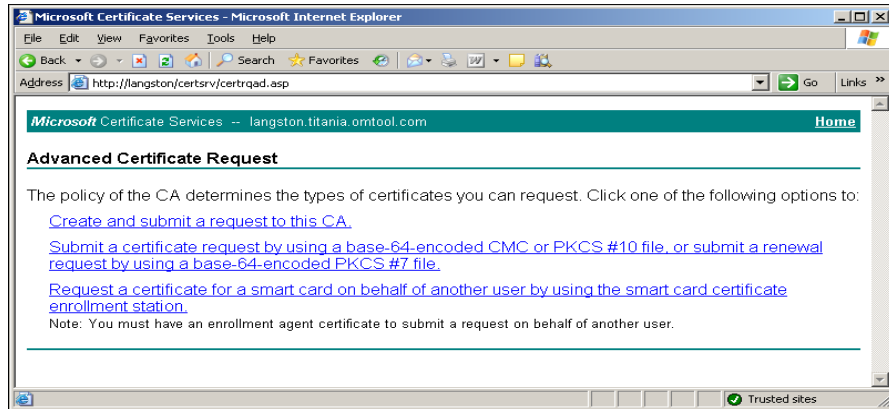
If Internet Explorer displays a message indicating that this site is not trusted, add the site to the list of trusted sites and continue.



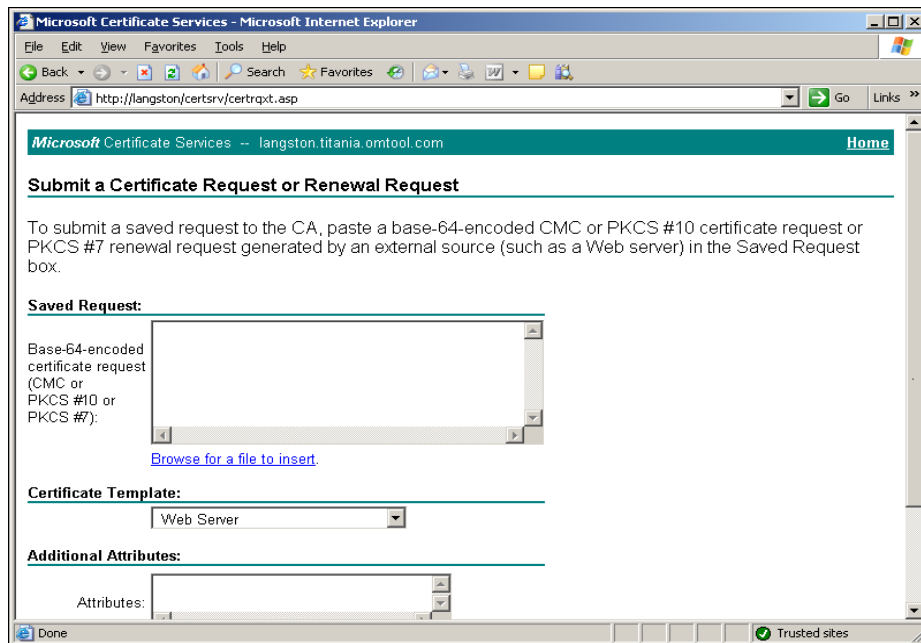
- 2 Click **REQUEST A CERTIFICATE**.



3 Click **ADVANCED CERTIFICATE REQUEST**.



4 Click **SUBMIT A CERTIFICATE REQUEST BY USING A BASE 64-ENCODED CMC OR PKCS #10 FILE, OR SUBMIT A RENEWAL REQUEST BY USING A BASE 64-ENCODED PKCS #7 FILE**.



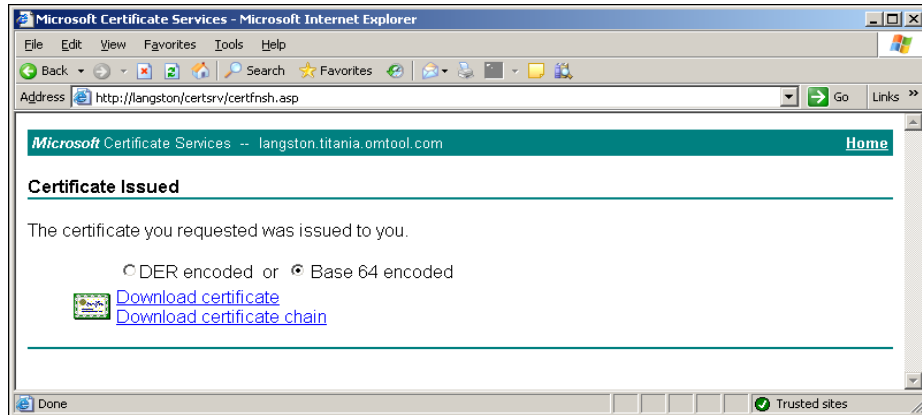
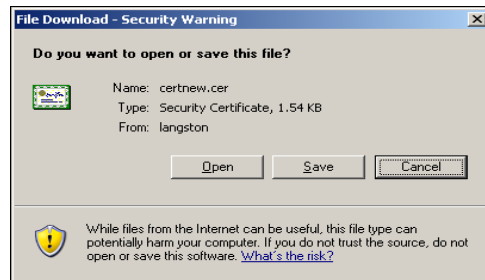
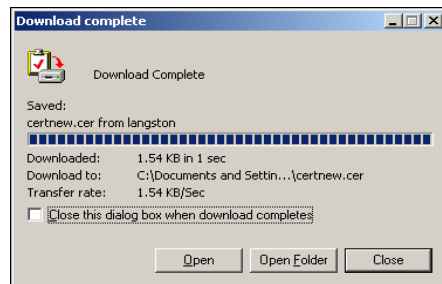
5 Complete the form:

- a Click **BROWSE FOR A FILE TO INSERT** and select the file containing the certificate request.

If Internet Explorer displays a warning that the security settings prevent the page from accessing the request file, go to the file, select and copy the content, and paste it into the Saved Request field.

- b Go to the **Certificate Template** menu and select **WEB SERVER**.

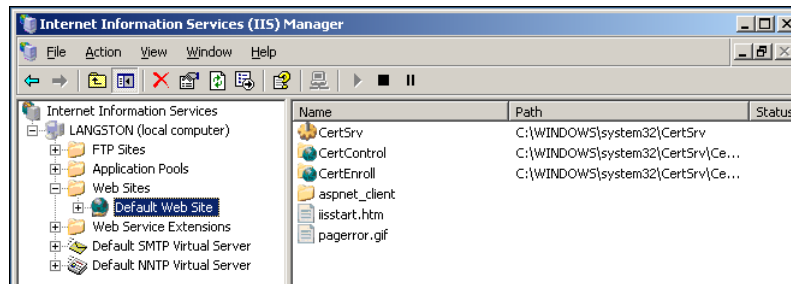
Appendix:

c Click SUBMIT.**6 Select BASE 64 ENCODED and click DOWNLOAD CERTIFICATE. A message prompts you to open or save the file.****7 Click SAVE, and save the file to your computer.****8 Click CLOSE.****9 Close the browser.**

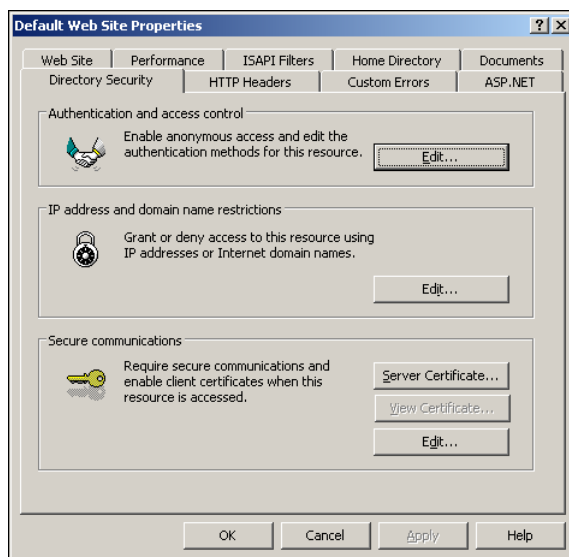
Installing the CA certificate on the Default Web Site

To install the CA certificate on the Default Web Site:

- 1 Start IIS and go to the Default Web Site in the console tree.



- 2 Right-click **DEFAULT WEB SITE** and select **PROPERTIES**.
- 3 Go to the **DIRECTORY SECURITY** tab.

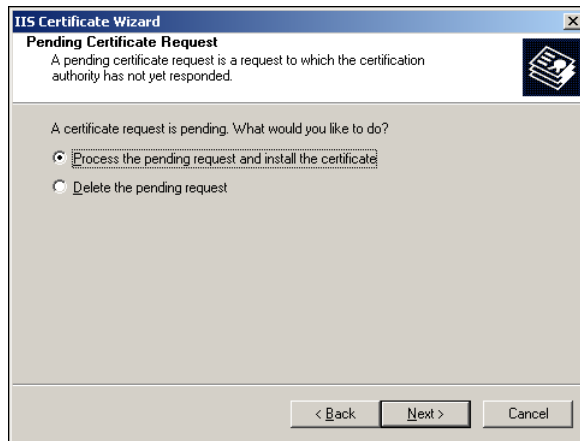


Appendix:

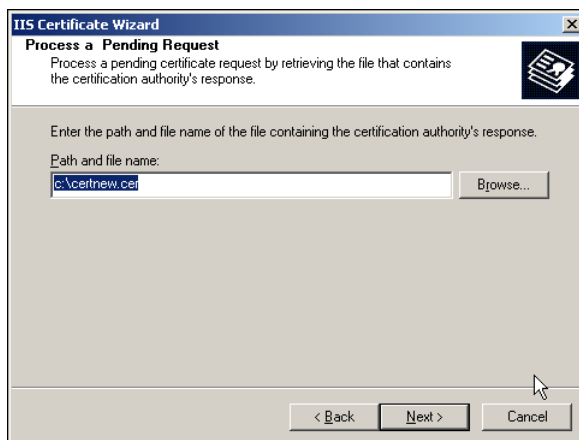
- 4 In the **Secure communications** section, click **SERVER CERTIFICATE**. The certificate wizard shows a welcome message.



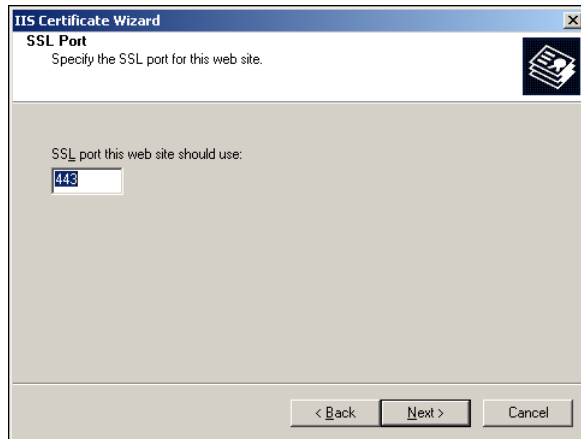
- 5 Click **NEXT**.



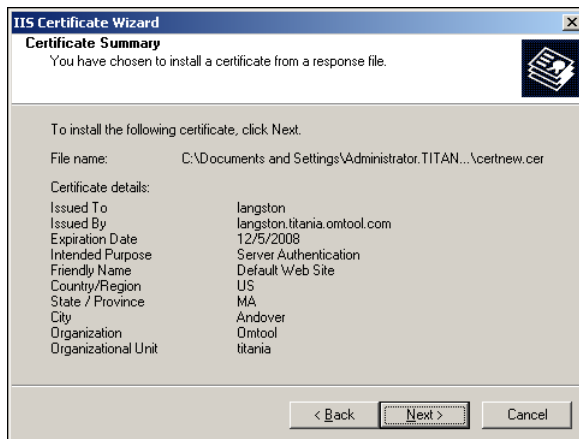
- 6 Verify that **PROCESS THE PENDING REQUEST AND INSTALL THE CERTIFICATE** is selected and click **NEXT**.



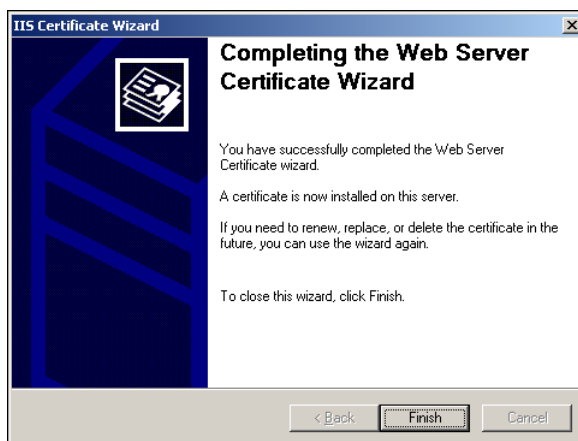
- 7 Verify that the field contains the path to the file containing the response to the certificate request and click **NEXT**.



- 8 Accept the default value (unless a different SSL port is required), and click **NEXT**.



- 9 Review the details and click **NEXT**. The certificate wizard installs the certificate. When installation is complete, you see the following message.



- 10 Click **FINISH** and then click **OK** to close the **Default Web Site Properties** page.

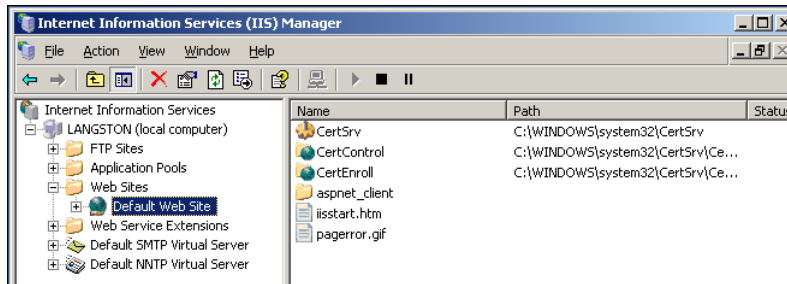
Appendix:

Enabling SSL on OmtoolDXPWebApp and OmtoolWebAPI

SSL (Secure Sockets Layer) must be enabled on the OmtoolDXPWebApp and the OmtoolWebAPI so that messages and requests can be submitted securely to AccuRoute Intelligent Device Client.

To enable SSL:

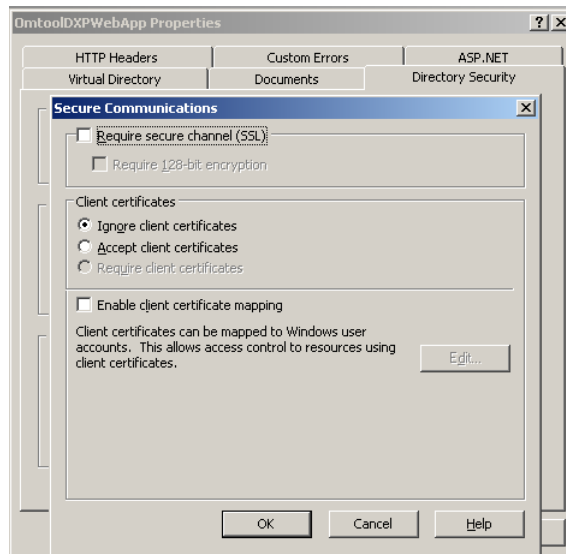
- 1 Start IIS and expand **Default Web Sites** in the console tree.



- 2 Right-click **OMTOOLDXPWEBAPP /OMTOOLWEBAPI** and select **PROPERTIES**.

The Properties page opens.

- 3 Go to the **DIRECTORY SECURITY** tab.
- 4 Go to **Secure communications** and click **EDIT**.



- 5 Select **REQUIRE SECURE CHANNEL (SSL)** and **REQUIRE 128-BIT ENCRYPTION**, and then click **OK**.
- 6 Click **OK** again to close the **Properties** page.

Instructions for setting the device to use SSL

To set the device to use SSL:

- Open the OMISAPI.xml and search for the code where it points to the file transfer directory. Change the default HTTP to HTTPS setting.
- When adding the device through the Omtool Server Administrator, change the Source URL path to HTTPS. For more information, see [Adding device using Omtool Server Administrator \(4-1\)](#)
- When adding the device through the Omtool Server Administrator, enable the "Device Enabled for Secure Communication" option. For more information, see [Adding device using Omtool Server Administrator \(4-1\)](#)

Appendix: