

AccuRoute[®] Server Installation and Integration Guide



Upland AccuRoute

6 Riverside Drive
Andover, MA 01810
Phone: (978) 327-5700
Toll-free US: 1-800 886-7845

Upland Software Headquarters

Frost Bank Tower
401 Congress Avenue, Suite 1850
Austin, TX 78701-3788
Toll Free: (855) 944-7526

About Upland Software

Upland Software (Nasdaq: UPLD) is an enterprise cloud software company that provides award-winning solutions in Project and IT Management, Workflow Automation and Digital Engagement. Our goal is 100% customer success, achieved through a unified operating platform that delivers the performance, scalability and support that over 2,500 Upland customers worldwide demand every day. Learn more at uplandsoftware.com.

© 2017 by Omtool, Ltd. (Upland AccuRoute) All rights reserved. Omtool, AccuRoute, Genifax, Image-In, ObjectArchive, ScanFacts, 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.

Upland AccuRoute Resources

The Upland Community

The Upland Community is the central hub for Upland customer information, in the community you can:

- Track tickets
- Search and Download Knowledge
- Interact in Upland Forums
- Stay up to date on AccuRoute and/or Upland News

Access the Community by logging in with your company email at:

<https://community.uplandsoftware.com/hc/en-us>

Customer Service and Technical Support Contact Information

- Phone: (978) 327 6800 or (1-888) 303 8098
- E-mail: omtool-support@uplandsoftware.com
- Community: <https://community.uplandsoftware.com/hc/en-us>

NOTE: Technical support requires an active support contract. For more information go to:

<https://uplandsoftware.com/accuroute/customer-success/support-overview/>

Sales, Consulting Services, Licenses and Training

- Phone: (978) 327 5700 or (1-800) 886 7845
- Email: ARmarketing@uplandsoftware.com

Contents

Section 1: Introduction

| | |
|--|-----|
| Introduction to AccuRoute..... | 1-1 |
| About Omtool..... | 1-1 |
| Scalability and automated failure | 1-1 |
| Built-in features for the AccuRoute server | 1-2 |
| Clients and specialized integrations | 1-3 |
| Summary for deploying the AccuRoute server | 1-4 |
| Icon Key..... | 1-4 |
| Related documentation..... | 1-5 |

Section 2: Requirements

| | |
|--|-----|
| Hardware and software requirements..... | 2-1 |
| Supported Devices..... | 2-2 |
| Additional software requirements for a local Composer | 2-2 |
| Additional installation requirements..... | 2-3 |
| Creating the AccuRoute service account..... | 2-3 |
| Creating AccuRoute Admins group..... | 2-4 |
| Configuring AccuRoute service account permissions for ExchangeX..... | 2-4 |
| ExchangeX 2010 and Exchange Server 2013..... | 2-4 |
| Installing Microsoft SQL Express on the AccuRoute server | 2-4 |

Section 3: Installing the AccuRoute Server

| | |
|---|------|
| Introduction to installing the AccuRoute server | 3-1 |
| Automated pre- and post-installation and configuration tasks..... | 3-2 |
| Installing the AccuRoute server..... | 3-2 |
| Creating and configuring the database | 3-11 |
| Completing the Server Configuration Wizard | 3-14 |
| Note about registry keys location when installing the AccuRoute server on a 64-bit machine..... | 3-16 |
| Activating the license..... | 3-16 |
| Automatic license activation..... | 3-16 |
| Manual license activation..... | 3-18 |
| Uninstalling the AccuRoute server..... | 3-22 |

Section 4: AccuRoute Mobile Client

| | |
|--|-----|
| Requirements | 4-1 |
| Installing the Mobile Device Application..... | 4-2 |
| Installing the Mobile Client | 4-3 |
| Configuring a local IIS system for mobile connectivity..... | 4-3 |
| Configuring a remote IIS system for mobile connectivity | 4-4 |
| Environment configuration to support AccuRoute Mobile Clients..... | 4-4 |
| Configuring the Mobile Client environment to support HTTPS | 4-5 |
| Configuring the email management system | 4-5 |
| Configuring the AccuRoute server | 4-6 |

Section 5: Post Installation Configurations

| | |
|--|-----|
| Specifying the originator of notification messages | 5-1 |
| Customizing access to client setup programs | 5-2 |
| Configuring the Compose component to convert Office message attachments using automation | 5-2 |
| Configuring the AccuRoute server to convert PCL message attachments | 5-3 |
| AccuRoute server on the same drive as the operating system | 5-3 |
| AccuRoute server on a drive different from the operating system | 5-4 |
| Configuring Integrated Windows Authentication on the Web Server | 5-5 |

Section 6: Optional Configurations

| | |
|---|-----|
| Disaster Recovery Solution | 6-1 |
| Requirements | 6-1 |
| Installing and configuring a Disaster Recovery server | 6-1 |
| Data Encryption | 6-3 |
| Requirements | 6-3 |
| Importing the encryption certificate | 6-3 |
| Enabling Data Encryption | 6-4 |
| Disabling Data Encryption | 6-4 |
| Configuring the SQL Database | 6-4 |
| Support for SQL Always On Availability Groups | 6-5 |
| Configuring the HP CR Server for SQL Always On | 6-5 |
| Support for the SSL/TLS v1.2 Protocol | 6-6 |
| Enabling TLS 1.2 on your HP device | 6-6 |

Section 7: ExchangeX Integration

| | |
|--|-----|
| Adding an AccuRoute connector for ExchangeX | 7-1 |
| Specifying an email address for ExchangeX non-delivery reports | 7-2 |
| Configuring lookup methods | 7-3 |

Section 8: Lotus Notes Integration

| | |
|----------------------------------|-----|
| Configuring lookup methods | 8-1 |
|----------------------------------|-----|

Section 9: SMTP Integration

| | |
|--|-----|
| Configuring lookup methods | 9-1 |
| Reviewing the default DID/DTMF lookup configuration for inbound faxing | 9-1 |

Section 10: Installing ObjectArchive

| | |
|---|-------|
| Introduction to ObjectArchive | 10-1 |
| Requirements for ObjectArchive | 10-2 |
| Installing ObjectArchive | 10-2 |
| Configuring ObjectArchive | 10-11 |
| Creating a new Volume List | 10-11 |
| Configuring the AccuRoute server to route to Volume Lists | 10-11 |
| Removing ObjectArchive | 10-12 |

Section 11: Installing Remote Administrator

| | |
|--|-------|
| Introduction to Remote Administrator | 11-1 |
| Requirements for Remote Administrator | 11-2 |
| Installing Remote Administrator | 11-3 |
| Starting AccuRoute Server Administrator and connecting to the AccuRoute server | 11-8 |
| Problems connecting to the AccuRoute server using Remote Administrator | 11-10 |
| Connecting AccuRoute Server Administrator to additional AccuRoute servers | 11-10 |
| Disconnecting AccuRoute Server Administrator from an AccuRoute server | 11-11 |

Section 12: Installing an additional Composer

| | |
|---|-------|
| Installing a Remote Composer | 12-1 |
| Requirements for a Remote Composer | 12-2 |
| Installing a Remote Composer | 12-3 |
| Adding a Composer to the AccuRoute server | 12-10 |
| Applying the Compose license activation code | 12-10 |
| Adding a new Composer to the AccuRoute server | 12-10 |
| Replacing the local Composer with the new Remote Composer | 12-13 |

Section 13: Installing Remote Modem Server

| | |
|--|-------|
| Introduction to Remote Modem Server | 13-1 |
| Requirements for Remote Modem Server | 13-2 |
| Installing and testing the fax board and Dialogic Brooktrout System Software | 13-3 |
| Installing the Remote Modem Server | 13-3 |
| Detecting the channels on the Modem Server | 13-9 |
| Configuring the path to the Telco share directory | 13-10 |

Section 14: Installing Remote Embedded Directive Manager

| | |
|--|-------|
| Introduction to Remote Embedded Directive Manager | 14-1 |
| Requirements for Remote Embedded Directive Manager | 14-2 |
| Installing Remote Embedded Directive Manager | 14-3 |
| Adding Remote Embedded Directive Manager to the AccuRoute server | 14-9 |
| Removing Embedded Directive Manager from the AccuRoute server or a remote system | 14-11 |

Section 15: Installing Remote AccuRoute Connector for DMS libraries

| | |
|---|-------|
| Introduction to Remote AccuRoute connector for DMS libraries | 15-1 |
| Requirements for Remote AccuRoute connector for DMS libraries | 15-2 |
| Installing Remote AccuRoute connector for DMS libraries | 15-2 |
| Adding Remote AccuRoute connector for DMS libraries to the AccuRoute server | 15-9 |
| Removing Remote AccuRoute connector for DMS libraries | 15-12 |

Section 16: AccuRoute Intelligent Device Client

| | |
|--|-------|
| Introduction to AccuRoute Intelligent Device Client..... | 16-1 |
| AccuRoute Intelligent Device Client components..... | 16-2 |
| IIS implementation..... | 16-2 |
| Optional configurations..... | 16-4 |
| Configuring HTTPs connectivity for AccuRoute Desktop..... | 16-4 |
| Modifying the directory security configuration of virtual directories..... | 16-5 |
| Testing and troubleshooting AccuRoute Intelligent Device Client..... | 16-6 |
| Test connectivity to AccuRoute Intelligent Device Client..... | 16-6 |
| Troubleshoot connectivity issues..... | 16-7 |
| Installing AccuRoute Intelligent Device Client on a remote system..... | 16-8 |
| Requirements..... | 16-8 |
| Installing remote AccuRoute Intelligent Device Client..... | 16-9 |
| Configuring the remote AccuRoute Intelligent Device Client..... | 16-14 |
| Specifying the AccuRoute server..... | 16-14 |
| Adding the remote server's name to DCOM..... | 16-15 |
| Adding the application pool logon account to the AccuRoute Admins group..... | 16-16 |
| Other configurations..... | 16-17 |
| Removing remote AccuRoute Intelligent Device Client..... | 16-17 |

Appendix A: Setting up an AccuRoute Server Cluster

| | |
|--|------|
| Introduction to failover..... | A-1 |
| Requirements for an AccuRoute server cluster..... | A-3 |
| AccuRoute server requirements..... | A-3 |
| Database server requirements..... | A-4 |
| Remote device server requirements..... | A-4 |
| Installing and configuring the Cluster server..... | A-4 |
| Setting up the Database server..... | A-4 |
| Setting up the Active server..... | A-5 |
| Applying licenses..... | A-9 |
| Setting up the Passive server..... | A-9 |
| Setting up the Telco share..... | A-12 |
| Creating the Telco Share..... | A-12 |
| Configuring the AccuRoute connector for Telco to use the Telco Share on the database server..... | A-12 |
| Testing the failover configuration..... | A-13 |
| Optional configurations for cluster environments..... | A-14 |
| Setting up the remote device server..... | A-14 |
| Configuring the AccuRoute Web Client for failover..... | A-14 |
| Configuring the Mobile Client setup to support a cluster..... | A-14 |
| Configuring Image-In Connect for failover..... | A-15 |
| Configuring Omtool Workflow Integration Application (OWIA) for failover..... | A-16 |
| Clustering and Composer thread awareness..... | A-16 |

Appendix B: Configuration for HTTPS Support

| | |
|--|------|
| Setting up a CA certificate and enabling SSL with Windows 2008 R2 64-bit | B-1 |
| Requirements for setting up a CA certificate | B-1 |
| Downloading the MakeCert executable..... | B-2 |
| Creating the certificate..... | B-2 |
| Installing the certificate to Internet Information Services (IIS)..... | B-2 |
| Exporting the certificate to the OXPd v1.6 Device Client directory..... | B-3 |
| Creating an SSL binding..... | B-3 |
| Requiring SSL for the virtual web sites | B-3 |
| Verifying the SSL binding..... | B-4 |
| Enabling directory browsing in IIS | B-4 |
| Verifying HTTPS browsing..... | B-4 |
| Editing the OmISAPIU.xml file..... | B-5 |
| Editing the Bootstrap.xml file..... | B-5 |
| Requirements for setting up a CA certificate | B-5 |
| Downloading the MakeCert executable..... | B-6 |
| Running the MakeCert executable and creating the certificate..... | B-6 |
| Exporting the certificate to the OXPd v1.6 Device Client directory..... | B-6 |
| Requiring SSL for web sites | B-13 |
| Editing the OmISAPIU.xml file..... | B-14 |
| Editing the Bootstrap.xml file..... | B-15 |

Section I: Introduction

This guide contains instructions on installing and configuring the AccuRoute server v6.0, an enterprise application. It is written for System Administrators with detailed knowledge of Windows operating systems and LANs. TM®©

This section includes:

[Introduction to AccuRoute](#) (I-1)

[Built-in features for the AccuRoute server](#) (I-2)

[Clients and specialized integrations](#) (I-3)

[Summary for deploying the AccuRoute server](#) (I-4)

[Icon Key](#) (I-4)

[Related documentation](#) (I-5)

Introduction to AccuRoute

AccuRoute is Upland AccuRoute's award-winning document-handling platform that captures, converts, and distributes paper and electronic-based documents enabling fast, secure, simultaneous distribution of data to multiple destinations in multiple formats. Using AccuRoute, an organization can deliver information faster with more efficient workflows while reducing cost, complexity, and risk.

Upland AccuRoute

Upland AccuRoute is a leading provider of document handling solutions that simplify the integration of paper and electronic documents in enterprise information management systems. Upland AccuRoute solutions are used worldwide by businesses in document-intensive industries that demand secure handling, integration and tracking of documents in full compliance with a range of regulatory requirements.

Scalability and automated failure

AccuRoute is a highly scalable enterprise application that can be deployed in organizations of all sizes. Its robust server-client architecture supports distributed workloads, versatile throughput, and unmatched document distribution capabilities using numerous delivery systems and methods. Moreover, AccuRoute supports automated failover. In case of a system failure on the AccuRoute server, automated failure promises seamless recovery using a standby server.

With smaller workloads, the AccuRoute server can suitably perform all the functions required for document distribution. As an organization grows, the AccuRoute server workload can be distributed or completely off-loaded using one or all of the following components:

Table I-1: AccuRoute Components

| Component | Description | Reference in this document |
|---|--|---|
| ObjectArchive database | A remote system hosting the ObjectArchive database. | Section 10: Installing ObjectArchive |
| Remote Administrator | A remote system hosting the AccuRoute Server Administrator, which is the management application for AccuRoute. | Section 11: Installing Remote Administrator |
| Remote AccuRoute Compose Component (Composer) | A remote system hosting a Composer, which performs document conversion tasks. | Section 12: Installing an additional Composer |
| Remote Modem Server | A remote system hosting a Modem Server. | Section 13: Installing Remote Modem Server |
| Remote Embedded Directive Manager component | A remote system hosting the Embedded Directive Manager component, which is used to process Distribution Rules. | Section 14: Installing Remote Embedded Directive Manager |
| Remote AccuRoute connector for DMS libraries | A remote system hosting an AccuRoute connector for DMS libraries. | Section 15: Installing Remote AccuRoute Connector for DMS libraries |
| Remote AccuRoute Intelligent Device Client | A remote system that provides an interface between devices and the AccuRoute server. | Section 16: AccuRoute Intelligent Device Client |
| Secondary server | A secondary system in a failover configuration. | Appendix A: Setting up an AccuRoute Server Cluster |

To purchase additional connectors or components, contact [Upland AccuRoute Customer Service](#).

Built-in features for the AccuRoute server

The AccuRoute server has the following built-in features:

- **Centralized administration** - You can manage the AccuRoute server using the AccuRoute Server Administrator, a snap-in for Microsoft Management Console. After you connect the AccuRoute Server Administrator to your AccuRoute server in the LAN, you can:
 - ▶ Monitor message processing
 - ▶ Troubleshoot errors
 - ▶ Manage the server connectors
 - ▶ Modify the configuration of server components
 - ▶ Manipulate rules for handling inbound and outbound messages
 - ▶ Manage user permissions and feature access
- **Automated self-maintenance** - You can manage the databases of the AccuRoute server using the Maintenance component and configure:
 - ▶ Cleanup feature to remove messages and billing entries from the message database after a specified length of time.

- ▶ Archive feature to copy messages to an archive database and remove the messages and the billing entries from the archive after a specified length of time.
- **Customized document workflow** - You can create rules (called Distribution Rules) to determine how the AccuRoute server will process inbound and outbound messages. The rules are highly configurable and can be manipulated to achieve specific results.
- **Configurable user permissions and feature access** - You can create users and configure user permissions in the AccuRoute Server Administrator. The collection of user records determines each user's access privileges to the AccuRoute Desktop, Web Apps, the Legacy Web Views Client, and Approval. (Approval is a configurable feature that results in a user's messages being reviewed or approved before they are sent.) The user default configuration applies globally to users who do not require special permissions or feature access.

Clients and specialized integrations

AccuRoute features are accessible where the users need them most—on desktops, the web, mobile devices, office machines, multifunction devices, and business systems that are an integral part of the communication workflow.

AccuRoute can be licensed for desktop and intranet-based applications for:

- **Multifunction devices and business systems** - Upland Accuroute is a premier provider of software solutions complementing the hardware solutions offered by leading manufacturers of multifunction devices and business machines such as Hewlett Packard, Ricoh Corporation, and Xerox Corporation.

Upland Accuroute has also become a premier provider of software solutions that complement the hardware solutions offered by these highly successful companies with established global presence. This partnership enabled Accuroute to join the esteemed HP Platinum Partner Program in 2007. Accuroute won the Ricoh and Sun Java Solutions Developer Challenge in 2006.

- **Document and records management systems** - AccuRoute integrates with leading document and records management solutions including:

CA MDY FileSurf, Dropbox™, box, WebDav, Google Drive™, EMC® Documentum®, HP Records Manager, Hyland® OnBase®, iManage, OpenText Document Management (formerly Livelink ECM - eDocs™ DM and Hummingbird DM), Microsoft® SharePoint®, Microsoft OneDrive™ (Personal and Business), World Software WORLDOX®, Xerox® DocuShare, Iron Mountain Accutrak (XE)®, and OpenText LegalKEY®.

Note The software may enable you to send data to third parties in connection with the use of one of their services, including box, Google (for Google Drive) or Microsoft (for Microsoft OneDrive).

Additionally, Accuroute has developed unique systems for streamlined document routing: Accuroute™ ObjectArchive™, FileShare, MyFolder, and Single Page Image Files.

- **Cost management systems** - AccuRoute integrates with Control Systems Copitrak®, Equitrac Professional®, and nQueue® Billback iA Cost Recovery interfaces.
- **Litigation support systems** - AccuRoute can distribute documents to litigation support systems such as CT Summation, FTI® Ringtail™, and LexisNexis® Concordance®.

For more information on these and other AccuRoute integrations, contact [Upland AccuRoute Service and Support](#).

Summary for deploying the AccuRoute server

- 1 Ensure that you meet the installation requirements outlined in [Section 2: Requirements](#).
- 2 Install the AccuRoute server using the instructions in [Section 3: Installing the AccuRoute Server](#).
- 3 Perform required configurations using the instructions in [Section 5: Post Installation Configurations](#).
- 4 Perform optional configurations, if needed, using the steps in [Section 6: Optional Configurations](#).
- 5 Set up Microsoft ExchangeX integration, if required, using the instructions in [Section 7: ExchangeX Integration](#).
- 6 Set up Domino/Lotus Notes integration, if required, using the instructions in [Section 8: Lotus Notes Integration](#).
- 7 Set up SMTP integration using the instructions in [Section 9: SMTP Integration](#).
- 8 Set up other server-side features such as:
 - ▶ ObjectArchive ([Section 10: Installing ObjectArchive](#))
 - ▶ Remote Administrator ([Section 11: Installing Remote Administrator](#))
 - ▶ Remote Composer ([Section 12: Installing an additional Composer](#))
 - ▶ Remote Modem Server ([Section 13: Installing Remote Modem Server](#))
 - ▶ Remote Embedded Directive Manager ([Section 14: Installing Remote Embedded Directive Manager](#))
 - ▶ Remote AccuRoute connector for DMS libraries ([Section 15: Installing Remote AccuRoute Connector for DMS libraries](#))
 - ▶ Remote AccuRoute Intelligent Device Client ([Section 16: AccuRoute Intelligent Device Client](#))

Depending on your licenses, you can set up the AccuRoute Desktop Client or the AccuRoute Web Apps Client for users to create Distribution Rules. Consult the [AccuRoute v6.0 documentation](#) page that has links to AccuRoute Desktop, AccuRoute Web Apps Client, and all other related documentation for AccuRoute server v6.0.

Use the AccuRoute Server Administrator to monitor system failures and troubleshoot workload bottlenecks.

Icon Key

AccuRoute uses icons to identify both the type of message routed and the state (successfully sent or not) of each message. The following tables list these icons and their corresponding meanings.

Table I-2: Successful Queue Icons



| Icon | Meaning |
|---|-----------------|
|  402 | Completed Fax |
|  223 | Completed Email |

Table I-2: Successful Queue Icons








| Icon | Meaning |
|---|------------------------------|
|  324 | Notification |
|  397 | Successful FaxCenter Routing |

Table I-3: General Failure Queue Icons

| Icon | Meaning |
|---|----------------------------|
|  401 | Failed Fax |
|  322 | Failed Email |
|  389 | Failed Notification |
|  405 | Failed FaxCenter |
|  393 | Failed Fax (Issue Sending) |

Related documentation

A complete list of related documentation is available online on the [AccuRoute v6.0 documentation](#) page.

Section 2: Requirements

The streamlined AccuRoute Server installation and configuration process automates a series of verification, installation and configuration tasks. However, before you can install the AccuRoute server on a system, you need to make some initial server configurations and assure hardware and software requirements are met.

This section discusses hardware and software requirements for the AccuRoute server installation, as well as the required server configurations.

[Hardware and software requirements](#) (2-1)

[Creating the AccuRoute service account](#) (2-3)

[Creating AccuRoute Admins group](#) (2-4)

[Configuring AccuRoute service account permissions for ExchangeX](#) (2-4)

[Installing Microsoft SQL Express on the AccuRoute server](#) (2-4)

Hardware and software requirements

The AccuRoute server installation requires a dedicated system that meets the following minimum requirements:

- Windows NT domain computer that always runs in the same domain and is not a domain controller
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device

Note Hardware requirements are subject to change based on the configuration of implementation.

AccuRoute recommends using a core for each compose thread that is configured to do OCR. The AccuRoute server comes with two Compose threads. You can increase the number of threads as needed. contact [Upland AccuRoute Service and Support](#) for more information.

-
- Microsoft Windows 2012 x64, Windows 2012 R2 x64, or Windows 2016 x64
 - Windows Active Directory - AccuRoute v6.0 can only be installed in Windows Active Directory environment. All server security and authentications are dependent on the Active Directory authentication.
 - Microsoft.Net Framework:
 - ▶ MS.Net 4.6.1 is required to install the AccuRoute Server.

Note The installation includes MS.Net 4.6.1, if not currently installed.

- ▶ MS.Net 3.5.1 is required to install the Embedded Device Client, the Intelligent Device Client, the Web Apps Client, and the Legacy Web Views Client.

Note In a Windows 2012 environment, MS.Net 3.5.1 is not included or configured with the pre-installation package. As a requirement for Device Client installations, you need to independently download and install MS.Net 3.5.1 to your Windows 2012 system.

Important For **Exchange 2010**, the Exchange server must have a Foreign Connector specified with FAX address type. For general information on Foreign Connector, see <http://technet.microsoft.com/en-us/library/aa996779.aspx>. For information on how to create a Foreign Connector, see <http://technet.microsoft.com/en-us/library/aa996397.aspx>. For information on “Set-ForeignConnector” cmdlet to modify an existing foreign connector, see <http://technet.microsoft.com/en-us/library/bb123789.aspx>.

- Notes v5.x / v6.x /v6.5 client (for Notes integration only)
 - Microsoft Internet Explorer 11, or later
 - Acrobat Reader 9.0 or 11.0 or later
 - Internet connection (required for installing Microsoft.Net and for using cloud-based Folders)
-

Note Do not run any other enterprise application on the AccuRoute server system.

Supported Devices

AccuRoute supports the AccuRoute Embedded Device Clients on many devices. Refer to the [AccuRoute v6.0 Release Notes](#) for a current and comprehensive list of supported devices.

Additional software requirements for a local Composer

The AccuRoute server setup automatically installs a local Composer on the AccuRoute server. This is needed to compose documents into the specified final formats. You can also install a Remote Composer if needed. For installation instructions, see [Installing an additional Composer](#) (12-1).

The Local and Remote Composers must have the following applications installed if using the native application to convert documents. For example, if you are planning to use Crystal Reports for compose, it must be installed on the compose server.

- Microsoft Visio 2007 for *.VSD and *.VDX message attachments.
- Crystal Reports v10.0 or earlier for *.RPT message attachments

Important Visual Basic for Applications is required for PowerPoint document conversion. You must install this component for PPT and PPTX document formats to compose successfully on the AccuRoute server. If this component is not installed, and you try to compose a PowerPoint document, you will get an error.

Note Routing Sheet templates are provided in *.DOC and *.OMTPL format, and these templates can be edited in Word and WordPad respectively. For more information on Routing Sheet templates, consult the *AccuRoute Desktop Installation Guide*, which is available on the [AccuRoute v6.0 documentation page](#).

Additional installation requirements

An AccuRoute server installation also requires the following:

- AccuRoute service account. For instructions on how to create the AccuRoute service account, see [Creating the AccuRoute service account](#) (2-3)
- Windows user account that belongs to the local Administrators group. For instructions on how to create this group, see [Creating AccuRoute Admins group](#) (2-4)
- AccuRoute server license key
- Licenses for any additional features that require a license
- Configuring AccuRoute service account for ExchangeX.

Note This is required only if you are integrating with ExchangeX environment.

For instructions, see [Configuring AccuRoute service account permissions for ExchangeX](#) (2-4). If you have an ExchangeX Virtual server, see [Installing Microsoft SQL Express on the AccuRoute server](#) (2-4)

- Installed MS SQL application. For instructions, see [Installing Microsoft SQL Express on the AccuRoute server](#) (2-4)
- Fax boards/modules that has been installed, configured, and tested. This is required only for an AccuRoute server that supports faxing. For information on fax board installation, consult the *Dialogic Modem Driver Installation and Configuration Guide*, which is available on the [AccuRoute v6.0 documentation page](#).

Creating the AccuRoute service account

The AccuRoute service account is a dedicated Windows user account that is designed to run AccuRoute services on the AccuRoute server.

Important AccuRoute recommends that you do not change this account or the password associated with it.

The AccuRoute service account user:

- Must belong to Domain Users group in the domain where the AccuRoute server is being installed
- Must belong to local Administrators group on the system where the AccuRoute server is being installed
- Must have a password that never expires

You can create or select a Windows user account as the AccuRoute service account. For instructions on creating Windows user accounts, consult Windows help.

Creating AccuRoute Admins group

The AccuRoute Admins group consists of all AccuRoute users who run the AccuRoute Server Administrator (either on the AccuRoute server or on a Remote Administrator). These AccuRoute users must have Distributed COM access, launch, and configuration permissions on the AccuRoute server.

To create an AccuRoute Admins group:

- 1 Go to Active Directory. Locate the domain where the AccuRoute server is being installed.
- 2 Create a group for AccuRoute Server Administrator users. Name this group AccuRoute Admins.
- 3 Add all AccuRoute users who will run the AccuRoute Server Administrator to the AccuRoute Admins group.
- 4 Log in to the system where the AccuRoute server is being installed using an account that belongs to the local Administrators group.
- 5 Add the AccuRoute Admins group to the local Administrators group.

When you need to add additional users to run the AccuRoute Server Administrator, you can add them to the AccuRoute Admins group.

Configuring AccuRoute service account permissions for ExchangeX

The AccuRoute connector for ExchangeX on the AccuRoute server is a gateway to ExchangeX, and the AccuRoute service account (the logon account for the AccuRoute Connector Manager service) must have specific permissions.

ExchangeX 2010 and Exchange Server 2013

For ExchangeX 2010 and Exchange Server 2013, permission is needed is access to the drop directory when creating the AccuRoute connector for ExchangeX. For more information on the drop directory, consult Microsoft documentation in <http://technet.microsoft.com/en-us/library/aa996779.aspx>.

Installing Microsoft SQL Express on the AccuRoute server

The AccuRoute server utilizes the MS SQL Express database to store and archive messages. It requires access to one of the following SQL database applications: SQL Express 2016, 2012 or 2008.

Use one of the following SQL database applications:

- **SQL Express 2016, 2012 or 2008** - This limited Microsoft SQL database application provides the basic database services the AccuRoute server needs to maintain its SQL databases. It is licensed as part of the AccuRoute installation.
 - ▲ SQL Express must be installed local to the AccuRoute server.
 - ▲ SQL Express installation requires Microsoft .NET Framework 3.0.

When installed on the AccuRoute server, SQL Express must only service databases for AccuRoute. Consider that installing an instance of SQL Express on the AccuRoute server might require the purchase of an additional SQL Express license.

Important Installing the full SQL Server (2016/2012/2008) on the AccuRoute server is not recommended.

Note If undetected during the automated prerequisites check, a minimum version of Microsoft SQL Express 2012 is automatically installed.

Section 3: Installing the AccuRoute Server

This section includes:

- [Introduction to installing the AccuRoute server](#) (3-1)
- [Automated pre- and post-installation and configuration tasks](#) (3-2)
- [Installing the AccuRoute server](#) (3-2)
- [Creating and configuring the database](#) (3-11)
- [Completing the Server Configuration Wizard](#) (3-14)
- [Activating the license](#) (3-16)
- [Uninstalling the AccuRoute server](#) (3-22)

Introduction to installing the AccuRoute server

The AccuRoute server is installed with:

- Specialized Windows services that carry out the document distribution responsibilities of the server
- Components used to complete message processing tasks
- Connectors used to connect the AccuRoute server with external systems that submit messages to the server and distribute them to their final destinations
- AccuRoute Server Administrator, the management application for the AccuRoute server

The AccuRoute server setup program has a verification utility that checks the server for compliance with installation requirements. All installation requirements must be met before AccuRoute can be installed (see [Section 2: Requirements](#)).

If you are setting up an AccuRoute server cluster, review the AccuRoute cluster setup instructions in [Appendix A: Setting up an AccuRoute Server Cluster](#) before beginning the AccuRoute server installation.

Important The AccuRoute server installs with a 30-day demonstration license.

Automated pre- and post-installation and configuration tasks

The pre-installation package automatically verifies, installs, and/or configures a variety of prerequisites, including:

- Minimum versions of the OS, Internet Explorer, .NET, and Microsoft SQL
- SMTP and IIS services
- 32-bit IIS applications
- DCOM and IIS configuration
- Installation of required runtime libraries
- Internet Enhanced Security (IE ESC) is disabled
- 8.3 Naming Convention is disabled
- IIS large scanning setting is enabled
- Application of Windows firewall settings
- Print spooler and IIS services set to automatic
- User Access Control (UAC) set to required setting

Post-installation configuration requirements are automated as well. Post-installation configurations for the server include:

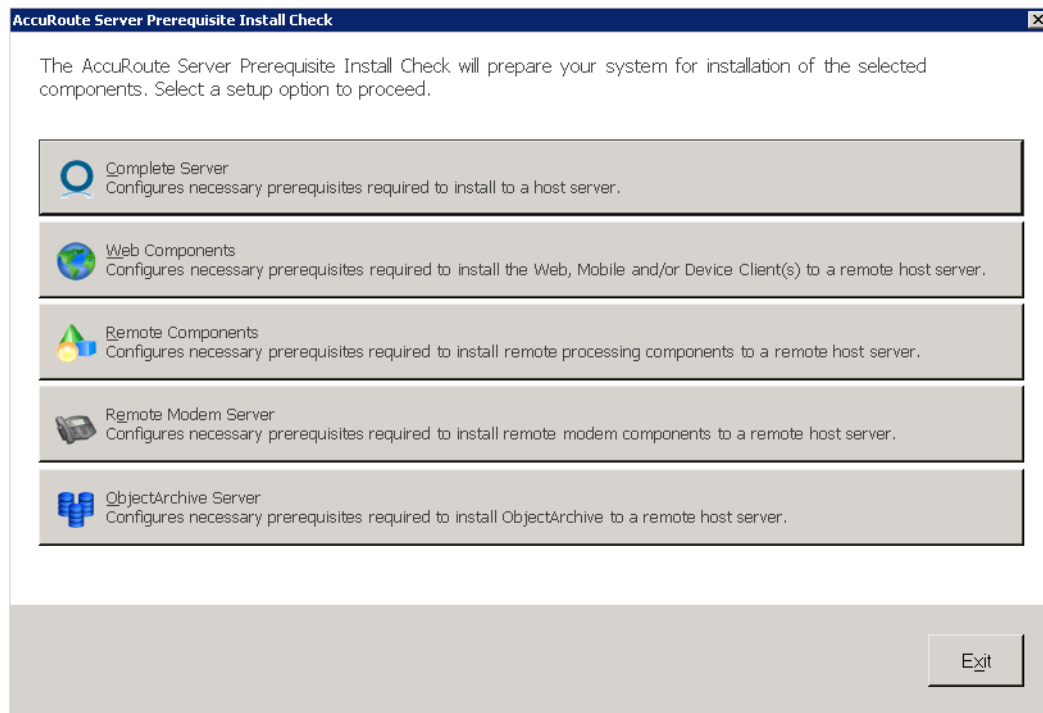
- Setting the Doc, Docx, XLS, XLSX, PPT, PPTX, HTM and HTML formats to use the Aspose compose engine
- Setting a Cleanup task in Maintenance for 30 days

Note It is recommended to run this program on all servers that will run AccuRoute or remote AccuRoute components.

Installing the AccuRoute server

- 1 Log in to the system where the AccuRoute server is being installed using the Omttool service account.
- 2 Go to the network copy of the AccuRoute server setup and run `\AccuRoute\Setup.exe`.

3 The AccuRoute Prerequisite Install Check screen appears.



Select the option for which you want your system automatically prepared.

Each option checks for and (if not already present) installs and/or configures the necessary prerequisites for your selection.

Complete Server – prepares the system to install the AccuRoute Server onto one host server, including:

- ▲ Microsoft.NET Framework 4.6.1
- ▲ Microsoft.NET Framework 3.5 SPI
- ▲ Microsoft SQL Server 2012 Express
- ▲ Web Server IIS installation
- ▲ Sets the W3SVC Service (from the Web Server) to Automatic Startup
- ▲ SMTP Service installation
- ▲ Sets the SMTP Service to Automatic Startup
- ▲ Adds a DCOM Exception in the Windows Firewall
- ▲ Sets the Print Spooler Service to Automatic Startup

Web Components – prepares the system to install the Web, Mobile and/or Device Client(s) to a remote host server, including:

- ▲ Microsoft.NET Framework 4.6.1
- ▲ Microsoft.NET Framework 3.5 SPI
- ▲ Web Server IIS installation
- ▲ Sets the W3SVC Service (from the Web Server) to Automatic Startup

- ▲ Adds a DCOM Exception in the Windows Firewall

Remote Components – prepares the system to install remote processing components onto a remote host server, including:

- ▲ Microsoft.NET Framework 4.6.1
- ▲ SMTP Service installation
- ▲ Sets the SMTP Service to Automatic Startup
- ▲ Adds a DCOM Exception in the Windows Firewall
- ▲ Sets the Print Spooler Service to Automatic Startup

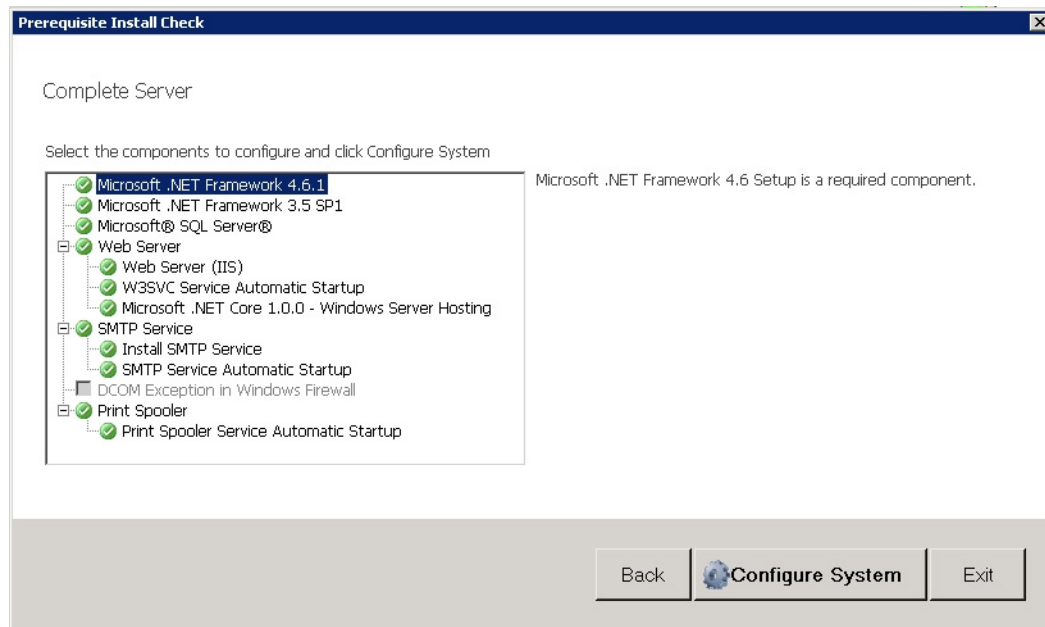
Remote Modem Server – prepares the system to install remote modem components to a remote host server, including:

- ▲ Microsoft.NET Framework 4.6.1
- ▲ Adds a DCOM Exception in the Windows Firewall

ObjectArchive Server – prepares the system to install ObjectArchive to a remote host server, including:

- ▲ Microsoft.NET Framework 4.6.1
- ▲ Microsoft SQL Server 2012 Express
- ▲ Adds a DCOM Exception in the Windows Firewall

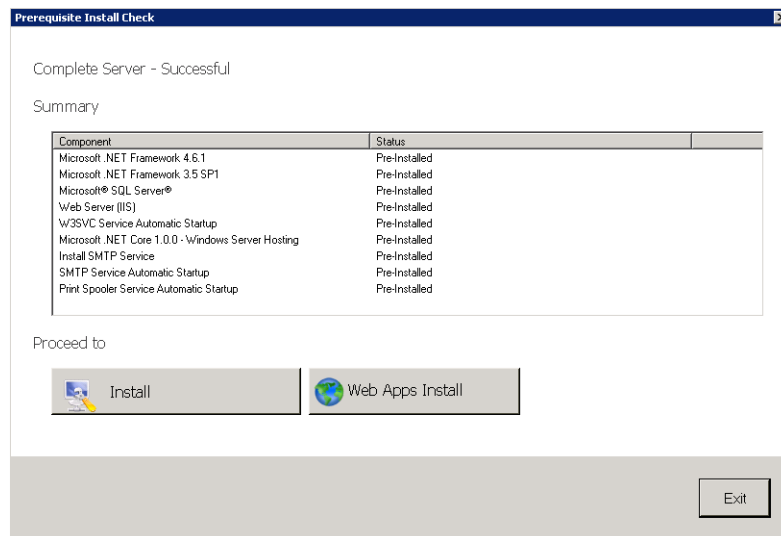
- 4 A default list of components to be configured before installation appears in the next screen.



Click **Configure System**.

Note A **File In Use** Windows dialog may appear in the background. Find the dialog and click **OK** to proceed with the configuration.

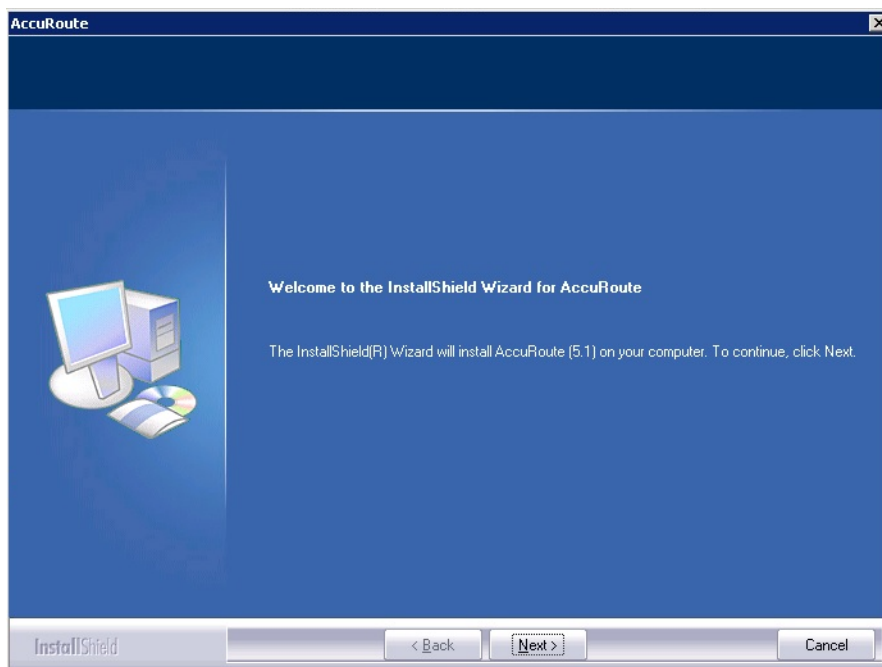
- 5 When the system finishes configuring your prerequisites, a **Successful Summary** screen appears, listing components and their status.



Click the installation type with which you want to proceed (**AccuRoute Server** or **Web Apps Install**).

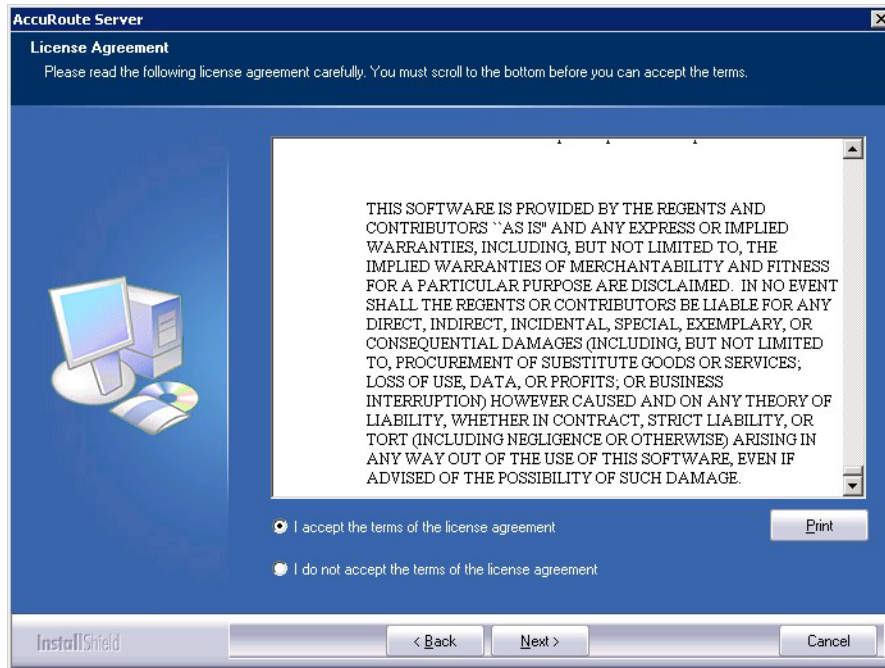
The system prepares the InstallShield wizard for the installation process.

The InstallShield wizard opens and displays a **Welcome** message.

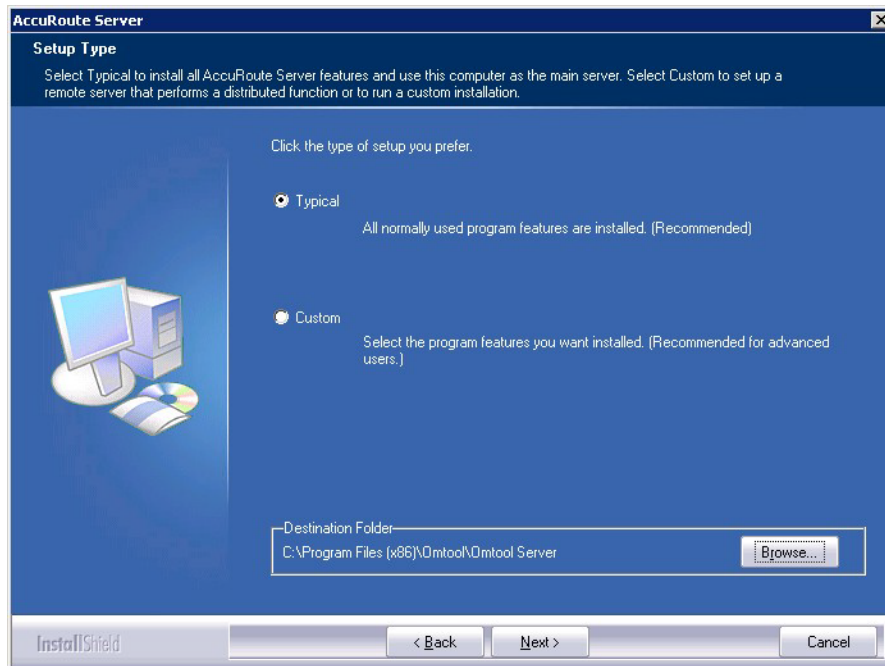


- 6 Click **Next**. The setup shows the **License Agreement** page.

- 7 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms. Select **I accept the terms of the license agreement**.



- 8 Click **Next**. The **Setup Type** options are displayed.



Note The default destination folder is `C:\Program Files (x86)\Omtool\Omtool Server\`. You can change the destination, if necessary, by clicking **Browse** and then navigating to the desired location. However, you cannot install the server on the root of a drive (for example, `C:\`).

9 Select one of the following:

- ▶ **Typical** for an installation that does not support faxing
- ▶ **Custom**, to select options, such as the modem server

If you select **Custom**, select options for the AccuRoute server installation. The following features are selected by default:

- ▲ Message Server
- ▲ Connector Package
- ▲ Component Package
- ▲ Server Administrator
- ▲ Intelligent Device Client
- ▲ Client Installs
- ▲ Server Tools
- ▲ Mobile Device API

The following features **must** be selected for a server installation:

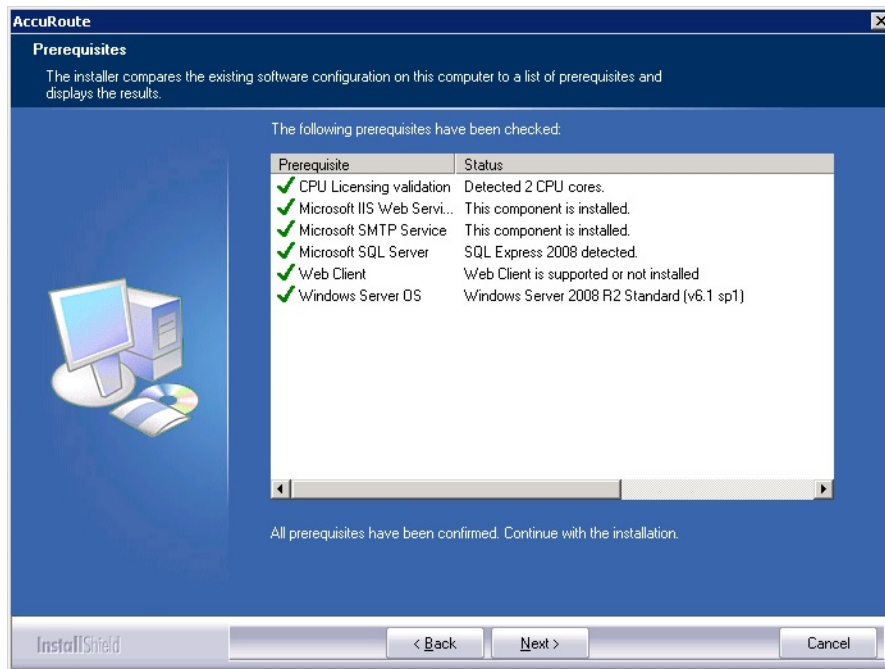
- ▲ Message server
- ▲ Connector Package
- ▲ Component Package
- ▲ Server Administrator
- ▲ Client Installs

The remaining features can be installed on remote systems depending on the planned environment structure.

Important Select the Modem Server option to support faxing with a local Modem Server.

Important ObjectArchive is only supported when installed on a system remote from AccuRoute server. Go to [Section 10: Installing ObjectArchive](#) for more information. Note that ObjectArchive is not cluster aware.

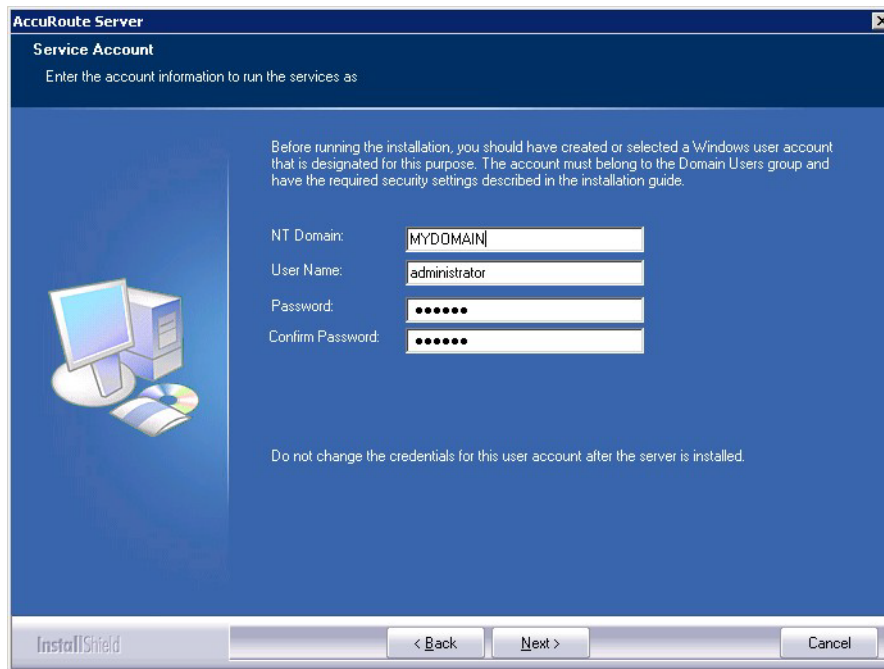
10 Click **Next**. The setup checks the system for installation requirements and displays the results.



11 Review the results and perform one of the following actions.

- ▶ To exit the setup or to install components that are required for the installation, click **Cancel** and then click **Yes** to exit the setup.
- ▶ To continue with the installation, click **Next**.

- 12** On the **Service Account** screen, provide the login credentials of the Omtool service account.

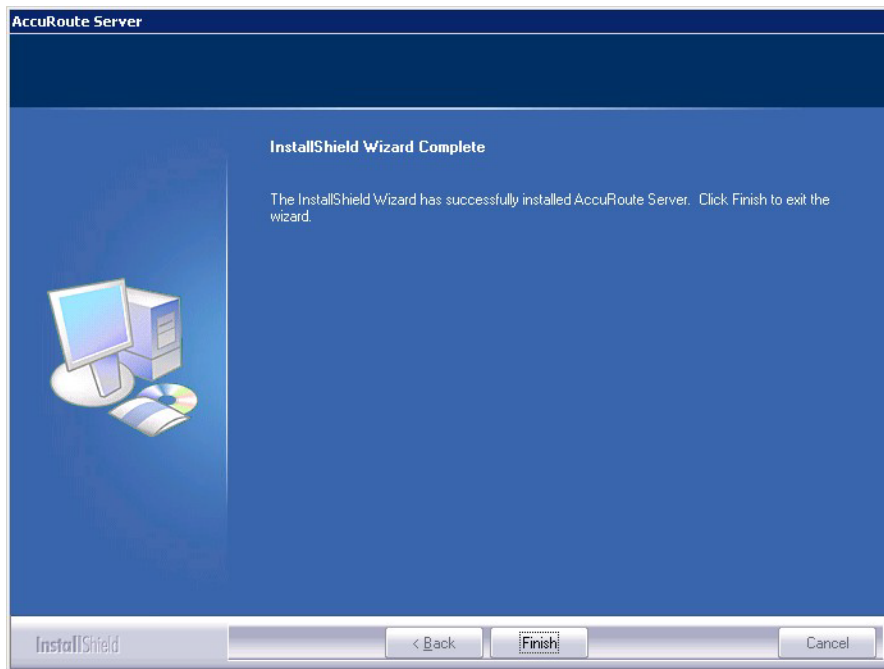


The screenshot shows the 'Service Account' screen in the AccuRoute Server installation wizard. The window title is 'AccuRoute Server' and the subtitle is 'Service Account'. Below the subtitle, it says 'Enter the account information to run the services as'. On the left, there is an illustration of a computer monitor, tower, and mouse. On the right, there is a text box with instructions: 'Before running the installation, you should have created or selected a Windows user account that is designated for this purpose. The account must belong to the Domain Users group and have the required security settings described in the installation guide.' Below this text are four input fields: 'NT Domain:' with 'MYDOMAIN', 'User Name:' with 'administrator', 'Password:' with six dots, and 'Confirm Password:' with six dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is in the bottom left corner.

- a** In the **NT Domain** field, enter the name of the Windows domain.
 - b** In the **User Name** field, enter the user name. By default, the **User Name** field is populated with the name of the user logged in to Windows.
 - c** In the **Password** and **Confirm Password** fields, enter the password for the user.
 - d** Click **Next**.
- 13** Review the installation settings on the **Installation Settings** screen. Click **Next** to proceed with the installation.

Progress details appear on the **Setup Status** screen.

14 The **InstallShield Wizard Complete** screen appears. Click **Finish**.

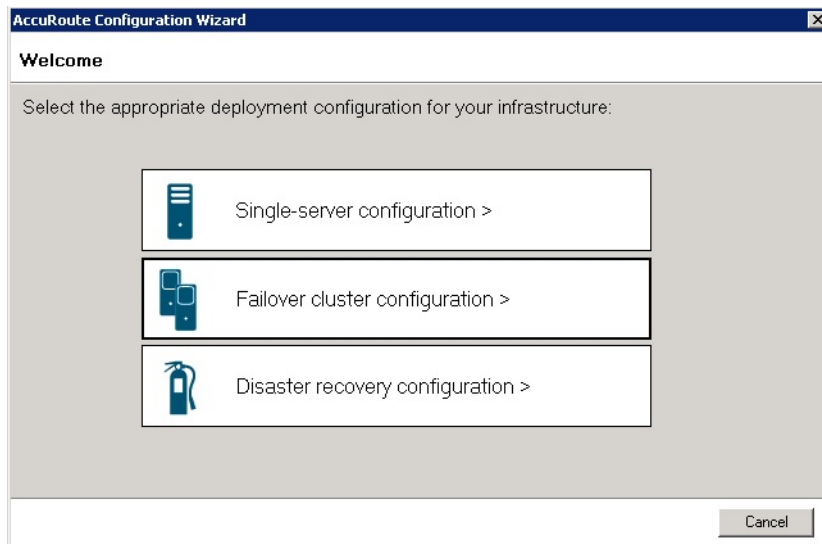


The setup launches the **Database Configuration Wizard**. Continue with the procedure for [Creating and configuring the database](#) below.

Creating and configuring the database

Continue the installation process by creating and configuring the database.

- 1 The AccuRoute **Database Configuration Wizard Welcome** screen opens.

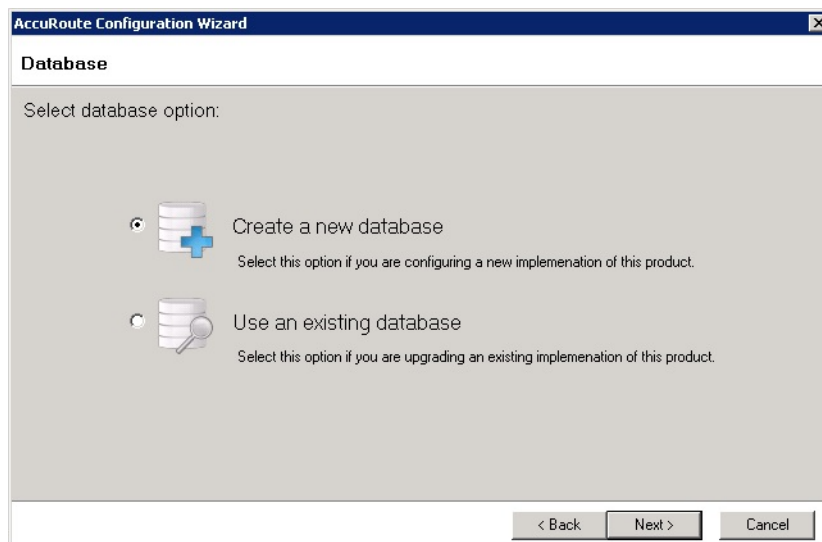


- 2 For a typical server installation, select **Single-server configuration**.

Note For more information about **Failover cluster configuration**, refer to [Setting up an AccuRoute Server Cluster \(A-I\)](#).

Also note, for more information about **Disaster recovery configuration**, refer to [Configuring Disaster Recovery](#).

- 3 The **Database** screen opens.



Select **Create a new database** and click **Next**.

Note Only select **Use an existing database** if you are upgrading an existing release of this product. See the [AccuRoute Server and Clients Upgrade Guide](#) on the [AccuRoute v6.0 documentation page](#) for more information.

4 The **Create New Database** screen opens.

To create the database:

- a Enter the SQL Server name:
 - ▲ If the setup detects **Microsoft SQL Server Express 2008/2012**, verify that the **SQL Server** field is populated with the name of the server running the Microsoft SQL server database application and that `\SQLExpress` is appended to the server name.
 - ▲ If the setup detects **SQL Server 2008 SP2** or **SQL Server 2012**, verify that the **Server** field is populated with the name of the server running the Microsoft SQL server database application.

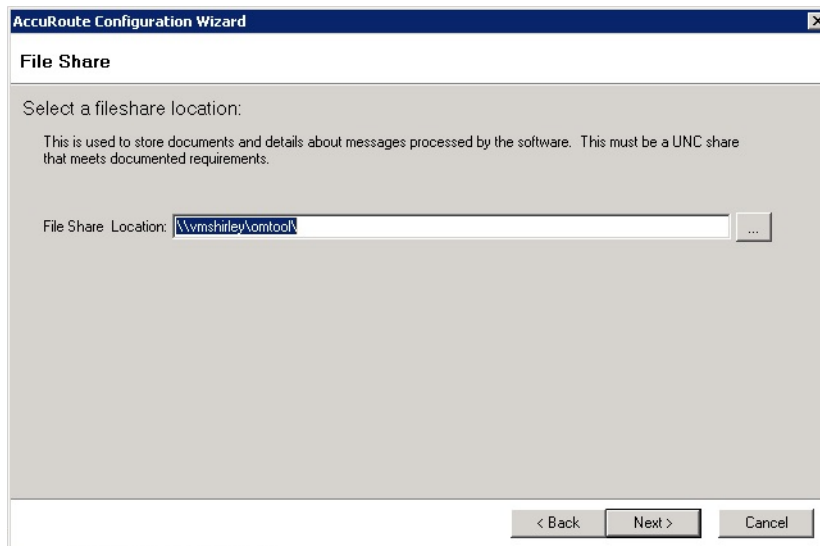
Note The default value is the local server where the setup is running.

- b Select the authentication method that the AccuRoute services use to access the database. Choose one of the following:
 - ▲ **Use Windows Integrated Authentication** to use the AccuRoute service account. This is the default choice.
 - ▲ **Use SQL Authentication Login** to use SQL server authentication. If you select this option, enter the login credentials in the **Username** and **Password** fields.
- c In the **Database Name** field, review the database name and modify it if necessary.

Note Special instructions apply to an AccuRoute server cluster. For the first server being set up, enter the database server name. For the second server being set up, allow the setup to create a local database. (The second server is configured to use the database server, so the local database is not used.) For more information, refer to [Section A: Setting up an AccuRoute Server Cluster \(A-1\)](#).

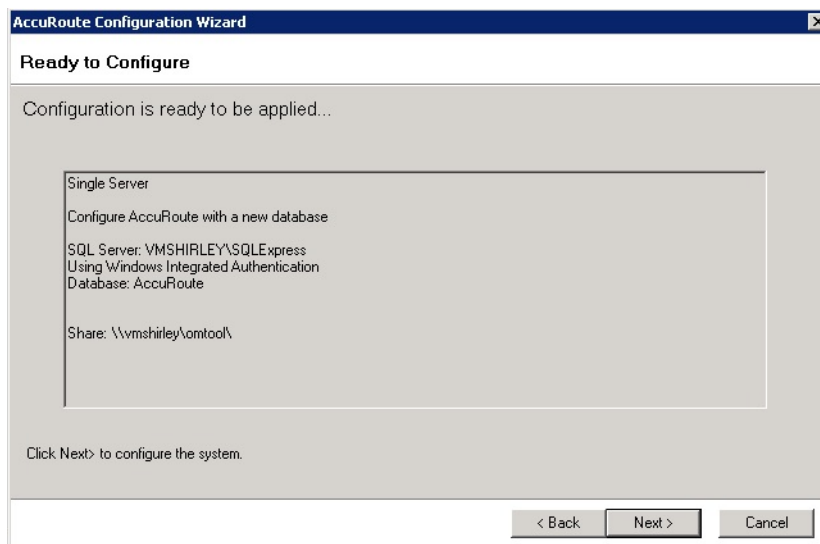
d Click **Next**.

5 The **File Share** screen appears.



Enter the **File Share Location** at which you want the system to store message documents and details, and click **Next**.

6 The **Ready to Configure** screen opens. Click **Next** to configure the new database.



7 You can view progress of the configuration on the **Configuring...** screen.

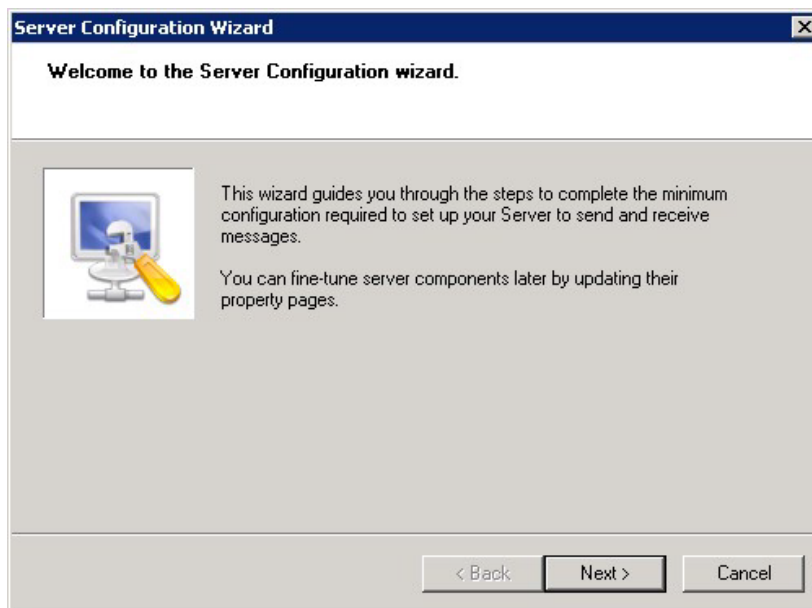
Click **Next** when the process is complete to launch the **Server Configuration Wizard** (described in the next section).

Continue with the procedure for [Completing the Server Configuration Wizard](#) below.

Completing the Server Configuration Wizard

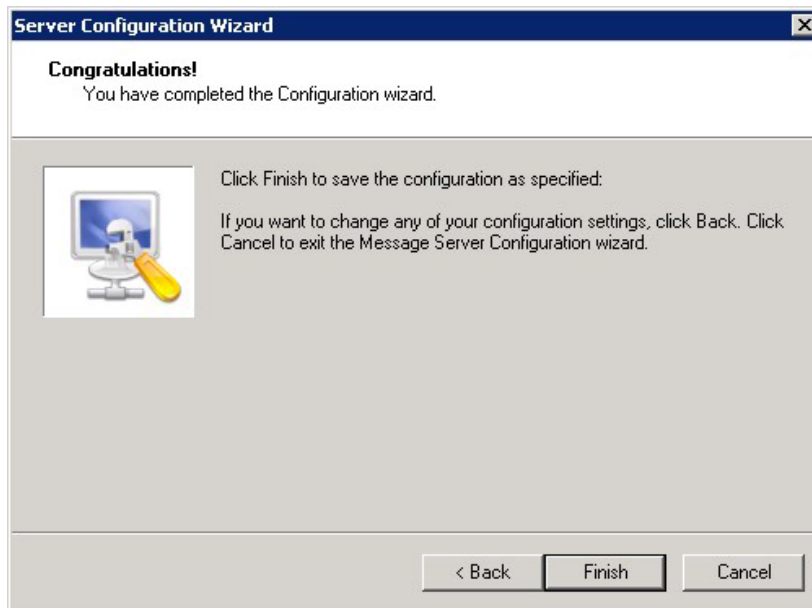
After the AccuRoute server and database are installed, the Server Configuration wizard automatically launches. You must complete this wizard before starting the AccuRoute Server Administrator.

- I When the Server Configuration wizard opens to the **Welcome** screen, click **Next**.



Important When setting up the passive server in an AccuRoute server cluster, exit the Server Configuration wizard and click **Cancel** when prompted to run the wizard again after the AccuRoute Server Administrator starts.

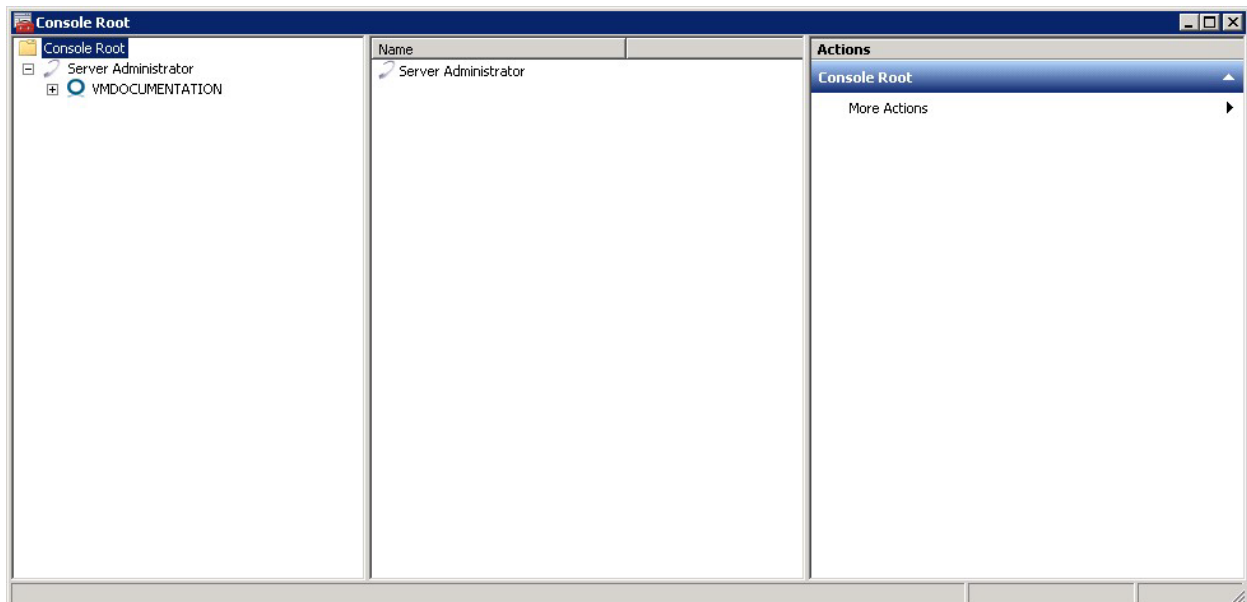
- 2 The **Congratulations!** screen appears to indicate the Server Configuration is complete.



- 3 Click **Finish** to close the wizard. The Server Configuration wizard saves the configuration.



After the configuration is saved, the AccuRoute Server Administrator opens.



When you close the AccuRoute Server Administrator, Microsoft Management Console displays a message about saving changes to the MSC file. This file records the current position of items in the console tree. To preserve the console state, save the changes.

If prompted to update the MSC file, click **Yes**.

Note about registry keys location when installing the AccuRoute server on a 64-bit machine

The 64-bit operating system stores registry keys for 32-bit applications under Wow6432Node. When installing the AccuRoute server on a 64-bit machine, the Omtool registry keys are located in **HKLM\SOFTWARE\Wow6432Node\Omtool** and not in the **HKLM\SOFTWARE\Omtool** directory.

Activating the license

After installation, the server uses a 30-day demonstration license. At some point during this time, you should activate the server license. This can be accomplished:

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

Automatic license activation

Be sure the AccuRoute server has access to the internet. Have available a copy of the activation code received with the software package.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and select the server name.
- 3 Right-click and select the **Licensing** option.

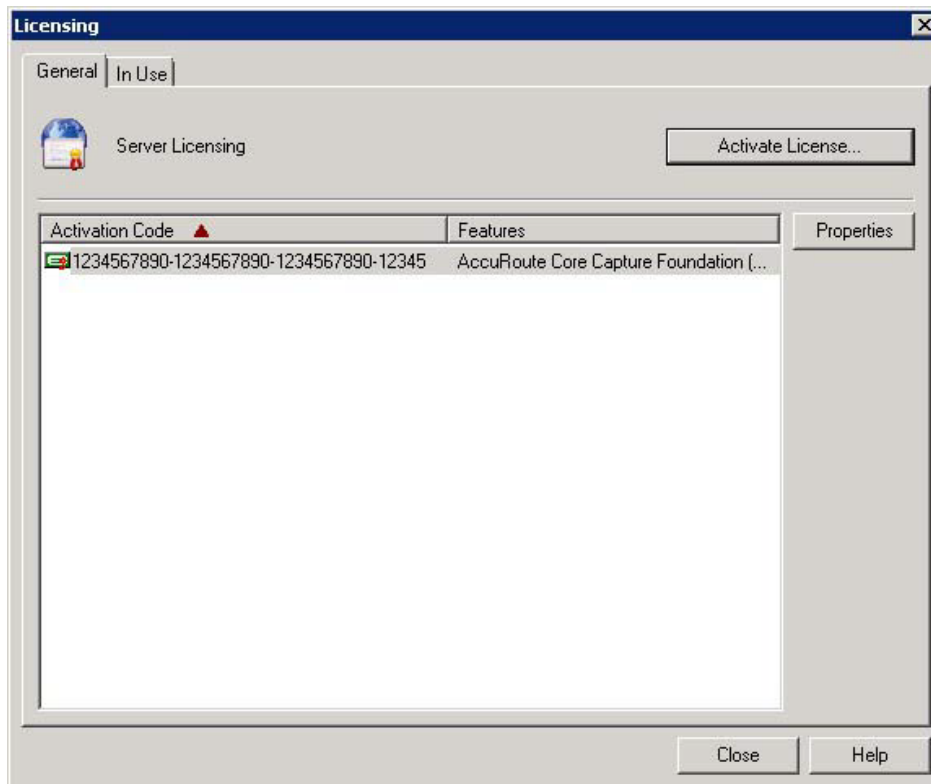
Manual license activation

Have available a copy of the activation code received with the software package.

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

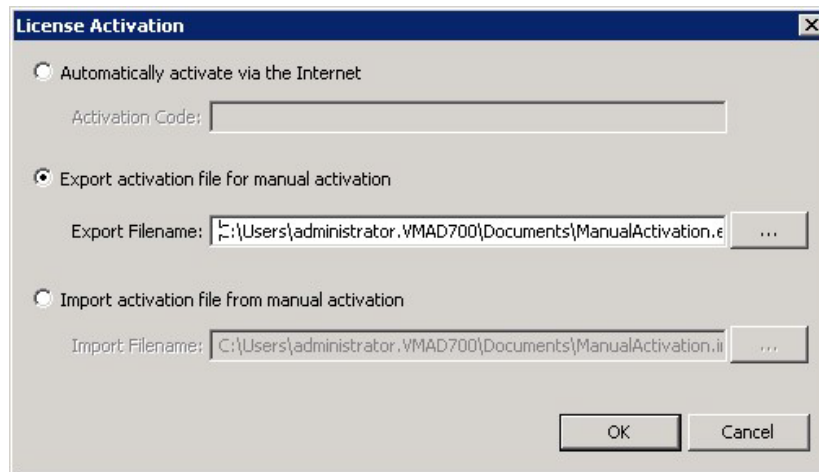
- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and select the server name.
- 3 Right-click and select the **Licensing** option.

The **Licensing** page is displayed.



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

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



6 Create an Export license file:

- a Browse to a location where you want to save the license file. By default, the file is an Export file named `ManualActivation.exp`. After specifying the file name and location, click **Save**.
- b The path will appear in the **Export Filename** field on the **License Activation** page. Click **OK**.

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

<https://license.omtool.com/accuroute>

The **Manual Licensing Portal** page opens.



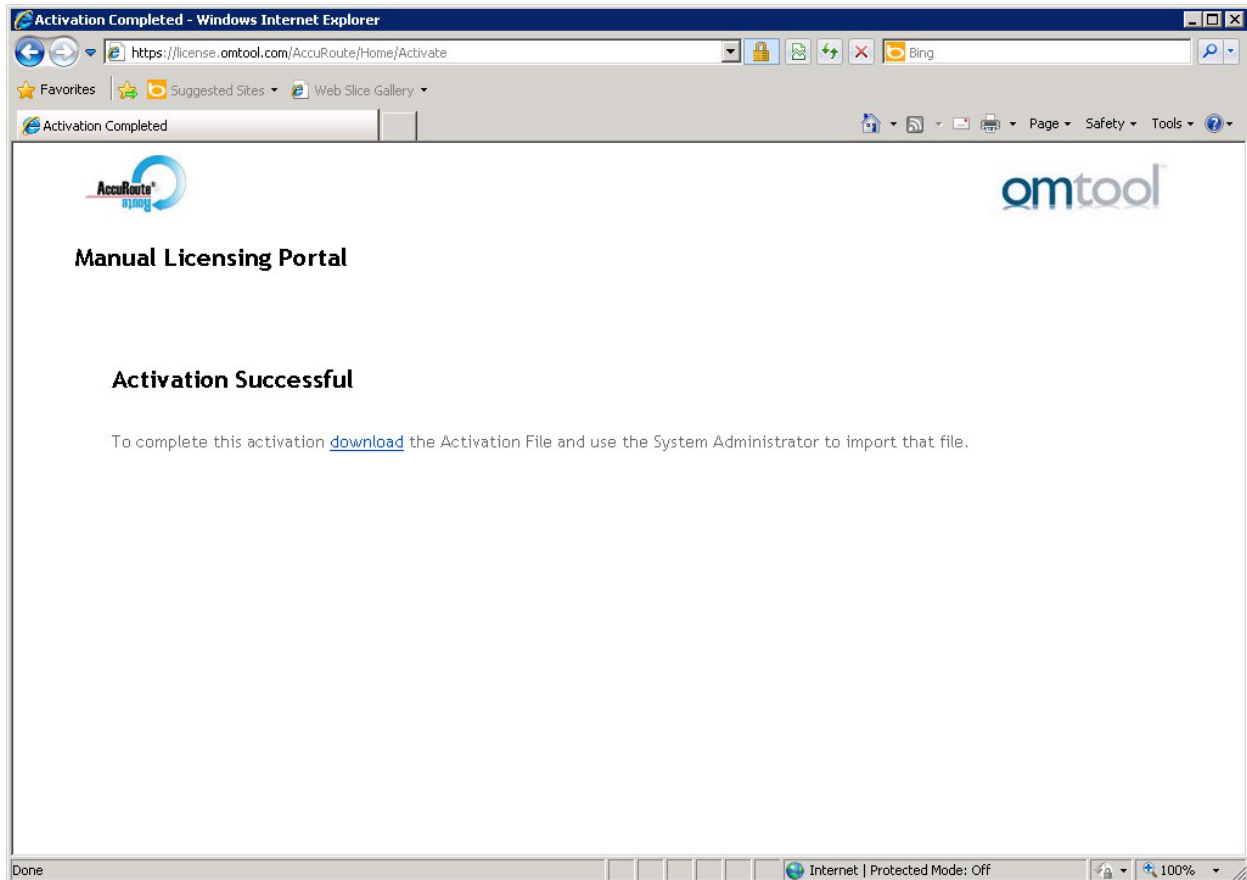
Manual Licensing Portal

Enter your activation code and select the Exported Activation File made using the Server Administrator.

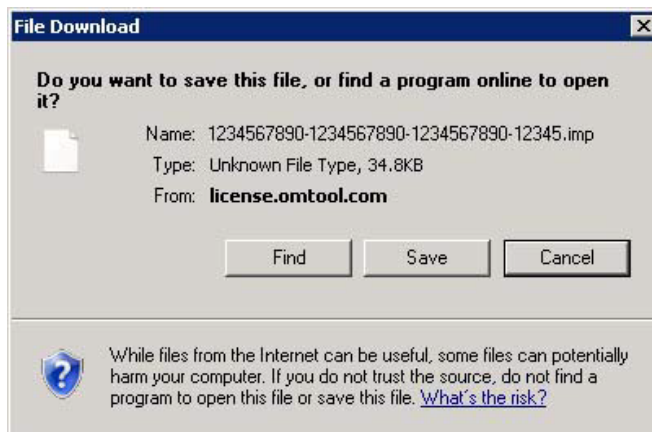
| | |
|--|--|
| Activation Code: | <input type="text"/> |
| | <input checked="" type="radio"/> Activate License <input type="radio"/> Deactivate License |
| Exported Activation File: | <input type="text"/> <input type="button" value="Browse..."/> |
| <input type="button" value="NEXT >"/> | |

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

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

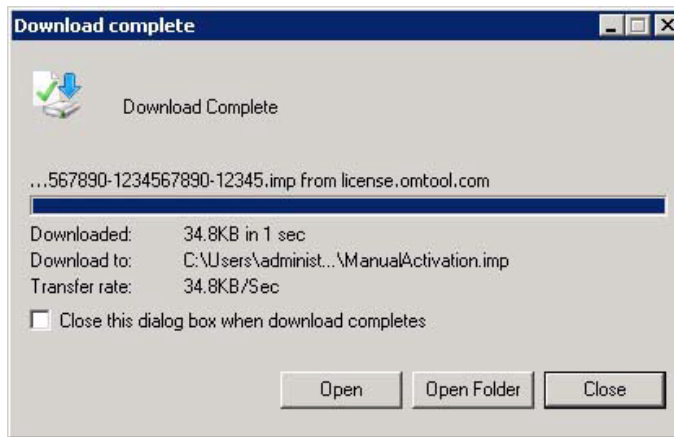


13 To complete the activation, click **Download**. The **File Download** page is displayed.



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

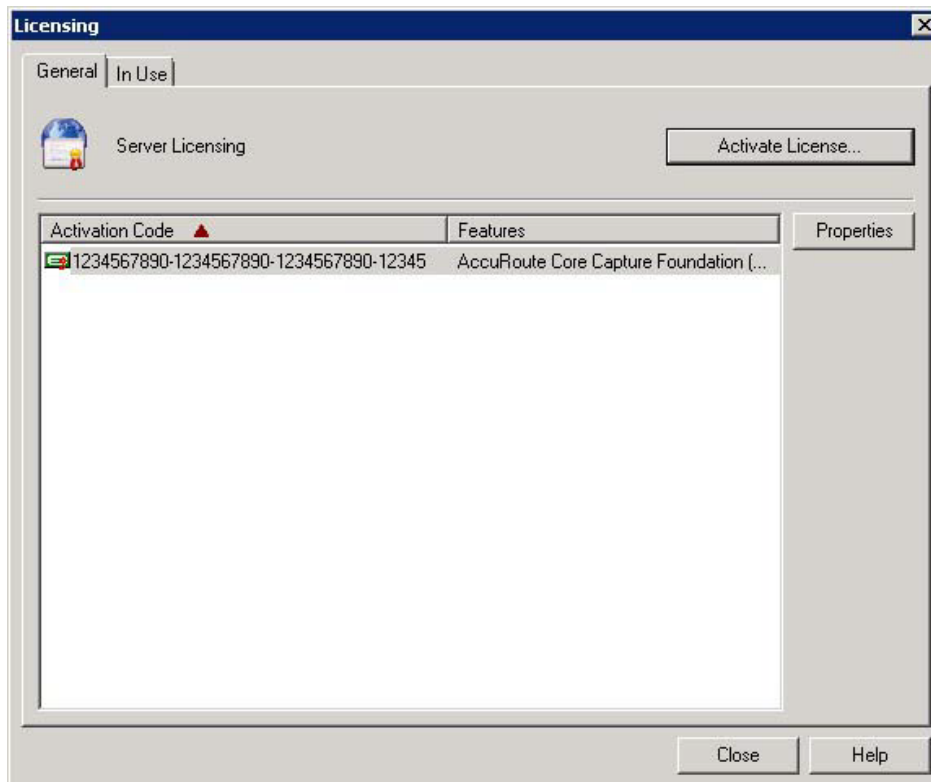
- 15 Click **Save**. The **Download Complete** page shows that status of the file download.

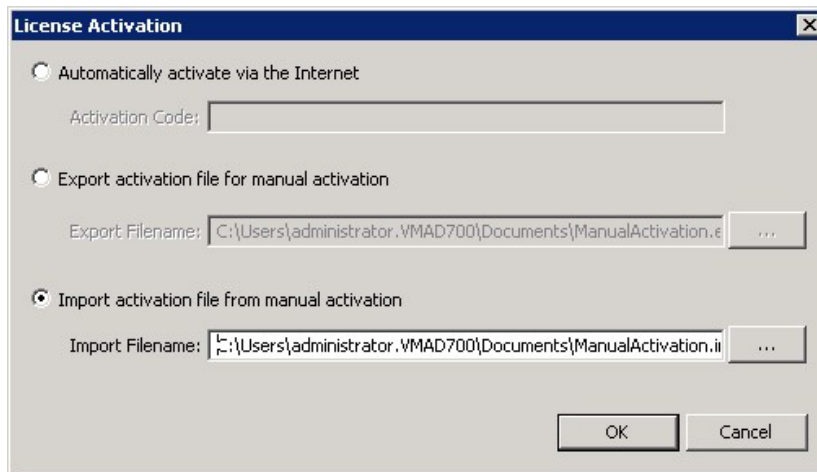


- 16 Click **Close**.

Note You can minimize or close the browser.

- 17 On the **Licensing** page, select the **Activate License...** button.



18 Select the **Import activation file from manual activation** option.**19** Browse to the saved `ManaulActivation.imp` file. Select the file and click **Open**.**20** Click **OK** on the **License Activation** page. The license is updated.**21** Click **Close** to complete the procedure.

Uninstalling the AccuRoute server

- 1** Go to the **Control Panel** and start **Add/Remove Programs** applet.
- 2** Select **AccuRoute Server** and click **Change/Remove**.
- 3** The InstallShield Wizard is initiated and prompts you to confirm that you want to uninstall the software.
- 4** Click **Remove**.

AccuRoute server is removed from your system. A progress indicator shows the status of the uninstallation.

Note After you have uninstalled the AccuRoute server, the associated folder registry entries will remain. Similarly, if you modify the server configuration after you have completed the AccuRoute v6.0 server installation, associated program files are not removed and associated services are not stopped or removed. For example, if you uninstall the Modem Server after an upgrade, associated program files are not removed and modem services are not stopped or removed. Associated program files and services remain until a complete uninstallation is performed.

Section 4: AccuRoute Mobile Client

Using the AccuRoute Mobile Client, AccuRoute users can preview and send documents from their mobile device, create Mobile Reservations for future scanning, and configure Personal Distributions. Access Group and Preset Distributions can be configured by the System Administrator and made available on a permission basis. Users can also define alerts and set default preferences.

Server Administrators configure permission to use the Mobile Client in **Group Properties** on the **Configuration** node. For more information on using the Mobile Client, refer to the [AccuRoute Server Administrator Help](#).

When AccuRoute Mobile Client users make **Mobile Reservations**, they are creating a **Mobile Scan Reservation Code** for later use at an MFP inside or outside their business network. The system uses the Mobile Scan Reservation Code to appropriately distribute the submitted document information.

If you want include remote systems in your setup or be able to accept Mobile Reservations from an external source, you must properly configure your system ahead of time:

- [Installing the Mobile Device Application](#) (4-2)
- [Installing the Mobile Client](#) (4-3)
- [Configuring a local IIS system for mobile connectivity](#) (4-3)
- [Configuring a remote IIS system for mobile connectivity](#) (4-4)
- [Environment configuration to support AccuRoute Mobile Clients](#) (4-4)

Requirements

- Licenses for both the Mobile Client and the Mobile Server Application
- AccuRoute Server v6.0
- Mobile device running either
 - ▲ iOS™ 6.x or higher
 - ▲ Android™ v4.4 or higher
- Mobile Client application downloaded directly to your device from either
 - ▲ iTunes Store®
 - ▲ Google Play™ store

Installing the Mobile Device Application

The AccuRoute v6.0 installation program includes the **Mobile Client** and the **Mobile Device Application (API)**. If you have a remote IIS system on which to install the AccuRoute Mobile Device API, you will need to install the Mobile API prior to setting up the Mobile Client.

Note Follow the steps below if your IIS system is remote from the AccuRoute Server. Depending on the needs of your organization, you may prefer to do so for security purposes.

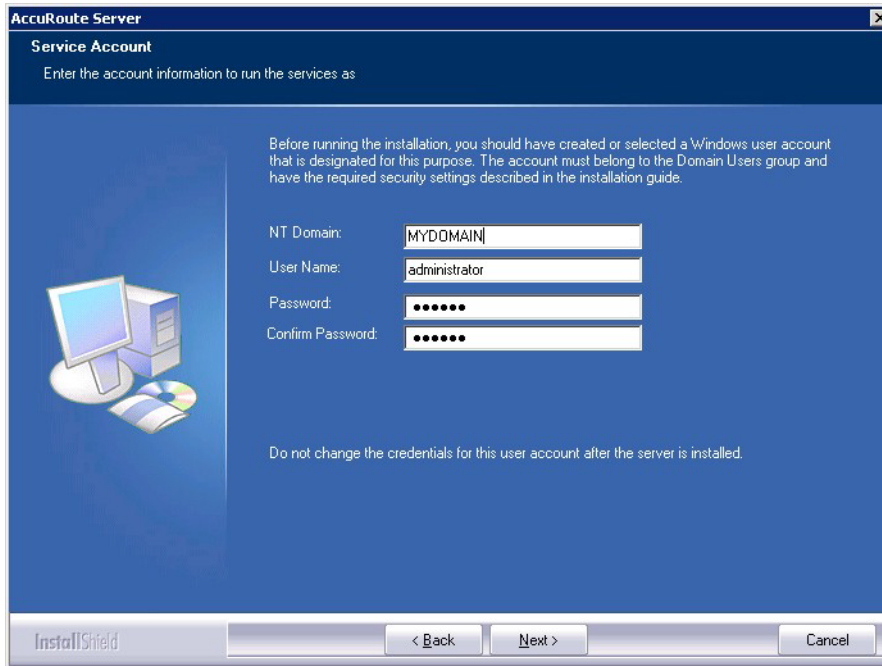
To install the Mobile Device API on a system remote from the AccuRoute Server:

- 1 First, you need to change the DCOM login on the installation server to use the Computer Account instead of the Service account.
- 2 Refer to steps 1 through 8 in [Installing the AccuRoute server \(3-2\)](#) and return here.
- 3 At Step 8, on the **Setup Type** screen, select **Custom**. All options for the AccuRoute server installation are selected by default.
- 4 Clear all options *except* the **Mobile Device API**. To continue the installation, click **Next**.
- 5 The **Prerequisites** screen appears as the installer compares your configuration with the required setup components and lists the results. Click **Next**.
- 6 In the **Service Account** screen, the setup requests logon credentials for the AccuRoute computer account. By default, the **User Name** field is populated with the name of the user logged into Windows.

Provide the AccuRoute computer account logon credentials:

- a In the **NT Domain** field, enter the Windows domain name.
- b In the **User Name** field, enter the computer name.

- c In the **Password** and **Confirm Password** fields, enter the user password.
- d Click **Next**.



- 7 The setup validates the user account, and you can review the installation settings on the **Installation Settings** screen. Click **Next** to proceed with the installation.
- 8 Progress details appear on the **Setup Status** screen.
- 9 The **InstallShield Wizard Complete** screen appears. Click **Finish**.

Installing the Mobile Client

To download the **Mobile Client** application to your device, download it directly from either the iTunes Store or Google Play onto your device.

Configuring a local IIS system for mobile connectivity

The Mobile IIS virtual pages are installed by default with the AccuRoute Server installation. No configuration is required if this system is local to the AccuRoute Server.

Configuring a remote IIS system for mobile connectivity

To allow connectivity between the Mobile Client and a remote IIS system:

- 1 Once the installation is complete, go to `C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\MobileWebAPI\Scripts`, where you must open and modify the `omISAPIU.xml` file.
- 2 In the `omISAPIU.xml` file, you need to edit the server name from that of your remote IIS Server, which appears by default, to your AccuRoute server name.

For example, the default `omISAPIU.xml` file content includes:

```
</Server>
<Server Name="OmtoolServer">
<ServerName>REMOTE IIS Server name</ServerName>
</Server>
```

Change the text to the following:

```
</Server>
<Server Name="OmtoolServer">
<ServerName>AccuRoute Server Name</ServerName>
</Server>
```

- 3 For user access to the Mobile Device Client, connect to the AccuRoute server with the following login path: [HTTPS://RemotelISserverName/Mobile](https://RemotelISserverName/Mobile)

Environment configuration to support AccuRoute Mobile Clients

Before you begin, you may want to create a secure connection for communications between Mobile Clients and your office environment. To do so, you need to modify the default IIS configuration from using HTTP to using HTTPS. For more information, see [Configuring the Mobile Client environment to support HTTPS](#) below.

To set up your system for incoming Mobile Reservations from an external source, you need to define a recipient for them in your email management system. You also need to be able to forward the messages to the AccuRoute server for processing.

Note The steps outlined below use Microsoft Exchange as an example for configuring the email management system. Reference your email vendor's documentation for more specific information.

The recipient email address you create needs to be associated with a user group in the AccuRoute Server Administrator. You also need to create an outbound rule to handle the messages from the Mobile Client.

Once your system is configured, Mobile Client users can send a scanned message to the recipient email address using the Mobile Reservation Code as the subject line text.

To configure your environment, see:

- [Configuring the Mobile Client environment to support HTTPS](#)
- [Configuring the email management system](#)
- [Configuring the AccuRoute server](#)

Configuring the Mobile Client environment to support HTTPS

To create a secure connection between your office environment and Mobile Clients connecting from outside your LAN, you must modify the default IIS configuration from using HTTP to HTTPS.

Changing your configuration to HTTPS requires you to request, download and install an **SSL certificate** from a trusted Certificate Authority (CA). Refer to the CA you select for specific certificate installation instructions.

Note iOS devices include certificates from several trusted Root Certificate Authorities (CA). For a list of supported CA's, go to <http://support.apple.com/kb/ht5012>.

The basic steps to acquire an SSL certificate are as follows:

- 1 Request your SSL Certificate from the CA.
- 2 Once your request is approved by the CA, you can download and install the certificate on your IIS web server. This enables Secure Socket Layer (SSL) for your IIS system.
- 3 To verify your installation, visit your website using HTTPS.

Configuring the email management system

In your email management system, use the steps below to define a recipient email address for Mobile Reservation scan messages.

Note The steps outlined below use Microsoft Exchange as an example for configuring the email management system. Reference your email vendor's documentation for more product-specific information.

- 1 Open the **Exchange Management Console**, and create a new **Mail Contact** from the **Recipient Configuration** section.
- 2 While entering information on the **New Mail Contact** page, be sure that when you enter the new contact's **External e-mail address** you assign it to the internal address of your AccuRoute server. For example: `mobilscan@accuroutesrv.omtool.com`
- 3 After you create the new Mail Contact, return to the contact **Properties** and add your **email domain** as a **secondary email address**. This allows it to be accessed from outside your organization.
For example: `mobilscan@omtool.com` will now forward to `mobilscan@accuroutesrv.omtool.com` (the AccuRoute server).

Configuring the AccuRoute server

You can configure the AccuRoute Server for Mobile Reservations by associating the new recipient email address with specific user groups and creating an outbound rule to handle Mobile Reservation messages.

Group properties

To assign the new external email address to specific user groups:

- 1 Open the **AccuRoute System Administrator** and select **Groups**.
- 2 Right-click the group of interest and select **Properties**.
- 3 In the **Mobile** tab, select **Enable members of this group to use the mobile client**.
- 4 Enter the external email address (created in step 2 of [Configuring the email management system](#) above) in the **Scans to Email** field and click **OK**.

Outbound rule

To create an outbound rule for handling Mobile Reservation messages:

- 1 Open the **AccuRoute System Administrator**, expand the **Rules** node and select **Outbound**.
- 2 Right-click **Outbound** and select **New > Rule**. The **Create New Rule** screen appears.
- 3 Click **Add**. The **Add Rule Criteria** screen appears.
- 4 Select **Destination is an e-mail address** and click **Next**.
- 5 In the **Items to Match** screen, select the **is** radio button and enter the **External email address** in the text box.
- 6 Click **Add** and then click **Finish**.
- 7 Returning to the **Specify the Criteria for this Rule** screen, click **Next**.
- 8 In the **Specify actions to take for this Rule** screen, click **Add**. The **Add Rule Action** screen appears.
- 9 Select **Route to Embedded Directive Manager** and click **Next**.
- 10 The **Route to Embedded Directive Manager** screen appears. Select **Scan subject line for Reservation Code** and click **Finish**.
- 11 Click **Next**, **Next**, and **Finish**.

Note See the [Omtool Server Administrator Help](#) for optional server configuration for use with the AccuRoute Mobile Client.

Section 5: Post Installation Configurations

This section includes:

[Specifying the originator of notification messages](#) (5-1)

[Customizing access to client setup programs](#) (5-2)

[Configuring the Compose component to convert Office message attachments using automation](#) (5-2)

[Configuring the AccuRoute server to convert PCL message attachments](#) (5-3)

[Configuring Integrated Windows Authentication on the Web Server](#) (5-5)

Specifying the originator of notification messages

The AccuRoute server generates notification messages for various events and sends them to users through the AccuRoute connectors for ExchangeX, Notes, and SMTP. The display name and email address associated with these notification messages can be set in the AccuRoute server properties. Omtool recommends setting these attributes using a valid email address so that users can reply to notification messages if they require assistance. (The default email address is MessageServer and the default display name is Message Server.)

To specify the originator of notification messages generated by the AccuRoute server:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click on the AccuRoute server.
- 3 Select **Properties**. The **Server Properties** page opens.
- 4 Click the **Settings** tab.
- 5 In the **E-mail Address** text box, enter the email address that should be associated with notification messages generated by the AccuRoute server.

Omtool recommends using a valid email address so that users can reply to notification messages if they require assistance.
- 6 In the **Display Name** text box, enter the name that should be associated with notification messages generated by the AccuRoute server.
- 7 Click **OK** to save changes to the server properties.

Customizing access to client setup programs

The AccuRoute server has a Clients folder where it stores all the setup programs for its client applications, such as AccuRoute Desktop, AccuRoute Web Client, CostRecovery, and FaxCenter. After the AccuRoute server is installed, the Clients folder is shared but only the Omttool service account has permissions to access it.

Note The network path to the Clients folder is \\server\omttool\clients where server represents the network name of the AccuRoute server.

Omttool recommends customizing the permissions on this folder so that the users who are installing these applications on clients can access the setup programs conveniently from anywhere in the LAN. If necessary, the setup programs can be copied to a network location where all applications are stored for deployment purpose, and can be copied to the client before installation. For more information on modifying Windows sharing and security permissions, consult Windows help.

Configuring the Compose component to convert Office message attachments using automation

Note This is an optional procedure. For best results Omttool recommends this procedure for customers who have Microsoft Office installed on the server.

The Compose component can be configured to convert documents using the “automation” conversion method, which utilizes a document’s native application to open the document so that it can be converted to the required delivery format. Automation is the recommended conversion method for Office documents because this method produces the highest quality conversion results and eliminates conversion errors that can occur with other methods.

The procedure to configure the Compose component to convert Office message attachments using automation is highly recommended but not required. If Office is not used in the LAN, or if automation is not the preferred method for converting Office documents, you can skip this procedure and go to the next section.

The Compose component manages conversion methods for all Composers for the AccuRoute server. For this reason, it is necessary to complete this procedure only once.

To configure the Compose component to use automation as the conversion method for Office documents:

- 1 Verify that a supported version of Microsoft Office is installed on the AccuRoute server. For supported Office versions, see [Additional installation requirements](#) (2-3).
- 2 Start the AccuRoute Server Administrator (click **Start > All Programs > Omttool > AccuRoute Server Administrator**).
- 3 Select the AccuRoute server in the console tree.
- 4 Go to the details pane and double-click **Components**.
- 5 Double-click **Compose**. The **Properties for Compose** page is displayed.
- 6 Click the **Conversions** tab.

- 7 Enable automation for Office files:
 - a Select **doc**.
 - b Click the **Properties** button.
 - c Select **Word Automation**.
 - d Click **OK**.

Repeat these steps to select the automation option for the **DOCX**, **PPT**, **PPTX**, **XLS**, and **XLSX** file types.

Note DOCX, PPTX, and XLSX are file types associated only with Office 2007. DOC, PPT, and XLS files are file types associated with Office 2003 and earlier, and compatible with Office 2007.

- 8 Click **OK** to save changes to the Compose component.

Configuring the AccuRoute server to convert PCL message attachments

The AccuRoute server requires additional configuration to convert PCL files. Omttool recommends completing this configuration, but it may be omitted if the AccuRoute server is not required to convert PCL attachments.

Follow the instructions appropriate for the AccuRoute server location:

[AccuRoute server on the same drive as the operating system](#) (5-3)

[AccuRoute server on a drive different from the operating system](#) (5-4)

AccuRoute server on the same drive as the operating system

To configure the AccuRoute server to convert PCL message attachments:

- 1 Find the short name path to:

```
...\Omttool\Omttool Server\Vendors\GhostScriptPCL
```

Tip To obtain the short name of a directory, run **dir /x** in the parent directory. For example, to obtain the short name of **C:\Program Files**, set the working directory to **C:** and run **dir /x**. This returns the short name of all folders under **C:**.

- 2 Right-click **My Computer** and select **Properties** from the drop-down menu to open the **Properties** page.
- 3 Click **Advanced**.
- 4 Click **Environmental Variables**.
- 5 In the **System Variables** section, add the variable **PCLFONTSOURCE**. Set the variable value to the short path to the GhostScriptPCL directory.

Note Use forward slashes, and include a forward slash at the end of the path, for example, /PROGRA~1/Omtool/OMTOOL~1/Vendors/GHOSTS~2/

- 6 Click **OK** to close the **Environmental Variables** page.
- 7 Click **OK** to close the **System Properties** page.

AccuRoute server on a drive different from the operating system

To configure the AccuRoute server to convert PCL message attachments:

- 1 Copy the font files from:
`...\Omtool\Omtool Server\Vendors\GhostScriptPCL`
to:
`C:\Winnt\Fonts`
- 2 Create `...\Winnt\Fonts` at the root level of the drive where the AccuRoute server is installed.
- 3 Copy the font files from:
`...\Omtool\Omtool Server\Vendors\GhostScriptPCL`
to:
`...\Winnt\Fonts` on the drive where the AccuRoute server is installed.
- 4 Right-click **My Computer** and select **Properties** from the drop-down menu to open the **Properties** page.
- 5 Click **Advanced**.
- 6 Click **Environmental Variables**.
- 7 In the **System Variables** section, verify that there is no **PCLFONTSOURCE** variable. (If it exists from a previous version of AccuRoute server, delete it.)

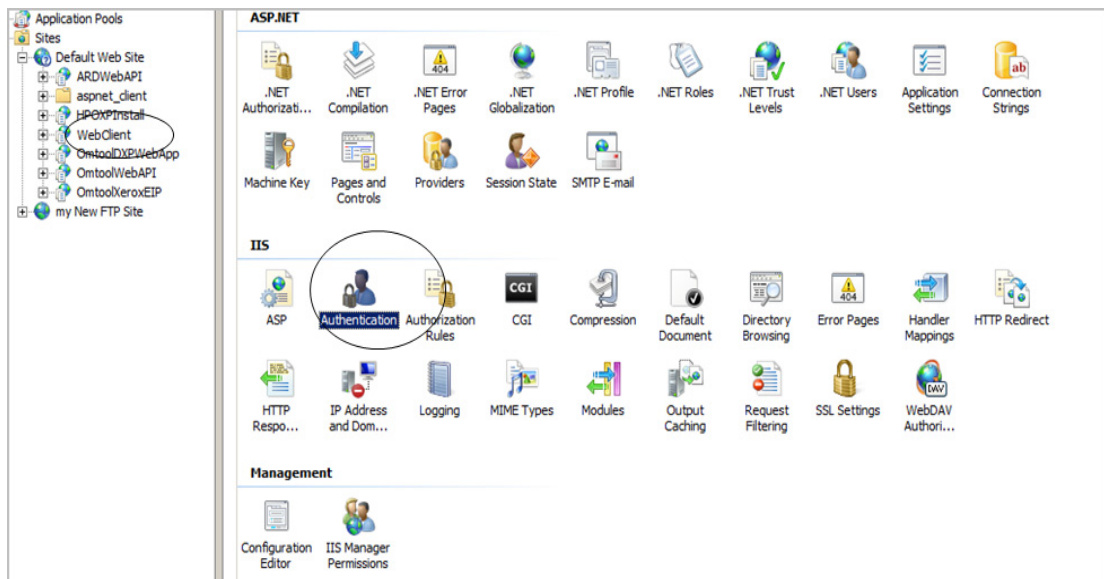
Tip When the PCLFONTSOURCE does not exist as an environmental variable, the AccuRoute server uses `\Winnt\Fonts`.

- 8 Click **OK** to close the **Environmental Variables** page.
- 9 Click **OK** to close the **System Properties** page.

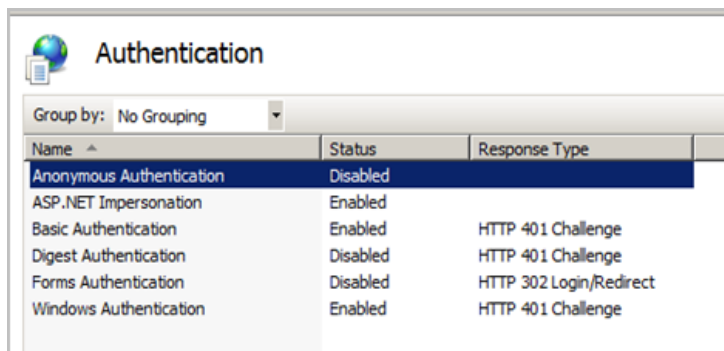
Configuring Integrated Windows Authentication on the Web Server

The following procedure applies only if you are using the Web Client.

- 1 Click **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- 2 Expand the server running AccuRoute Web Client. Expand **Sites** and then expand **Default Web Site**.
- 3 Click the virtual directory for AccuRoute Web Client. (The default name is [WebClient](#).) The Internet Information Services features view opens in the details pane.



- 4 In the **IIS** section, click **Authentication**. The following page opens.



- 5 Verify the **Anonymous Authentication** option is disabled. If not disable the option.
- 6 Verify the **Windows Authentication** option is enabled. If not, enable the option.

- 7** Perform an iisreset.
 - a** Open a command prompt.
 - b** Type `iisreset`.
- 8** Press **Enter**.

Section 6: Optional Configurations

This section includes:

[Disaster Recovery Solution](#) (6-1)

[Data Encryption](#) (6-3)

[Support for SQL Always On Availability Groups](#) (6-5)

[Support for the SSL/TLS v1.2 Protocol](#) (6-6)

Disaster Recovery Solution

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

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

The accuracy of data recovered from your environment depends on the sync timing. For example, if your system syncs 5 minutes behind, there would be a 5 minute data loss in recovery. Also, the database and the files must be synced at the same time to ensure integrity.

Also note, the Disaster Recovery Server is designed to be a “cold” option and is not expected to be used as an active production system.

For more information on setting up HP CR server clusters and failover, see [Section 16: Setting up an HP CR Server Cluster](#) (16-119).

Requirements

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

- Installed a primary HP CR Server.
- Applied a Disaster Recovery license (and any other licenses needed).

Installing and configuring a Disaster Recovery server

- 1 Begin by configuring a replication of a FileShare and database(s) for your system.
- 2 Install HP CR on your Disaster Recovery server using the same installation options that you applied to your production server. Set up your Disaster Recovery server to use the replicas you created in Step 1. Your primary production server must be currently on-line.
- 3 When the **HP CR Configuration wizard** appears, select **Disaster recovery configuration** on the **Welcome** screen.

- 4 On the **Disaster Recovery Standby** screen, enter the **Server Name** of your production HP CR server and click **Next**.

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

- 5 On the **Existing Database** screen, enter the name of your **SQL Server**.
- 6 Select either **Use Windows Integrated Authentication** or **Use SQL Authentication Login**. If required, enter the appropriate **Username** and **Password**. Then click **Next**.
- 7 On the **Select Existing Database** screen, select your preferred database from the list of existing databases and click **Next**.
- 8 On the **File Share** screen, enter or browse to the **File Share Location** you want associated with your Disaster Recovery Server. Click **Next**.
- 9 The **Ready to Configure** screen appears. This screen identifies whether you are configuring Disaster Recovery for a single server or a clustered environment. Click **Next** to configure the Disaster Recovery system.
- 10 The **Completed** screen appears. Click **Finish** to close the Configuration wizard.

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

- 11 Power down the Disaster Recovery server(s).
- 12 In the HP CR Administrator, with your Primary server highlighted, select **Action > Recovery Settings...** The **Disaster Recovery Settings** screen appears.
- 13 Edit the Backup Site entries as needed and select **OK**.
- 14 To bring your Disaster Recovery server(s) back on-line, first power up the server(s).
- 15 Open the HP CR Administrator. You may need to wait several minutes for Services to start.
- 16 Select **Action > Recovery Settings...** to return to the **Disaster Recovery Settings** screen. Confirm and/or edit the Backup Site entries as necessary. Click the **Switch Site** button.
- 17 A message appears warning you that any services running will be stopped. Any other error messages that appear are likely normal, given that the production servers would be off-line in a real disaster.
- 18 Restart the Disaster Recovery server (or just the services) to bring the server fully on-line.
- 19 Bring the Disaster Recovery servers off-line.
- 20 Make needed repairs to the Primary server. Services should be stopped.
- 21 On the Disaster Recovery Server’s HP CR Administrator, select **Action > Recovery Settings...** and click **Switch Sites** to return to Primary settings. The Disaster Recovery Server disconnects and services stop.
- 22 Power down the Disaster Recovery server(s).
- 23 Perform any manual steps required to sync the Disaster Recovery database & FileShare back with the Primary server.
- 24 Restart the Production server (or start services).
- 25 The Disaster Recovery server(s) are ready for the next time.

Data Encryption

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

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

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

Requirements

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

Note HP is not responsible for the certificate or the data if the certificate is lost.

Setting up Data Encryption for HP CR v1.6.0 involves:

- [Importing the encryption certificate](#) (6-3)
- [Enabling Data Encryption](#) (6-4)

Also see steps for

- [Disabling Data Encryption](#) (6-4)
- [Configuring the SQL Database](#) (6-4)

Importing the encryption certificate

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

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

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

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

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

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

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

Enabling Data Encryption

To enable data encryption:

- 1 Make sure you are Administrator on the system, open **Command Prompt** and enter
`omcertutils -apply [certificatename]`
The certificate name is the value used for the certificate's **Subject** field when it was created.
- 2 When it appears, read and agree to the legal warning by typing **YES** to continue.
- 3 The existing server disk files are encrypted. The process duration varies based on the number of files. Your HP CR is enabled for encryption and the Services are started.

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

Disabling Data Encryption

To disable data encryption:

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

```
omcertutils -remove
```

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

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

Configuring the SQL Database

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

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

For more information on database encryption, refer to:

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

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

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

Support for SQL Always On Availability Groups

HP CR offers support for using the HP CR Server in a **SQL Always On Availability Group** environment.

Note The relevant **SQL Always On Group** must be configured before installing the HP CR Server.

After installing the HP CR Server, the Server Administrator needs to update the database DSN entries to allow the configuration to work with SQL Always On functionality.

Configuring the HP CR Server for SQL Always On

- 1 Complete the configuration of your **SQL Always On Availability Group**.
- 2 Install HP CR, selecting the **Primary SQL server** for the database.
- 3 To change the DSN settings for the Primary SQL server, navigate to this registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Omtool\Genifax\Current Version\DSN`
- 4 Edit two sections of the DSN as follows:
 - ▶ Change the `Driver=` section to `{SQL Server Native Client 11.0}`
 - ▶ Change the `Server=` section to `TCP:YOURLISTENERHERE, YOURPORTNUMBER`

For example:

```
Driver={SQL Server Native Client 11.0}; Server=TCP:TestAccuListner, 1433;
```

```
Database=AccuRoute; Trusted_Connection=Yes
```

This change needs to be made on the following four DSN entries:

- ▶ ActivityDB
- ▶ ArchiveDB
- ▶ DB
- ▶ DBMETADATA

And depending on your configuration, this change may also need to be made for these DSN entries within the Administrator:

- ▶ Billing Archive
- ▶ Volume Lists
- ▶ Audit

Support for the SSL/TLS v1.2 Protocol

To use TLS v1.2 in your environment, you will need to acquire a certificate with the appropriate signature algorithm. You will also need to enable TLS v1.2 on the HP CR Server and on the relevant HP devices. You may also need to update relevant DSN entries on the HP CR Server.

Note The HP CR v1.6.0 release supports SSL/TLS v1.2 only on Windows 2012 and 2016.

6-0-1 Enabling TLS 1.2 on the HP CR Server

If you were previously using TLS v1.0 or v1.1, when you are turning those off and selecting TLS v1.2 instead, you also need to edit the HP CR Server's DSN entries to point to the correct SQL Server driver.

- 1 To change the DSN settings for the SQL Server driver, navigate to this registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Omtool\Genifax\Current  
Version\DSN
```

- 2 Edit the `Driver={SQL Server}` section of the DSN to `Driver={SQL Server Native Client 11.0}`

For example:

```
Driver={SQL Server Native Client 11.0}; Server=TCP:TestAccuListner,  
1433;
```

```
Database=AccuRoute; Trusted_Connection=Yes
```

This change needs to be made on the following four DSN entries:

- ▶ ActivityDB
- ▶ ArchiveDB
- ▶ DB
- ▶ DBMETADATA

And depending on your configuration, this change may also need to be made for these DSN entries within the Administrator:

- ▶ Billing
- ▶ Archive
- ▶ Volume Lists
- ▶ Audit

Enabling TLS 1.2 on your HP device

Sign in to the device via your browser and:

- For **FutureSmart 3** devices — Go to the **Networking** tab, select **Mgmt. Protocols**, and in the **Web Mgmt. Secure Communication** section, select the **TLS 1.2** check box. Click **Apply**
- For **FutureSmart 4** devices — Go to the **Networking** tab, select **Secure Communication**, and in the **SSL/TLS Protocol** section, select the **TLS1.2** check box. Click **Apply**.

Section 7: ExchangeX Integration

This section includes:

[Adding an AccuRoute connector for ExchangeX \(7-1\)](#)

[Specifying an email address for ExchangeX non-delivery reports \(7-2\)](#)

[Configuring lookup methods \(7-3\)](#)

Tip The Omtool Knowledgebase has technical articles on troubleshooting the AccuRoute connector for ExchangeX.

Adding an AccuRoute connector for ExchangeX

Note The AccuRoute connector for ExchangeX is a licensed connector.

For **ExchangeX 2010**, the ExchangeX server must have a foreign connector specified with an address type that is not SMTP (valid address types are FAX, FAXI, MYFAX).

Note For general information on foreign connectors, see:
<http://technet.microsoft.com/en-us/library/aa996779.aspx>
For information on how to create a foreign connector, see:
<http://technet.microsoft.com/en-us/library/aa996397.aspx>
For information on “Set-ForeignConnector” cmdlet to modify an existing foreign connector, see:
<http://technet.microsoft.com/en-us/library/bb123789.aspx>

To add the AccuRoute connector for Exchange 2010 to your AccuRoute server:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator.
- 3 Right-click **Connectors > New AccuRoute Server Connector for > ExchangeX**. The **Server Address** page opens.
- 4 Select the Server Address option:
 - ▶ **Run on the Message Server**
 - ▶ **Remote Server** and enter the server address in the text box.
- 5 Click **Next**. The **Display Name** page opens.
- 6 In the **Name** text box, enter a friendly name for the connector and click **Next**. The **Connector folder** page opens.

- 7 In the **Specify a folder to scan** text box, browse and select the folder for the connector to scan for input messages.

- 8 Click **Next**. The **Lookup Connection** page opens.

The folder you select is the drop directory specified when creating the foreign connector using the Exchange 2010 Management Shell. For information on drop directory and foreign connectors, consult Microsoft documentation in <http://technet.microsoft.com/en-us/library/aa996779.aspx>.

- 9 Verify the **Host Name** and **Search Base** for the lookup connection and click **Next**. The **Lookup Authentication** page opens.

Note The **Host Name** is the Active Directory server.

- 10 In the **Username** and **Password** text boxes, enter the logon credentials associated with the lookup user account. Click **Next** and the **Congratulations** page opens.

- 11 Click **Finish**.

Specifying an email address for ExchangeX non-delivery reports

ExchangeX generates non-delivery reports (NDRs) when it cannot deliver email messages. These non-delivery reports are returned to the AccuRoute server through the AccuRoute connector for ExchangeX. The AccuRoute connector for ExchangeX can either re-route non-delivery reports to a known valid email address or delete them automatically. By default, non-delivery reports are deleted.

Omtool recommends configuring this feature with a known valid email address so that an administrator can be alerted about failures when they occur. To specify an email address for ExchangeX non-delivery reports:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and double-click the AccuRoute connector for ExchangeX in the details pane.
- 3 Go to the **Folders** tab.
- 4 Go to **Report**, select **Notify system administrator**, and enter a known valid email address.
- 5 Click **OK** to save the changes to the AccuRoute connector for ExchangeX.

Configuring lookup methods

The AccuRoute server utilizes the lookup configurations in the AccuRoute connector for ExchangeX properties to retrieve information about users.

- **DID/DTMF lookup** identifies the recipient of an inbound fax.

Note For Exchange 2010, lookup is configured in the AccuRoute connector for SMTP. Refer to [Section 9: SMTP Integration](#) for details.

- **Sender lookup** retrieves user attributes associated with the message sender, and these values are used to populate variables in cover pages, Routing Sheets, and notification messages.

Section 8: Lotus Notes Integration

This section includes:

[Configuring lookup methods](#) (8-1)

Tip The Omtool Knowledgebase has technical articles on troubleshooting the AccuRoute connector for Lotus Notes.

Configuring lookup methods

Integration with Lotus Notes is supported by message delivery to and from the Lotus Notes clients by way of the SMTP connector. Inbound message delivery is accomplished by configuring the lookup for the SMTP connector to the Domino server.

The AccuRoute server utilizes its connection to the Notes server to accomplish the following tasks:

- Authenticate users
- Retrieve sender and recipient information for cover pages and Routing Sheets
- Identify the recipient of inbound messages based on the recipient's DID extension or fax number
- Display the contents of the global directory when queried from the AccuRoute Server Administrator

By default, the Server Configuration wizard adds a search base for DID/DTMF lookup configuration.

Section 9: SMTP Integration

This section includes:

[Configuring lookup methods \(9-1\)](#)

[Reviewing the default DID/DTMF lookup configuration for inbound faxing \(9-1\)](#)

Tip The Omtool Knowledgebase has technical articles on troubleshooting the AccuRoute connector for SMTP.

Configuring lookup methods

The AccuRoute server utilizes the lookup configurations in the AccuRoute connector for SMTP properties to retrieve information about users.

DID/DTMF lookup identifies the recipient of an inbound fax.

Reviewing the default DID/DTMF lookup configuration for inbound faxing

DID/DTMF lookup identifies the recipient of an inbound fax. To retrieve the recipient email address, the AccuRoute server submits a lookup request using the last 4 digits of the DID/DTMF string captured by the Modem Server. When the recipient email address is returned, the AccuRoute connector for SMTP can deliver the message to the SMTP server.

Tip The default AccuRoute connector for SMTP configuration specifies the `facsimileTelephoneNumber` attribute for DID/DTMF lookup. (This is the Active Directory and LDAP attribute that stores the fax number of users.) Change the attribute, if necessary, and confirm that the lookup attribute is indexed. Indexing the lookup attribute optimizes lookup speed.

The DID/DTMF lookup configuration can be modified and tested in the AccuRoute connector for SMTP properties. For information on modifying the DID/DTMF lookup configuration, consult the Omtool Server Administrator Help, which is available on the [AccuRoute v6.0 documentation](#) page.

Note If faxing is not enabled for the AccuRoute server, no modification is necessary.

Section 10: Installing ObjectArchive

This section includes:

[Introduction to ObjectArchive](#) (10-1)

[Requirements for ObjectArchive](#) (10-2)

[Installing ObjectArchive](#) (10-2)

[Configuring ObjectArchive](#) (10-11)

[Removing ObjectArchive](#) (10-12)

Introduction to ObjectArchive

ObjectArchive provides for storage and retrieval of stored data. The data can be scanned images, multimedia, and other textual/non-textual data. The data is stored as individual objects with unique object keys. The object keys are 128-bit (16 bytes) Universally Unique IDs (UUIDs) and are the primary methods of accessing (storing/retrieving) data from the archive database.

Important ObjectArchive must be installed on a system remote from the AccuRoute server.

When scaling an environment with additional connectors or components, always consult an Omtool Technical Support engineer. For information, contact [Omtool Support and Sales](#). The Omtool Technical Support engineer can assist you in correctly identifying potential bottlenecks in the system based on workload and other factors. Moreover, the Support engineer can provide helpful information on the overall impact of increasing the speed and efficiency of the system. Performance and stability consulting are available for a fee.

If a detailed analysis of the environment is necessary, the Omtool Technical Support engineer may recommend a fee-based consultation.

Important ObjectArchive is not cluster aware.

Requirements for ObjectArchive

Hardware and software minimum requirements

- Windows NT domain computer that always runs in the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit or Windows 2008 R2 64-bit
- SQL Server 2012 or SQL Server 2008 SP2

Important The SQL Server does not have to be the same one used for the AccuRoute server databases.

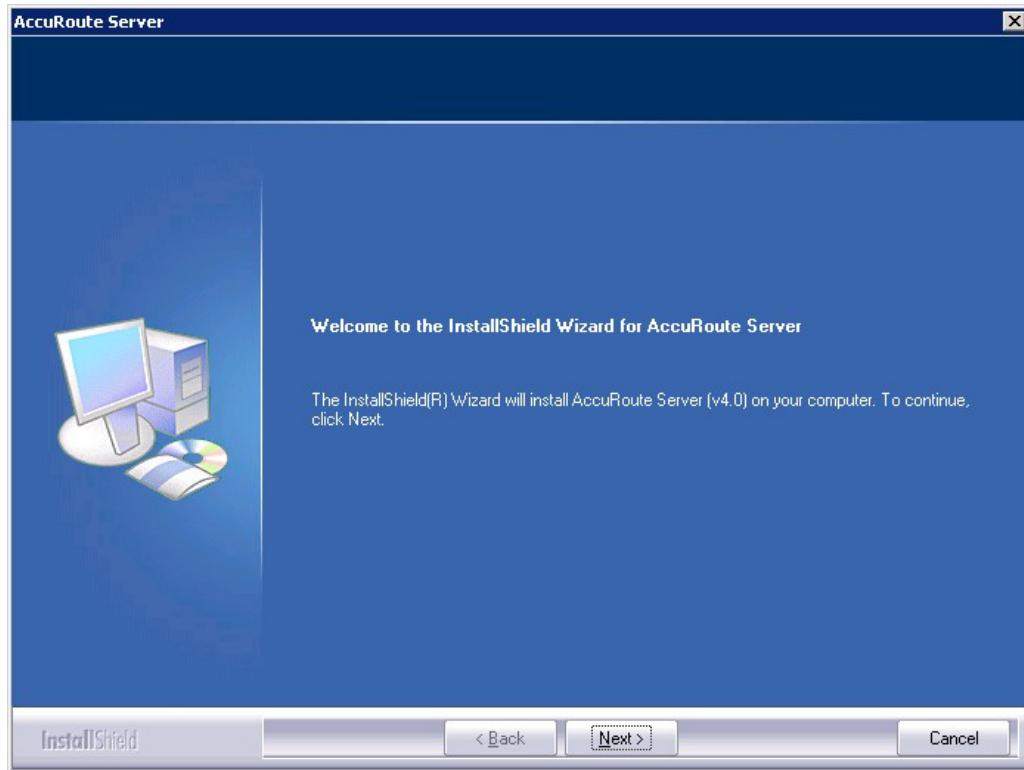
Additional requirements

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group
- License for the Object Archive Volume List

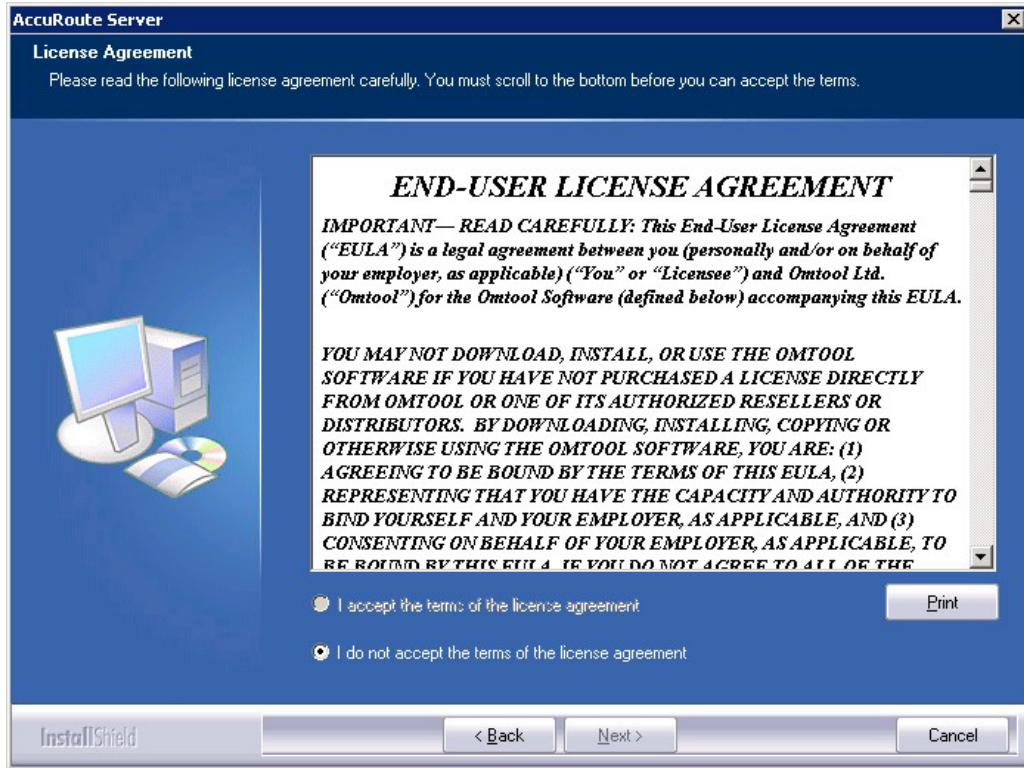
Installing ObjectArchive

- 1 Log in to the system where you will install the ObjectArchive using an account that belongs to the AccuRoute Administrators group. This system must be a system other than the AccuRoute server.
- 2 Navigate to the network where you store the AccuRoute server setup files.

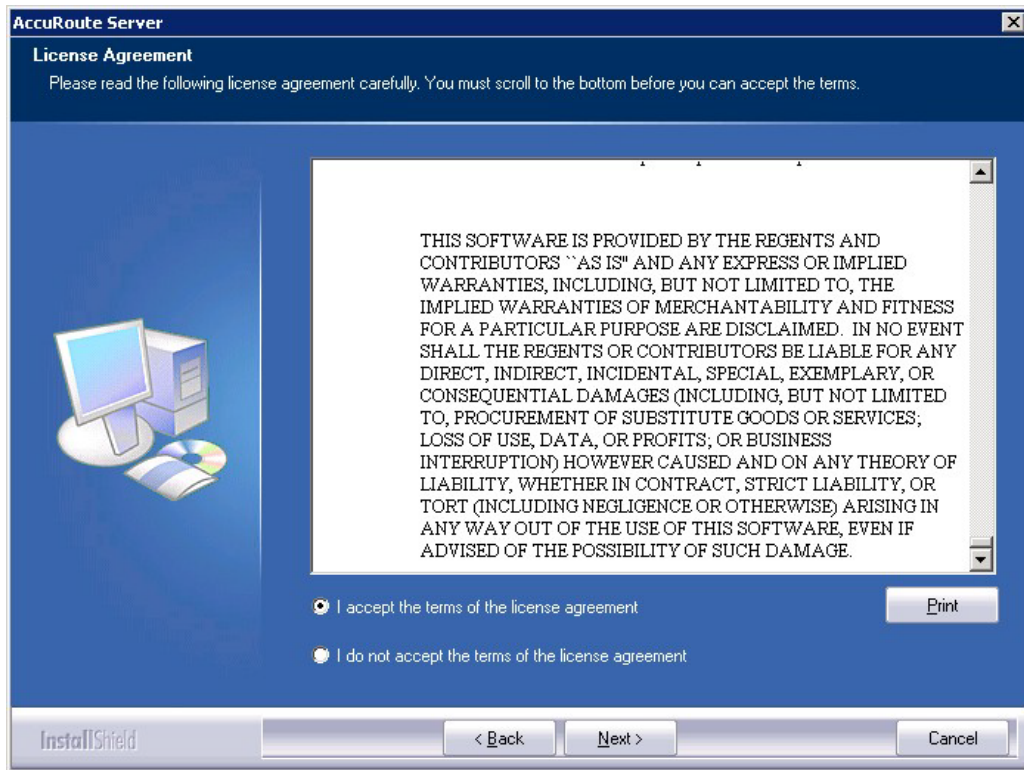
- 3 Run `\\MessageServer\setup.exe`. The InstallShield wizard opens and configures your system for installation and displays a Welcome message.



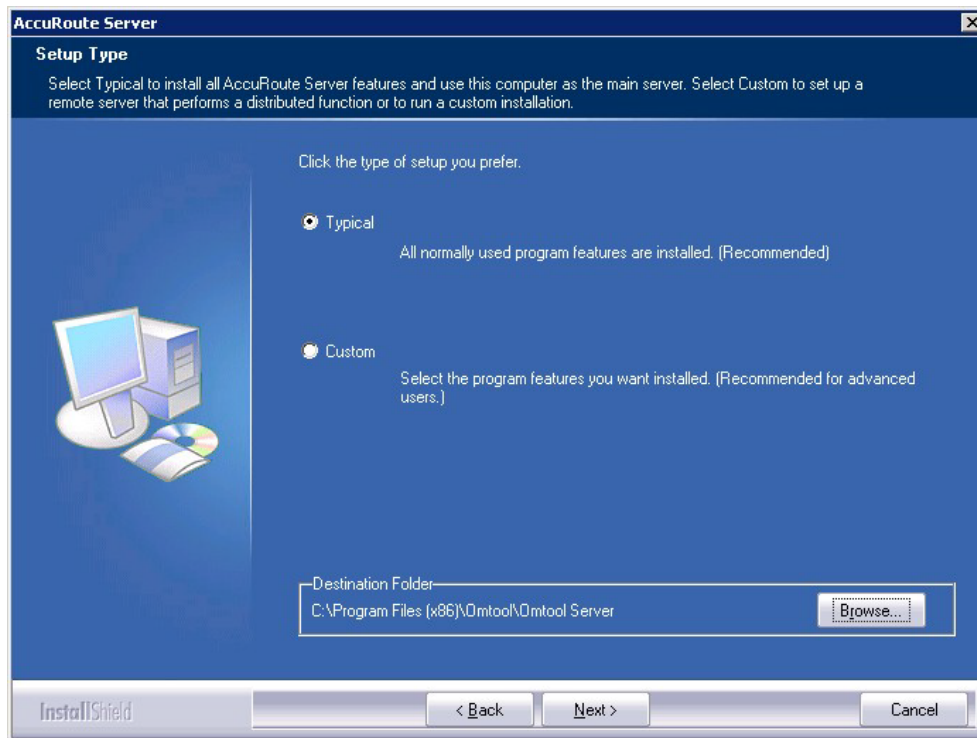
- 4 Click **Next**. The setup shows the **License Agreement** page.
- 5 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



6 Select I accept the terms of the license agreement.

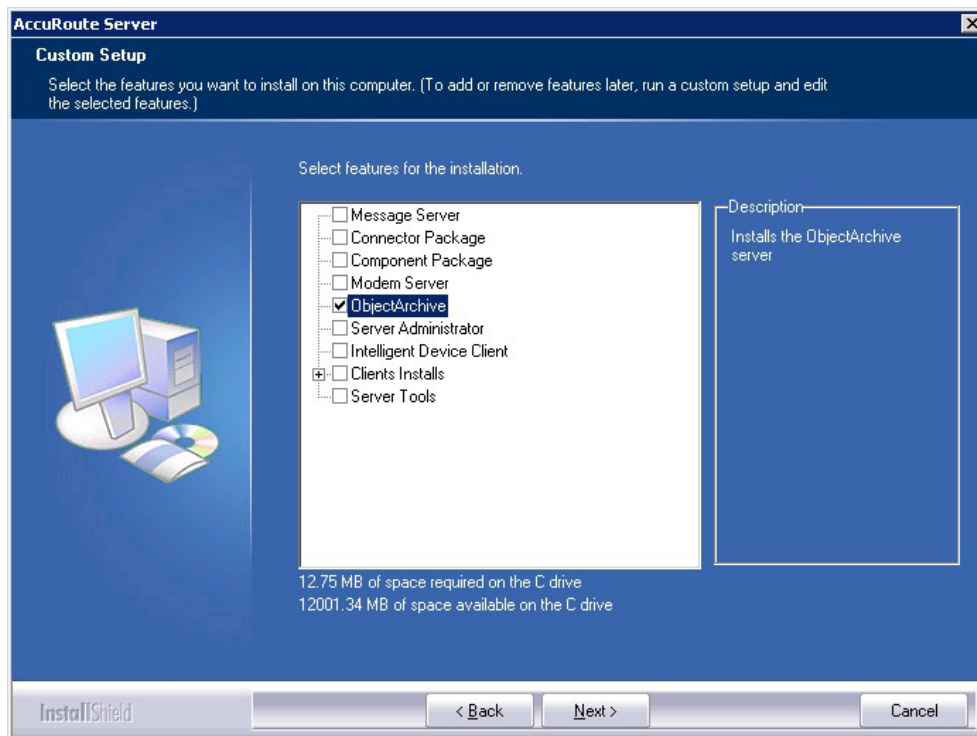


7 Click **Next**. The **Setup Type** options are displayed.

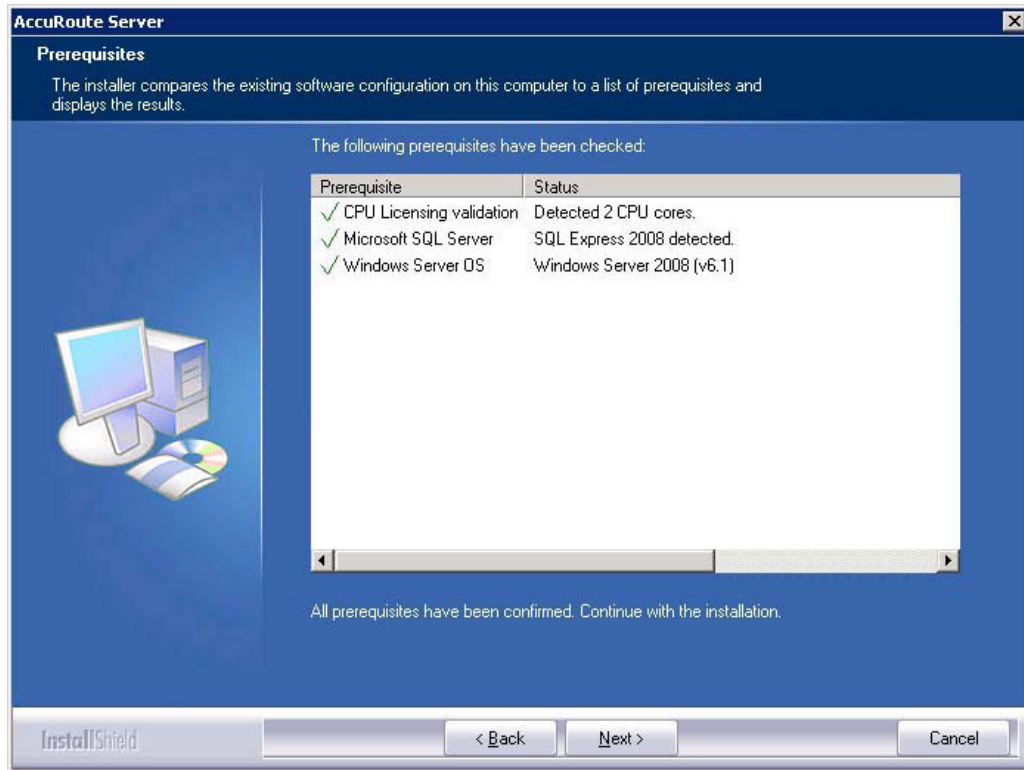


8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.

9 Select **ObjectArchive**. Clear all the other features you are not installing at this time.



10 Click **Next**. The setup checks the system for installation requirements and displays the results.



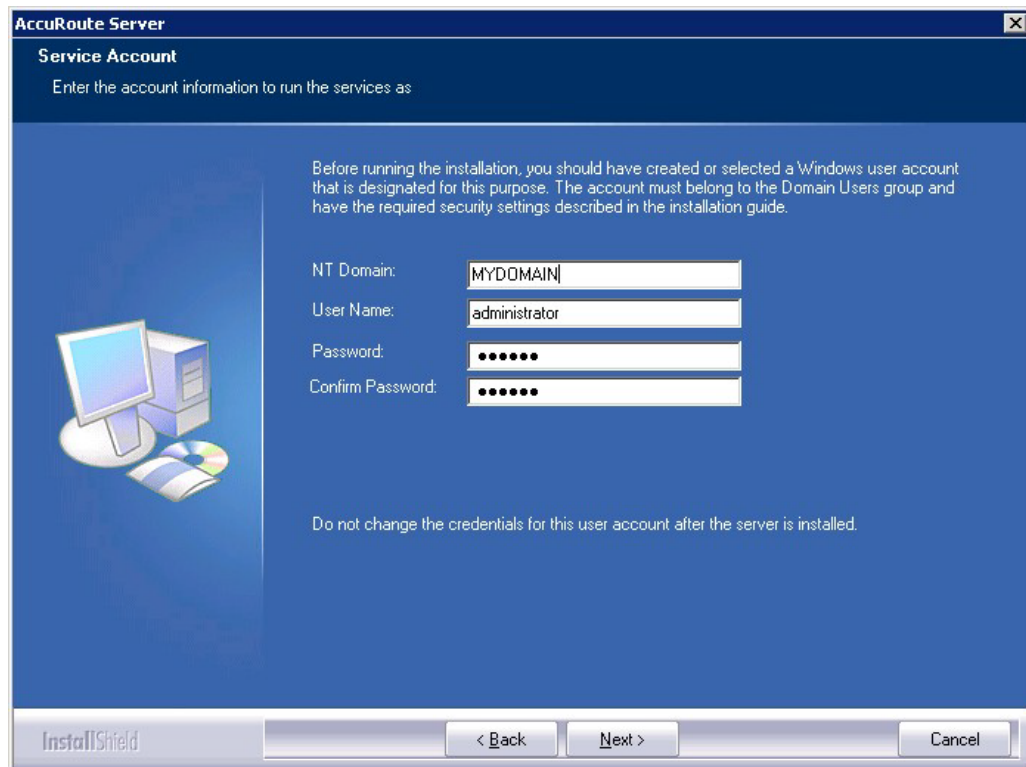
Note The setup cannot continue until all requirements are installed and configured. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

11 Click **Next** to continue the installation.

The setup requests logon credentials for the Omtool service account. The **NT Domain** and **User Name** fields are populated automatically based on the current Windows user.

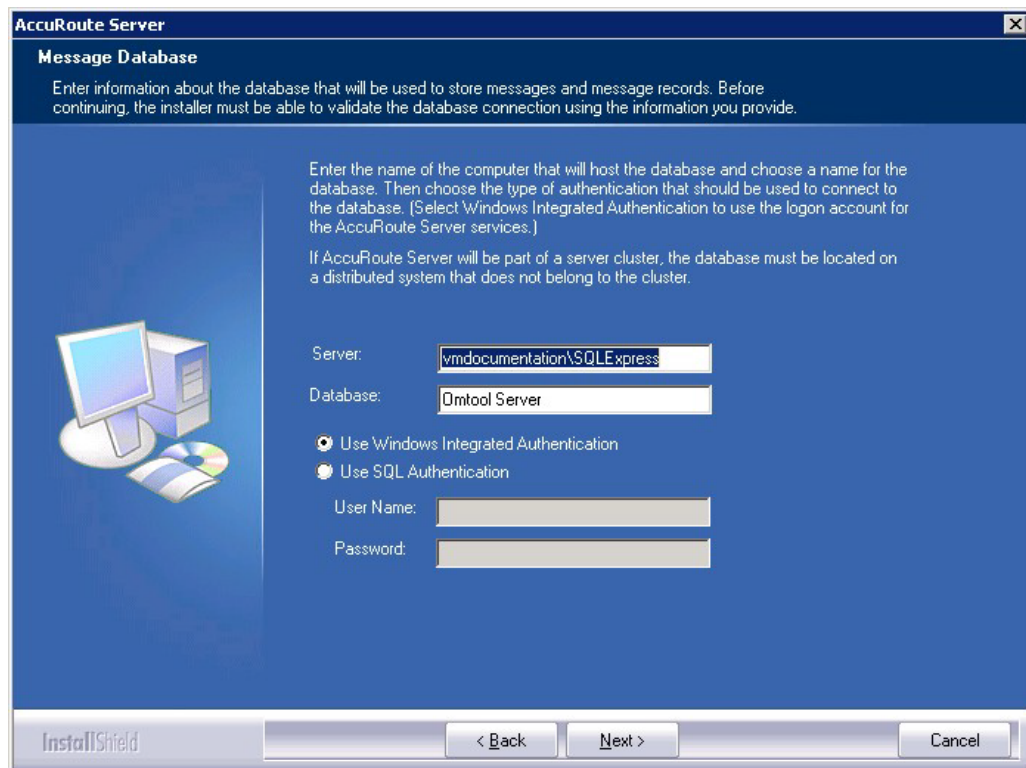
12 Enter the logon credentials of the Omtool service account.

- a** In the **NT Domain** text box, enter the name of the Windows domain.
- b** In the **User Name** text box, enter the user name.
- c** In the **Password** and **Confirm Password** text boxes, enter the password for the user.



The screenshot shows the 'Service Account' configuration window in the AccuRoute Server installer. The window title is 'AccuRoute Server' and the subtitle is 'Service Account'. Below the subtitle, it says 'Enter the account information to run the services as'. A large blue area contains a computer icon on the left and instructional text on the right: 'Before running the installation, you should have created or selected a Windows user account that is designated for this purpose. The account must belong to the Domain Users group and have the required security settings described in the installation guide.' Below this text are four input fields: 'NT Domain:' with 'MYDOMAIN', 'User Name:' with 'administrator', 'Password:' with six dots, and 'Confirm Password:' with six dots. At the bottom, there is a footer with the 'InstallShield' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

- d Click **Next**. The setup validates the user account and then displays options for the message database.



The screenshot shows the 'Message Database' configuration window in the AccuRoute Server installer. The window title is 'AccuRoute Server' and the subtitle is 'Message Database'. Below the subtitle, it says 'Enter information about the database that will be used to store messages and message records. Before continuing, the installer must be able to validate the database connection using the information you provide.' A large blue area contains a computer icon on the left and instructional text on the right: 'Enter the name of the computer that will host the database and choose a name for the database. Then choose the type of authentication that should be used to connect to the database. [Select Windows Integrated Authentication to use the logon account for the AccuRoute Server services.] If AccuRoute Server will be part of a server cluster, the database must be located on a distributed system that does not belong to the cluster.' Below this text are four input fields: 'Server:' with 'vmdocumentation\SQLEXPRESS', 'Database:' with 'Omtool Server', 'User Name:' (empty), and 'Password:' (empty). There are two radio button options: 'Use Windows Integrated Authentication' (selected) and 'Use SQL Authentication'. At the bottom, there is a footer with the 'InstallShield' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

13 Complete the database configuration:

- a** The setup detects **SQL Server 2008**. Verify that the **Server** field is populated with the name of the server running the Microsoft SQL Server database application. Then manually add the name of the SQL instance after the server name. For example: `Servername\SQLInstanceName`. Otherwise you will get the following error: Failed to validate SQL connection information.

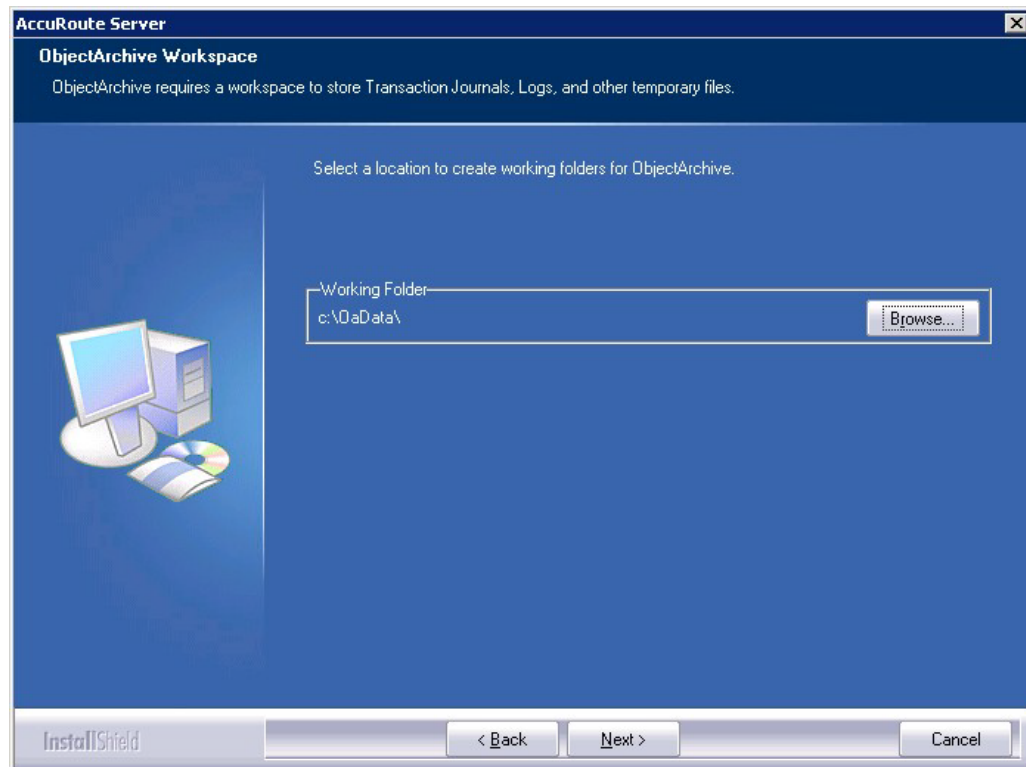
Note The default value is the local server where the setup is running.

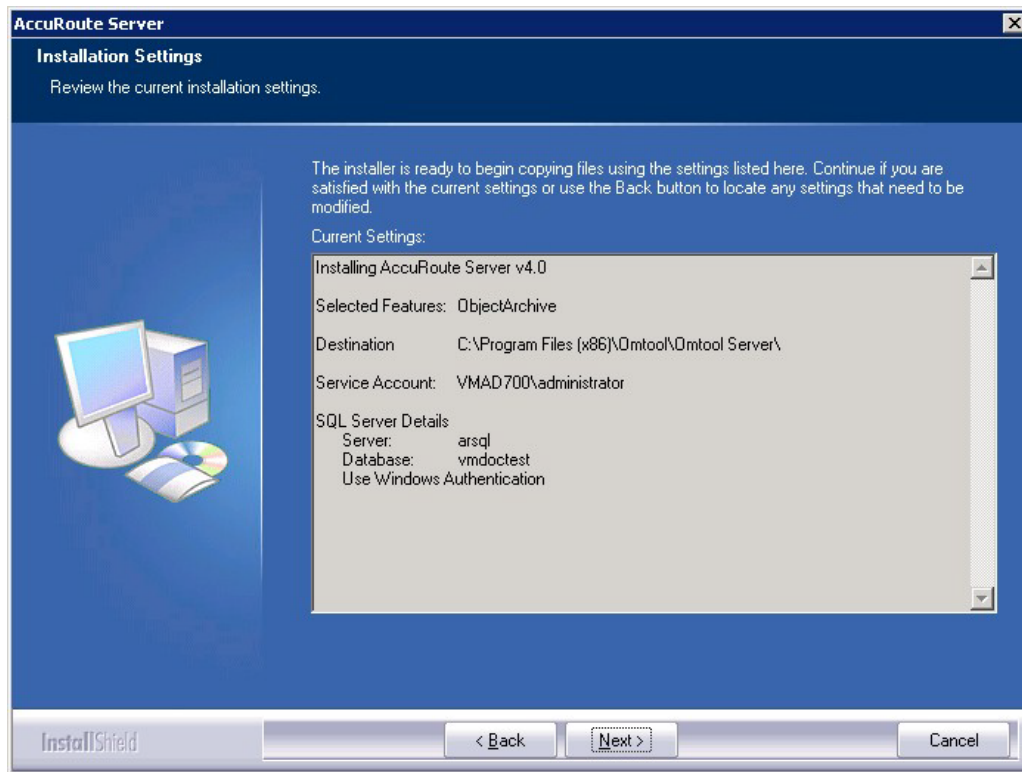
- b** In the **Database** field, review the name of the message database name and modify it if necessary.

Note During installation, the database is created on the AccuRoute server in:
`...\omtool\OmtoolServer\Database`

- c** Select the authentication method that the Omtool services use to access the database. Choose one of the following:
- ▲ **Use Windows Integrated Authentication** to use the Omtool service account. This is the default.
 - ▲ **Use SQL Authentication** to use SQL Server authentication. If you select this option, enter the logon credentials in the **User Name** and **Password** fields.

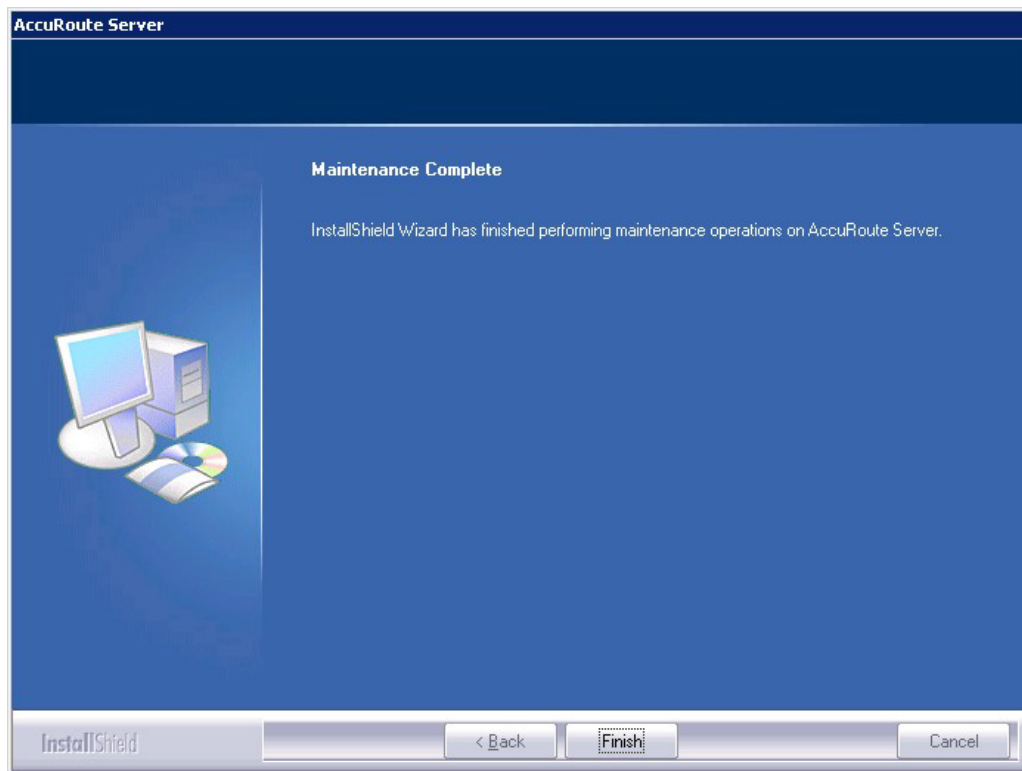
- 14** Click **Next**. The setup prompts you to choose the **ObjectArchive Workspace**. The default is `C:\OaData`. To choose another location, click **Browse** and select the location.



15 The setup validates the user account and then shows installation settings.

Note If other installation features are included, the setup might request additional information before displaying installation settings.

- 16** Review the installation settings and click **Next** to start the installation. The setup installs the selected component and displays a message indicating that the installation is complete.



- 17** Click **Finish**.

After installation is complete, navigate to the C:\OaData folder and verify that the installation was successful. The folder will contain four subfolders as shown below:

| Name | Size | Type | Date Modified | Attributes |
|-----------|------|-------------|--------------------|------------|
| OaBackup | | File Folder | 11/3/2009 11:14 AM | |
| OaJournal | | File Folder | 11/3/2009 11:14 AM | |
| OaLog | | File Folder | 11/3/2009 11:14 AM | |
| OaWorking | | File Folder | 11/3/2009 11:14 AM | |

Configuring ObjectArchive

Creating a new Volume List

Note A license is required for this feature.

Any properties you specify in the newly created Volume List must also be specified in the Active Volume List.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **Volume Lists** from the drop-down menu. The **New Volume List** page opens.
- 3 Select the destination from one of these options:
 - ▶ ObjectArchive
 - ▶ FileShare
 - ▶ NetDocuments
 - ▶ SharePoint
- 4 In the **Name** text box, enter an appropriate name.
- 5 In the **Folder** text box, the path to the list is listed as by default. If you want to change the default path, make the necessary change.

Note By default 4 GB is allocated for OaVolumes. If the space is less than 4 GB, messages will fail. You can manually configure the value to be greater or equal to 4GB.

- 6 Next, click **Indexing** tab to open the **Indexing** page.
- 7 In the **Properties to Index** section, click **Add** to open the **Index Properties** page.
- 8 Select from the **Property** drop box the message properties for indexing. Depending on your environment, some message properties should always be indexed.
- 9 Click **OK** to close the **Index Properties** page.
- 10 Click **OK** to close the **New Volume List** page.

Configuring the AccuRoute server to route to Volume Lists

In order to configure the AccuRoute server to route to the Volume Lists, create the AccuRoute connector for ObjectArchive.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **Connectors**.
- 3 Select **New Accuroute Server connector for > Volume List**.

- 4 Click **Next**. The **Server Address** page opens.
- 5 Click **Next**. The **Display Name** page opens.
- 6 In the **Name** text box, enter **OBJECTARCHIVE**.
- 7 Click **Next**. The **Select Volume List** page opens.
- 8 Select the Volume List from the list and click **Next** and then **Finish**.

Volume List configuration is now complete and the AccuRoute connector for Volume List is now listed in the Connectors details pane. Users can now use this connector to route documents for archiving.

Removing ObjectArchive

- 1 Click **Start > All Programs > Control Panel > Add/Remove Programs**.
- 2 Select **AccuRoute Server** and click **Change**.

You are prompted to confirm that you want to delete the selection.

Note Always select **Change** and not the **Remove** option. This is specially relevant if you have other components installed on your system. If you select the **Remove** option, it will remove all components and not just ObjectArchive.

- 3 Click **Yes** to continue.

Section 11: Installing Remote Administrator

This section includes:

[Introduction to Remote Administrator](#) (11-1)

[Requirements for Remote Administrator](#) (11-2)

[Installing Remote Administrator](#) (11-3)

[Starting AccuRoute Server Administrator and connecting to the AccuRoute server](#) (11-8)

[Connecting AccuRoute Server Administrator to additional AccuRoute servers](#) (11-10)

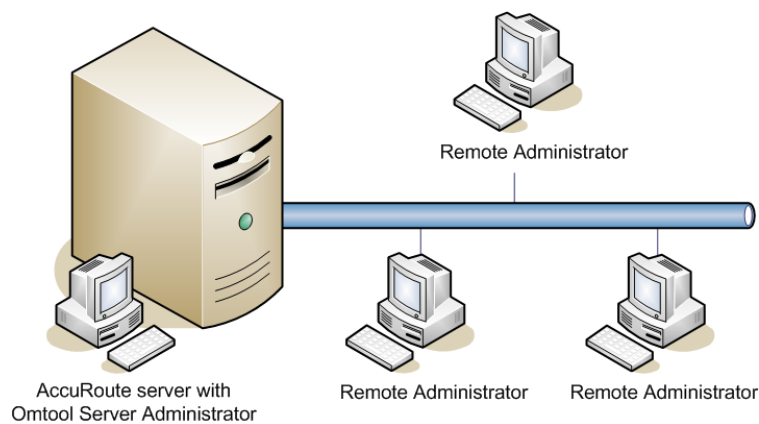
[Disconnecting AccuRoute Server Administrator from an AccuRoute server](#) (11-11)

Introduction to Remote Administrator

AccuRoute Server Administrator is the management application for the AccuRoute server. When installed on a remote system, this server management application is called a **Remote Administrator**.

The Remote Administrator provides convenient access to the AccuRoute server for administrators who support the implementation. It includes support for Windows XP Professional, which allows administrators to manage the AccuRoute server from their personal workstations.

Note There is no known limit on the number of Remote Administrators that the AccuRoute server can support.



The AccuRoute server shown here has AccuRoute Server Administrator installed and three Remote Administrators. (This is an example of a supported configuration. The AccuRoute server must be installed with AccuRoute Server Administrator, but the environment can have more or fewer Remote Administrators than shown in this illustration.)

Figure 11-1: AccuRoute server with AccuRoute Server Administrator and Remote Administrators

Requirements for Remote Administrator

Hardware and software requirements

Remote Administrator requires a system that meets the following minimum requirements:

- Windows NT domain computer that belongs to the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit, Windows 2008 R2 64-bit
- Microsoft Internet Explorer 7.0 or later
- Acrobat Reader 7.0 or later

Other installation requirements

Remote Administrator installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group

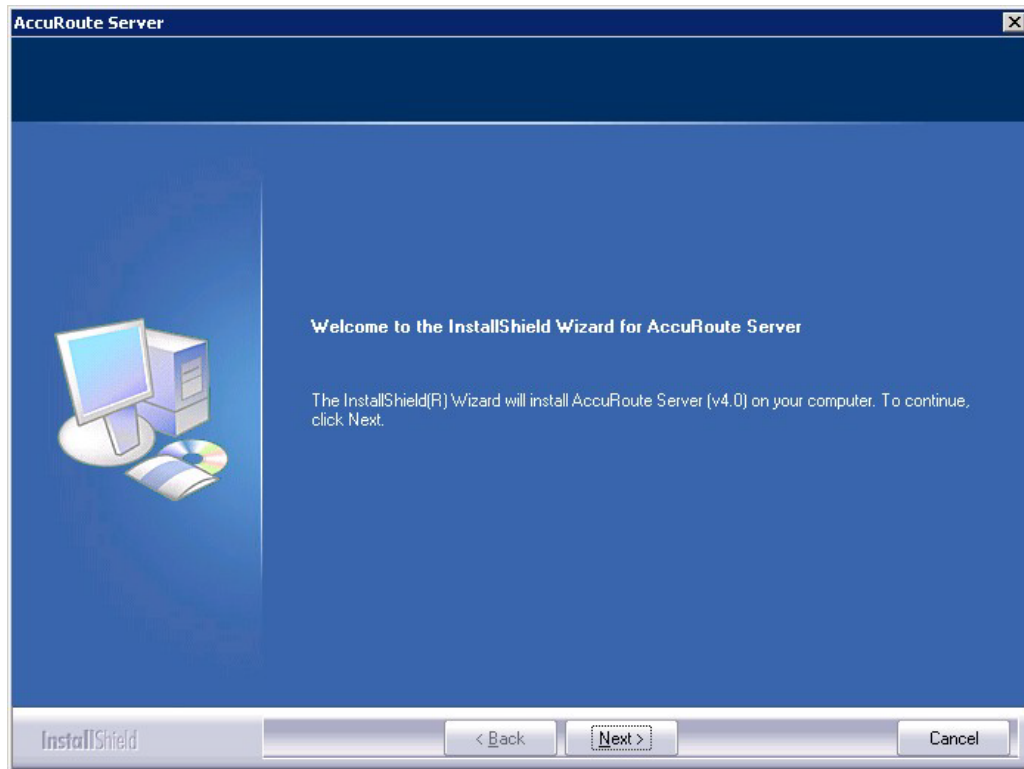
Permissions requirements

- Remote Administrator user accounts - Windows user running Remote Administrator belongs to AccuRoute Admins group (Go to [Creating AccuRoute Admins group](#) on 2-4.)
- Omttool service account - Omttool service account has Distributed COM access, launch, and configuration permissions on the Remote Administrator, and belongs to the local Administrators group on the Remote Administrator

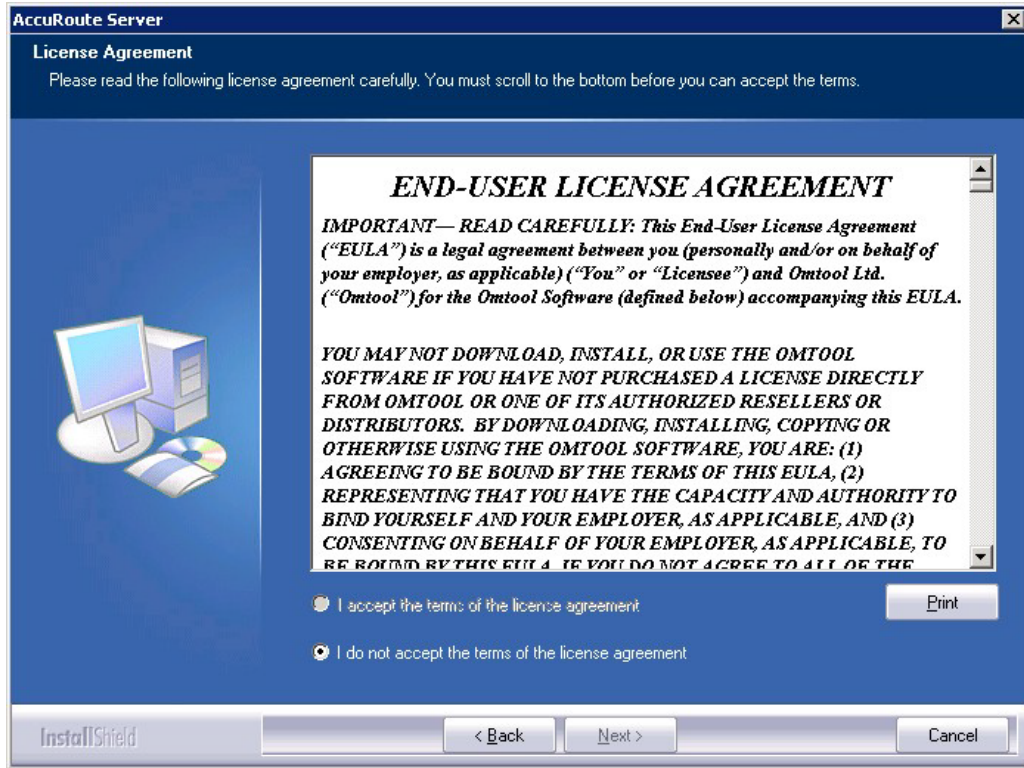
Tip For instructions on configuring these Distributed COM permissions, consult Windows help. Where the procedure indicates to log in to the AccuRoute server, log in to the Remote Administrator instead.

Installing Remote Administrator

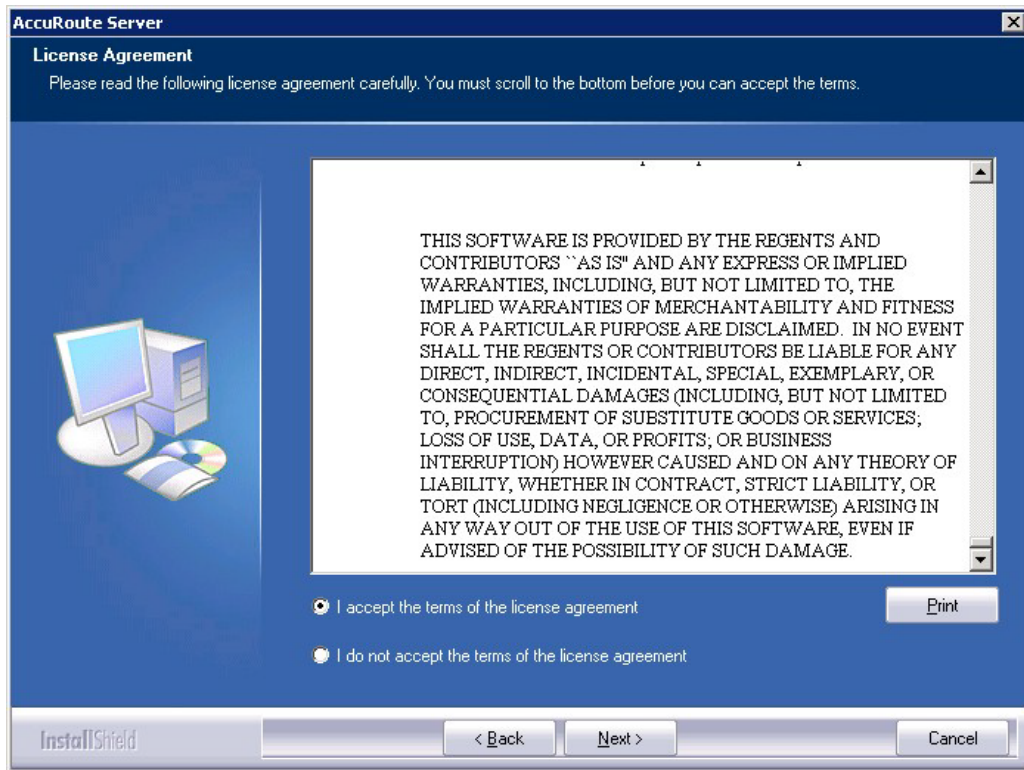
- 1 Log in to the system where you will install the Remote Administrator using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network share where you have kept the AccuRoute server setup files.
- 3 Run `\\MessageServer\setup.exe`. The InstallShield wizard opens and configures your system for installation and displays a welcome message.



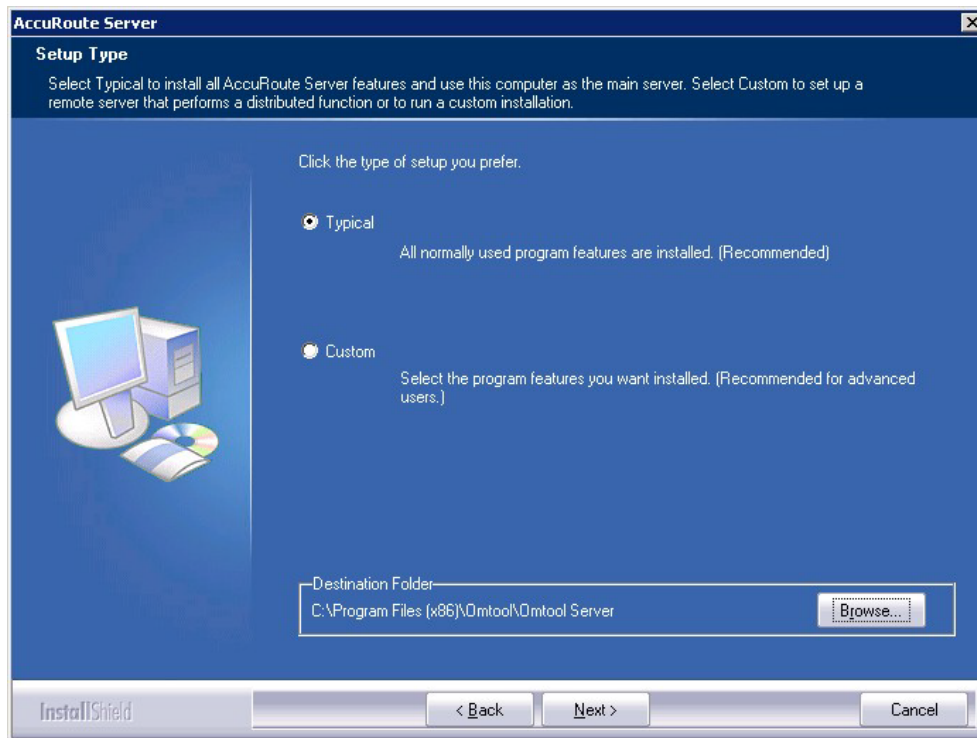
- 4 Click **Next**. The setup shows the **License Agreement** page.
- 5 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



6 Select I accept the terms of the license agreement.

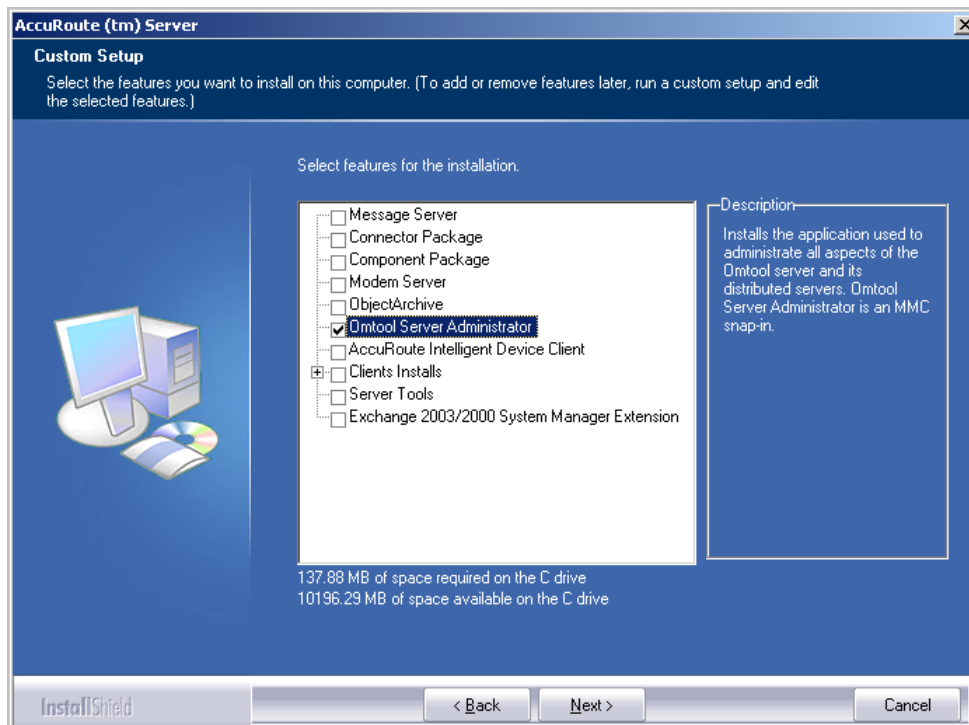


7 Click **Next**. The **Setup Type** options are displayed.

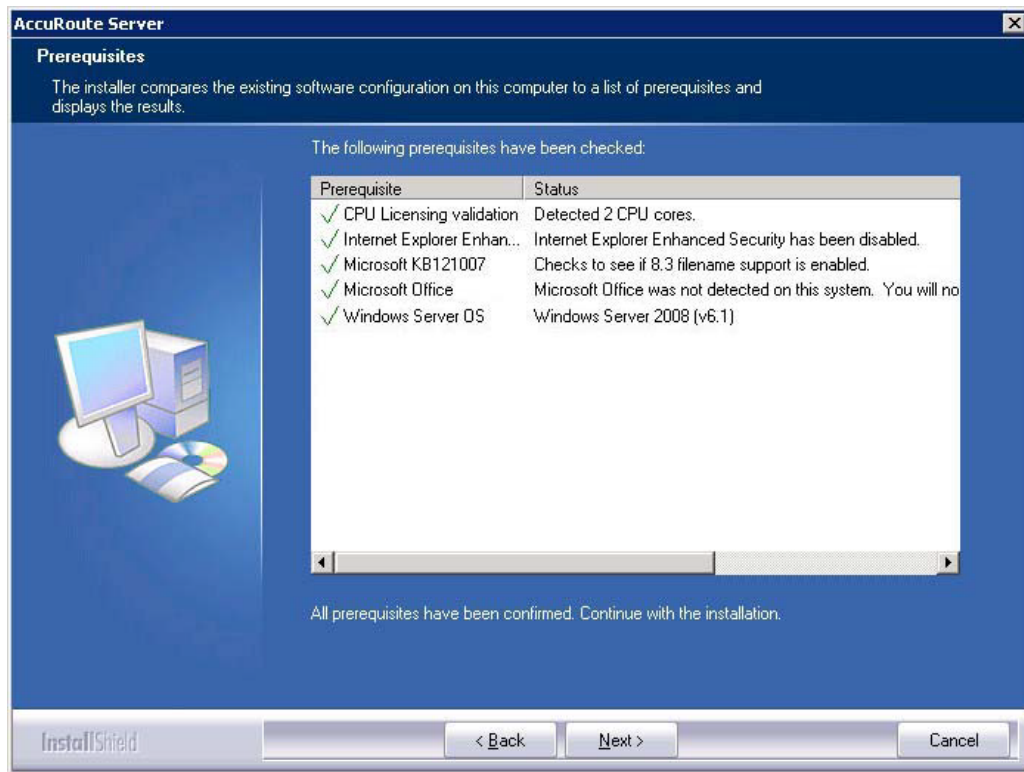


8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.

9 Select **AccuRoute Server Administrator**, clear all the other features that you are not installing.

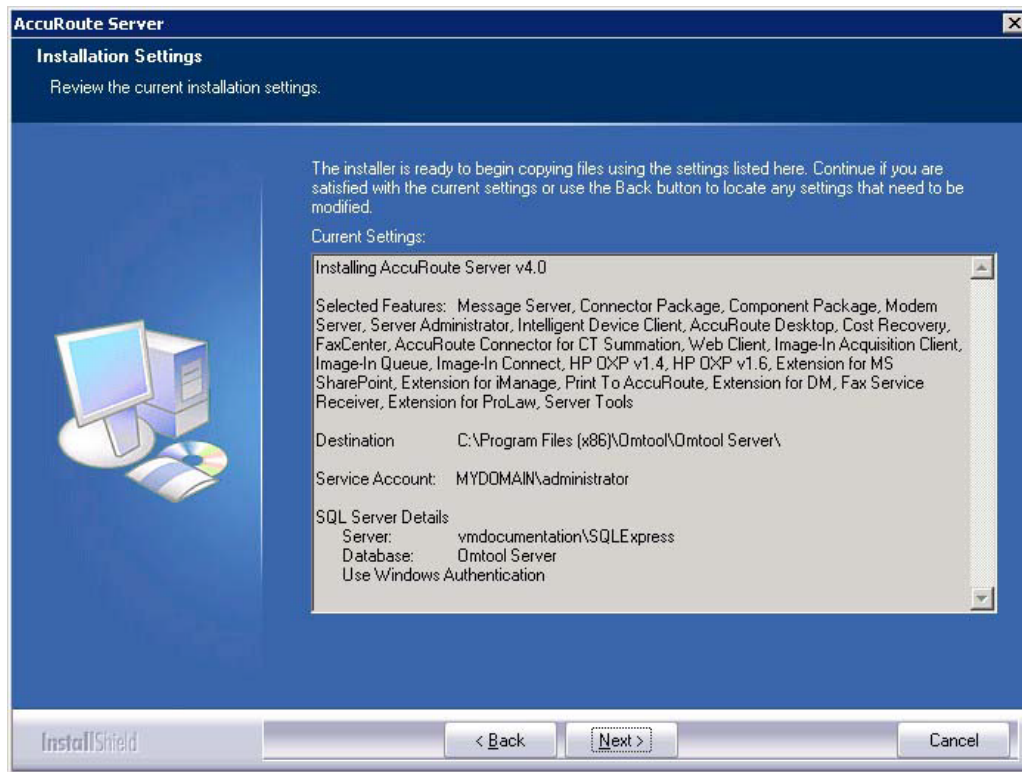


10 Click **Next**. The setup checks the system for installation requirements and displays the results.



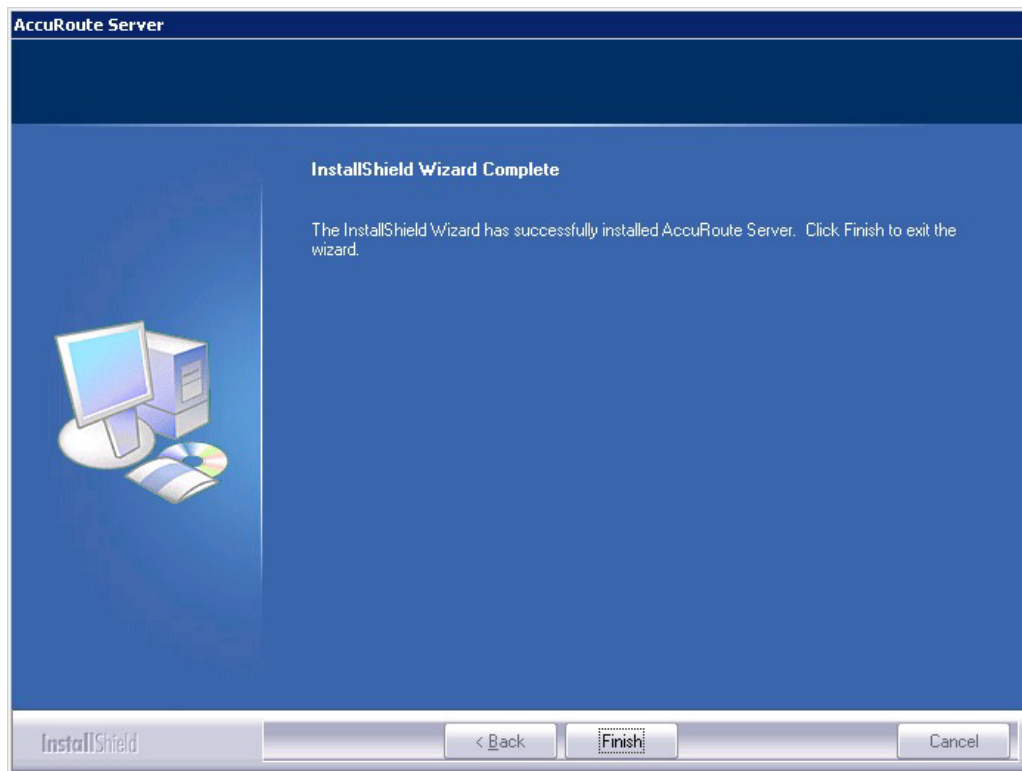
Note The setup cannot continue until all requirements are installed and configured. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

11 Click **Next**. The setup shows installation settings.



Note If other installation features are included, the setup might request additional information before displaying installation settings.

- 12 Review the installation settings and click **Next** to start the installation. The setup installs the selected features and displays a message indicating that the installation is complete.



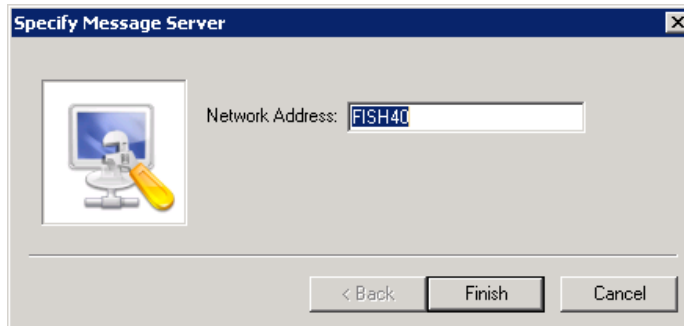
- 13 Click **Finish**.

Now that Remote Administrator is installed on the remote system, start AccuRoute Server Administrator and connect to the AccuRoute server.

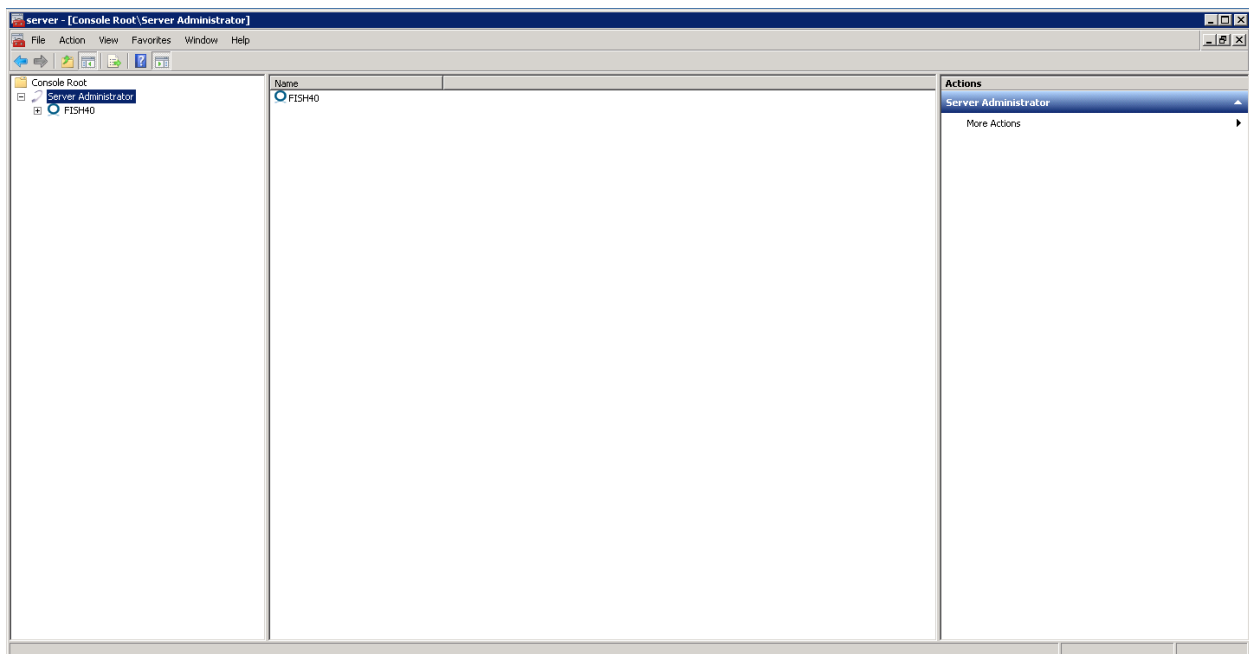
Starting AccuRoute Server Administrator and connecting to the AccuRoute server

- 1 Log in to the system where you installed the Remote Administrator using an account that belongs to the AccuRoute server admins group.
- 2 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.

The **Specify Omtool Message Server** page opens. The **Network Address** field is populated with the name of the local system.



- 3 Enter the computer name or IP address of the AccuRoute server and click **Finish**. The Microsoft Management Console starts and opens the AccuRoute Server Administrator snap-in.



Tip When AccuRoute Server Administrator is closed, Microsoft Management Console displays a message about saving changes to the MSC file. This file records the current position of items in the console tree. To preserve the console state, save the changes.

If prompted to update the MSC file, click **Yes**.

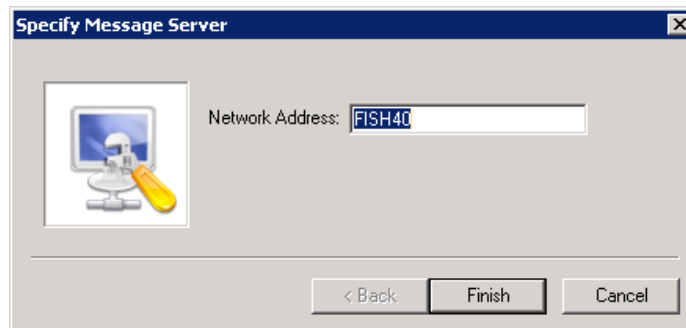
Problems connecting to the AccuRoute server using Remote Administrator

If you are having trouble connecting to the AccuRoute server using Remote Administrator, add the DCOM port [135](#) to the Exceptions list by keeping the Firewall [ON](#). Now you should be able to connect to and launch the AccuRoute server without any issues.

Connecting AccuRoute Server Administrator to additional AccuRoute servers

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **AccuRoute Server Administrator**.
- 3 Select **Connect**.

The **Specify Omtool Message Server** page opens. The **Network Address** field is populated with the name of the local system.



- 4 Enter the computer name or IP address of the AccuRoute server and click **Finish**.

The AccuRoute Server Administrator establishes a connection to the AccuRoute server and creates a new node in the console tree under **AccuRoute Server Administrator**.

Disconnecting AccuRoute Server Administrator from an AccuRoute server

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and locate the AccuRoute server that you want to disconnect.
- 3 Right-click the AccuRoute server and select **Disconnect** from the drop down menu options. The AccuRoute Server Administrator removes the server from the console tree.

Section 12: Installing an additional Composer

Composers are licensed based on a thread count. By default, the server includes two threads and will activate up to two composers (limited only by the total thread count.). Additional composers can be added to the server or they can be installed and run on a remote system.

To install a remote composer, refer to the information in:

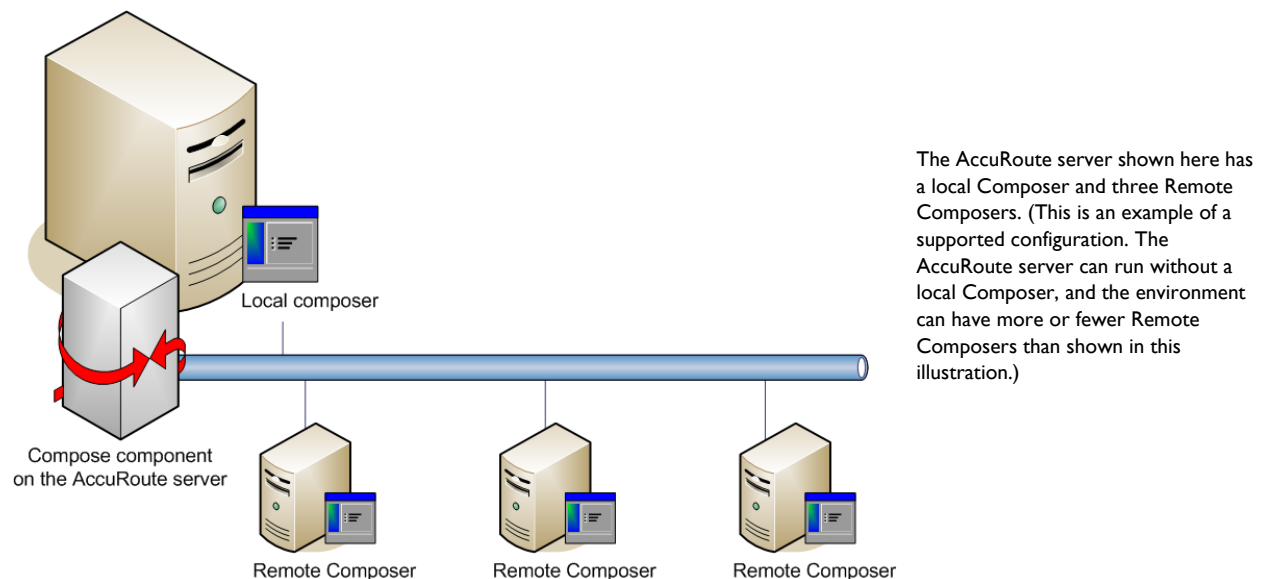
[Installing a Remote Composer \(12-1\)](#)

To install another compose thread on the server, refer to:

[Adding a Composer to the AccuRoute server \(12-10\)](#)

Installing a Remote Composer

AccuRoute Compose Component (Composer) is a system that performs message conversion tasks for the AccuRoute server. An AccuRoute server supports multiple Composers, all managed by the Compose component on the AccuRoute server. A remote system that hosts a Composer is called a **Remote Composer**.



The AccuRoute server shown here has a local Composer and three Remote Composers. (This is an example of a supported configuration. The AccuRoute server can run without a local Composer, and the environment can have more or fewer Remote Composers than shown in this illustration.)

Figure 12-1: AccuRoute server with local composer and Remote Composers

When you install an AccuRoute server, the Compose component is installed as part of the Component Package and a Composer is created locally. As Composers are added, the Compose component workload is distributed automatically. Workload distribution can be manipulated by modifying the capabilities of each Composer. By default,

a General Composer composes all types of messages, all enabled file types and final formats, and all template types, but each Composer can be modified to accept only certain types of jobs. This filtering enables a Composer to become specialized for certain types of conversions. It is also possible to enforce policies that would cause messages with certain types of files or templates to fail. For more information on configuring Composers, consult the Omtool Server Administrator Help, which is available on the [AccuRoute v6.0 documentation](#) page.

When scaling an environment with additional connectors or components, always consult an Omtool Technical Support engineer. For information, contact [Upland AccuRoute Service and Support](#). The Omtool Technical Support engineer can assist you in correctly identifying potential bottlenecks in the system based on workload and other factors. Moreover, the Support engineer can provide helpful information on the overall impact of increasing the speed and efficiency of the system. Performance and stability consulting are also available for a fee.

To purchase additional Composers, contact an Upland AccuRoute Sales representative. If a detailed analysis of the environment is necessary, the AccuRoute Technical Support engineer may recommend a fee-based consultation.

Requirements for a Remote Composer

Hardware and software requirements

Remote Composer requires a system that meets the following minimum requirements:

- Windows NT domain computer that always runs in the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device

Note Omtool recommends using a core for each compose thread that is configured to do OCR. The AccuRoute server comes with 4 Compose threads. You can increase the number of threads as needed. Contact [Omtol Sales](#) for more information.

- Windows 2012 64-bit, Windows 2008 R2 64-bit
- Disable **Internet Explorer Enhanced Security Configuration** (Windows Component).
If this component is not disabled, it will not let you proceed with the installation. After you disable the component, you must reboot you system before proceeding with the installation.
- Microsoft Internet Explorer 7.0 (minimum)

Software requirements for message conversion

The Remote Composer requires one of the following applications. An item is required only if the Composer needs to convert documents into file types associated with the application. For example, if you are planning to use Crystal Reports for compose, it must be installed on the Composer.

- Microsoft Visio 2007 for *.VSD and *.VDX message attachments
- Crystal Reports v10.0 or earlier for *.RPT message attachments

Note Routing Sheet templates are provided in *.DOC and *.OMTPL format, and these templates can be edited in Word and WordPad respectively.

Important Visual Basic for Applications is required for PowerPoint document conversion. You must install this component for PPT and PPTX document formats to compose successfully on the AccuRoute server. If this component is not installed, and you try to compose a PowerPoint document, you will get an error.

Additional installation requirements

Remote Composer installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group
- License key for each additional Composer

Note A license key is not required if the local Composer is being moved to a remote system.

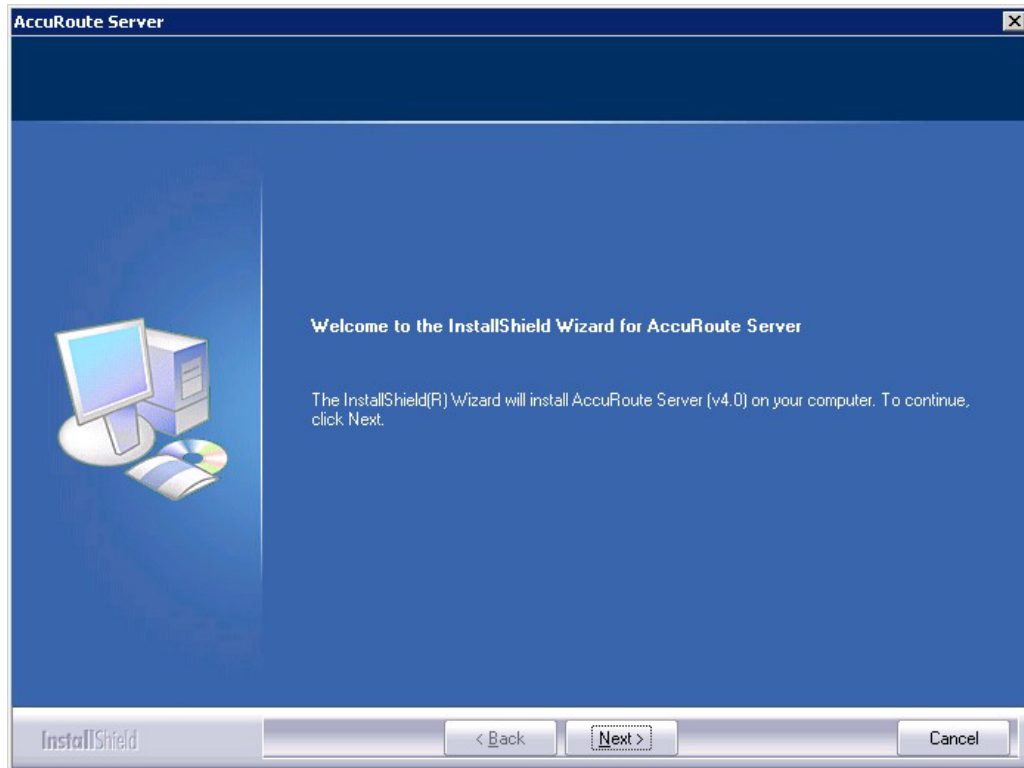
- Verifying the **NtfsDisable8dot3NameCreation** registry value is set to 0

Installing a Remote Composer

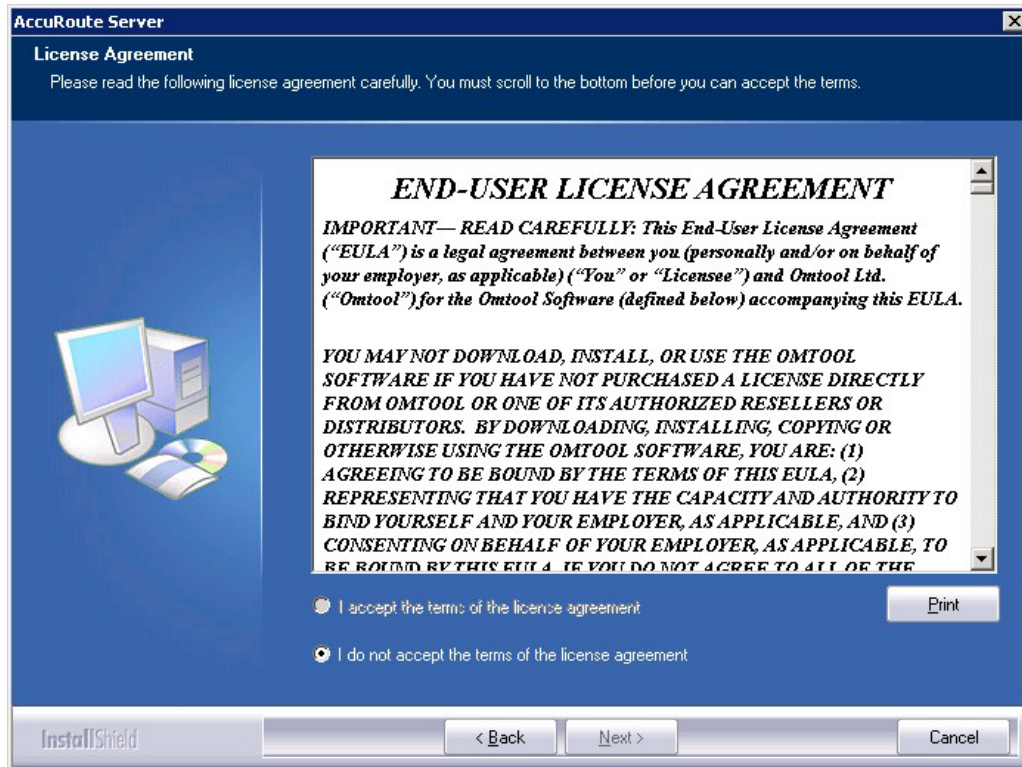
Note Before installing a Remote Composer on a Windows 2008 R2 system, allow DCOM port 135 as an exception. Otherwise you will not be able to add the Remote Composer.

- 1 Log in to the system where you will install the Remote Composer using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network share where you have kept the AccuRoute server setup files.
- 3 Run **\\MessageServer\setup.exe**.

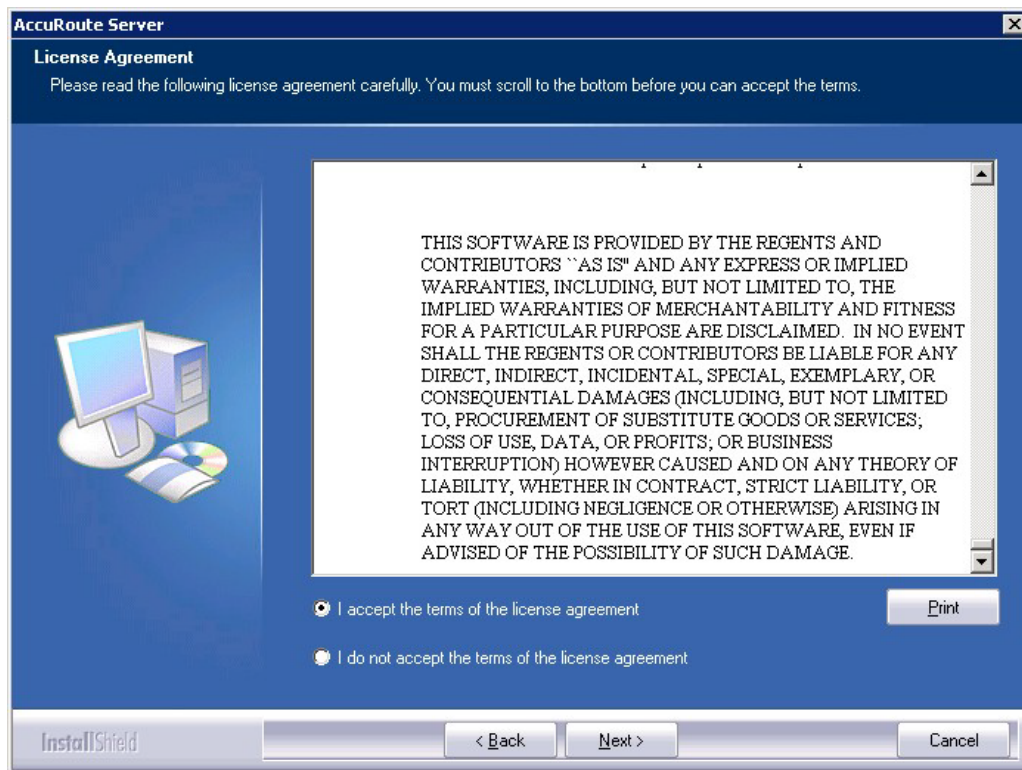
The InstallShield wizard opens and configures your system for installation and displays a welcome message.



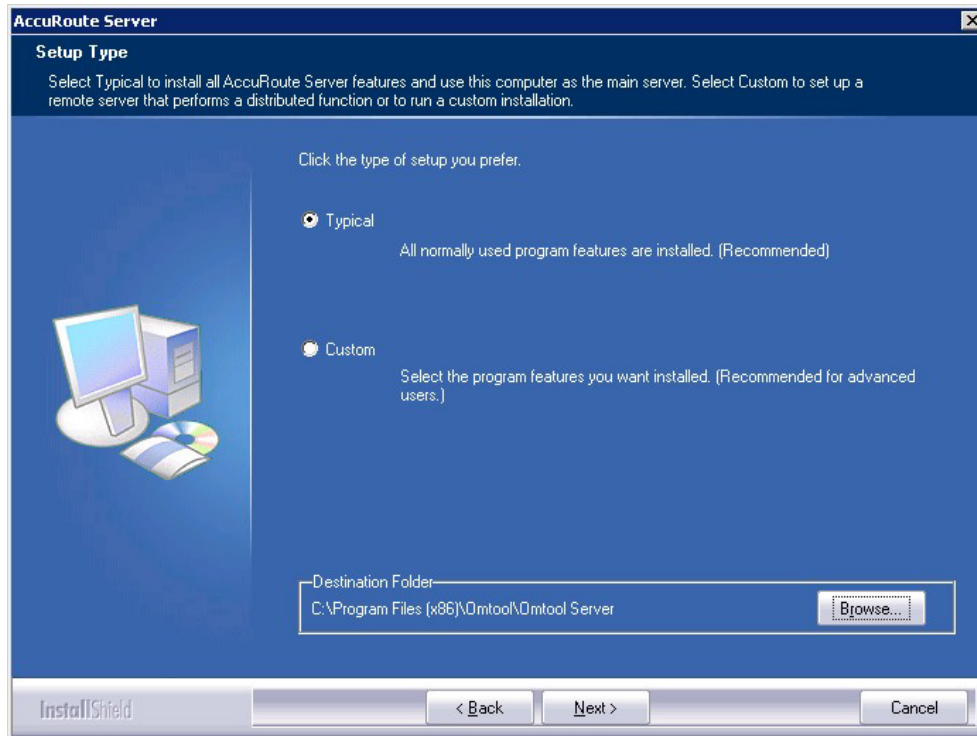
- 4 Click **Next**. The setup shows the **License Agreement** page.
- 5 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



6 Select I accept the terms of the license agreement.

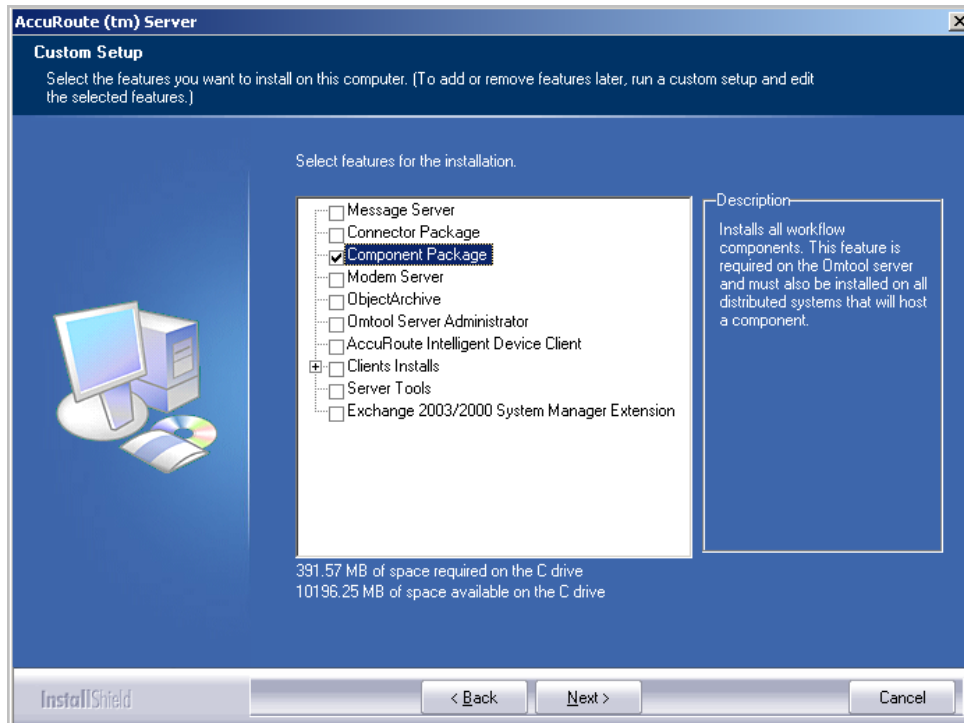


7 Click **Next**. The **Setup Type** options are displayed.

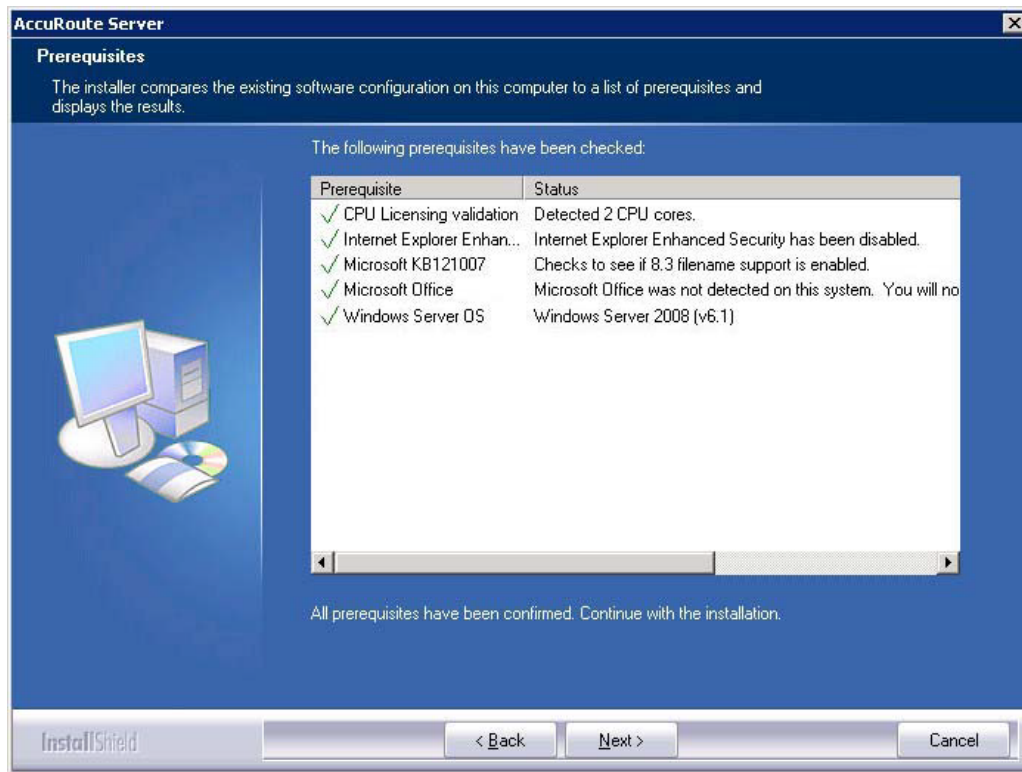


8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.

9 Select **Component Package**, clear all the other features that you are not installing at this time.

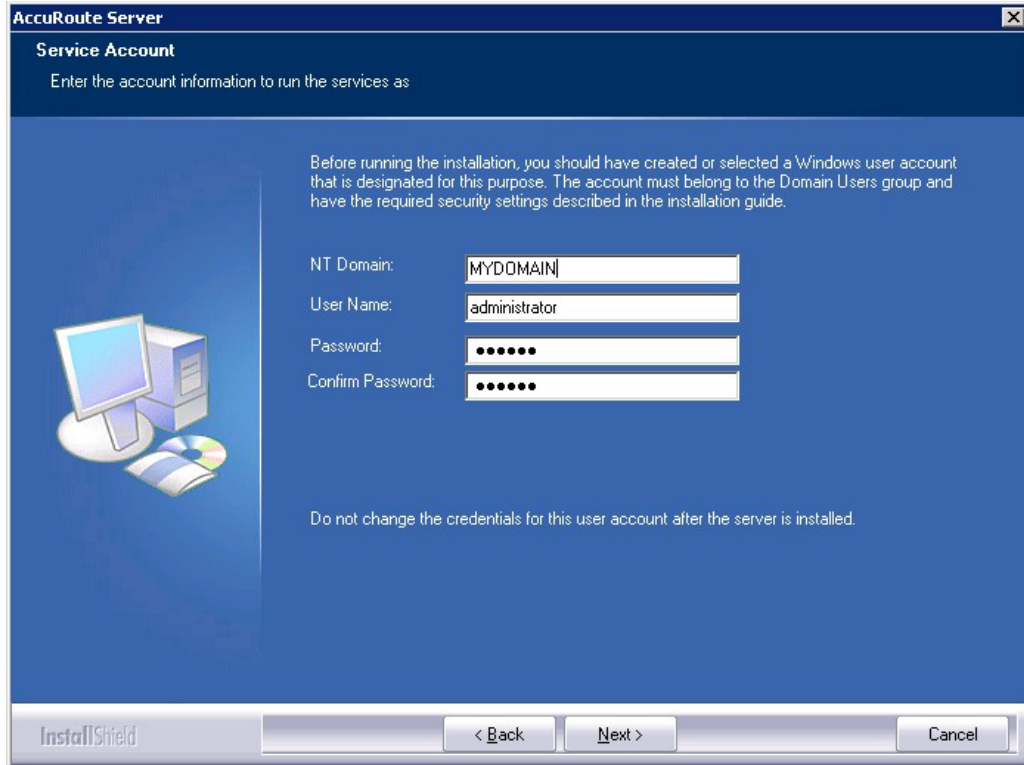


- 10 Click **Next**. The setup checks the system for installation requirements and displays the results.

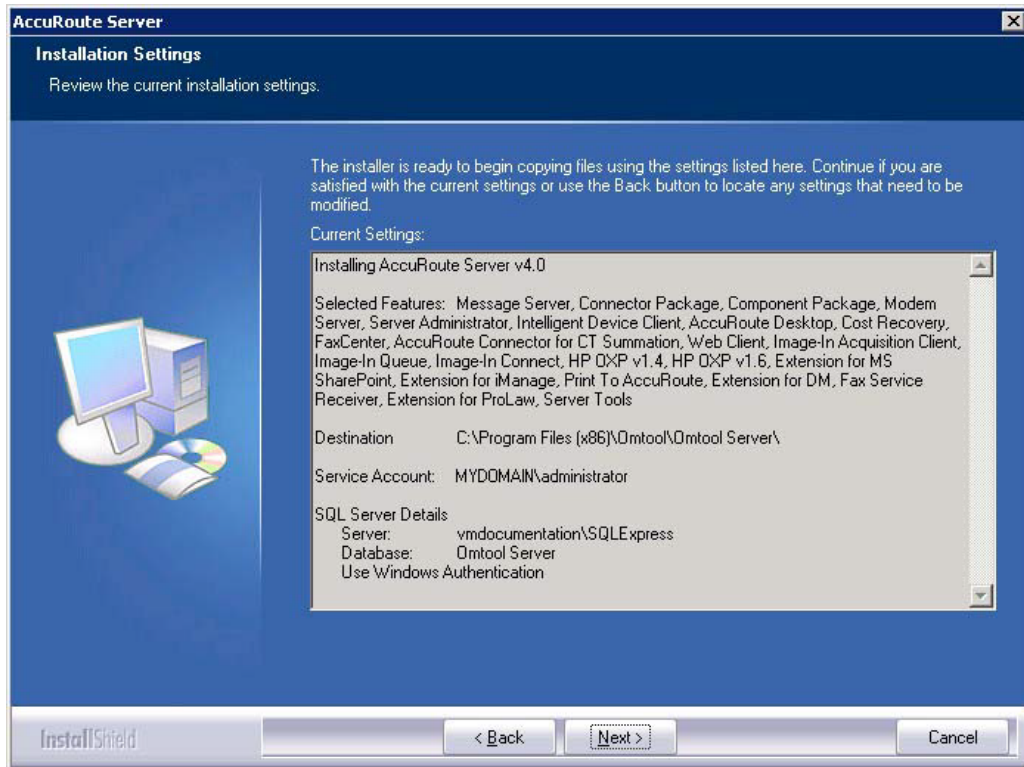


Note The setup cannot continue until all required components are installed. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

- 11 Click **Next** to continue the installation. The setup requests logon credentials for the Omtool service account. The **NT Domain** and **User Name** fields are populated automatically based on the current Windows user.
- 12 Enter the logon credentials of the Omtool service account.
- In the **NT Domain** field, enter the name of the Windows domain.
 - In the **User Name** field, enter the user name.
 - In the **Password** and **Confirm Password** fields, enter the password for the user.

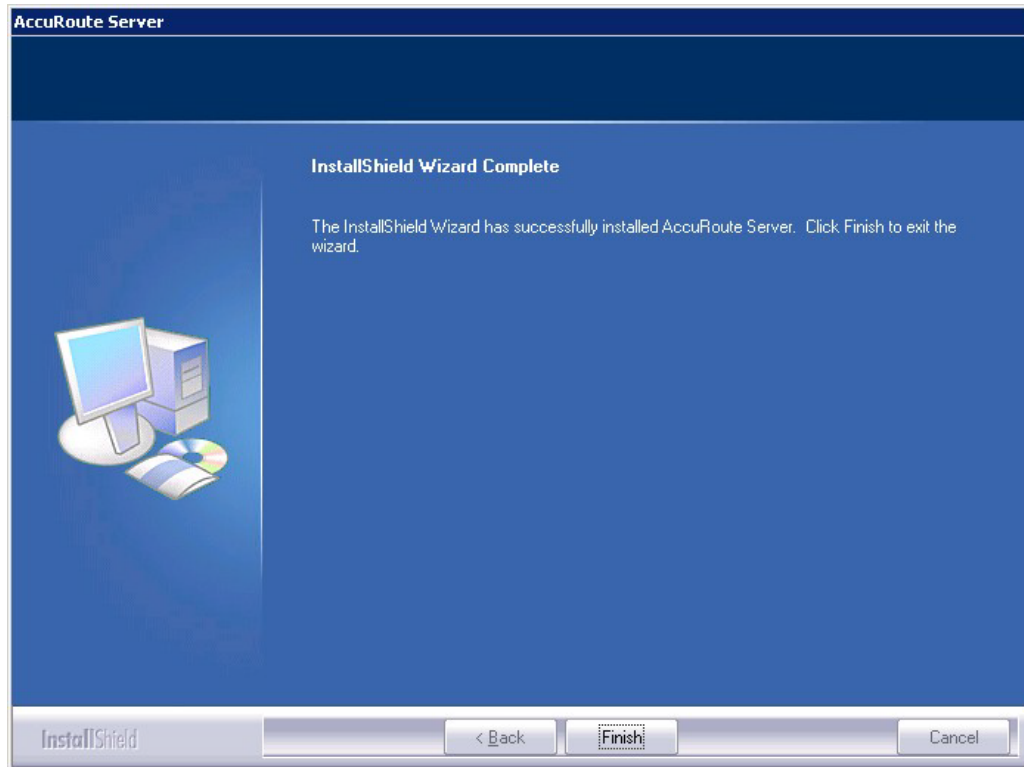


13 Click **Next**. The setup validates the user account and then shows installation settings.



Note If other installation features are included, the setup might request additional information before displaying installation settings.

- 14 Review the installation settings and click **Next** to start the installation. The setup installs the selected component and displays a message indicating that the installation is complete.



- 15 Click **Finish**.

Now that Remote Composer is installed on the remote system, add the Composer to the Compose component on the AccuRoute server. Continue to [Adding a Composer to the AccuRoute server](#).

Adding a Composer to the AccuRoute server

To add a new Composer to the AccuRoute server, go to [Adding a new Composer to the AccuRoute server](#) (12-10). To replace the local Composer with the new Remote Composer, go to [Replacing the local Composer with the new Remote Composer](#) (12-13).

For each additional Composer you add to your environment, you must get a license key from Omtool. Contact [Omtool Sales](#) for more information.

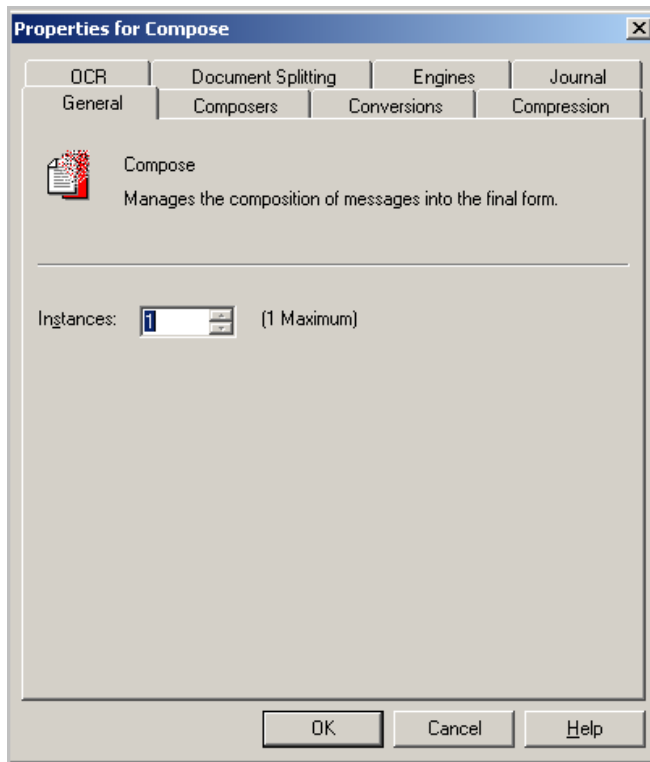
Applying the Compose license activation code

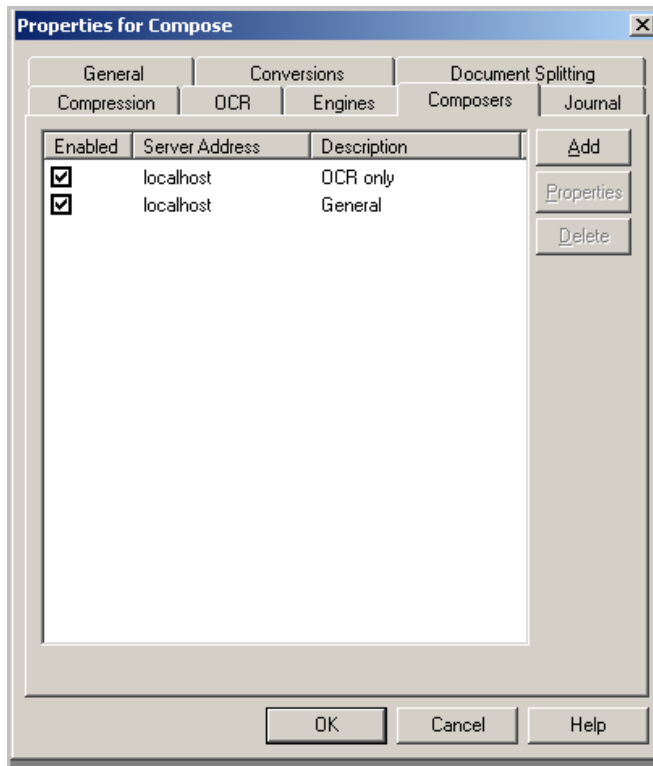
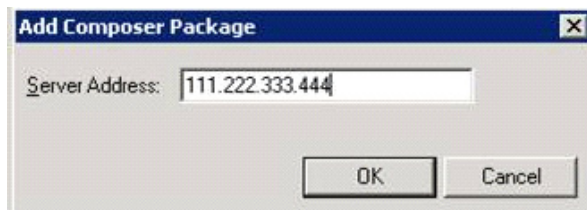
- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and select the server name.
- 3 Right-click the server name and select **Licensing**.
- 4 Click the **Activate License...** button. The **License Activation** page is displayed.
- 5 You can activate the license automatically or manually. Both procedures are described in [Activating the license](#) (3-16).
- 6 After activating the license, click **Close** to complete the procedure.

Adding a new Composer to the AccuRoute server

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Components**.

- 3 Double-click **Compose** in the details pane to open the **Compose Properties** page.



4 Click the **Composers** tab.**5** Click **Add**. The **Add Composer Package** page opens.**6** In the **Server Address** text box, enter the machine name or IP address of the Remote Composer. Enter `localhost` if the composer is being added to the AccuRoute server.**7** Click **OK**.**8** Click **OK** to close the Composer page.

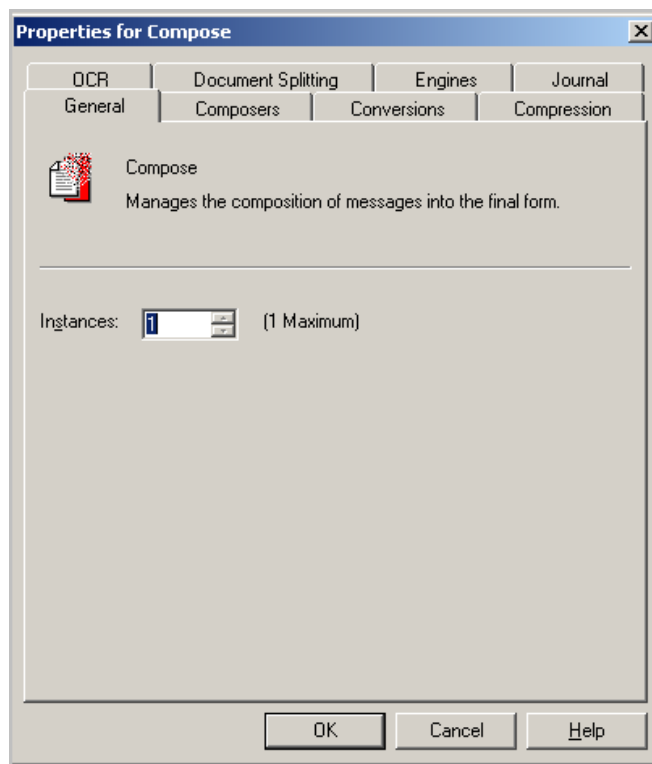
The Remote Composer begins performing conversion tasks immediately.

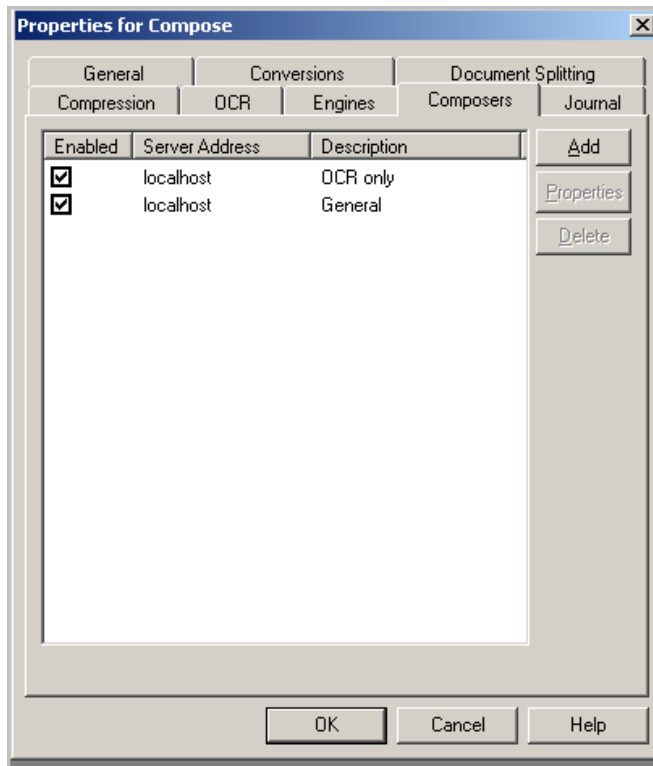
Replacing the local Composer with the new Remote Composer

For each additional Composer you add to your environment, you must purchase a license key from Omtool.

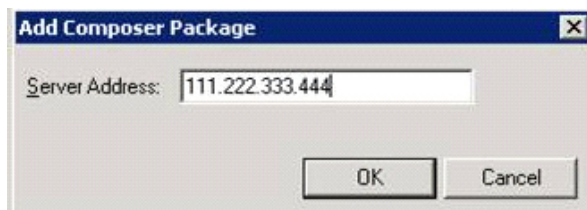
Note You will remove the General Composer in the procedure below and replace the local Composer with the new Remote Composer:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Components**.
- 3 Double-click **Compose** in the details pane to open the **Properties** page.



4 Click **Composers** option.**5** Select **localhost**, click **Delete**, and then click **Yes** to continue. The local Composer is removed.

Tip The local Composer must be removed first so that the new Composer can be added without a license key.

6 Click **Add**. The Add Composer Package page opens.**7** In the **Server Address** text box, enter the machine name or IP address of the Remote Composer.**8** Click **OK** to close the Composer page.

The Remote Composer begins performing conversion tasks immediately.

Section 13: Installing Remote Modem Server

This section includes:

[Introduction to Remote Modem Server](#) (13-1)

[Requirements for Remote Modem Server](#) (13-2)

[Installing and testing the fax board and Dialogic Brooktrout System Software](#) (13-3)

[Installing the Remote Modem Server](#) (13-3)

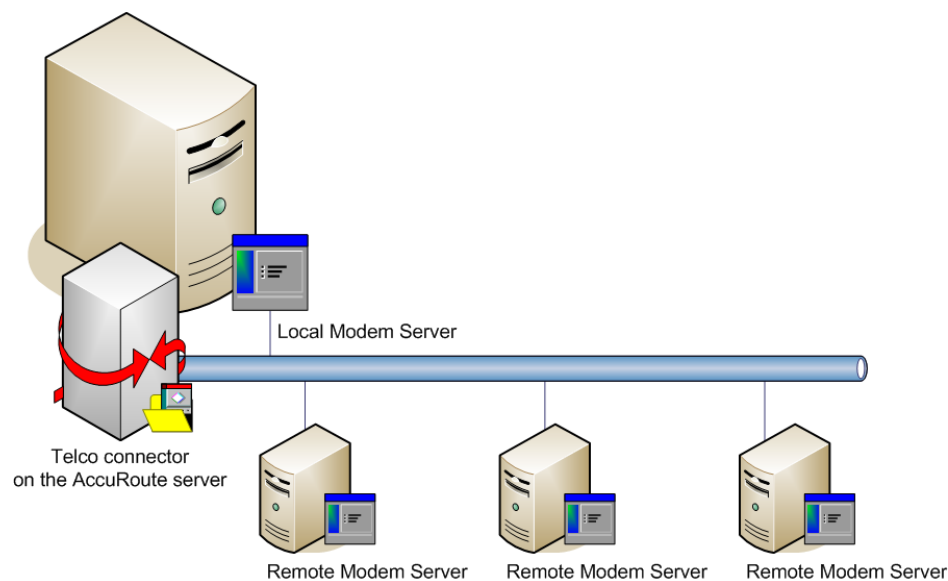
[Detecting the channels on the Modem Server](#) (13-9)

[Configuring the path to the Telco share directory](#) (13-10)

Introduction to Remote Modem Server

A Modem Server is a server that sends and/or receives faxes for the AccuRoute server. It consists of at least one locally installed fax board, Brooktrout System Software / Drivers, and AccuRoute Modem Server software.

An AccuRoute server supports multiple Modem Servers, all managed by the AccuRoute connector for Telco on the AccuRoute server. A remote system that hosts a Modem Server is called **Remote Modem Server**.



The AccuRoute server shown here has a local Modem Server and three Remote Modem Server with a AccuRoute connector for Telco managing all of them. (This is an example of a supported configuration.)

Figure 13-1: AccuRoute server with local Modem Server and Remote Modem Servers

The AccuRoute server can run without a local Modem Server, and the environment can have more Telco connectors or fewer Remote Modem Servers than shown in this illustration. The AccuRoute connector for Telco can be configured to monitor one Telco share, an intermediary repository for inbound and outbound faxes.

Modem Servers are supported in these configurations:

- AccuRoute connector for Telco with one Modem Server in the LAN
- AccuRoute connector for Telco with multiple Modem Servers in the LAN
- multiple AccuRoute connectors for Telco, each with one or more Modem Servers in the LAN

Using multiple AccuRoute connectors for Telco delivers additional benefits to environments with special faxing requirements:

- **Reduced faxing costs** - With multiple AccuRoute connectors for Telco, the AccuRoute server can be configured to deliver faxes using the Modem Server that is closest to the destination which can reduce long distance telephone charges.
- **Failover support** - Through rules, the AccuRoute server can be configured to route outbound faxes to one AccuRoute connector for Telco but if delivery fails, the AccuRoute server can route the outbound faxes to another AccuRoute connector for Telco.
- **Increased efficiency** - Multiple AccuRoute connectors for Telco provide built-in workload distribution based on the AccuRoute server configuration, the AccuRoute connector for Telco configuration, and rules.

When scaling an environment with additional connectors or components, always consult an AccuRoute Technical Support engineer. For information, contact [Upland AccuRoute Service and Support](#). The AccuRoute Technical Support engineer can assist you in correctly identifying potential bottlenecks in the system based on workload and other factors. Moreover, the Support engineer can provide helpful information on the overall impact of increasing the speed and efficiency of the system. Performance and stability consulting are also available for a fee.

To purchase additional Modem Server, contact an Upland AccuRoute Sales representative. If a detailed analysis of the environment is necessary, the AccuRoute Technical Support engineer may recommend a fee-based consultation.

Requirements for Remote Modem Server

Hardware and software requirements

A Remote Modem Server requires a system that meets the following minimum requirements:

- Windows NT domain computer that always runs in the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 2GB of RAM for T1 line (2-24 channels) or 4 GB RAM for two T1 lines (24-48 channels)
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit, Windows 2008 R2 64-bit
- AccuRoute connector for Telco - this requires a purchased license
- Modem Channels require a license for each port enabled.
- Microsoft Internet Explorer 7 or later

Additional installation requirements

Remote Modem Server installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group

Note Remote Modem Server requires installation of at least one supported Brooktrout fax board and Brooktrout System Software. For additional requirements on installing the fax board and Brooktrout System Software, consult the fax board installation guide: For information on fax board installation, consult the [Dialogic modem driver installation and configuration guide](#).

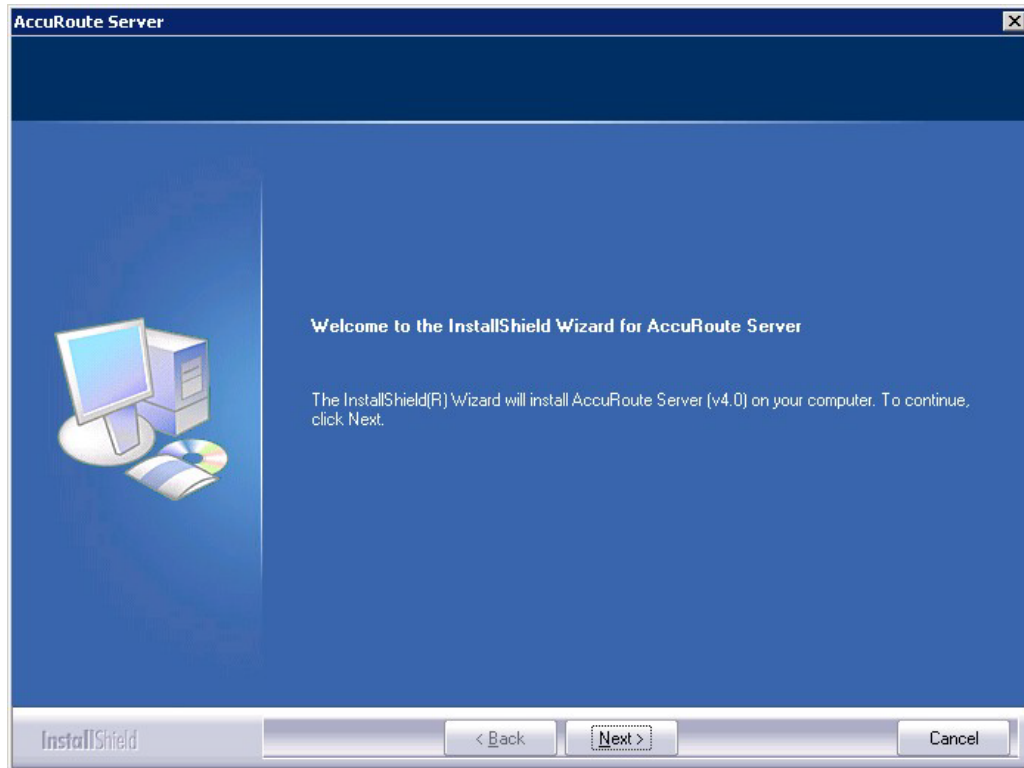
Installing and testing the fax board and Dialogic Brooktrout System Software

Before Remote Modem Server is installed, at least one fax board or the SRI40 Modem software must be installed locally with the Brooktrout System Software. For instructions on installing the fax board and Brooktrout System Software, consult the [Dialogic modem driver installation and configuration guide](#).

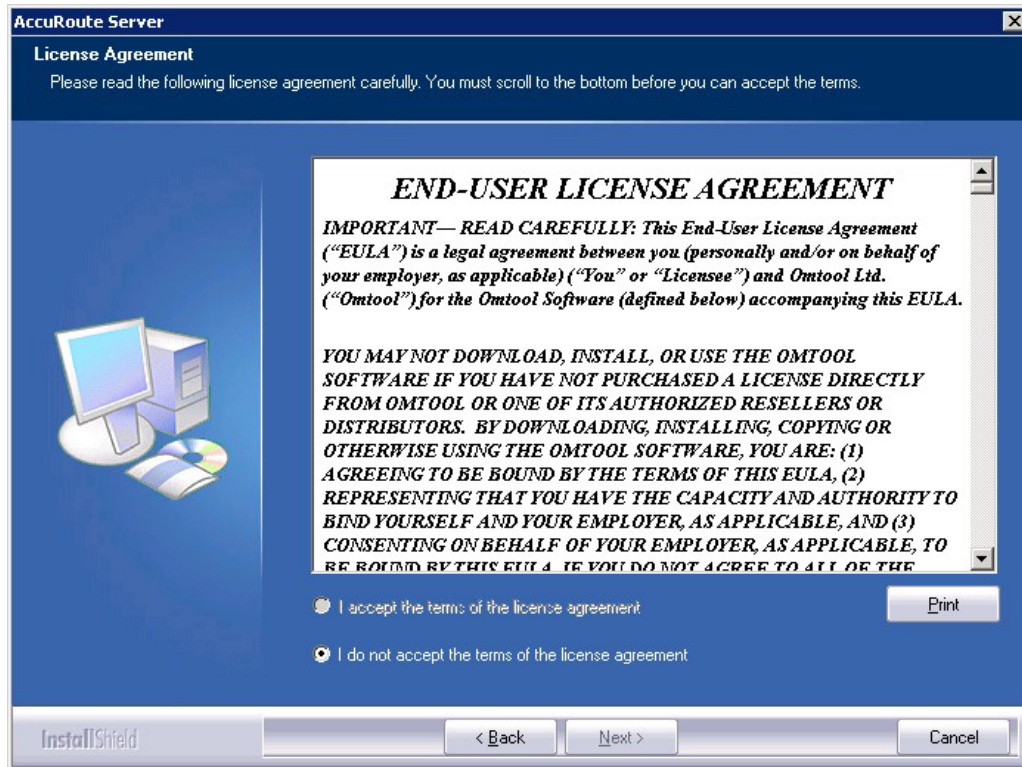
Installing the Remote Modem Server

- 1 Log in to the system where you will install the Remote Modem Server using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network where you have kept the AccuRoute server setup files.
- 3 Run **\\MessageServer\setup.exe**.

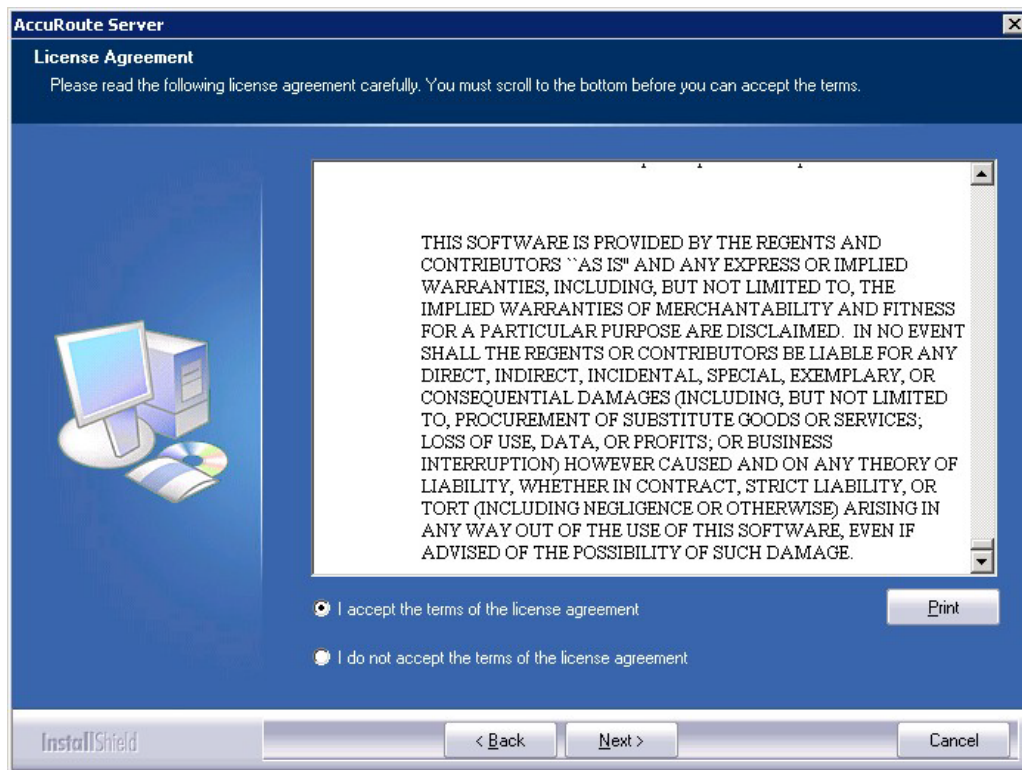
The InstallShield wizard opens and configures your system for installation and displays a welcome message.



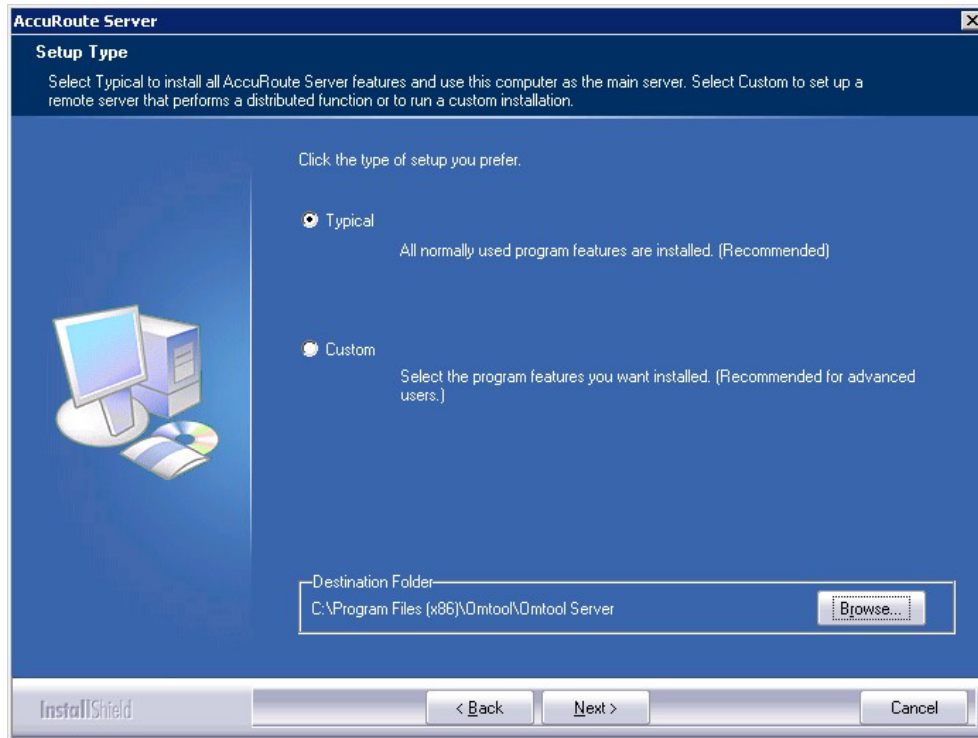
- 4 Click **Next**. The setup shows the **License Agreement** page.
- 5 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



6 Select I accept the terms of the license agreement.

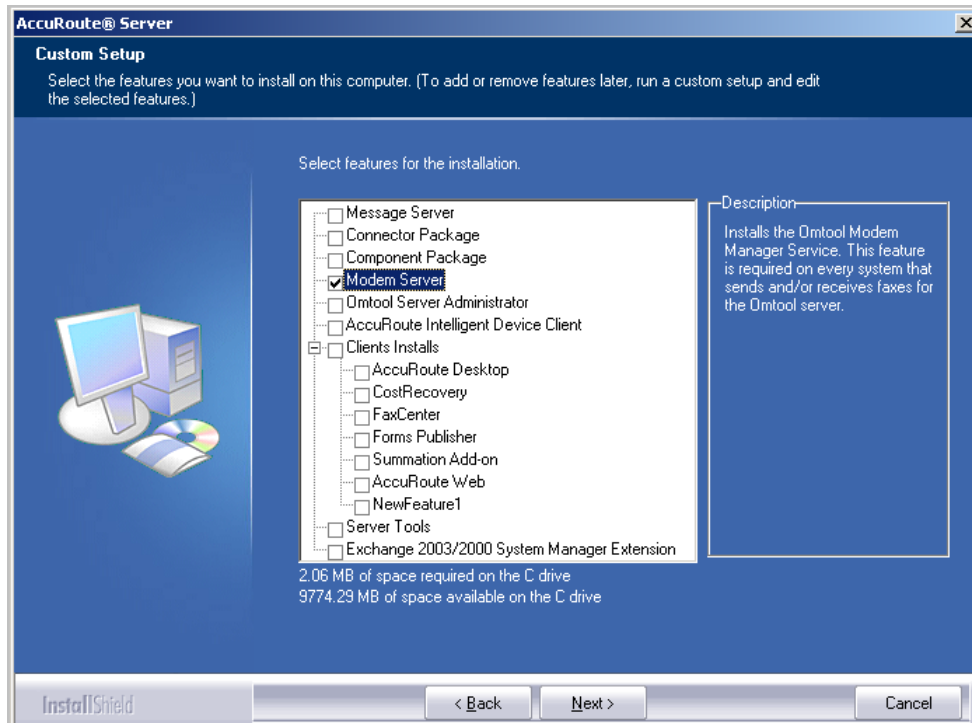


7 Click **Next**. The **Setup Type** options are displayed.

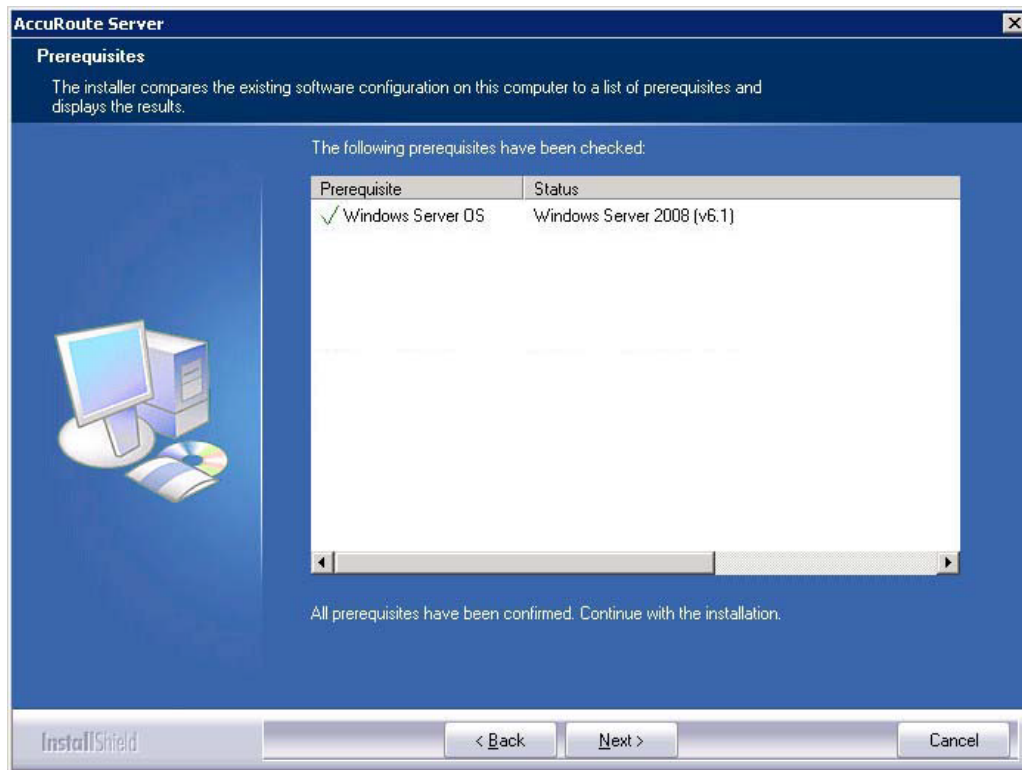


8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.

9 Select **Modem Server**, clear all the other features you are not installing at this time.



- 10 Click **Next**. The setup checks the system for installation requirements and displays the results.

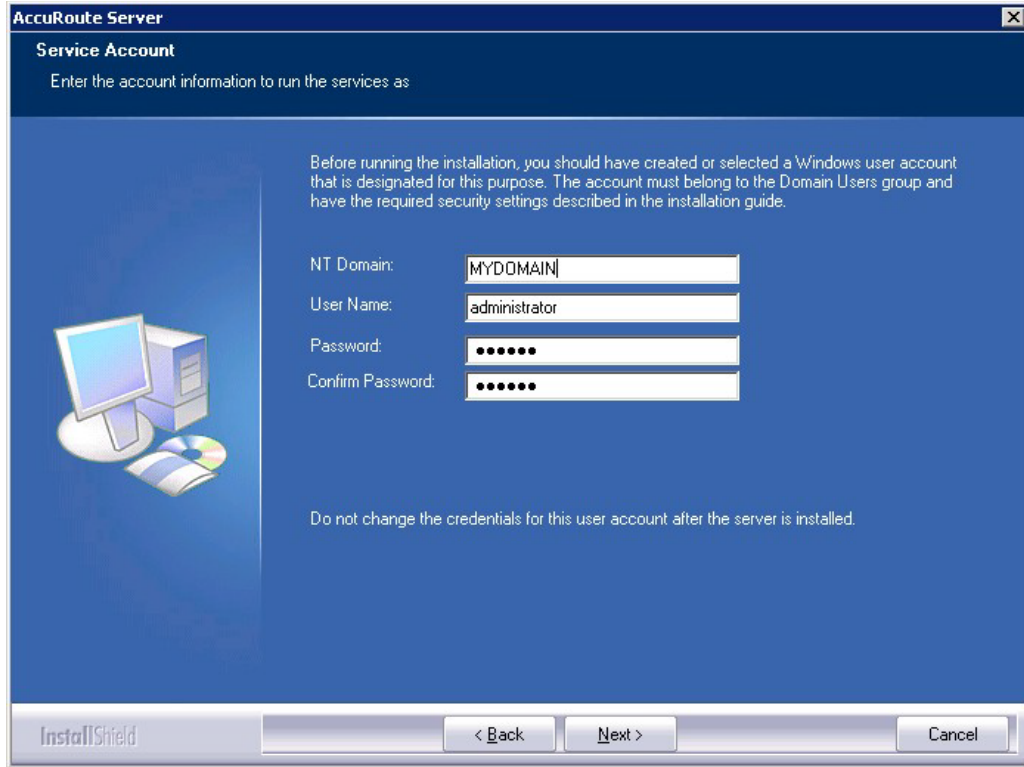


Note The setup cannot continue until all required components are installed. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

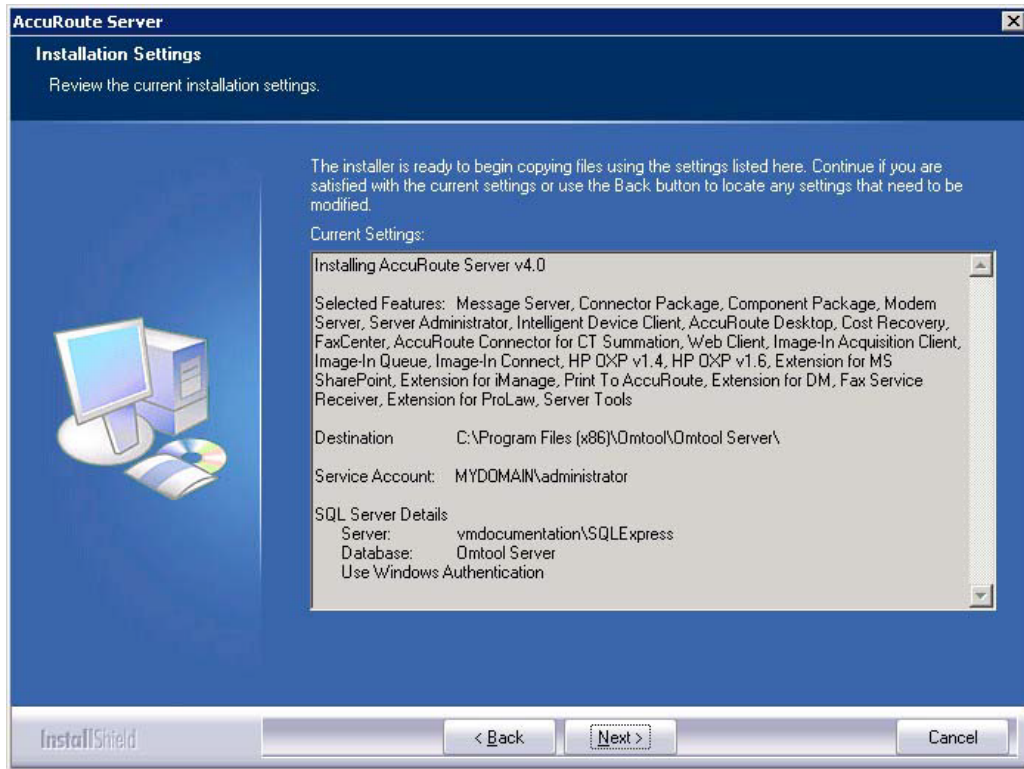
- 11 Click **Next** to continue the installation. The setup requests logon credentials for the Omtool service account. The **NT Domain** and **User Name** fields are populated automatically based on the current Windows user.
- 12 Enter the logon credentials of the Omtool service account.
- In the **NT Domain** field, enter the name of the Windows domain.
 - In the **User Name** field, enter the user name.
 - In the **Password** and **Confirm Password** fields, enter the password for the user.

Note If other installation features are included, the setup might request additional information before displaying installation settings.

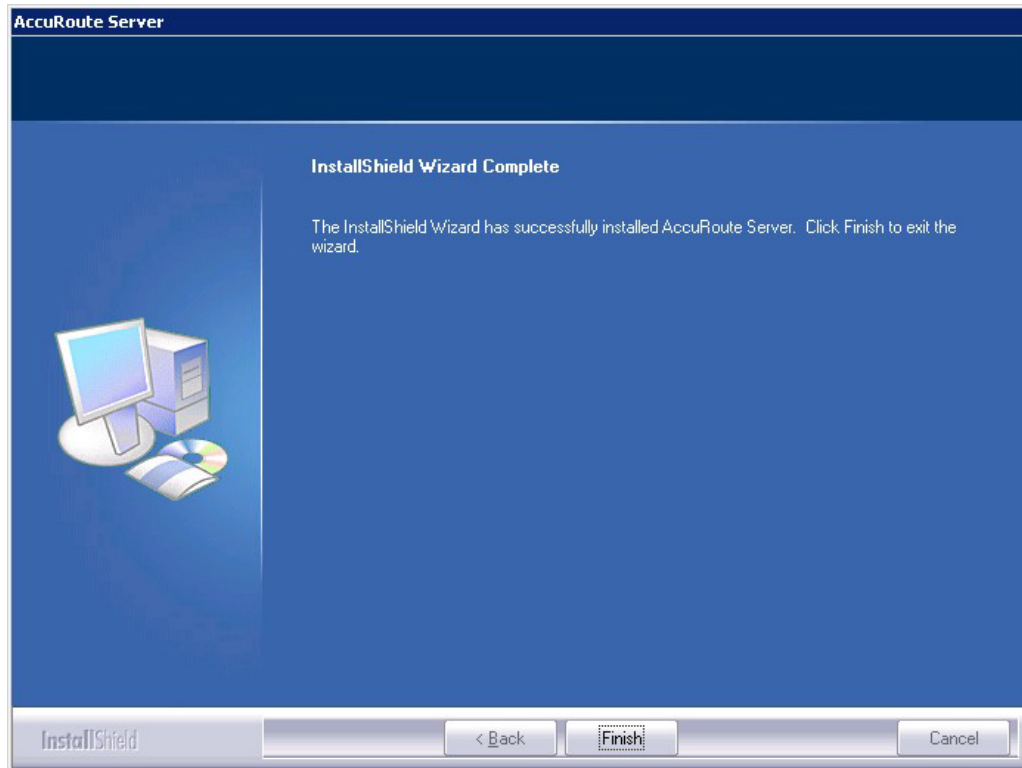
Section 13: Installing Remote Modem Server



13 Click **Next**. The setup validates the user account and then shows installation settings.



- 14 Review the installation settings and click **Next** to start the installation. The setup installs the modem server and displays a message indicating that the installation is complete.



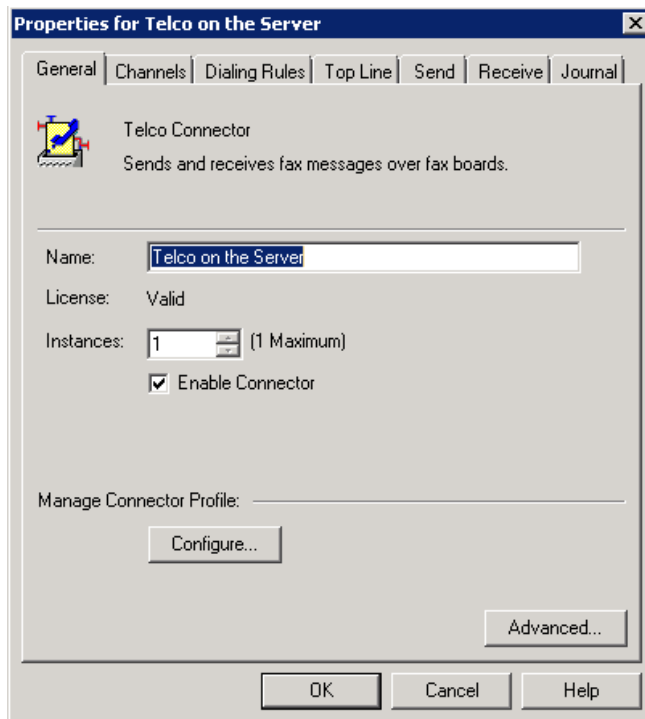
- 15 Click **Finish**.
- 16 Continue to [Detecting the channels on the Modem Server](#).

Detecting the channels on the Modem Server

After you have installed the Remote Modem Server, you must configure the AccuRoute connector for Telco to detect the channels on the Remote Modem Server. After the channels have been detected, the properties of each channel, such as send and receive properties, can be configured in the AccuRoute connector for Telco properties. To detect the channels on the Modem Server:

- 1 Click **Start > All Programs > Omttool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Connectors**.

- 3 Double-click **Telco** in the details pane. The **Properties** page opens.



- 4 Click **Channels** and then click **Detect Channels**. The **Detect Channels** page opens.
- 5 In the **Remote Server Address** text box, enter the machine name or the IP Address of the Remote Modem Server and click **Detect Now**.
- 6 Configure the channels if necessary, and then click **OK**.

For more information on configuring the channels, consult the AccuRoute Server Administrator Help, which is available on the [AccuRoute v6.0 documentation](#) page.

Configuring the path to the Telco share directory

After you have detected the channels, you can configure the path to the Telco share directory to be a UNC path.

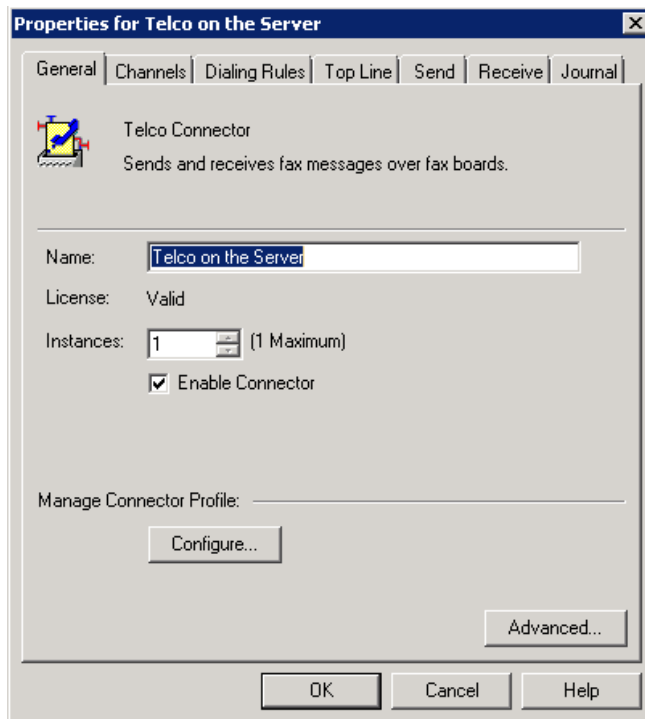
Note The UNC path of the AccuRoute server is filled in by default.

If you specify a full path what will happen is this: when the configuration file are written to the remote modem server, the remote modem channels will look for “c:\” for the send and receive queues. But they should be looking at the AccuRoute server for the queues.

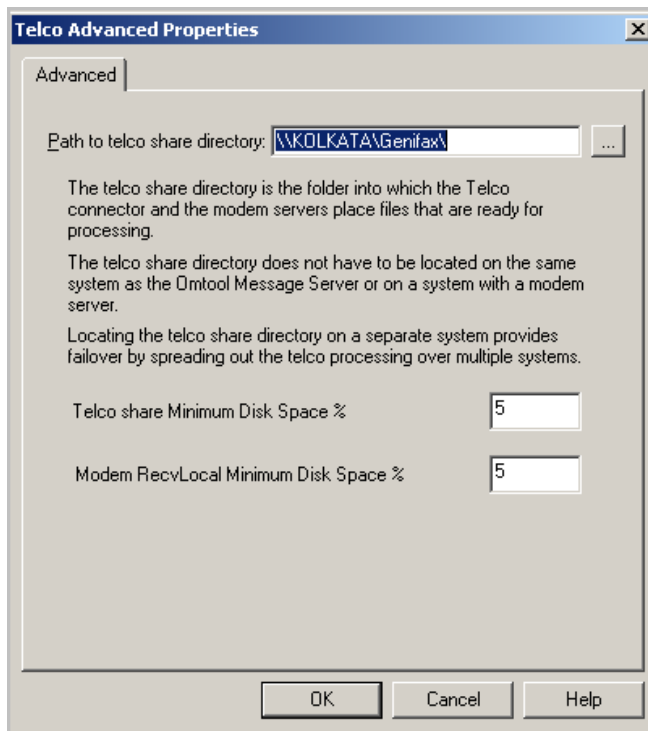
To configure the path to the Telco share directory:

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Connectors**.

- 3 Double-click **Telco** in the details pane. The **Properties** page opens.



- 4 Click **Advanced** to open the **Telco Advanced Properties** page.



In the **Path to telco share directory** text box, the UNC path of the AccuRoute server is filled in by default.

- 5 Modify the path if necessary. You can, for example, specify the name of the system instead of providing the IP Address. Add a trailing backslash at the end. (For example `\\123.4.5.678\telcoshare\`).
- 6 Click **Ok** and then **Ok** to save your changes and close the **Properties** page.

Section 14: Installing Remote Embedded Directive Manager

The Embedded Directive Manager is used to process Distribution Rules. The information in this section describes:

[Introduction to Remote Embedded Directive Manager](#) (14-1)

[Requirements for Remote Embedded Directive Manager](#) (14-2)

[Installing Remote Embedded Directive Manager](#) (14-3)

[Adding Remote Embedded Directive Manager to the AccuRoute server](#) (14-9)

[Removing Embedded Directive Manager from the AccuRoute server or a remote system](#) (14-11)

Introduction to Remote Embedded Directive Manager

Embedded Directive Manager is a component that processes messages that are routed to the Embedded Directive Manager based on rules (This includes scanning documents for bar codes and Routing Sheets that have an associated Distribution Rule, and applying Scan to Me configurations to messages.)

When the AccuRoute server is installed, the Embedded Directive Manager component is created locally. (It is installed automatically as part of the Component Package.) Embedded Directive Manager can also be installed on a remote system. This is called a **Remote Embedded Directive Manager**.

Having multiple Embedded Directive Managers distributes the component workload. Workload distribution is automatic; it is not configurable.

Note The local Embedded Directive Manager component on the AccuRoute server can be removed, but only if a Remote Embedded Directive Manager exists.

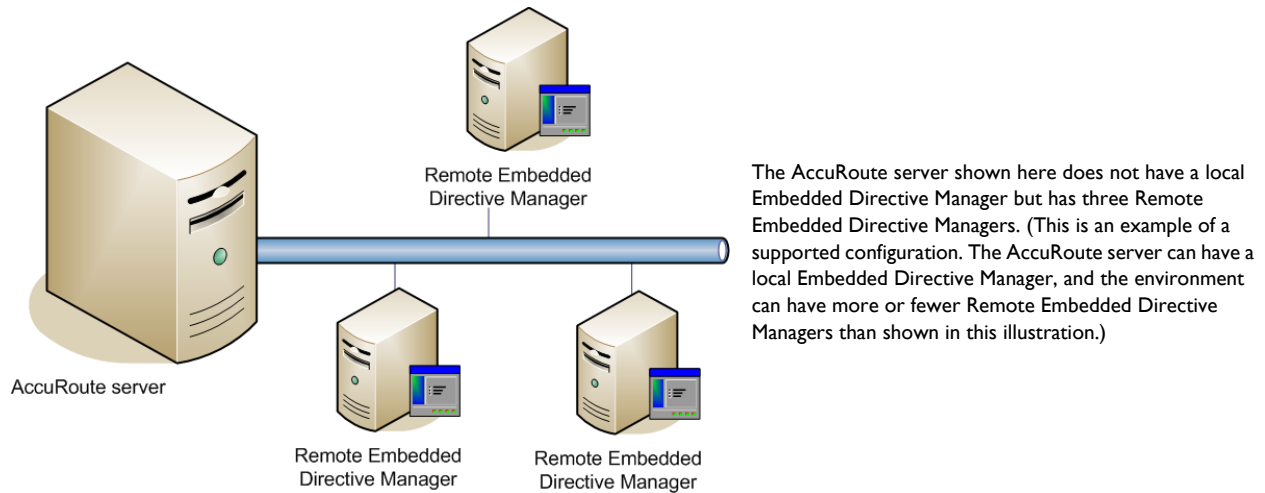


Figure 14-1: AccuRoute server with Remote Embedded Directive Managers

When scaling an environment with additional connectors or components, always consult an AccuRoute Technical Support engineer. For information, contact [Upland AccuRoute Service and Support](#). The AccuRoute Technical Support engineer can assist you in correctly identifying potential bottlenecks in the system based on workload and other factors. Moreover, the Support engineer can provide helpful information on the overall impact of increasing the speed and efficiency of the system. Performance and stability consulting are also available for a fee.

To purchase additional Embedded Directive Manager component licenses, contact an Upland AccuRoute Sales representative. If a detailed analysis of the environment is necessary, the AccuRoute Technical Support engineer may recommend a fee-based consultation.

Requirements for Remote Embedded Directive Manager

Hardware and software requirements

Remote Embedded Directive Manager requires a system that meets the following minimum requirements:

- Windows NT domain computer that always runs in the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit, Windows 2008 R2 64-bit
- Disable **Internet Explorer Enhanced Security Configuration** (Windows Component).

If this component is not disabled, it will not let you proceed with the AccuRoute server installation. After you disable the component, you must reboot the system before proceeding with the server installation.

Additional requirements

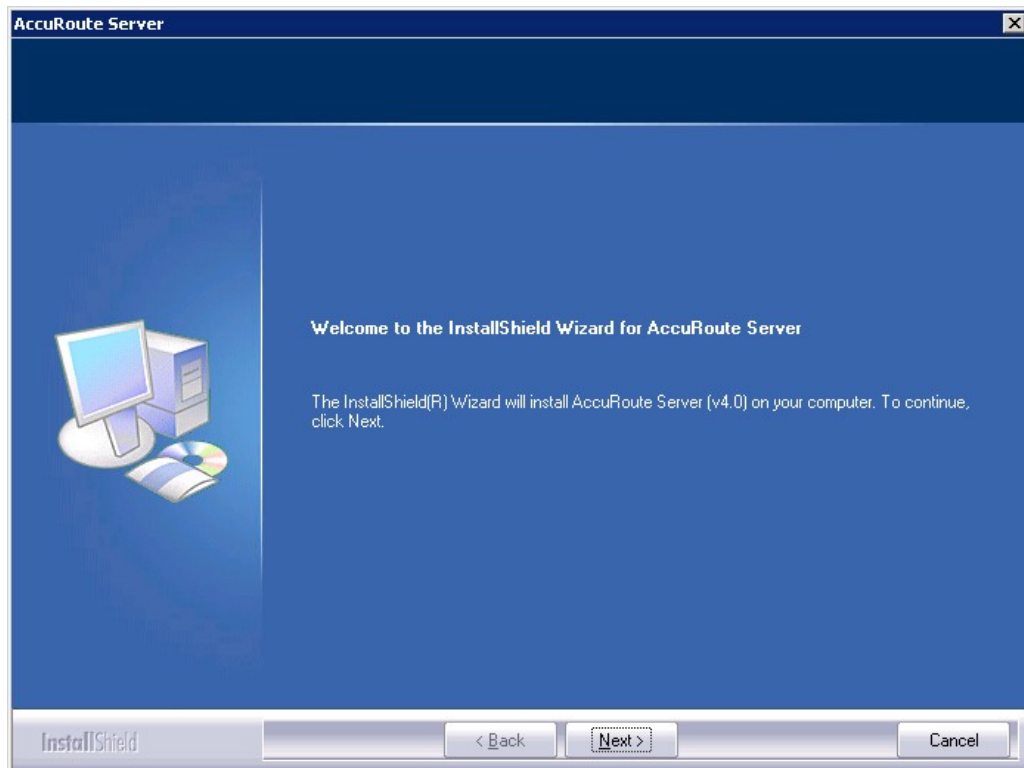
Remote Embedded Directive Manager installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group
- License key for Remote Embedded Directive Manager
- contact [Upland AccuRoute Service and Support](#). for the license key.
- Verifying the **NtfsDisable8dot3NameCreation** registry value is set to 0

Installing Remote Embedded Directive Manager

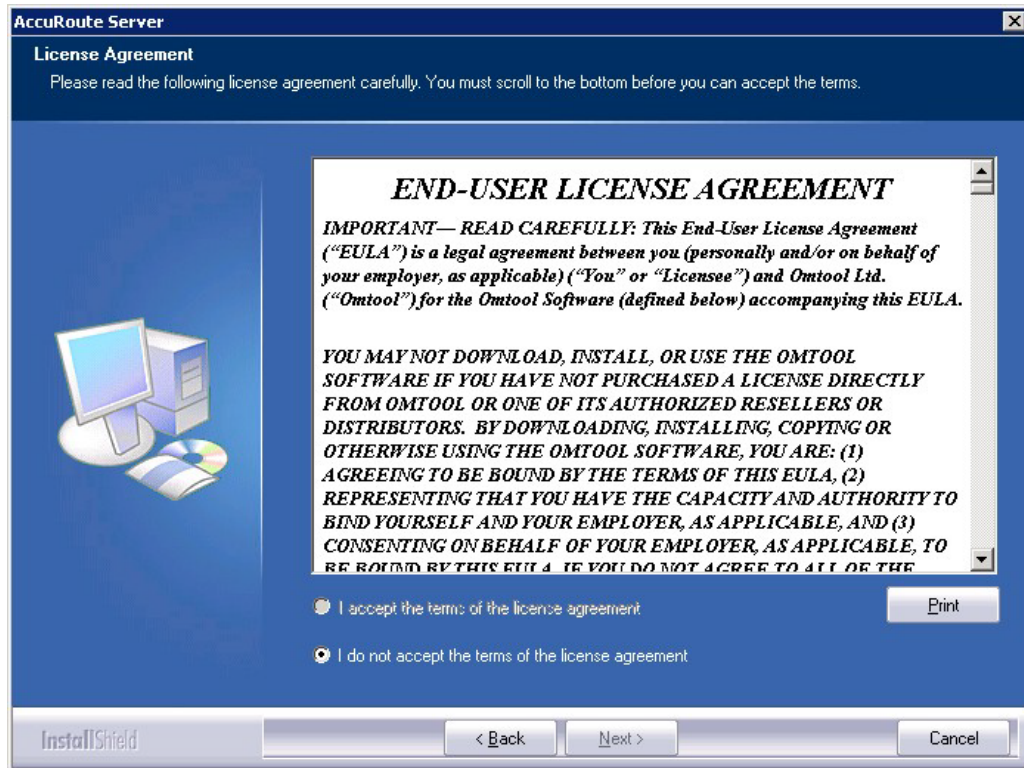
- 1 Log in to the system where you will install the Remote Embedded Directive Manager using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network where you have kept the AccuRoute server setup files.
- 3 Run **\\MessageServer\setup.exe**.

The InstallShield wizard opens and configures your system for installation and displays a welcome message.

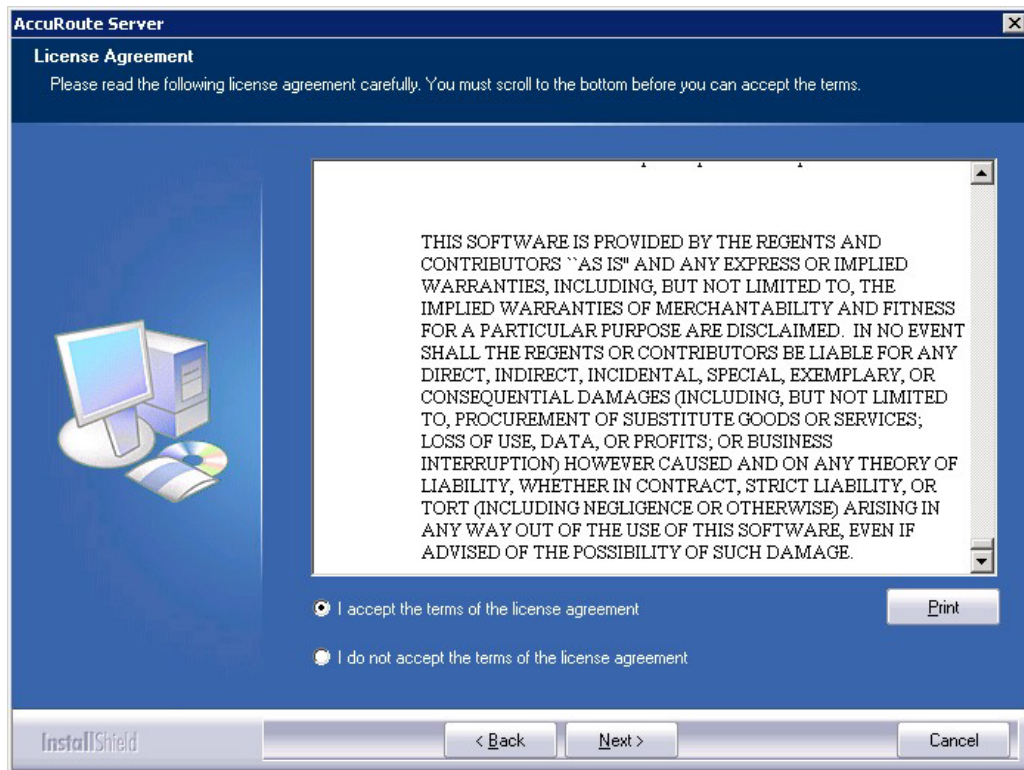


- 4 Click **Next**. The setup shows the **License Agreement** page.

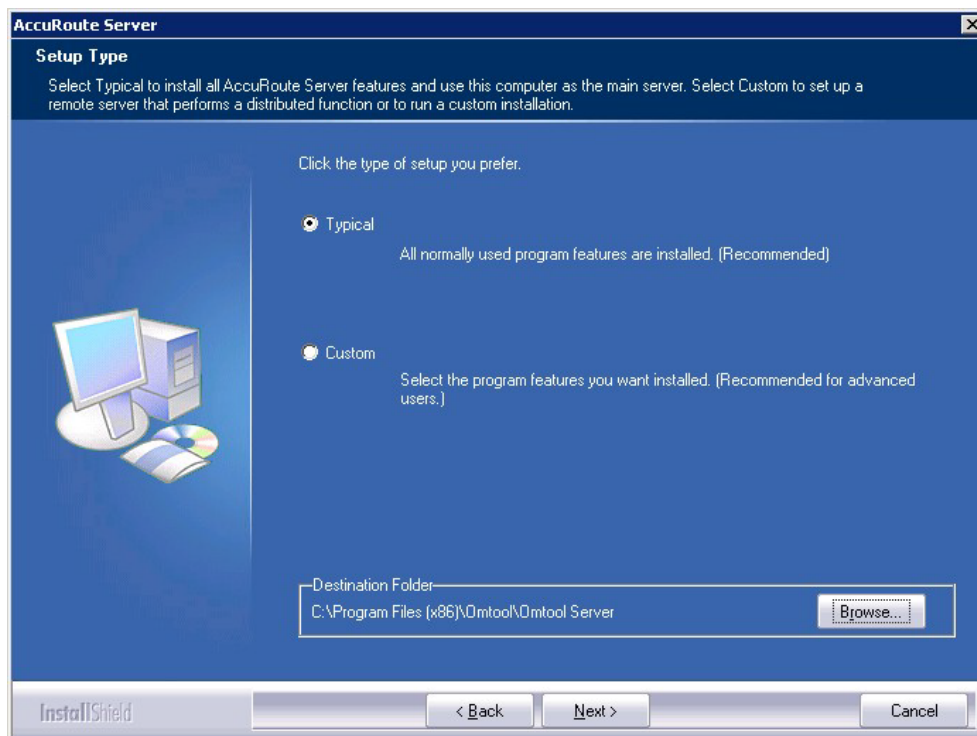
- 5 Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



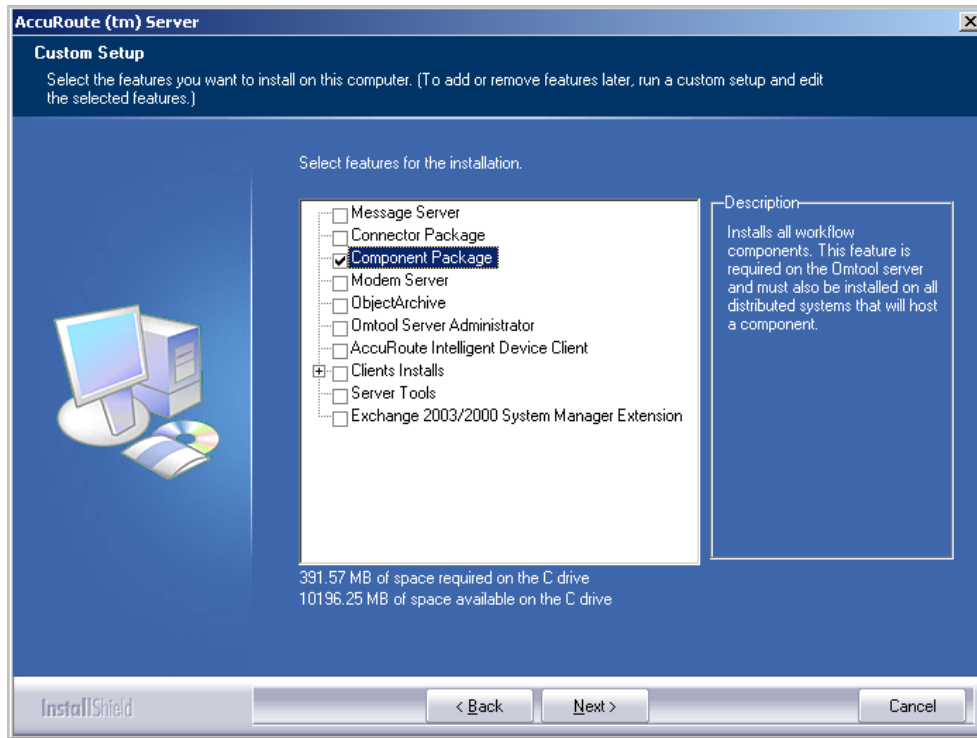
6 Select **I accept the terms of the license agreement**.



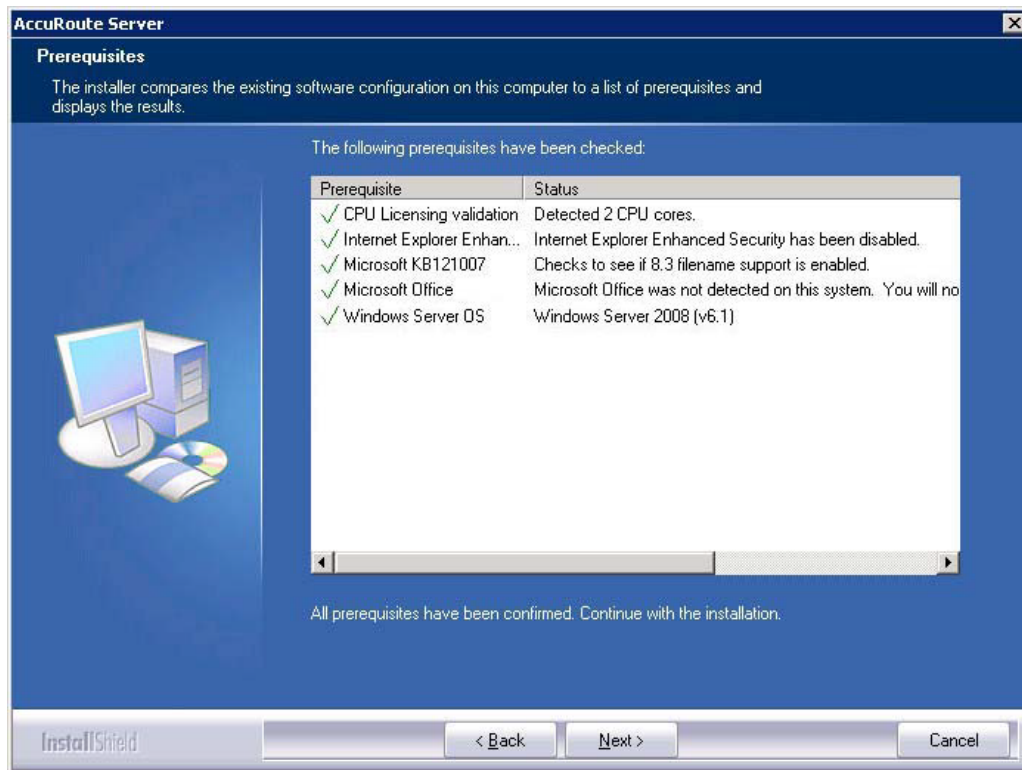
7 Click **Next**. The **Setup Type** options are displayed.



- 8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.
- 9 Select **Component Package**, clear all the other features you are not installing at this time.



- 10 Click **Next**. The setup checks the system for installation requirements and displays the results.



Note The setup cannot continue until all required components are installed. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

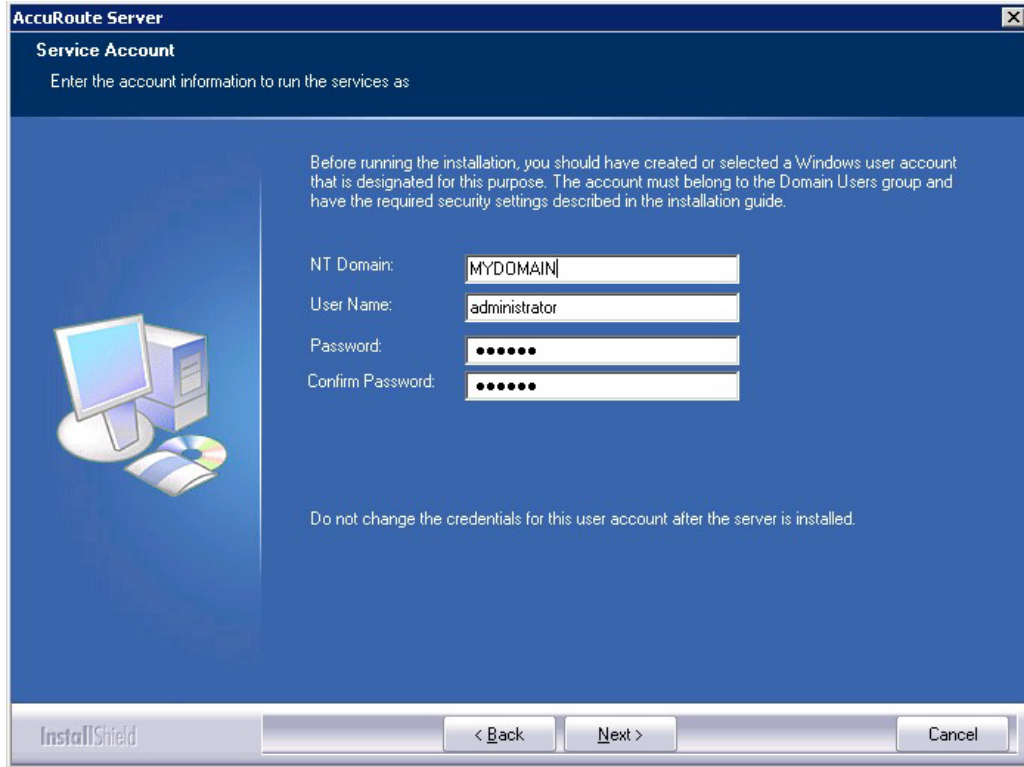
- 11 Click **Next** to continue the installation.

The setup requests logon credentials for the Omtool service account. The **NT Domain** and **User Name** fields are populated automatically based on the current Windows user.

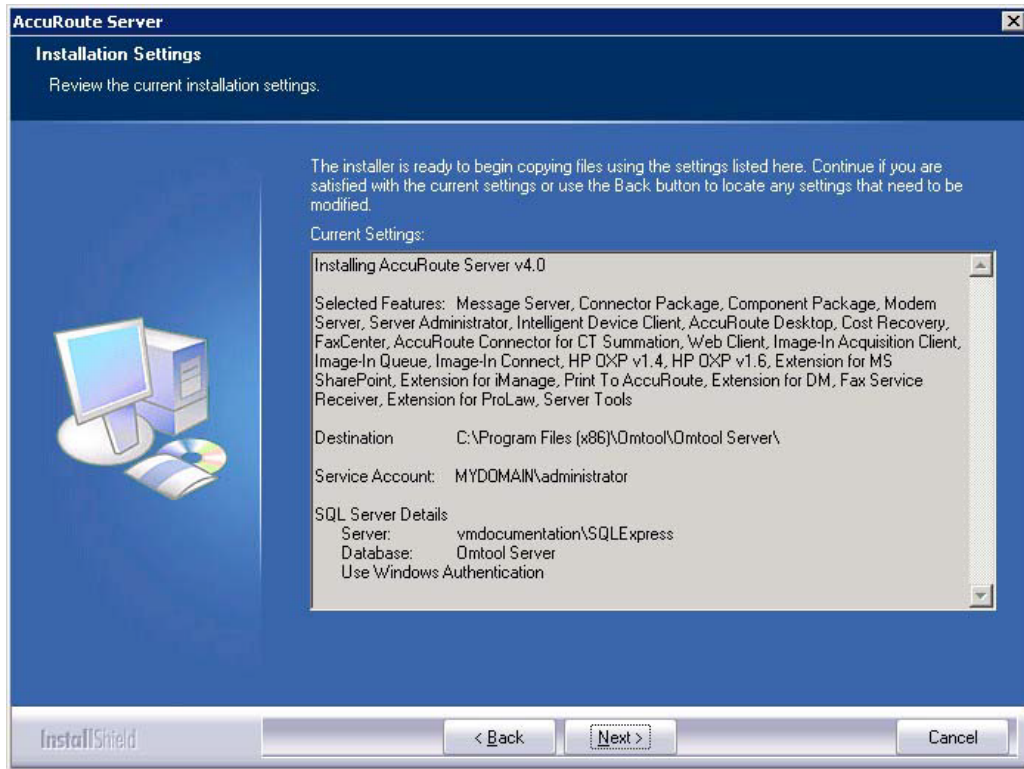
- 12 Enter the logon credentials of the Omtool service account.

- a In the **NT Domain** field, enter the name of the Windows domain.
- b In the **User Name** field, enter the user name.
- c In the **Password** and **Confirm Password** fields, enter the password for the user.

Section 14: Installing Remote Embedded Directive Manager

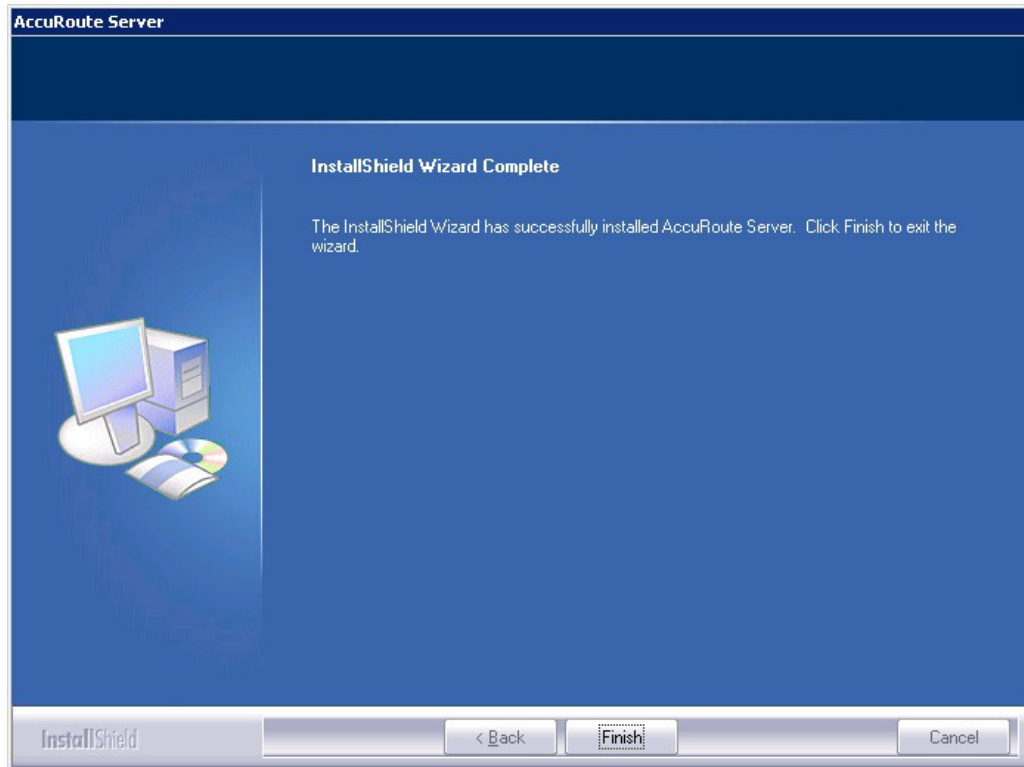


13 Click **Next**. The setup validates the user account and then shows installation settings.



Note If other installation features are included, the setup might request additional information before displaying installation settings.

- 14 Review the installation settings and click **Next** to start the installation. The setup installs the selected component and displays a message indicating that the installation is complete.



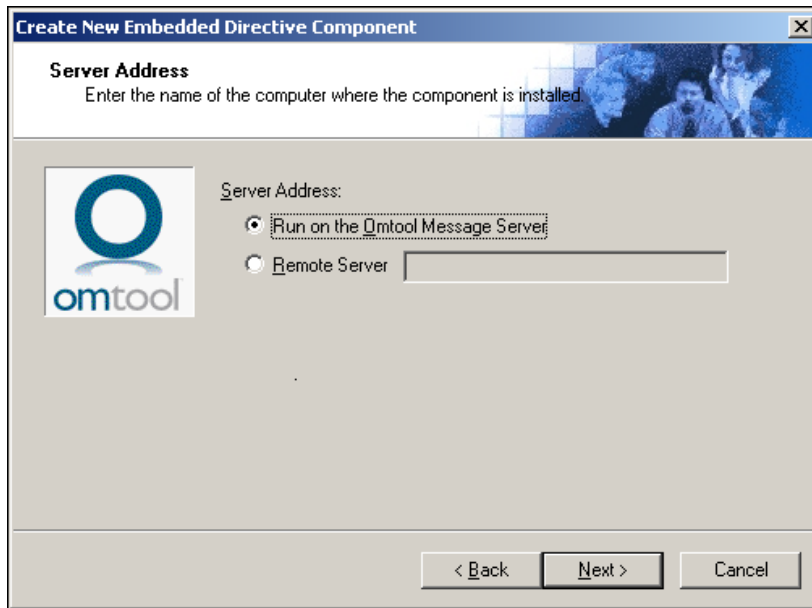
- 15 Click **Finish**.

Now that Remote Embedded Directive Manager is installed on the remote system, add the new Embedded Directive Manager component to the AccuRoute server. Continue to [Adding Remote Embedded Directive Manager to the AccuRoute server](#).

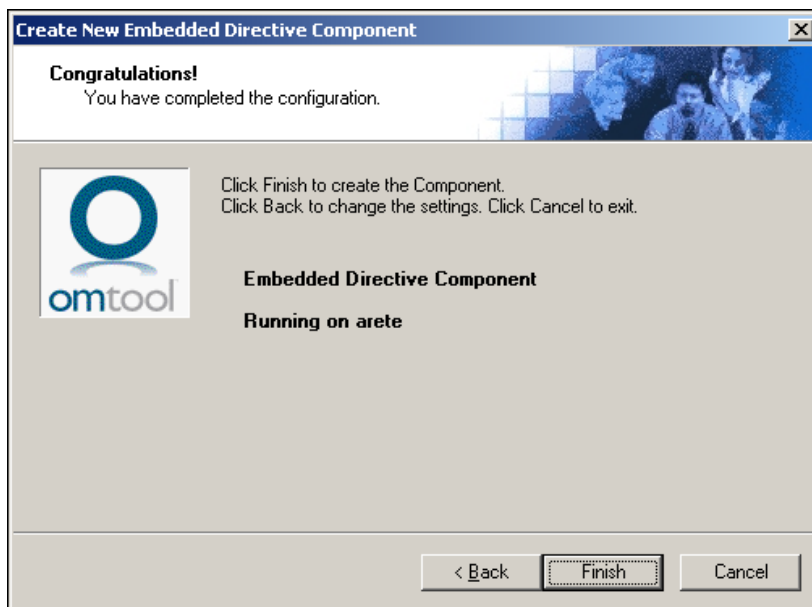
Adding Remote Embedded Directive Manager to the AccuRoute server

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **Components**.
- 3 Select **New > Embedded Directive Manager Component**.

The wizard opens the Server Address page.



- 4 Select **Remote Server** option and enter the computer name or IP address of the system running Remote Embedded Directive Manager.
- 5 Click **Next**. The wizard verifies that Remote Embedded Directive Manager is installed and displays a message indicating that the configuration is complete.



- 6 Click **Finish**. The wizard adds the component to the components list in the details pane.
- 7 Restart the Component Manager service on the AccuRoute server.
- 8 If removing the local instance of Embedded Directive Manager from the AccuRoute server, continue to [Removing Embedded Directive Manager from the AccuRoute server or a remote system](#).

Removing Embedded Directive Manager from the AccuRoute server or a remote system

Note Embedded Directive Manager on the AccuRoute server can be removed only if a Remote Embedded Directive Manager exists.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Components**.
- 3 Right-click the **Embedded Directive Manager** you want to remove and select **Delete** from the drop down menu options.
You are prompted to confirm that you want to delete the selection.
- 4 Click **Yes** to continue. The component is removed from the list.
- 5 Restart the Component Manager service on the AccuRoute server.

Section 15: Installing Remote AccuRoute Connector for DMS libraries

This section includes:

[Introduction to Remote AccuRoute connector for DMS libraries](#) (15-1)

[Requirements for Remote AccuRoute connector for DMS libraries](#) (15-2)

[Installing Remote AccuRoute connector for DMS libraries](#) (15-2)

[Adding Remote AccuRoute connector for DMS libraries to the AccuRoute server](#) (15-9)

[Removing Remote AccuRoute connector for DMS libraries](#) (15-12)

Introduction to Remote AccuRoute connector for DMS libraries

The AccuRoute connector for DMS libraries routes documents from the server to your company document management system (DMS).

When routing an inbound document, the AccuRoute connector for DMS libraries creates a document ID and a pending document in the DMS. When the actual document arrives at the destination DMS server, the AccuRoute connector for DMS libraries locates the placeholder and replaces it with the actual document.

After installing the AccuRoute server, you can create an AccuRoute connector for DMS libraries locally. The AccuRoute connector for DMS libraries that is installed on a remote system is called **Remote AccuRoute Connector for DMS Libraries**.

When scaling an environment with additional connectors or components, always consult an AccuRoute Technical Support engineer. For information, contact [Upland AccuRoute Service and Support](#). The AccuRoute Technical Support engineer can assist you in correctly identifying potential bottlenecks in the system based on workload and other factors. Moreover, the Support engineer can provide helpful information on the overall impact of increasing the speed and efficiency of the system. Performance and stability consulting are also available for a fee.

To purchase additional AccuRoute connector for DMS libraries licenses, contact an Upland AccuRoute Sales representative. If a detailed analysis of the environment is necessary, the AccuRoute Technical Support engineer may recommend a fee-based consultation.

Requirements for Remote AccuRoute connector for DMS libraries

Hardware and software requirements

Remote AccuRoute connector for DMS libraries requires a system that meets the following minimum requirements:

- Windows NT domain computer that always runs in the same domain as the AccuRoute server
- Dual core processor
 - 2 GHz
 - 4GB of RAM
 - RAID 5W with 100 GB of disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit, Windows 2008 R2 64-bit
- DMS client application. The client application must be installed on the system where you are installing the remote DMS client.

Additional requirements

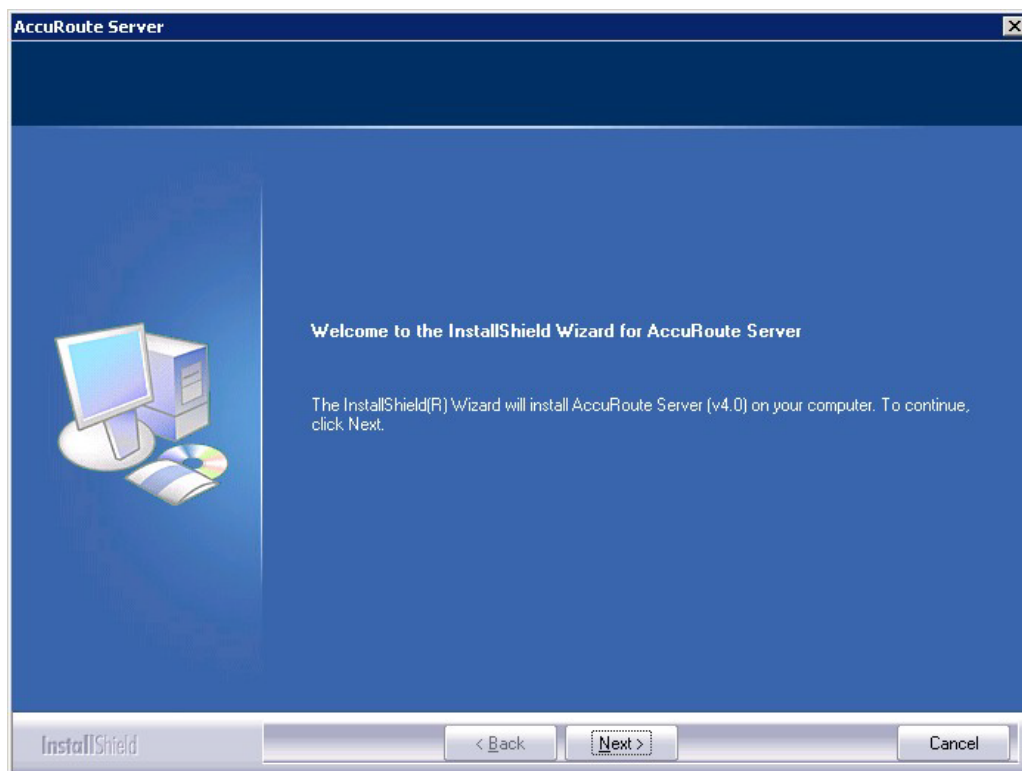
Remote AccuRoute connector for DMS libraries installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group
- Purchased license key for Remote AccuRoute connector for DMS
Contact [Upland AccuRoute Service and Support](#) for more information.

Installing Remote AccuRoute connector for DMS libraries

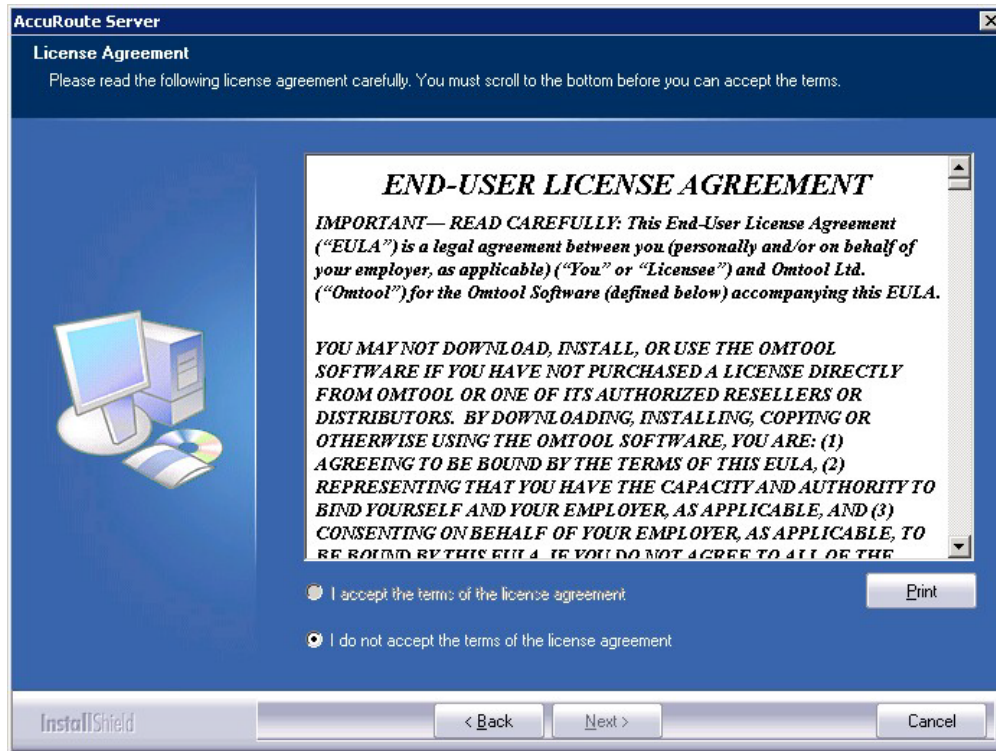
- 1 Log in to the system where you will install the Remote AccuRoute connector for DMS libraries using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network where you have kept the AccuRoute server setup files.
- 3 Run **\MessageServer\setup.exe**.

The InstallShield wizard opens and configures your system for installation and displays a welcome message.

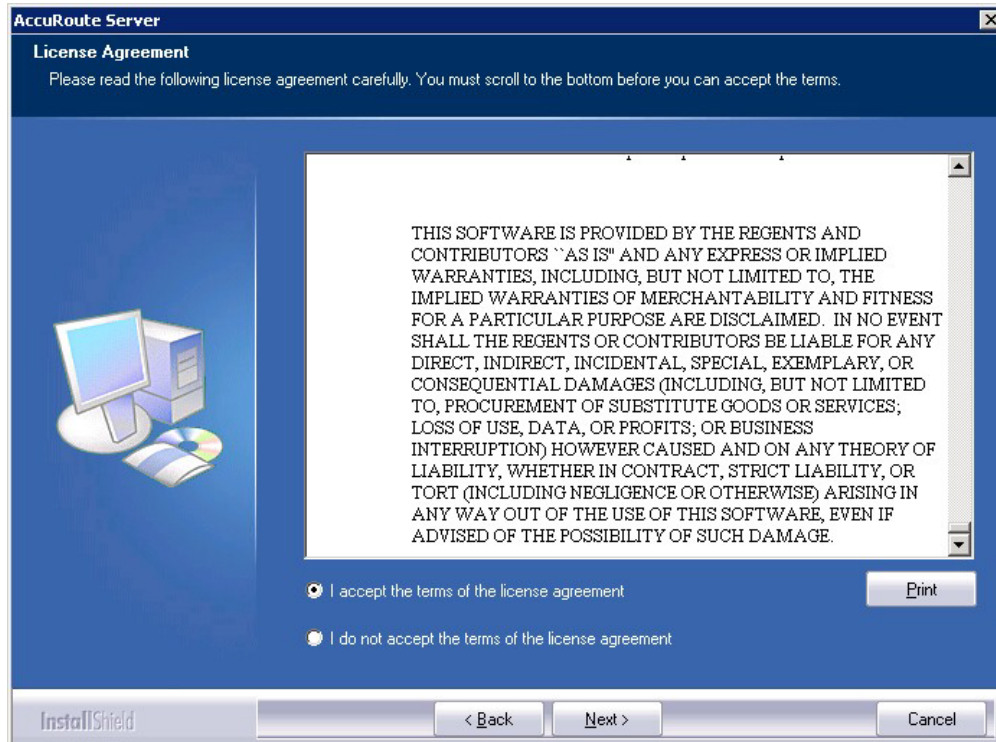


- 4 Click **Next**. The setup shows the **License Agreement** page.

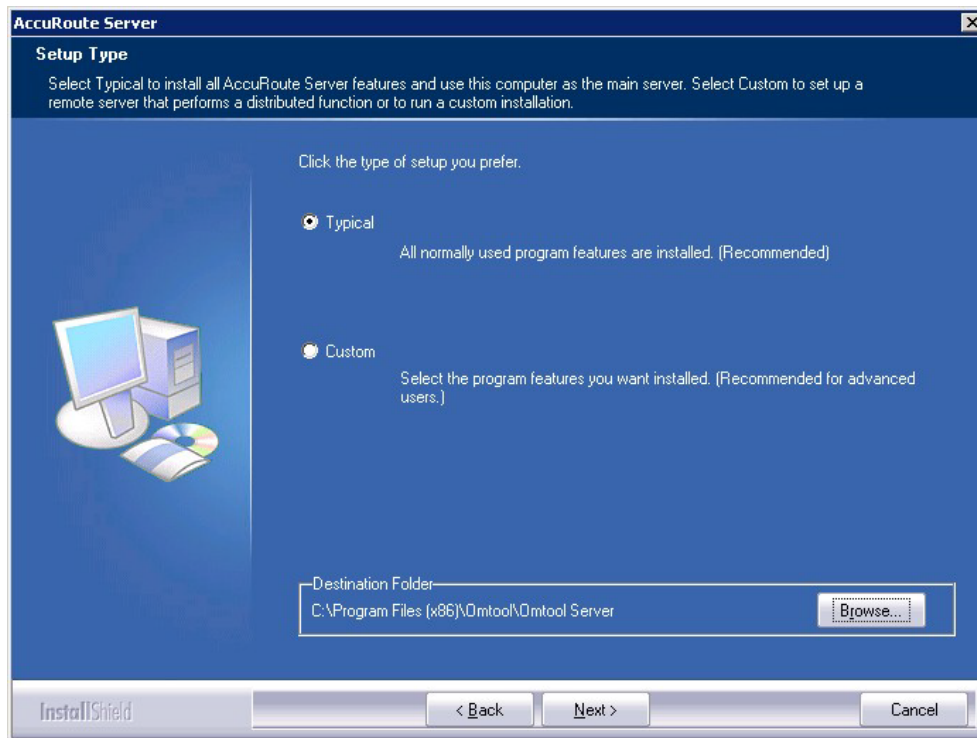
- Review the License Agreement. Note that you must scroll to the bottom of the Agreement before you can accept the terms.



- Select **I accept the terms of the license agreement**.

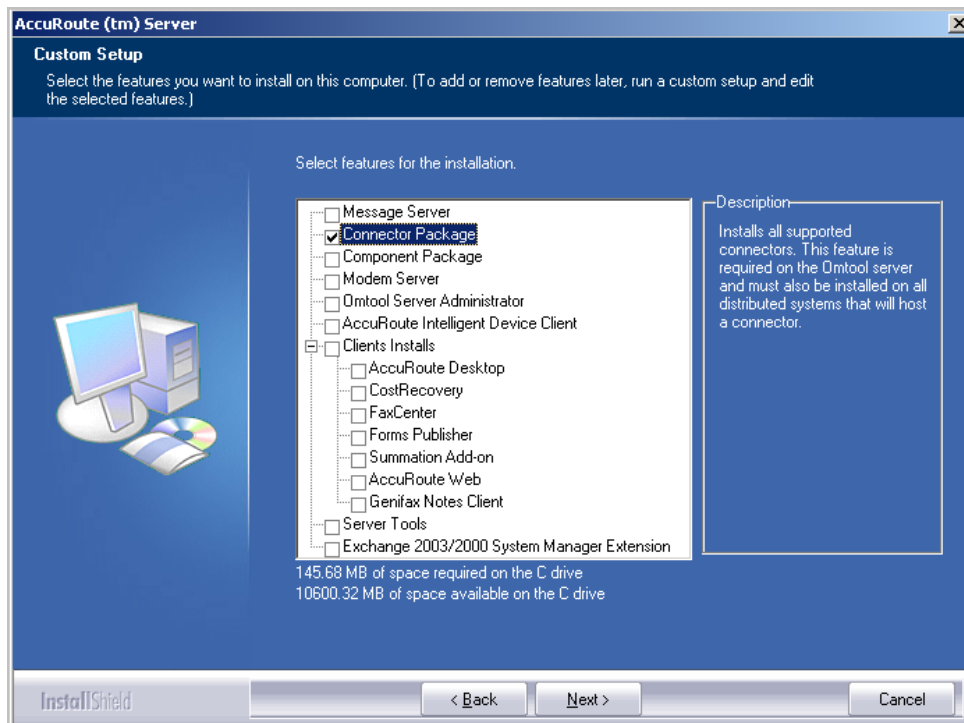


7 Click **Next**. The **Setup Type** options are displayed.

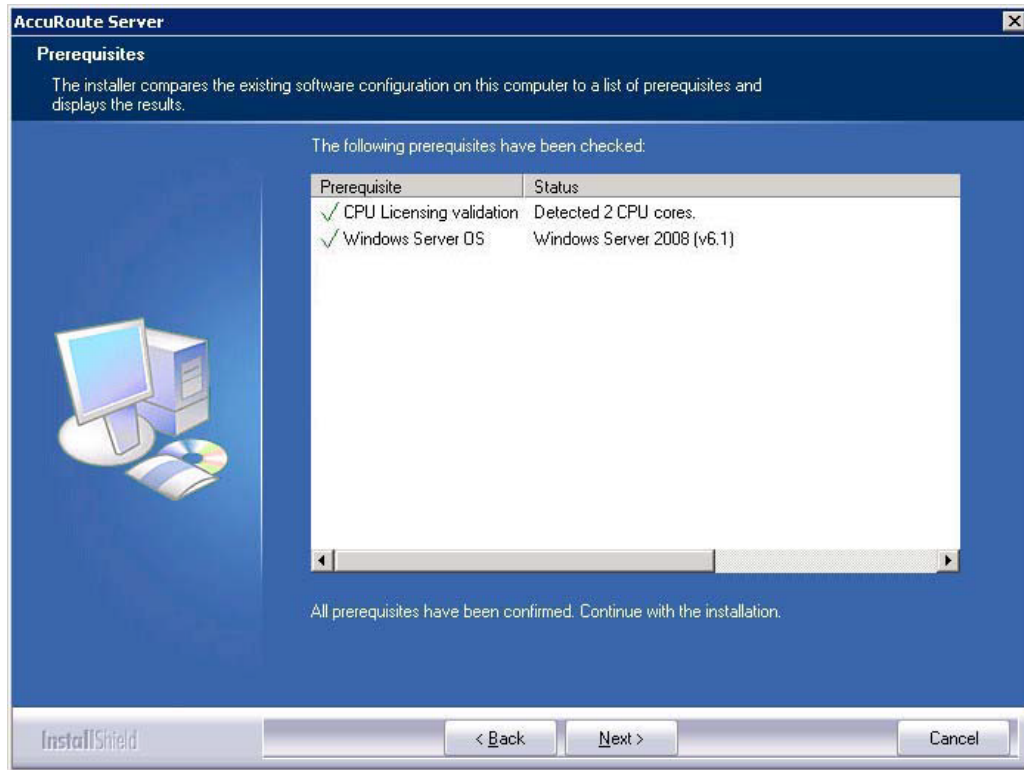


8 Select **Custom** and click **Next**. The setup shows a list of AccuRoute features.

9 Select **Connector Package**, clear all the other features you are not installing at this time.

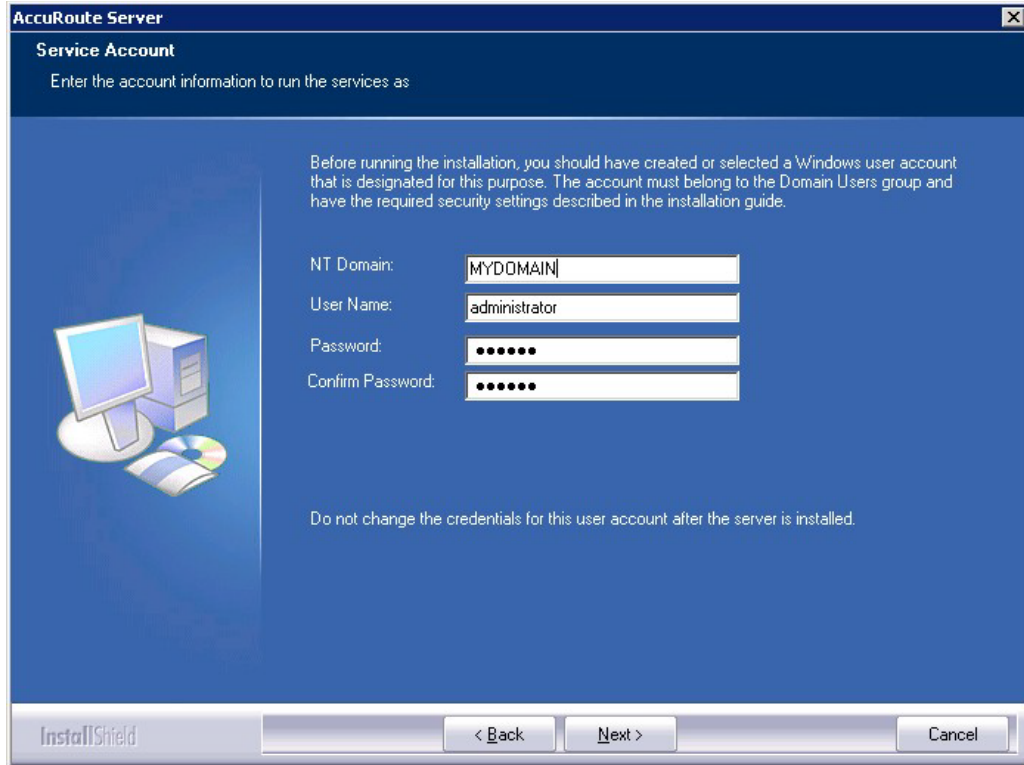


- 10** Click **Next**. The setup checks the system for installation requirements and displays the results.

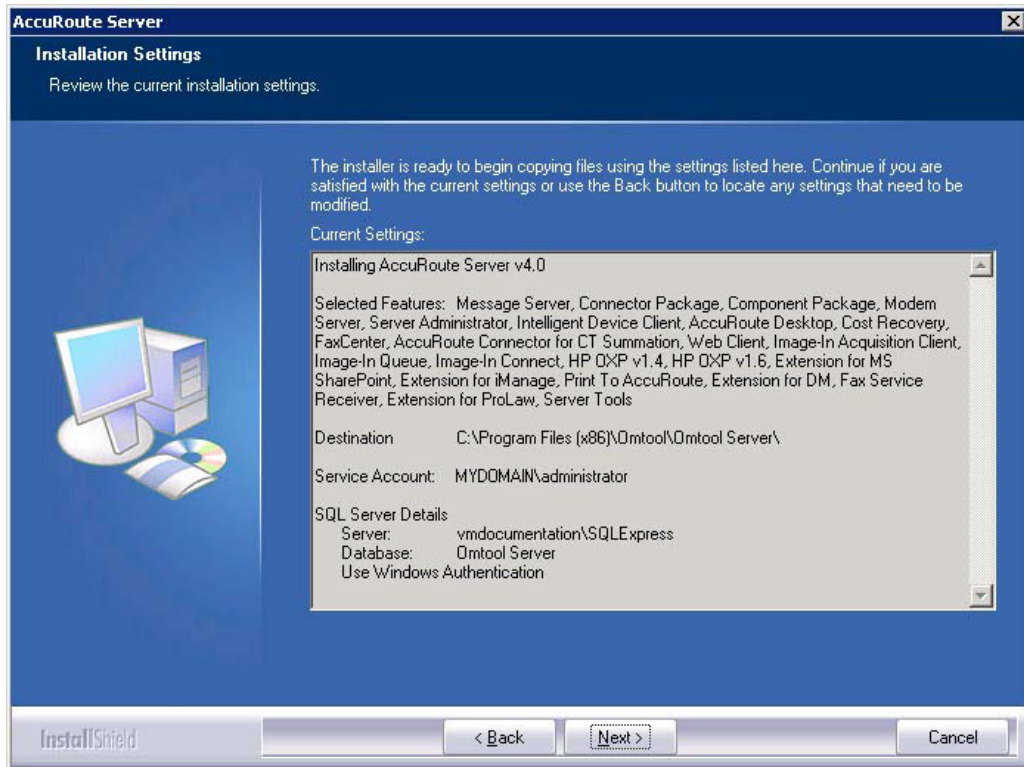


Note The setup cannot continue until all requirements are installed and configured. (Double-click an item in the list for more information.) If any required components were not detected, click **Cancel** and click **Yes** to exit the setup and install the components that are required to complete the installation.

- 11** Click **Next** to continue the installation. The setup requests logon credentials for the Omtool service account. The **NT Domain** and **User Name** fields are populated automatically based on the current Windows user.
- 12** Enter the logon credentials of the Omtool service account.
- In the **NT Domain** text box, enter the name of the Windows domain.
 - In the **User Name** text box, enter the user name.
 - In the **Password** and **Confirm Password** text boxes, enter the password for the user.

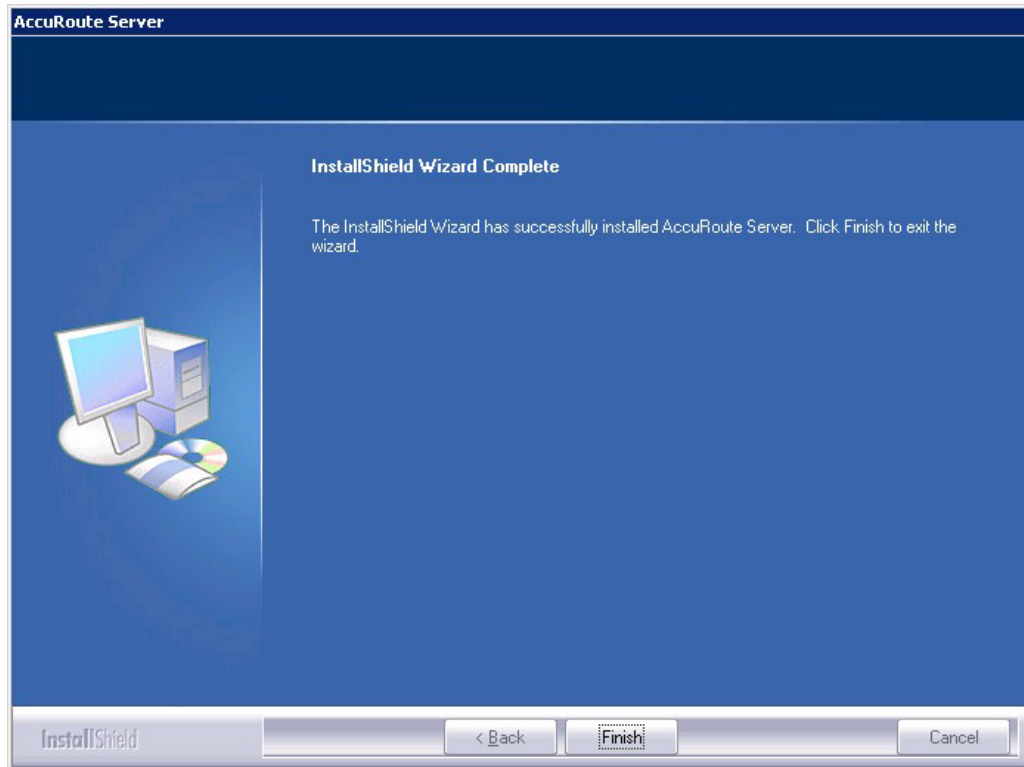


13 Click **Next**. The setup validates the user account and then shows installation settings.



Note If other installation features are included, the setup might request additional information before displaying installation settings.

- 14 Review the installation settings and click **Next** to start the installation. The setup installs the selected component and displays a message indicating that the installation is complete.



- 15 Click **Finish**.

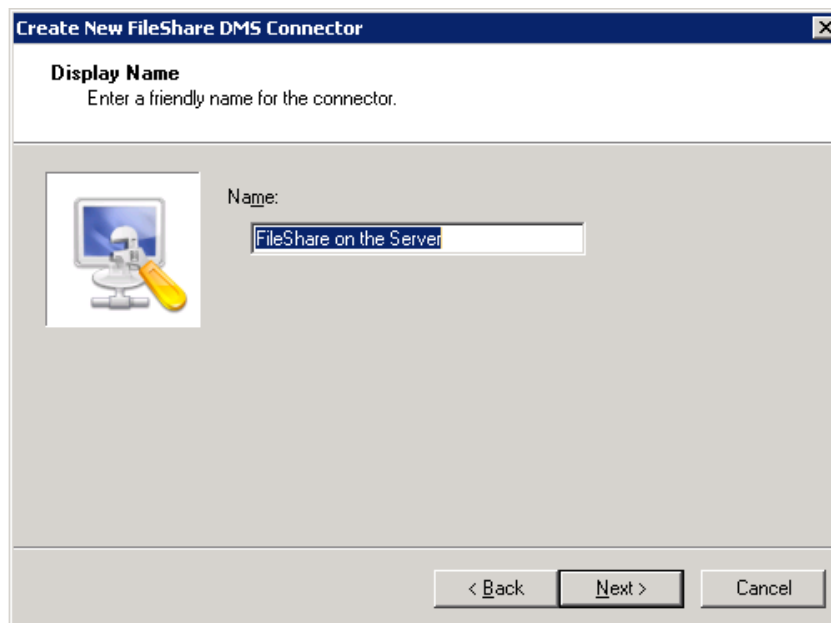
Now that Remote AccuRoute connector for DMS libraries is installed on the remote system, add the new AccuRoute connector for DMS libraries to the AccuRoute server. Continue to [Adding Remote AccuRoute connector for DMS libraries to the AccuRoute server](#).

Adding Remote AccuRoute connector for DMS libraries to the AccuRoute server

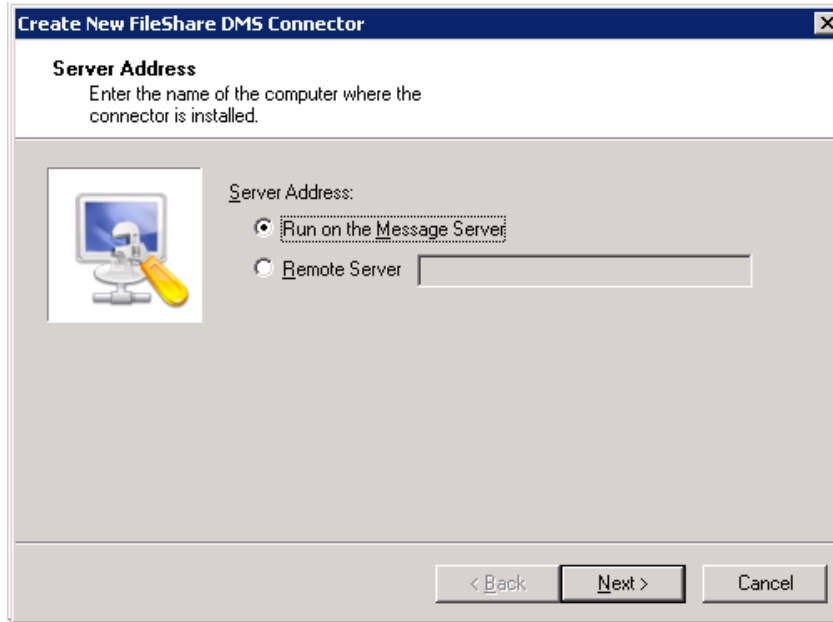
Note The DMS connector license must be added to the server prior to adding the connector. The AccuRoute server makes one connector available by default. Check the licensing properties on your server for connector availability.

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and right-click **Connector**.
- 3 Select **New > AccuRoute Connector for > [select the DMS]**. The **Display Name** page appears.

For example, if you selected **FileShare**, the display name appears, by default, as **FileShare on the Server**.



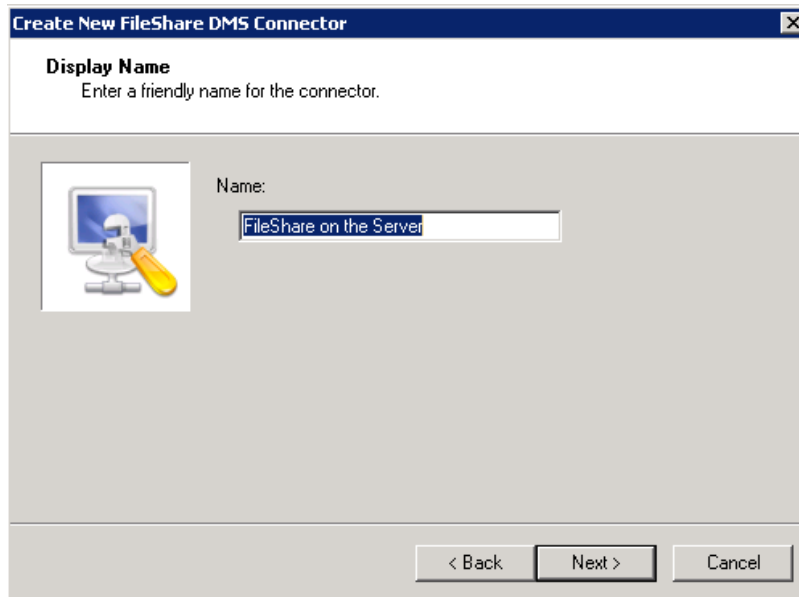
- 4 You can use the default name or type a friendly name for this connector in the **Name** text box. Click **Next** and the **Server Address** page appears.



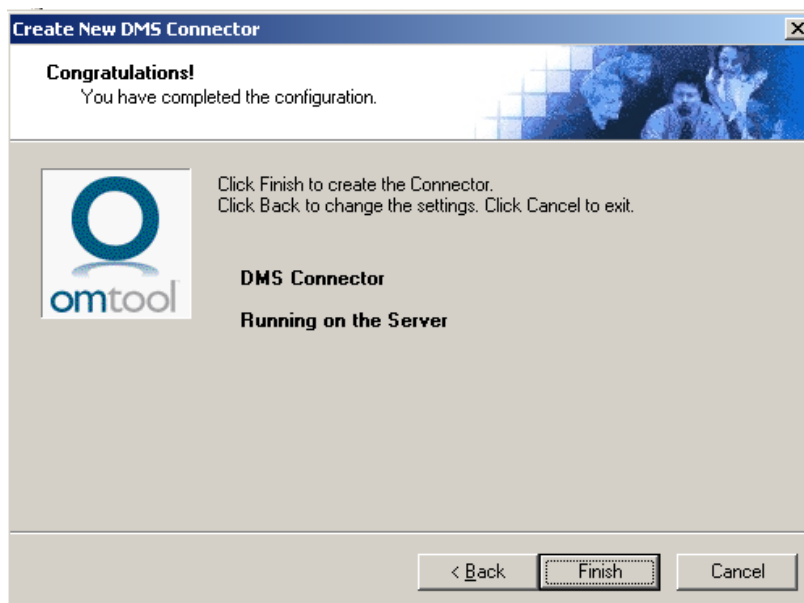
- 5 Select the server address to which you want this connector installed. Choose **Run on the Message Server** or **Remote Server**. If you selected **Remote Server**, enter the name of the server. Click **Next** and the **Congratulations** page appears.
- 6 Click **Finish**.

The DMS configuration wizard launches and prompts you to configure the connector to support the DMS.

- 7 Click **Next**. The wizard verifies that Remote AccuRoute connector for DMS libraries exists and opens the **Display Name** page.



- 8 In the **Name** text box, enter the name of the connector. The default is **DMS on the Server**. If you are adding multiple connectors, enter a unique name for the connector.
- 9 Click **Next**. You see the configuration complete message.



- 10 Click **Finish**. The DMS Configuration wizard opens.
- 11 Configure as necessary. When configuration is complete, the connector is added to the connector's list in the details pane.
- 12 Restart the AccuRoute Connector Manager service on the AccuRoute server.

Removing Remote AccuRoute connector for DMS libraries

- 1 Click **Start > All Programs > Omtool > AccuRoute Server > AccuRoute Server Administrator**.
- 2 In the console tree, expand the AccuRoute Server Administrator and click **Connector**.
- 3 Right-click the **AccuRoute Connector for DMS Libraries** that you want to remove and select **Delete** from the drop down menu options.

You are prompted to confirm that you want to delete the selection.

- 4 Click **Yes** to continue. The connector is removed from the list.
- 5 Restart the AccuRoute Connector Manager service on the AccuRoute server.

Section 16: AccuRoute Intelligent Device Client

This section includes:

[Introduction to AccuRoute Intelligent Device Client](#) (16-1)

[Optional configurations](#) (16-4)

[Testing and troubleshooting AccuRoute Intelligent Device Client](#) (16-6)

[Installing AccuRoute Intelligent Device Client on a remote system](#) (16-8)

[Configuring the remote AccuRoute Intelligent Device Client](#) (16-14)

[Removing remote AccuRoute Intelligent Device Client](#) (16-17)

Introduction to AccuRoute Intelligent Device Client

The AccuRoute Intelligent Device Client (formerly known as the Embedded AccuRoute for Intelligent Devices) is a request handler for AccuRoute client applications. It comprises of a group of IIS web server extensions providing a layer for communication between the clients and the AccuRoute server. For example, it allows a client like Ricoh Embedded Software Architecture (ESA) Device Client, to submit messages to the AccuRoute server. It also allows the clients to retrieve information about Distribution Rules from the server.

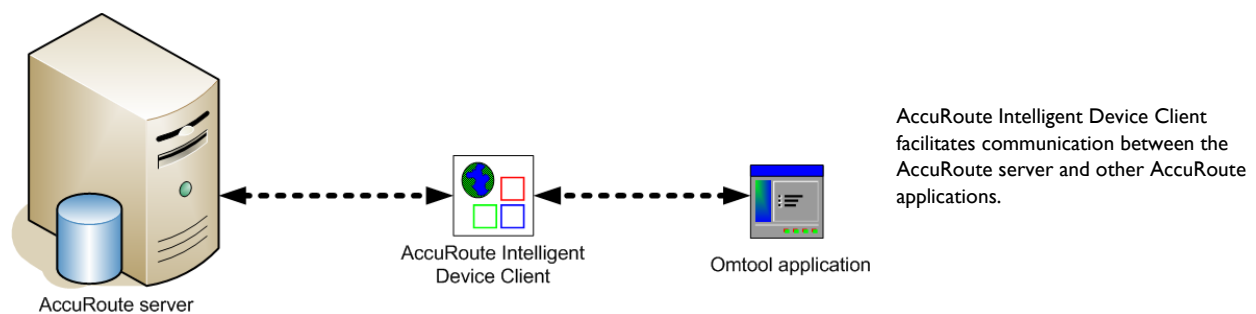


Figure 16-1: The AccuRoute Intelligent Device Client environment

Note AccuRoute v2.3 and all later versions install the AccuRoute Intelligent Device client by default. No separate installation is necessary. You must configure the client and test it using instructions in this chapter.

If necessary, you can install the client on a remote system. For instructions, see [Installing AccuRoute Intelligent Device Client on a remote system](#) (16-8).

AccuRoute Intelligent Device Client components

The AccuRoute Intelligent Device Client helps the following client applications communicate with the AccuRoute server.

- AccuRoute Desktop
- Embedded AccuRoute application like Embedded AccuRoute for HP and Embedded AccuRoute for Ricoh.

The AccuRoute Intelligent Device Client manages AccuRoute Desktop and the Embedded AccuRoute clients separately. Each category utilizes a unique web server extension, application pool, virtual directory and location.

The main components of the AccuRoute Intelligent Device Client environment are detailed in the following table.

Table 16-1: Description of web server components with location and function

| Component | Location | Function |
|---------------|--|--|
| DesktopWebAPI | \\Omtool\OmtoolServer\WebAPI\DesktopWebAPI | This folder is utilized for messages coming from AccuRoute Desktop. AccuRoute Desktop submits messages to ...\\DesktopWebAPI\FileTransfer. The messages are processed by OmlSAPIU.DLL, other supporting DLL files, and XML-based configuration files in ...\\DesktopWebAPI\Scripts. |
| WebAPI | \\Omtool\Omtool Server\WebAPI\WebAPI | This folder is utilized for Embedded AccuRoute Intelligent devices. <ul style="list-style-type: none"> • Applications like Embedded AccuRoute for Ricoh submit messages to ...\\WebAPI\FilePostings. • Applications like Embedded AccuRoute for HP OXP, Embedded AccuRoute for Xerox EIP submit messages to ...\\WebAPI\FileTransfer The messages are processed by OmlSAPIU.DLL, other supporting DLL files, and XML-based configuration files in ...\\WebAPI\Scripts. |

IIS implementation

Web server extensions and application pools

During installation, the AccuRoute Intelligent Device Client creates and modifies web server extensions. It also creates the application pools.

The installation setup:

- Checks the status of the web server extension **WebDAV**. If it is not allowed to run, the setup changes its status to **Allowed**.

Note WebDAV must be allowed to run; this is a requirement of AccuRoute Intelligent Device Client.

- Creates the web server extension **DesktopWebAPI** for AccuRoute Desktop and sets its status to **Allowed**.
- Creates the web server extension **WebAPI** for Embedded AccuRoute applications and sets its status to **Allowed**.

- Creates the application pool **DesktopWebAPI** for AccuRoute Desktop.
- Creates the application pool **WebAPI** for Embedded AccuRoute applications.

Dependencies

AccuRoute Intelligent Device Client runs under the World Wide Web Publishing Service in IIS 7.0, and has dependencies on the following web server extensions:

- WebDAV (WebDAV, or Web-based Distributed Authoring and Versioning, is a set of HTTP extensions that enables multiple users to edit and manage files on remote web servers.)
- DesktopWebAPI
- WebAPI

Important The status of these web server extensions must be set to **Allowed** at all times.

IIS integration

AccuRoute Intelligent Device Client has a dual implementation — one for AccuRoute Desktop, and another for Embedded AccuRoute applications. Each has a unique web server extension, application pool, virtual directory, and location so that each implementation can be managed separately.

Table 16-2: IIS implementation for AccuRoute Intelligent Device Client

| Function | Web server extension | Application pool | Virtual directory | Disk location |
|--|--|-----------------------------------|---------------------------------|--------------------------------------|
| Enabling HTTP or Secure HTTP connection between AccuRoute Desktop and the AccuRoute server | “DesktopWebAPI” represents ...\\Omtool\Omtool Server\WebAPI\DesktopWebAPI\Scripts\OmlSAPIU.DLL | Application Pools/ DesktopWebAPI/ | Default Web Site/ DesktopWebAPI | \\Omtool\Omtool Server\DesktopWebAPI |
| Allowing Embedded AccuRoute applications on multifunction devices to connect to the AccuRoute server | “WebAPI” represents ...\\Omtool\Omtool Server\WebAPI\WebAPI\Scripts\OmlSAPIU.DLL | Application Pools/ WebAPI/ | Default Web Site/ WebAPI | \\Omtool\Omtool Server\WebAPI |

For more information on IIS web server extensions, application pools, and virtual directories, consult the Windows documentation on IIS.

Message submission failures

AccuRoute Intelligent Device Client submits messages from an AccuRoute client application to the AccuRoute server. Each application that requires AccuRoute Intelligent Device Client, handles submission failures differently. For more information on how submission failures are handled, consult the appropriate client documentation, which is available on the [AccuRoute v6.0 documentation](#) page.

Optional configurations

[Configuring HTTPs connectivity for AccuRoute Desktop](#) (16-4)

[Modifying the directory security configuration of virtual directories](#) (16-5)

Configuring HTTPs connectivity for AccuRoute Desktop

When AccuRoute Desktop must be able to connect to AccuRoute Intelligent Device Client using Secure HTTP connectivity, additional configuration is required. Set the FileTransfer property for AccuRoute Intelligent Device Client to HTTPS, and then test the secure connection.

Setting the FileTransfer property to HTTPS

AccuRoute Intelligent Device Client has a FileTransfer property for AccuRoute Desktop that defines the file transfer protocol used between clients and the web server. By default, the property is set to HTTP. To use Secure HTTP connectivity, set the FileTransfer property to HTTPS.

To set the FileTransfer property to HTTPS:

- 1 Go to:
`...\Omtool\Omtool Server\WebAPI\DesktopWebAPI\Scripts`
Open `OmISAPIU.xml` in Notepad.
- 2 Locate the **FileTransfer** property and set the protocol type to `https`, for example,
`<FileTransfer>https://172.16.10.48/DesktopWebAPI/FileTransfer/</FileTransfer>`.
Verify that the URL includes the IP address of the web server running AccuRoute Intelligent Device Client. The computer name is not supported.
- 3 Save and close the file.

Testing the secure connection

Test the connection to the web server and verify that AccuRoute Intelligent Device Client accepts secure requests only. Run this test from any system in the LAN running AccuRoute server or client software. (Before this test can be run, a certificate must be installed on the Default Web Site and SSL must be enabled. Go to [Appendix B: Configuration for HTTPS Support](#).)

To test the secure connection:

- 1 Start the browser and go to:
`http://[web server]/DesktopWebAPI/Scripts/OmISAPIU.dll?Action=GetConfiguration`
where `[web server]` represents the host name or IP address of the web server.

Note The Action command in the URL is case-sensitive.

The browser displays an error indicating that the page must be viewed over a secure channel.

- 2 Go to the address bar and change `http` to `https`, and press **Enter**. The browser loads the requested page.

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

AccuRoute Intelligent Device Client is configured to use Secure HTTP connectivity with AccuRoute Desktop. The AccuRoute Intelligent Device Client installation is complete.

Tip The default directory security configuration can be modified if it does not comply with the security policy in the LAN. Go to [Modifying the directory security configuration of virtual directories](#) on 16-5.

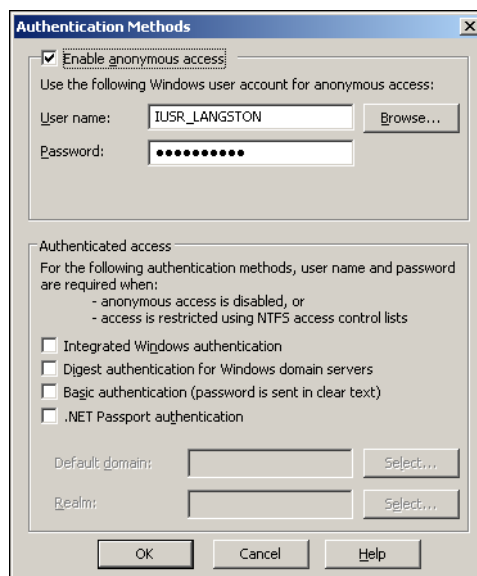
Modifying the directory security configuration of virtual directories

The virtual directories created by the AccuRoute Intelligent Device Client setup grant the following access:

- authenticated access via integrated Windows authentication.

The default authentication and access control configuration can be modified if it does not comply with the security policy in the LAN. AccuRoute Intelligent Device Client supports all IIS authentication methods except .NET Passport and Digest Authentication for Windows Domain server, and also supports IP address and domain name restrictions.

Note After AccuRoute Intelligent Device Client is installed, the virtual directory properties are set to allow read access, allow execute permissions on scripts and executable, and use its associated application pool (DesktopWebAPI or WebAPI). Do not modify these settings.



After AccuRoute Intelligent Device Client is installed, the authentication and access control configuration for the virtual directory enables anonymous access with the local IUSR account or the account specified during installation and enables integrated Windows authentication.

Figure 16-2: Default authentication and access control configuration for a virtual directory

A modified configuration must meet the following conditions:

- If anonymous access is enabled, the account used for anonymous access must have full control to read and write to the folder. These permissions are configured in the Windows security settings on the folder.

- If integrated Windows authentication is enabled, all accounts used to post and download files, and gain access to the OmISAPIU.DLL resource, must have full control to read and write to the folder. These permissions are configured in the Windows security settings on the folder. For information on accounts that are used to post and download files, and gain access to the OmISAPIU.DLL resource, consult the AccuRoute documentation (available on the [AccuRoute v6.0 documentation](#) page) for the application being used in conjunction with AccuRoute Intelligent Device Client.

Testing and troubleshooting AccuRoute Intelligent Device Client

AccuRoute Desktop or an embedded AccuRoute application must be able to access the AccuRoute Intelligent Device Client configuration file OmISAPIU.DLL. Test the connection to the web server and verify that AccuRoute Intelligent Device Client is installed and configured correctly.

Test connectivity to AccuRoute Intelligent Device Client

Run this test from any system in the LAN that is running AccuRoute server or client software.

- 1 Log in to any system in the LAN running AccuRoute server or client software.
- 2 Start the browser and go to:
[https://\[web server\]/\[virtual directory\]/Scripts/OmISAPIU.dll?Action=GetConfiguration](https://[web server]/[virtual directory]/Scripts/OmISAPIU.dll?Action=GetConfiguration)

where [web server] represents the host name or IP address of the web server and [virtual directory] represents the name of the virtual directory in IIS that is accessed by AccuRoute Desktop or Embedded AccuRoute applications.

Tip A connection to AccuRoute Intelligent Device Client from a client running AccuRoute Desktop looks similar to: <http://goliath/DesktopWebAPI/Scripts/OmISAPIU.dll?Action=GetConfiguration>

A connection to AccuRoute Intelligent Device Client from a device running an Embedded AccuRoute application looks similar to: <http://goliath/WebAPI/Scripts/OmISAPIU.dll?Action=GetConfiguration>

When constructing the URL, consider the following:

- ▶ The Action command in the URL is case-sensitive.
- ▶ If Secure HTTP connectivity is configured for AccuRoute Desktop, replace HTTP with HTTPS.

The browser displays the basic configuration for the AccuRoute Intelligent Device Client.

```
<?xml version="1.0" ?>
- <Omtool>
- <Product>
  <Name>Omtool ISAPI Services</Name>
  <Version>1.0</Version>
  <Build>1</Build>
  <Description>Provides a bridge between the Xlet and Server</Description>
</Product>
- <Servers>
- <Server Name="ServicesServer">
  <PostPath>WebAPI/FilePostings/</PostPath>
  <FileTransfer>http://172.16.20.48/WebAPI/FileTransfer/</FileTransfer>
</Server>
- <Server Name="OmtoolServer">
  <ServerName>FISH40</ServerName>
</Server>
</Servers>
</Omtool>
```

If an error occurs, troubleshoot the web server ([Troubleshoot connectivity issues](#), 16-7) and repeat the test until it is successful.

Troubleshoot connectivity issues

Use the following table to identify and resolve connectivity issues.

Table 16-3: Possible causes of connectivity issues with resolutions

| Issue description | Resolution |
|--|--|
| No connectivity to server. | A networking issue might be preventing access to the server. Ping the web server. If this test is successful but the connectivity issue remains, continue to the next issue. |
| World Wide Web service is stopped or disabled. | Open the Services applet on the web server and check the status of the World Wide Web service. If the service is stopped, verify that the service is enabled and then start it. Verify that the service is running before closing the Services applet. If the connectivity issue remains, continue to the next issue. |
| The Default Web Site is stopped in IIS. | Start IIS and expand the web server where AccuRoute Intelligent Device Client is installed. Expand the items in the console tree so that Default Web Site is visible. If the node is labeled Default Web Site (Stopped) , right-click the node and select Start . If the connectivity issue remains, continue to the next issue. |

Table 16-3: Possible causes of connectivity issues with resolutions

| Issue description | Resolution |
|---|--|
| The IIS application pool for AccuRoute Intelligent Device Client is disabled. | Start IIS and go to [web server]>Application Pools>[application pool]. Right-click the appropriate application pool and select Start . If the connectivity issue remains, continue to the next issue. |
| Execute permissions on the Scripts directory are inadequate. | Start IIS and go to [web server]>Default Web Site>[virtual directory]>Scripts. Right-click Scripts and select Properties . IIS displays the Directory properties. Go to Application Settings and verify that Execute Permissions is set to Scripts and Executables . If the connectivity issue remains, check the Knowledge Base for technical articles that are helpful in troubleshooting the web server, and then contact Upland AccuRoute Service and Support . |

Installing AccuRoute Intelligent Device Client on a remote system

The AccuRoute Intelligent Device Client is installed on the AccuRoute server with a complete installation. You can install the AccuRoute Intelligent Device Client on a remote system when needed using the instructions in this section.

Requirements

Hardware and software requirements

The hardware and software requirements for the Remote AccuRoute Intelligent Device Client are as follows:

- A Windows NT domain system that runs in the same domain as the AccuRoute server and is not a domain controller. If the system is in a different domain, it (the domain) must have bi-directional trust with the AccuRoute server's domain.
- Pentium III-compatible processor
 - 1 GHz
 - 512 MB RAM
 - 500 MB available hard disk space
 - Microsoft mouse or compatible pointing device
- Windows 2012 64-bit, Windows 2008 R2 64-bit
- IIS with the following components: Common Files, World Wide Web Service, and Internet Information Services Manager

Requirements for AccuRoute Desktop

AccuRoute Intelligent Device Client supports HTTP and HTTPS connectivity to AccuRoute Desktop. For HTTPS connectivity, you must perform the following tasks prior to installing AccuRoute Intelligent Device Client on a remote system.

- Create and install a CA certificate on the Default Web Site in IIS.

Tip To set up a CA certificate using Microsoft Certificate Services, go to [Appendix B: Configuration for HTTPS Support](#). For a CA certificate issued by a third party, use the certificate authority's instructions and apply the certificate to the Default Web Site in IIS.

- Enable SSL on the Default Web Site in IIS.

Additional requirements

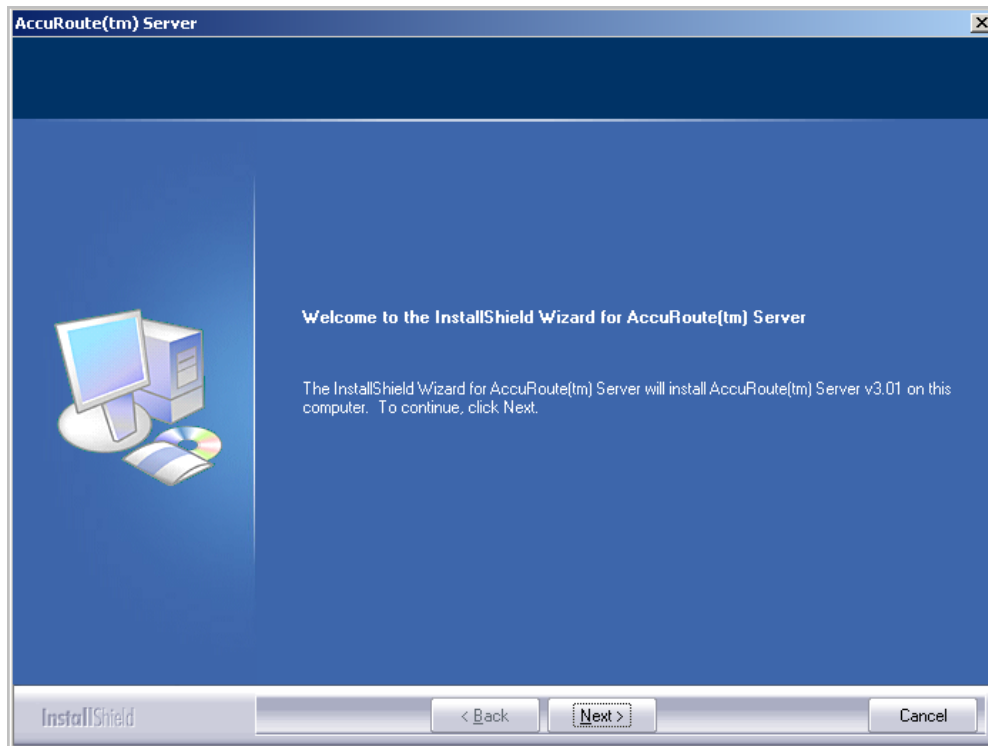
Remote AccuRoute Intelligent Device Client installation also requires the following:

- Access to the network copy of the AccuRoute server setup
- Windows user account that belongs to the AccuRoute Administrators group

Installing remote AccuRoute Intelligent Device Client

- 1 Log in to the system using an account that belongs to the AccuRoute Administrators group.
- 2 Navigate to the network where you have kept the AccuRoute server setup files.
- 3 Run **\\MessageServer\setup.exe**.

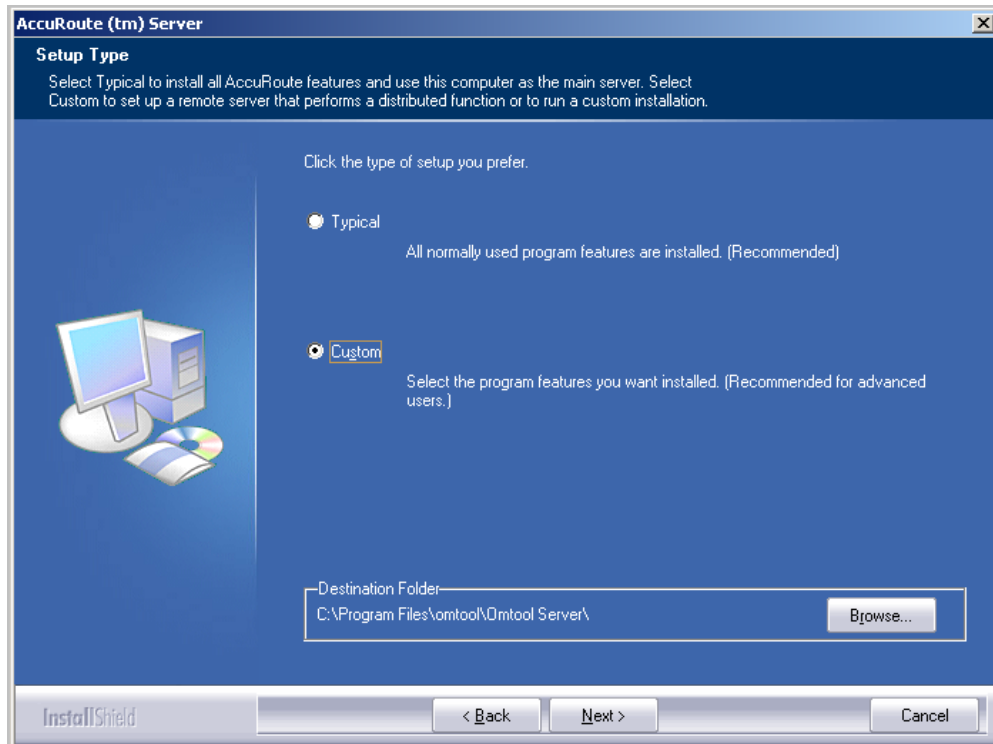
The InstallShield wizard configures your system and displays the welcome message.



- 4 Click **Next**. The setup shows the license agreement page.

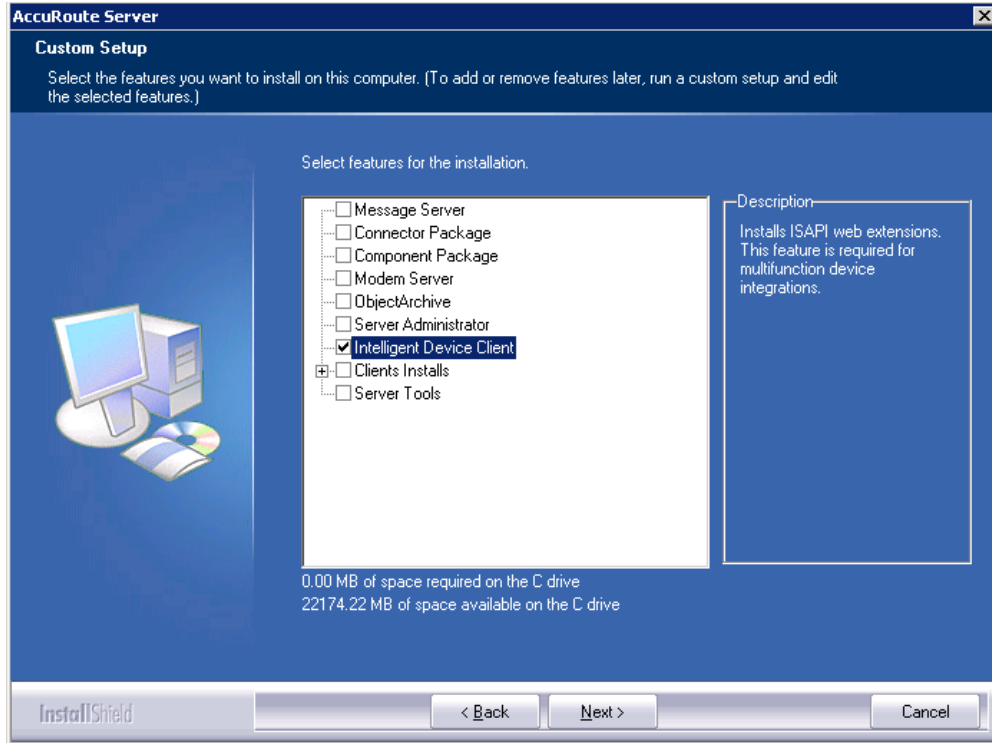


- 5 Read the agreement and select **I accept the terms of the license agreement** option.
- 6 Click **Next**. The setup shows the installation options.

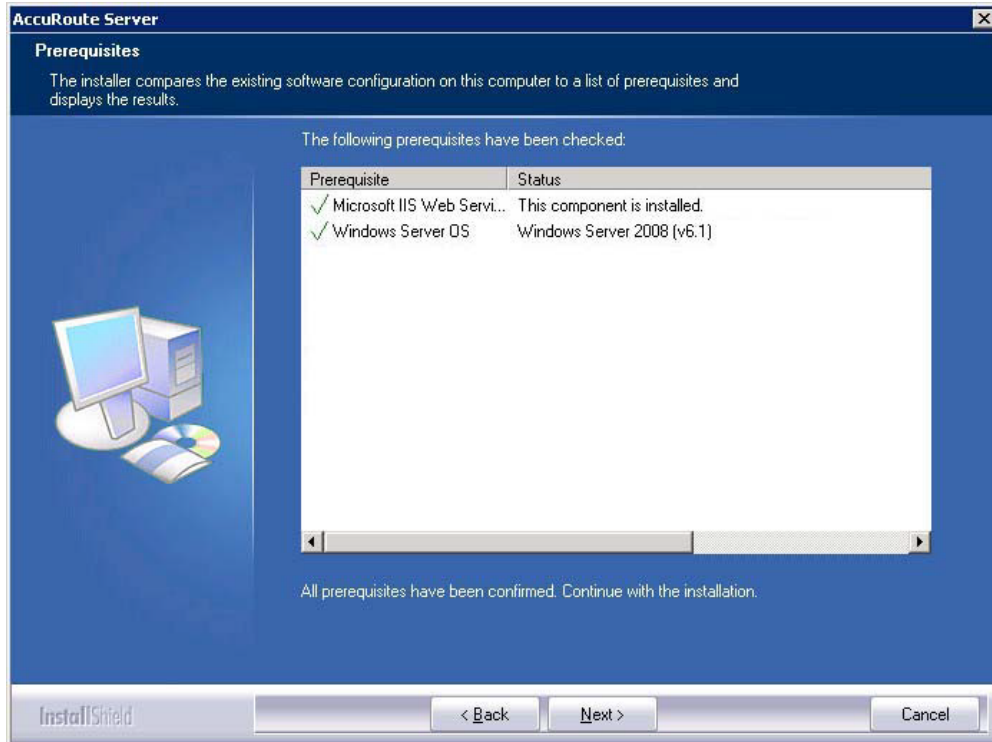


- 7 Select **Custom**. Click **Next**. The setup shows a list of AccuRoute features.

- 8 Select **AccuRoute Intelligent Device Client**. Clear any other feature you are not installing at this time.

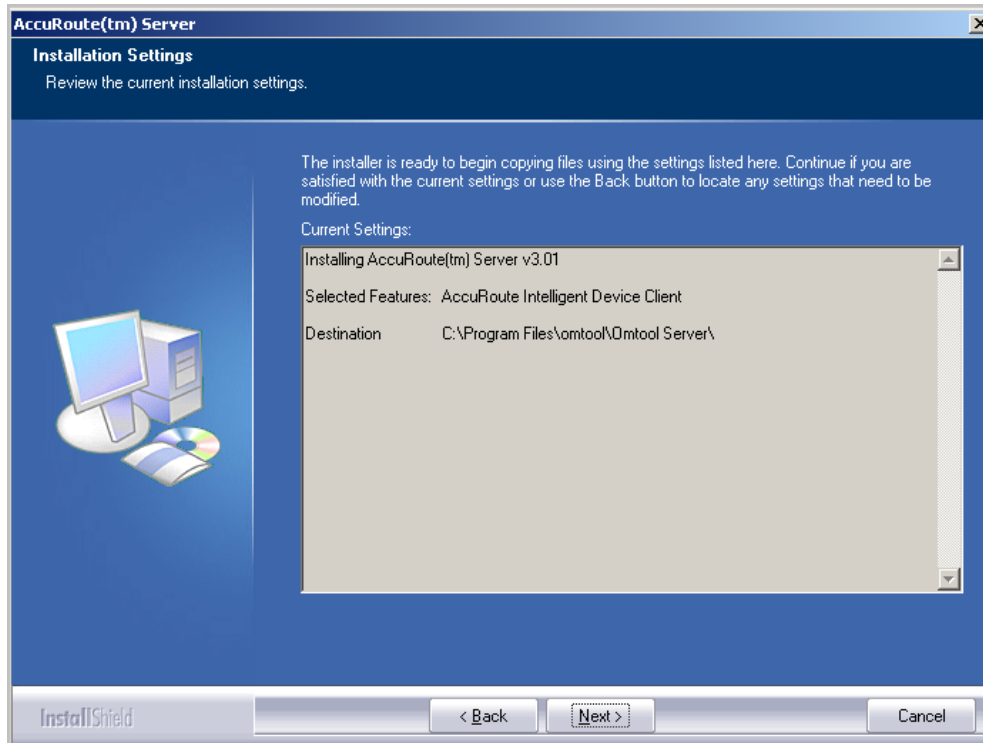


- 9 Click **Next**. The setup checks the system for installation requirements and displays the results.

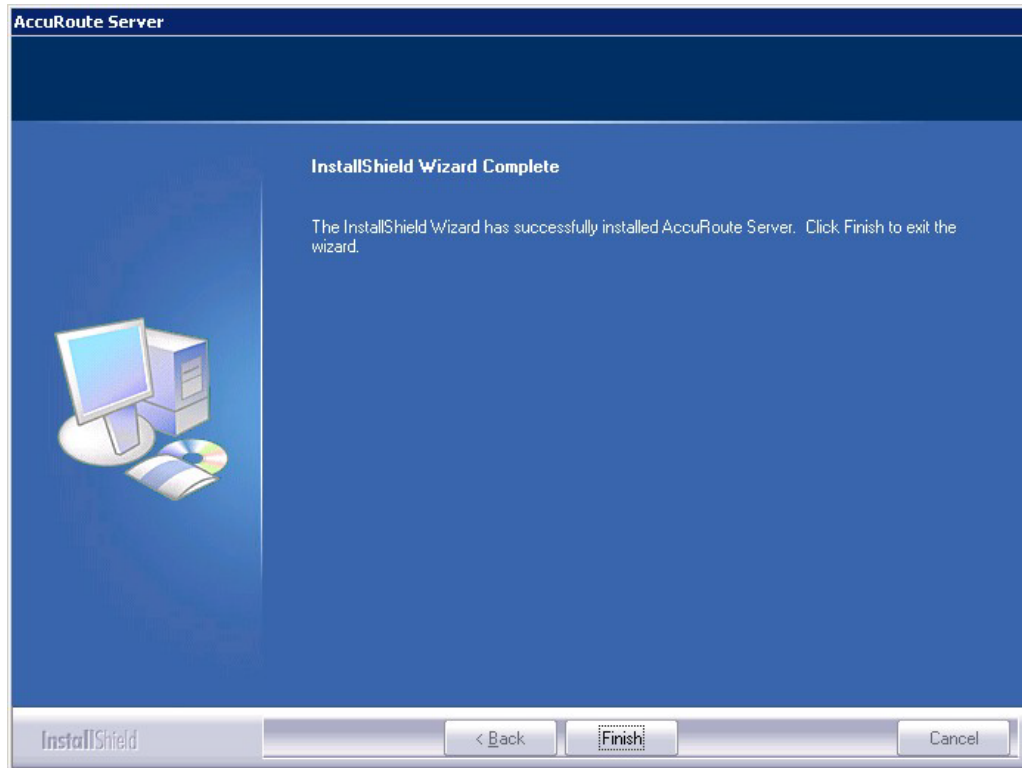


Note The setup cannot continue until all pre-requisite components are installed. (Double-click an item in the list for more information.) If any required components is missing, click **Cancel** and exit the installation setup. Install the components, then install AccuRoute Intelligent Device Client.

10 Click **Next**. The setup shows installation settings.



- 11 Review the installation settings. Click **Next** to start the installation. The setup installs the selected component and displays a message indicating that the installation is complete.



- 12 Click **Finish**.
- 13 Continue to [Configuring the remote AccuRoute Intelligent Device Client](#).

Configuring the remote AccuRoute Intelligent Device Client

Specifying the AccuRoute server

When you install AccuRoute Intelligent Device Client on a remote machine, you must specify the IP Address of the AccuRoute server in OmISAPIU.xml:

- 1 Go to:
`...\Omtool\Omtool Server\WebAPI\DesktopWebAPI\Scripts`
- 2 Open `OmISAPIU.xml` for editing.

Note If the server is part of a cluster, the following setting should be made in the file:

```
<Server Name="OmtoolServer"><ServerName>
Primary_Server_name</ServerName>

<Server Name="OmtoolServer"><ServerName>Secondary_Server_name</
ServerName>
</Server>
```

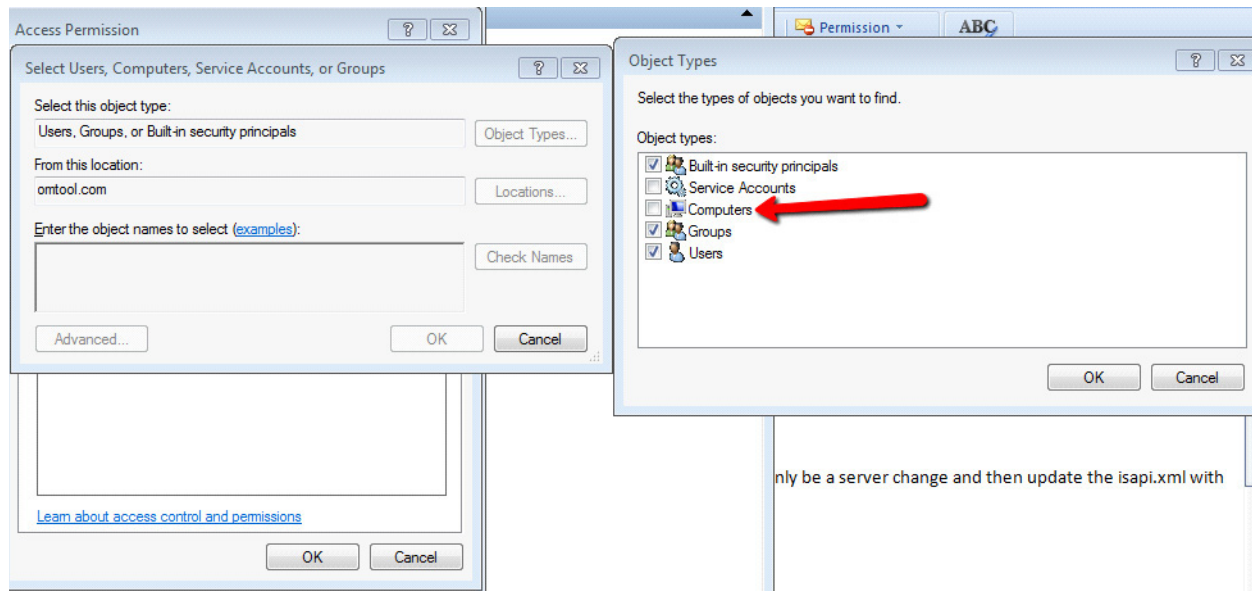
- 3 Locate the **ServerName** node.
- 4 Specify the name or the IP address of the AccuRoute server.
For example, `<ServerName>[IP Address]</ServerName>`.
- 5 Save and close the file.
- 6 Go to:
`...\Omtool\Omtool Server\WebAPI\WebAPI\Scripts`
- 7 Open `OmISAPIU.xml` for editing.
- 8 Locate the **ServerName** node.
- 9 Specify the name or the IP address of the AccuRoute server.
For example, `<ServerName>12.123.4.5</ServerName>`.
- 10 Save and close the file.

Adding the remote server's name to DCOM

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

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

2 Select **Computers** in the **Object Types** when adding the server name.



3 Reboot the AccuRoute server.

Adding the application pool logon account to the AccuRoute Admins group

There are two application pools (DesktopWebAPI and WebAPI) managing the worker processes handling requests from other AccuRoute client applications. By default, they run as Local System.

Note If the security policy in the LAN does not permit the application pool to run as Local System, the application pool identity can be reconfigured using any account that belongs to the Domain Users group.

If you change your login to a network account, Integrated Windows Authentication will not work for the virtual directories that use the application pool. The work around requires kerberos protocol changes in the active directory.

If necessary, modify the application pool identity. For instructions, consult the Windows documentation on IIS:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/c9b5db6f-874e-4ec9-93ed-1733367c117b.msp?mfr=true>

- If AccuRoute Intelligent Device Client is installed on a remote system, add the application pool logon account to the AccuRoute Admins group which has the required Distributed COM permissions to communicate with the AccuRoute server. For instructions, see (Also see [Creating AccuRoute Admins group](#) on 2-4.)
- If AccuRoute Intelligent Device Client is installed on the AccuRoute server and both application pools run as Local System, skip this step.

Other configurations

Other configurations include:

- Configuring HTTPs connectivity issues for AccuRoute Desktop
- Modifying the directory security configuration of virtual directories (optional).

For instructions, see [Optional configurations](#) (16-4).

Removing remote AccuRoute Intelligent Device Client

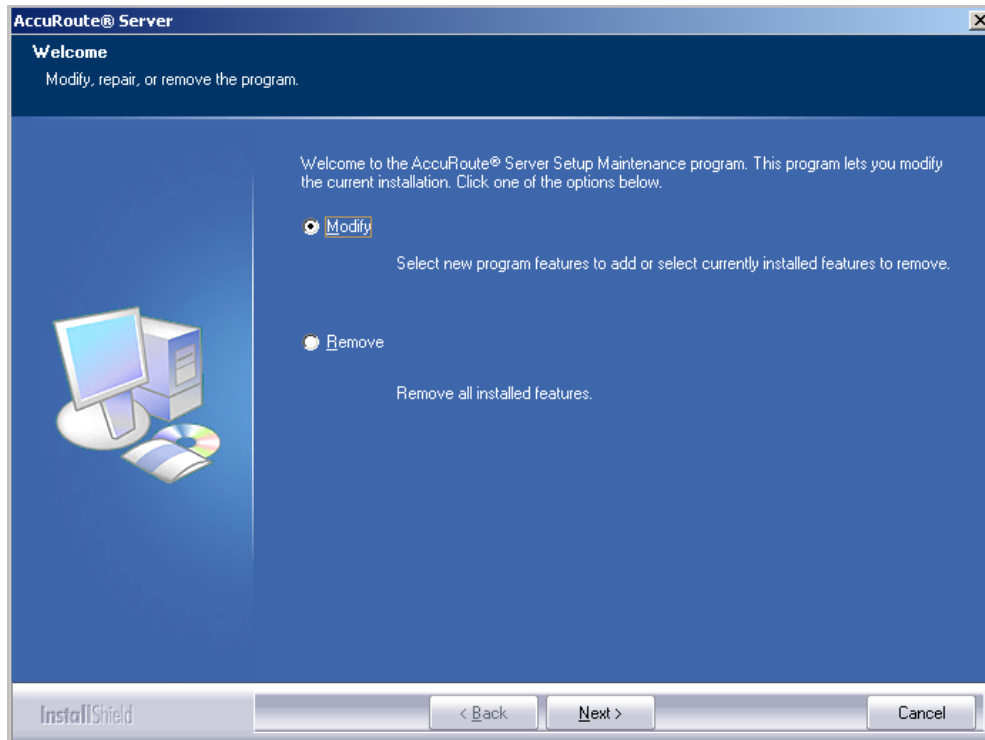
Before you remove the AccuRoute Intelligent Device Client, remove all other applications in the LAN that require/ use the AccuRoute Intelligent Device Client. Then remove AccuRoute Intelligent Device Client.

For information on removing AccuRoute applications that require AccuRoute Intelligent Device Client, consult the Omtool documentation for the application, which is available on the [AccuRoute v6.0 documentation](#) page.

AccuRoute Intelligent Device Client is not required for AccuRoute Desktop but can be used to establish a connection to the AccuRoute server using HTTP or Secure HTTP. After AccuRoute Intelligent Device Client is removed, AccuRoute Desktop can still connect to the AccuRoute server using DCOM. This requires reconfiguration. For configuration instructions, consult the AccuRoute Desktop installation guide, which is available on the [AccuRoute v6.0 documentation](#) page.

To remove AccuRoute Intelligent Device Client from a remote system:

- 1 Click **Start > Control Panel > Add or Remove Programs** to open the **Add or Remove Programs** page.
- 2 Select **AccuRoute Server** and click **Change/Remove**. The InstallShield wizard is initialized and it shows the following message.



- 3 Select **Remove** option and click **Next**.
- 4 Follow the prompts to remove AccuRoute Intelligent Device Client.

During installation, AccuRoute Intelligent Device Client allows the IIS web server extension WebDAV to run. After AccuRoute Intelligent Device Client is removed, WebDAV is still allowed to run. If WebDAV should be prohibited from running, change the status of this web server extension to Prohibited. For more information, consult the Windows documentation on IIS.

Appendix A: Setting up an AccuRoute Server Cluster

This section includes:

[Introduction to failover](#) (A-1)

[Requirements for an AccuRoute server cluster](#) (A-3)

[Installing and configuring the Cluster server](#) (A-4)

[Setting up the Database server](#) (A-4)

[Setting up the Active server](#) (A-5)

[Applying licenses](#) (A-9)

[Setting up the Passive server](#) (A-9)

[Setting up the Telco share](#) (A-12)

[Creating the Telco Share](#) (A-12)

[Configuring the AccuRoute connector for Telco to use the Telco Share on the database server](#) (A-12)

[Testing the failover configuration](#) (A-13)

[Optional configurations for cluster environments](#) (A-14)

Introduction to failover

Automatic failover, a native AccuRoute capability, ensures seamless and immediate recovery from a localized system failure on the AccuRoute server. It requires two redundant AccuRoute servers that are joined to form an AccuRoute server cluster, and a third system where critical server resources are stored.

The redundant AccuRoute servers are referred to as:

- **Active Server** - the current AccuRoute server
- **Passive Server** - the standby server

The third system that stores critical resources is called the “database server” because it hosts the server databases along with server configuration files. If the AccuRoute server is enabled for faxing, the database server also hosts the Telco share which is an intermediary repository for inbound and outbound faxes. (The database server can also function as a remote server such as Remote Administrator, Remote Composer, Remote Embedded Directive Manager, or Remote Modem Server.)

In some environments, where multi-function devices are used, a fourth system - Remote IIS - can be added to host the AccuRoute Intelligent Device client and specific AccuRoute device client installs.

Section A: Setting up an AccuRoute Server Cluster

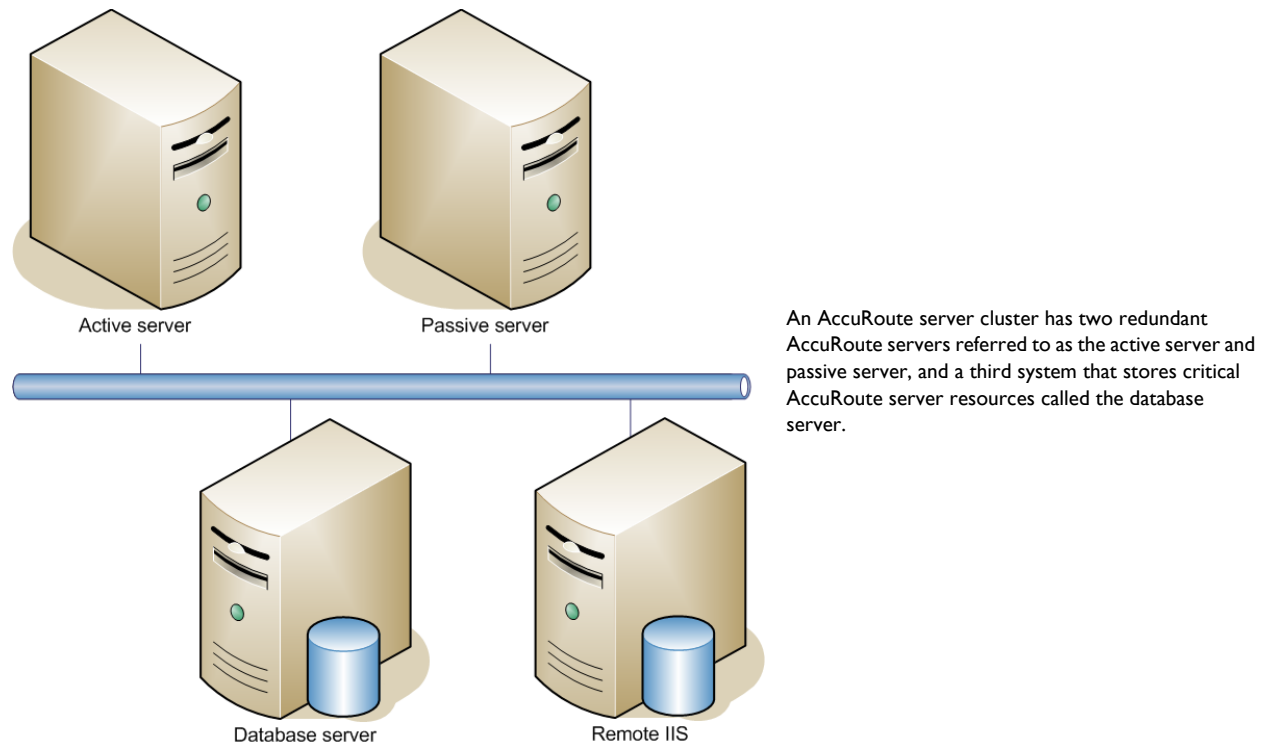


Figure A-1: Basic setup of the AccuRoute server cluster

Failover is driven by the Omtool Cluster Manager service which is installed on the AccuRoute server. (This service does not appear in the Services applet because it is not registered by default.) When an AccuRoute server cluster is created, this service is immediately registered and runs simultaneously on both AccuRoute servers in the cluster. During regular operation, the active server in the AccuRoute server cluster continuously writes to the server databases while Omtool Cluster Manager service on the passive server polls the database server in 45-second intervals to verify that the active server remains active.

When a localized system failure occurs on the active server, it loses communication with the database server and cannot write to the server databases. As soon as the Omtool Cluster Manager service on the passive server polls the database server again and finds no recent activity from the active server, the Omtool Cluster Manager service on the passive server starts all its local Omtool services and becomes the active server in the cluster. The transition is complete within 1 to 3 minutes of the failure.

After a failure occurs, an administrator needs to restore the server that is offline.

Tip Omtool Server Monitor is a monitoring application that detects failures on AccuRoute servers. Omtool recommends that Omtool Server Monitor or another monitoring application be used to alert administrators that a failure has occurred so that failures can be corrected in a timely manner.

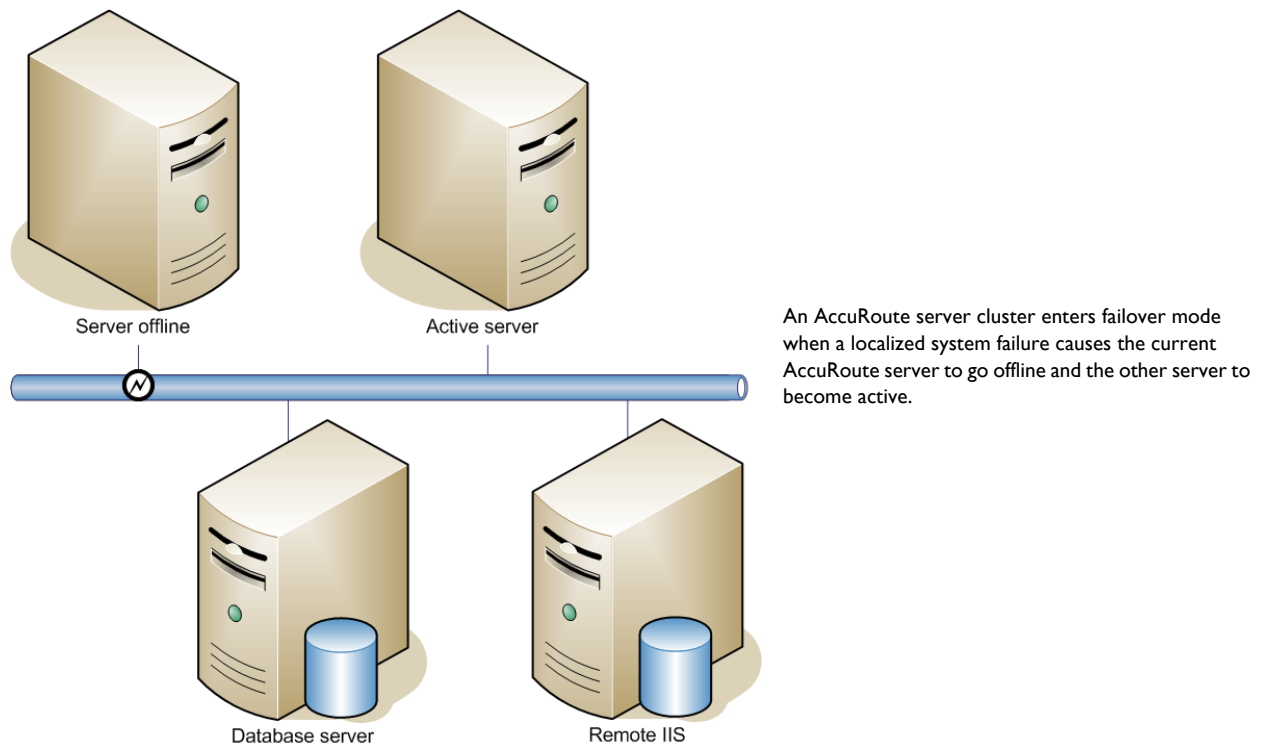


Figure A-2: AccuRoute server cluster in failover mode

An AccuRoute server in the cluster can be designated as the preferred server. If an AccuRoute server is preferred, it is always the active server whenever it is available. Therefore, if a system failure occurs and the preferred server goes offline, the non-preferred server becomes active, but when the preferred server is online again, it becomes the active server and the non-preferred server returns to a standby state.

Requirements for an AccuRoute server cluster

AccuRoute server requirements

The two AccuRoute servers must meet the minimum requirements for an AccuRoute server. For details, see [Hardware and software requirements](#) (2-1).

Licenses are required for both the AccuRoute server and the failover AccuRoute server. You must install both licenses on the Active server in the cluster.

Note The AccuRoute servers should have identical and redundant configurations. If resources are shared, such as a Remote Composer, the shared resource should be installed on the database server or another high availability system in the domain.

Database server requirements

The Database server must meet the following minimum requirements:

- Requirements for the AccuRoute server, as defined in [Hardware and software requirements](#) (2-1)
- Microsoft SQL Server 2008/2012/2016

Note Microsoft SQL Server 2008 Express Edition does not meet this requirement.

- Template files used by the server

Remote device server requirements

The Remote Device server must meet the following minimum requirements:

- Requirements for the Remote Device server, as defined in [Installing AccuRoute Intelligent Device Client on a remote system](#) (16-8)

Installing and configuring the Cluster server

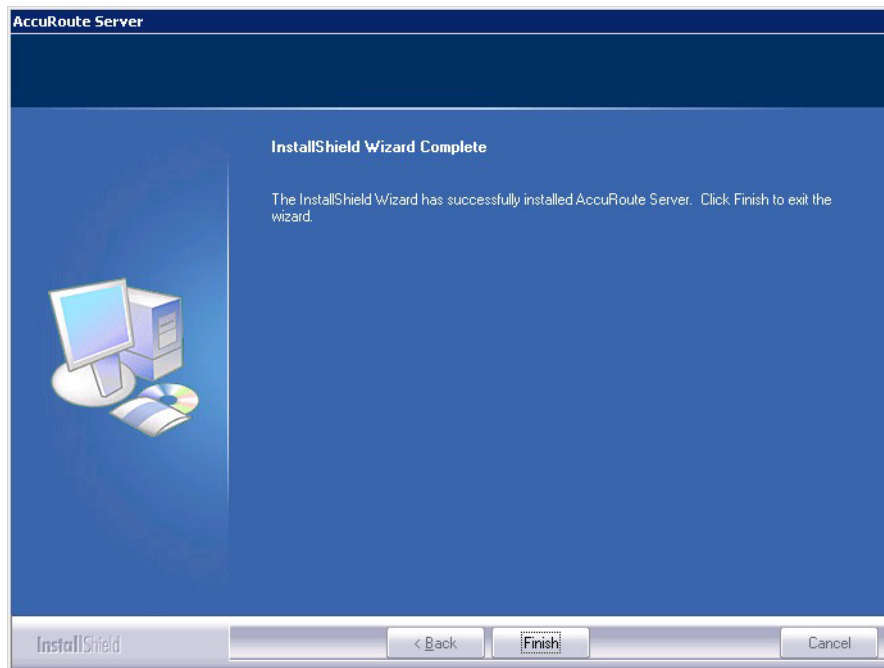
Begin setting up the Server Cluster by creating folders for the AccuRoute server resources that will be stored on the Database server.

Setting up the Database server

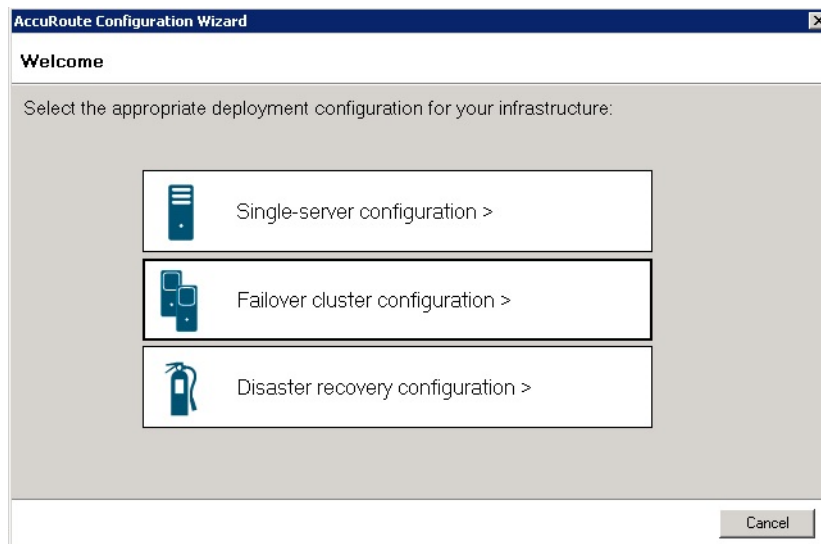
- 1 Log in to the system as an Administrator.
- 2 Select a location in the Database server and create the following folders:
 - ▶ **Messages** - Stores the message database.
 - ▶ **Config** - Stores server configuration files.
- 3 Share each folder.
- 4 Give the Omttool service account read, write, and delete permissions to each folder. For more information on modifying permissions, consult Windows help.

Setting up the Active server

- 1 Install AccuRoute v6.0 on the Primary server. For installation steps, see [Installing the AccuRoute server](#) (3-2).
- 2 On the **InstallShield Wizard Complete** screen (the last installation screen), click **Finish** to complete the installation.

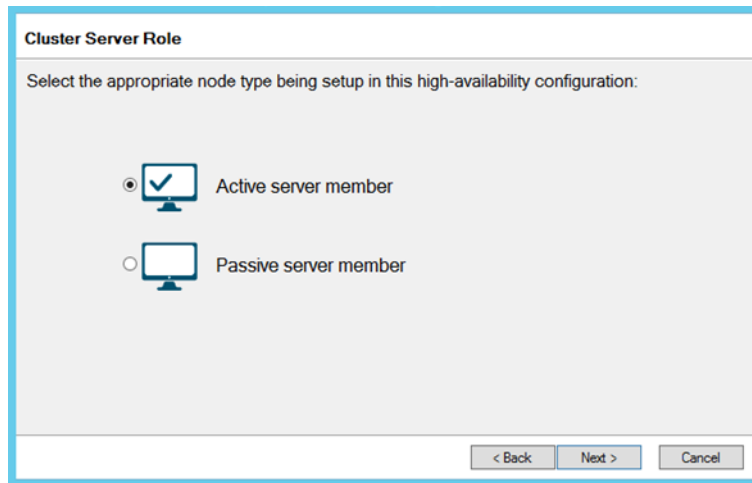


- 3 The **AccuRoute Configuration Wizard** automatically launches next.

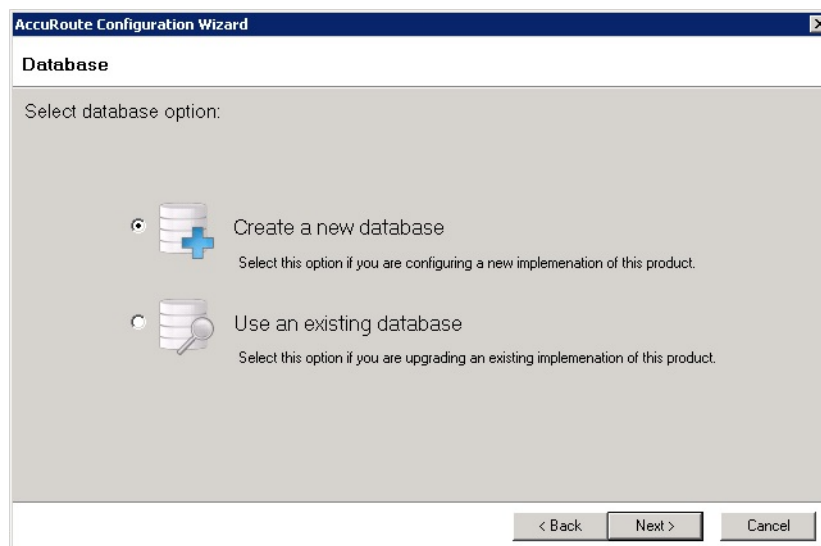


Select **Failover cluster configuration**.

- 4 On the **Cluster Server Role** screen, select **Active server member** and click **Next**.

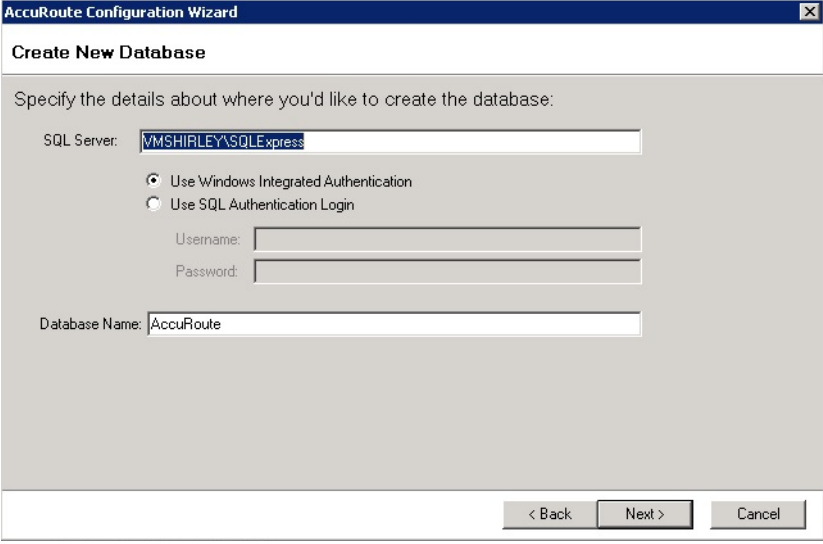


- 5 On the **Database** screen, select the appropriate database option:



- ▶ **Create a new database** — for configuring a new installation of AccuRoute.
- ▶ **Use an existing database** — for upgrading an existing installation of AccuRoute.

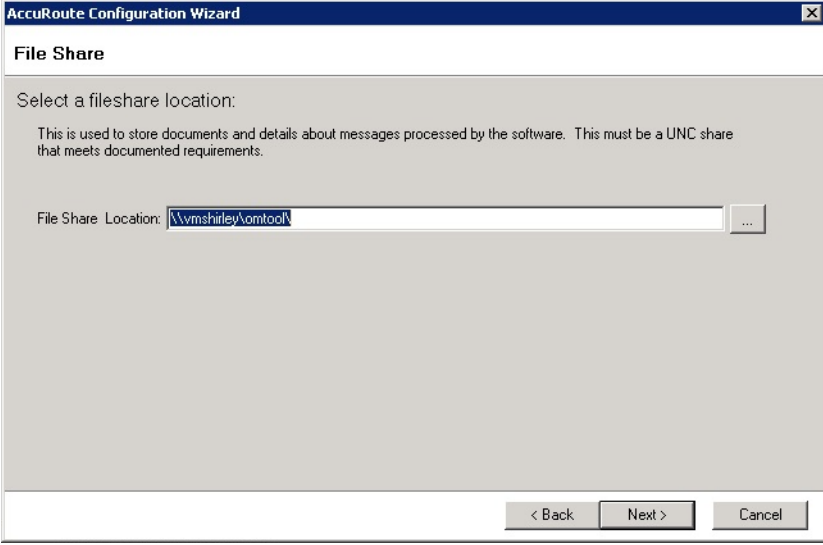
6 Click **Next**. The **Create New Database** screen opens.



The screenshot shows a window titled "AccuRoute Configuration Wizard" with a sub-header "Create New Database". Below the sub-header, it says "Specify the details about where you'd like to create the database:". There are three input fields: "SQL Server:" with the value "VMShirley\SQLexpress", "Username:" (empty), and "Password:" (empty). There are two radio buttons: "Use Windows Integrated Authentication" (selected) and "Use SQL Authentication Login". Below these is a "Database Name:" field with the value "AccuRoute". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

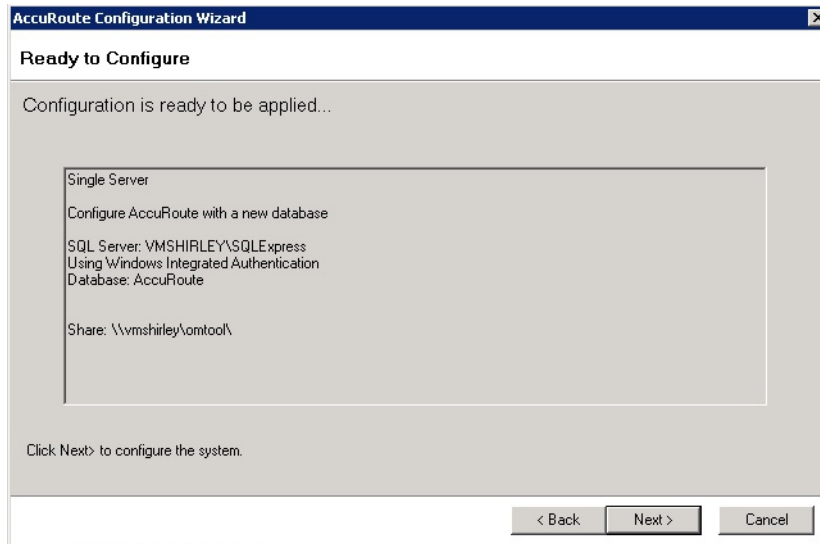
Enter your **SQL Server** and **Database Name** information and click **Next**.

7 At the **File Share Location** field on the **File Share** screen, enter or browse to the UNC path you want to use. (This is a path to the folder location you created in Step 1.) Click **Next**.



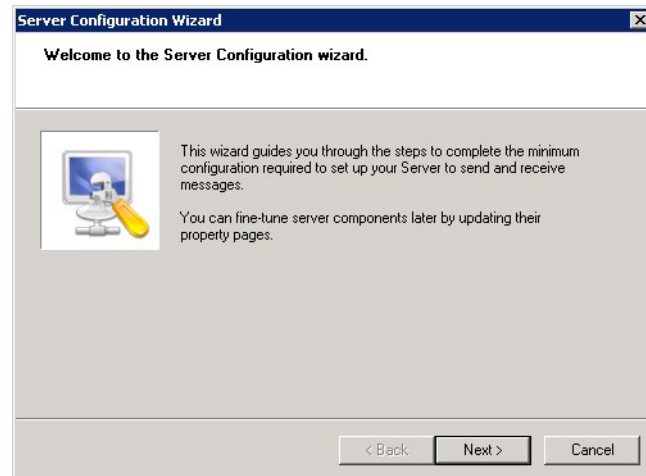
The screenshot shows a window titled "AccuRoute Configuration Wizard" with a sub-header "File Share". Below the sub-header, it says "Select a fileshare location:". There is a paragraph of text: "This is used to store documents and details about messages processed by the software. This must be a UNC share that meets documented requirements." Below this is a "File Share Location:" field with the value "\\vmshirley\omtoolk" and a browse button "...". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

- 8 The **Ready to Configure** screen appears. Click **Next** to configure the system.

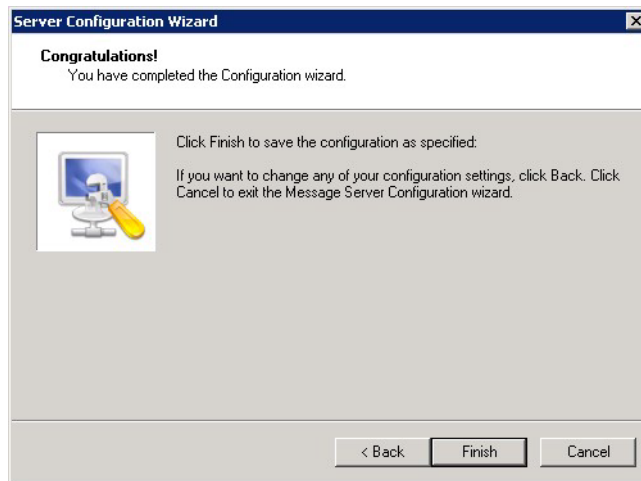


A **Configuring...** progress screen appears during configuration.

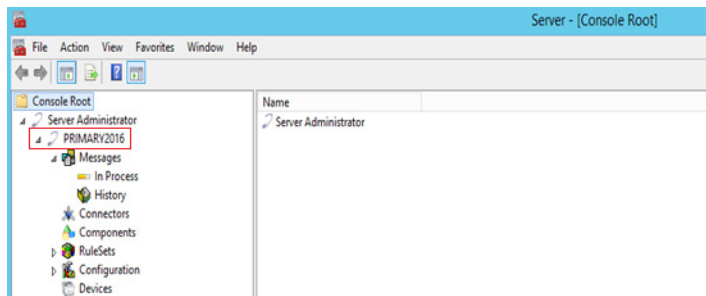
- 9 The **Server Configuration Wizard Welcome** screen opens. Click **Next**.



10 Click **Finish** on the **Congratulations** screen.



11 The following screen shows how the **Primary** server appears in the AccuRoute Server Administrator.



Applying licenses

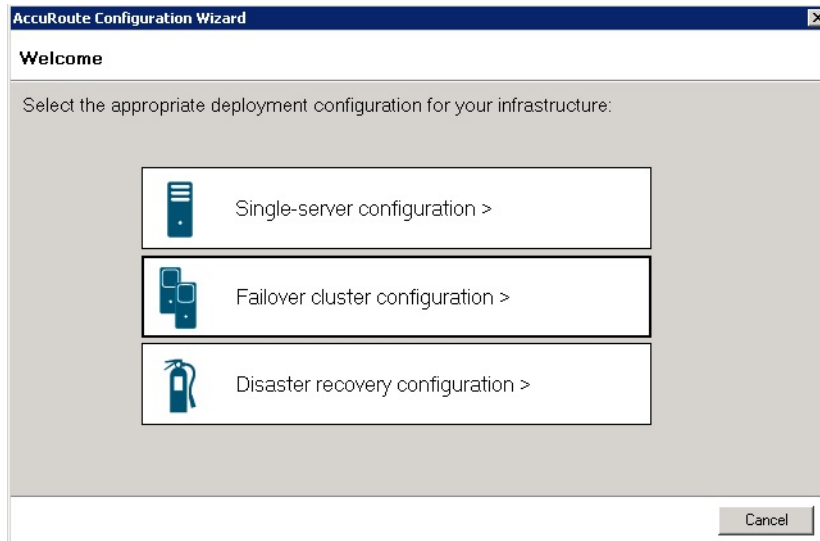
Apply your Base server and Failover licenses. See [Activating the license](#) (3-16) for more information.

Note The Failover server license is added to the Active (Primary) server in the environment.

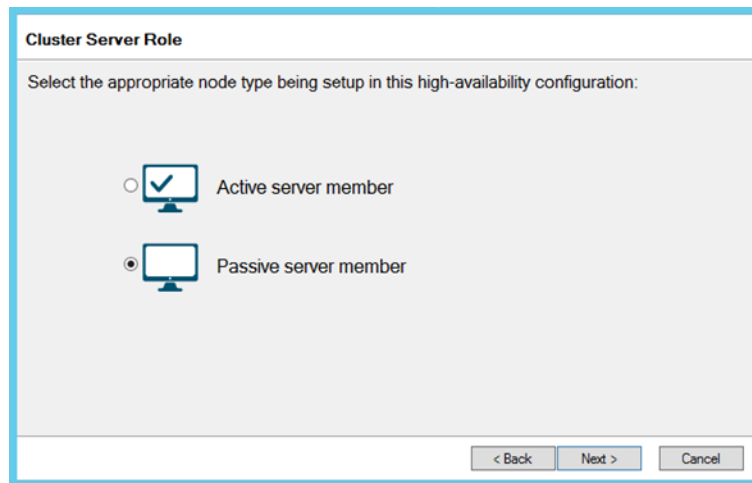
Setting up the Passive server

- 1 Install AccuRoute v6.0 on the Passive (secondary) server. For steps, see [Installing the AccuRoute server](#) (3-2).
- 2 On the **InstallShield Wizard Complete** screen (the last installation screen), click **Finish** to complete the installation.

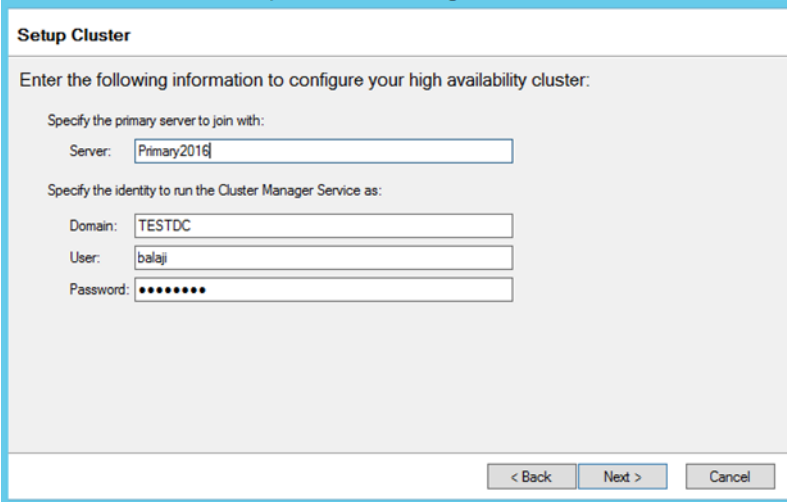
- 3 Once again, the **AccuRoute Configuration Wizard** opens to the **Welcome** screen. Select **Failover cluster configuration**.



- 4 On the **Cluster Server Role** screen, this time select **Passive server member** and click **Next**.



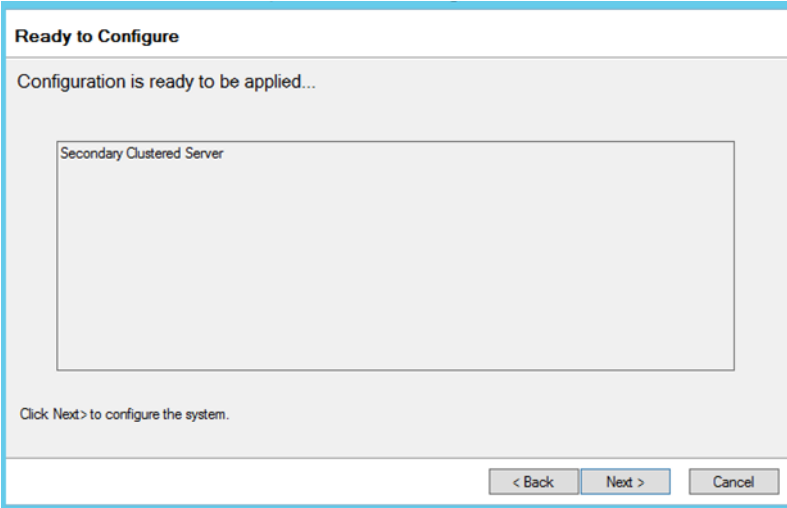
5 The **Setup Cluster** screen appears.



The screenshot shows a window titled "Setup Cluster". Below the title bar, it says "Enter the following information to configure your high availability cluster:". There are two sections of input fields. The first section is "Specify the primary server to join with:" with a "Server:" label and a text box containing "Primary2016". The second section is "Specify the identity to run the Cluster Manager Service as:" with three fields: "Domain:" containing "TESTDC", "User:" containing "balaji", and "Password:" containing seven dots. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Enter the Primary **Server** name and user information. Click **Next**.

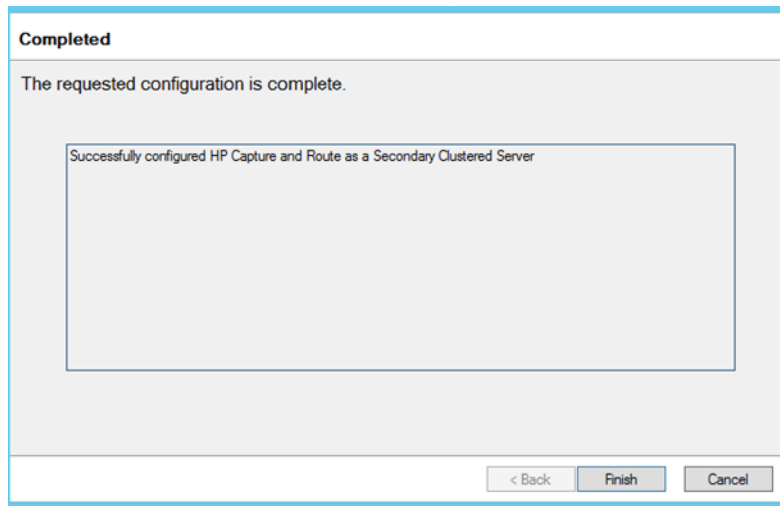
6 The **Ready to configure** screen appears. Click **Next** to configure the system.



The screenshot shows a window titled "Ready to Configure". Below the title bar, it says "Configuration is ready to be applied...". There is a large rectangular box with the text "Secondary Clustered Server" inside. Below this box, it says "Click Next> to configure the system.". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

A **Configuring...** progress screen appears during configuration.

- 7 The **AccuRoute Configuration Wizard Complete** screen appears.



- 8 Click **Finish** to close the wizard. Your clustered server environment is now configured.

Setting up the Telco share

Creating the Telco Share

Note Complete the following procedure if the AccuRoute server cluster supports faxing.

For an AccuRoute server cluster that supports faxing, create the Telco share. The Telco share is shared by both servers in the cluster. You must create it on any high availability system, such as the database server belonging to the same domain as the clustered AccuRoute servers.

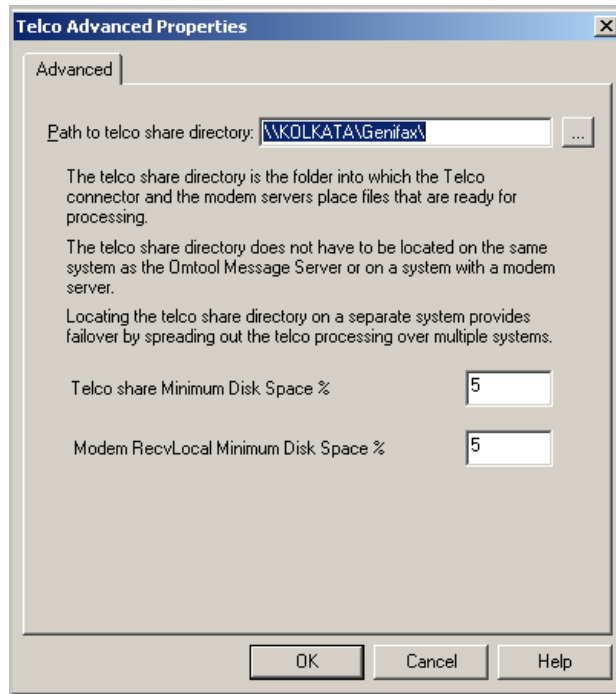
To create the Telco share on the database server:

- 1 Choose a location in the local directory structure and create a folder for the Telco share. Use a self-descriptive name such as `omtooltelcoshare`.
- 2 Share the folder.
- 3 Give the Omttool service account read and write permissions to the folder. For more information on modifying permissions, consult Windows help. (If the environment has AccuRoute servers that were installed with different Omttool service accounts, give all Omttool service accounts these permissions.)

Configuring the AccuRoute connector for Telco to use the Telco Share on the database server

- 1 Click **Start > All Programs > Omttool > AccuRoute Server > AccuRoute Server Administrator**.

- 2 In the console tree, expand the AccuRoute Server Administrator and click **Connectors**.
- 3 Double-click the **AccuRoute Connector for Telco** in the details pane to open the **Telco** properties page.
- 4 Click **Advanced** to open the **Telco Advanced Properties** page.



- 5 In the **Path to telco share directory** text box, enter the UNC path (that is the `\\ServerName\ShareName`) to the Telco share folder. Add a trailing backslash at the end. (For example `\\123.4.5.678\telcoshare\`).
- 6 Click **Ok** and then **Ok** to save your changes and close the **Properties** page.

Testing the failover configuration

You can test the Failover configuration by simulating a localized system failure on the Active server.

- 1 **Simulate a failure:** Shut down the active server. Wait approximately five minutes, and then verify that the Omtool Cluster Manager process (**OMSvrClusterMgr**) and the connector processes (**OmCon***) are running on the other server, which is now the active server.
- 2 **Restore the failed server:** Start the server that was shut down and wait for it to boot up. Wait approximately five minutes, and then verify that the Omtool Cluster Manager process (**OMSvrClusterMgr**) and the connector processes (**OmCon***) are running.

Optional configurations for cluster environments

Setting up the remote device server

Refer to the procedure for [Installing AccuRoute Intelligent Device Client on a remote system](#) (16-8).

Configuring the AccuRoute Web Client for failover

The Web Client should be installed on a system remote from the active and passive servers and meet all of the installation requirements found in the Web Client installation guide, which is available on the [AccuRoute v6.0 documentation](#) page.

- 1 Navigate to:

```
\Program Files (X86)\Omtool\WebClient\Configuration
```

Open the `Web.xml` file for editing.

- 2 In the **<Connection>** section of the xml, add the name of the secondary server in your cluster. For example:

```
<Connection>
<Server>MAGNOLIA</Server>
<FailoverServer>JASMINE</FailoverServer>
<Authentication type="Exchange">
```

Note In this example, the name of the active AccuRoute server is MAGNOLIA and the passive server is JASMINE.

- 3 Save your changes and close the xml file.
- 4 Restart the IIS services.

Configuring the Mobile Client setup to support a cluster

To configure cluster support for a setup with mobile clients:

- 1 Modify the `OmISAPU.xml` in the `\Omtool\OmtoolServer\WebAPI\MobileWebAPI\Scripts` directory as follows:
- 2 Add another line for the secondary server, changing

```
</Server>
    <Server Name="OmtoolServer">
        <ServerName>VMOXPTESTING</ServerName>
    </Server>
</Servers>
```


to the following:

```
</Server>
  <Server Name="OmtoolServer">
    <ServerName>VMPrimary</ServerName>

    <Server Name="OmtoolServer">
    <ServerName>VMSecondary</ServerName>

  </Server>
</Servers>
```

Configuring Image-In Connect for failover

- 1 Navigate to:

```
\\Omtool\Image-in Connect\
```

Open the `ImageInConnect.xml` file.

- 2 Locate the **<Server node>** section of the xml and add the name of the secondary server in your cluster. For example:

```
<ImageInConnect>
<XModels>
<XModel>http://ratchetx.com/installs/omtool/xmodels/
omaccuroutelink.xmodel</XModel>
<XModel>http://ratchetx.com/installs/omtool/xmodels/
omaccurouteview.xmodel</XModel>
<XModel>http://ratchetx.com/xmodels/companyinfo.xmodel</XModel>
</XModels>
<AccuRouteServer>MAGNOLIA</AccuRouteServer>
<AccuRouteServer>JASMINE</AccuRouteServer>
<AccuRouteWeb>url</AccuRouteWeb>
</ImageInConnect>
```

Note In this example, the name of the active AccuRoute server is MAGNOLIA and the passive server is JASMINE.

- 3 Save your changes.

Configuring Omtool Workflow Integration Application (OWIA) for failover

The Omtool Workflow Integration Application (OWIA) is included with the Image-In Queue (IIQ) client after installation. This application can be used to link third-party applications used by Image-In Connect (IIC) to view the active documents in IIQ.

Modifying the QueueWorkflow XML file

Use the following procedure to modify the `queueworkflow.xml` file to have the AccuRoute Server information in the **Server** section.

- 1 Navigate to:

```
\\Omtool\Image-in Queue\Bin
```

Open the `QueueWorkflow.xml` file.

- 2 Locate the **<Configuration>** section of the xml and add the name of the secondary server in your cluster. For example:

```
<Configuration>
  <Server>MAGNOLIA</Server>
  <Server>JASMINE</Server>
  <Demo>>false</Demo>
  <DebugEnabled>0</DebugEnabled>
  <CacheInitializationData>1</CacheInitializationData>
  <CacheRefreshInterval>1</CacheRefreshInterval>
  <Silent>0</Silent>
</Configuration>
```

Note In this example, the name of the active AccuRoute server is MAGNOLIA and the passive server is JASMINE.

- 3 Save your changes.

Clustering and Composer thread awareness

In a typical configuration, you use the local Composer on the active server while the passive server is in the waiting state. To improve throughput, an additional compose license can be added to access the compose engines on the passive server. However in the event of a failover, both the local and remote Composers would be on the same physical machine, and using them simultaneously can cause significant performance issues on the passive server. In order to utilize both servers, the active server compose should be removed and reinstalled with the server name specified. The passive server then can be added with its server name specified and, in the subsequent event of a failover, the passive server will not be subject to performance issues due to duplicate composers.

Appendix B: Configuration for HTTPS Support

This section describes setting up a CA certificate using Microsoft Certificate Services and enabling SSL.

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

If you require HTTPS support, you can follow the instructions below for [Setting up a CA certificate and enabling SSL with Windows 2008 R2 64-bit](#).

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

Note For instructions to set up HP Pro devices with HTTPS, refer to the [Embedded AccuRoute for HPOXPd Device Client Installation Guide](#).

Setting up a CA certificate and enabling SSL with Windows 2008 R2 64-bit

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

Requirements for setting up a CA certificate

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

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

The remainder of this section provides procedures for:

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

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

[Installing the certificate to Internet Information Services \(IIS\)](#) (B-2)

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

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

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

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

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

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

[Editing the OmlSAPIU.xml file](#) (B-5)

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

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

Downloading the MakeCert executable

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

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

Creating the certificate

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

```
makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server"  
-b 01/01/2006 -e 01/01/2013 -ss my -sr localMachine -sky exchange -sp  
"Microsoft RSA SChannel Cryptographic Provider" -sy 12  
"fully_qualified_domain_name_of_iis_server.cer"
```

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

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

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

Installing the certificate to Internet Information Services (IIS)

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

- 1 Select and right-click the certificate.
- 2 Select **Install Certificate**. The **Certificate Import** wizard is displayed.
- 3 Select **NEXT**.
- 4 Select **Place all certificates in the following store** and select **BROWSE**.
- 5 Select **Trusted Root Certification Authorities** and select **OK**.
- 6 You will be prompted with a security warning:

*You are about to install a certificate from a certification authority (CA) claiming to represent...
Do you want to install this certificate?*

Select **YES**. A message indicating the import was successful should display.

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

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

- 1 Navigate to the **IIS\Local machine** directory and locate **Server Certificates**.
- 2 Find the newly created certificate. Double-click and open the certificate **Properties** page.
- 3 Click on the **Details** tab.
- 4 Choose the **Copy to File** option. The **Certificate Export Wizard** opens.
- 5 Click **Next**.
- 6 On the **Export Private Key** dialog, select **No, do not export the private key**.
- 7 Click **Next**.
- 8 On the **Export File Format** dialog, select **DER encoded X.509 (.CER)**.
- 9 Click **Next**.
- 10 On the **File to Export** dialog, select **Browse**. The **Save As** dialog opens.
- 11 Browse to the directory:
`C:\Program Files (x86)\Omtool\OXPl.6\Certificate`
- 12 In the **File Name** text box, enter **WebServer.cer with DER Encoded Bindary X.509 (*.cer)** as the **Save type**.
- 13 Click **Save** and then **Next**. The **Completing the Certificate Export Wizard** opens.
- 14 Click **Finish**.
- 15 When a message appears stating that the export was successful, click **OK**.

Creating an SSL binding

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

Requiring SSL for the virtual web sites

- 1 Open the IIS Manager.
- 2 Expand **Local machine > Default WebSite** and select **OXPI.6** (or **OXPI.4**).

- 3 Open **SSL Settings** and check **Require SLL**. Under **Client certificates**, select **Ignore**.
- 4 Expand **Local machine > Default WebSite** and select **WebAPI**.
- 5 Open **SSL Settings** and check **Require SLL**. Under **Client certificates**, select **Ignore**.

Verifying the SSL binding

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

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

Note This message is expected and safe to ignore.

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

Enabling directory browsing in IIS

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

Verifying HTTPS browsing

- 1 Open the IIS Manager.
- 2 Expand the **Default Web Site**.
- 3 Expand **OXP v1.6** (or **OXP v1.4**).
- 4 Select the **Configuration** folder.
- 5 In the actions pane, select **Browse*:443(https)**.
- 6 Select **Continue to this website (not recommended)**.
- 7 Verify that the local page is displayed:

For HP OXPd v1.6:

`...\OXPl.6\Configuration\`

For HP OXPd v1.4:

```
...\OXPl.4\Configuration\
```

- 8 In the IIS Manager with **Default Web Site** expanded, expand **WebAPI**.
- 9 In the actions pane, select **Browse*:443(https)**.
- 10 Select **Continue to this website (not recommended)**.
- 11 Verify that the localhost page is displayed:

```
...\WebAPI\
```
- 12 Select **Continue to this website (not recommended)**.

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.

```
C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts
```
- 2 In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

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

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path.
For HP OXPd v1.6:

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


For HP OXPd v1.4:

```
C:\Program Files (x86)\Omtool\OXPl.4\Configuration\
```
- 2 In bootstrap.xml, change `http` to `https`.

```
<Server>https://fully_qualified_domain_name/webapi/scripts/  
omisapiu.dll </Server>
```
- 3 Save the file.
- 4 Reset IIS.

Requirements for setting up a CA certificate

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

- Web server that meets the requirements for AccuRoute Intelligent Device Client.

- Windows user account that belongs to the Administrators group

This section includes:

[Downloading the MakeCert executable](#) (B-6)

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

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

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

[Editing the OmlSAPIU.xml file](#) (B-14)

[Editing the Bootstrap.xml file](#) (B-15)

Downloading the MakeCert executable

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

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

Running the MakeCert executable and creating the certificate

- 1 Open a command prompt and navigate to the directory where you saved the MakeCert executable.
- 2 Run the following command:

```
makecert.exe -r -pe -n "CN=fully_qualified_domain_name_of_iis_server"  
-b 01/01/2006 -e 01/01/2013 -ss my -sr localMachine -sky exchange -sp  
"Microsoft RSA SChannel Cryptographic Provider" -sy 12  
"fully_qualified_domain_name_of_iis_server.cer"
```

fully_qualified_domain_name_of_iis_server should be in this format:

`servername.domain.com`

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

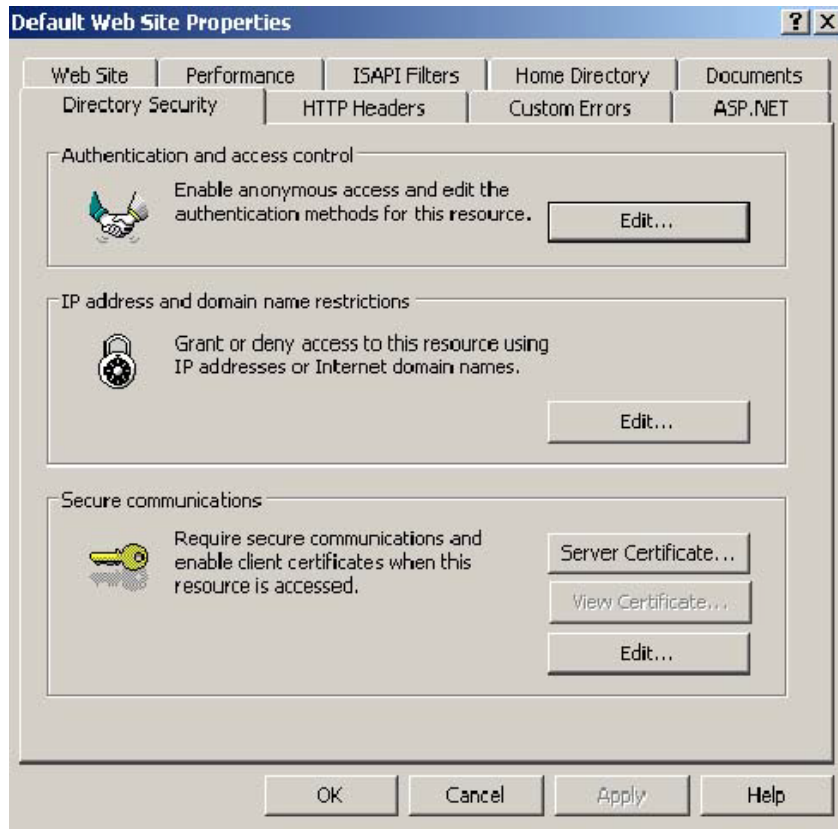
When the command is run properly, the system will display a message indicating that it succeeded.

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

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

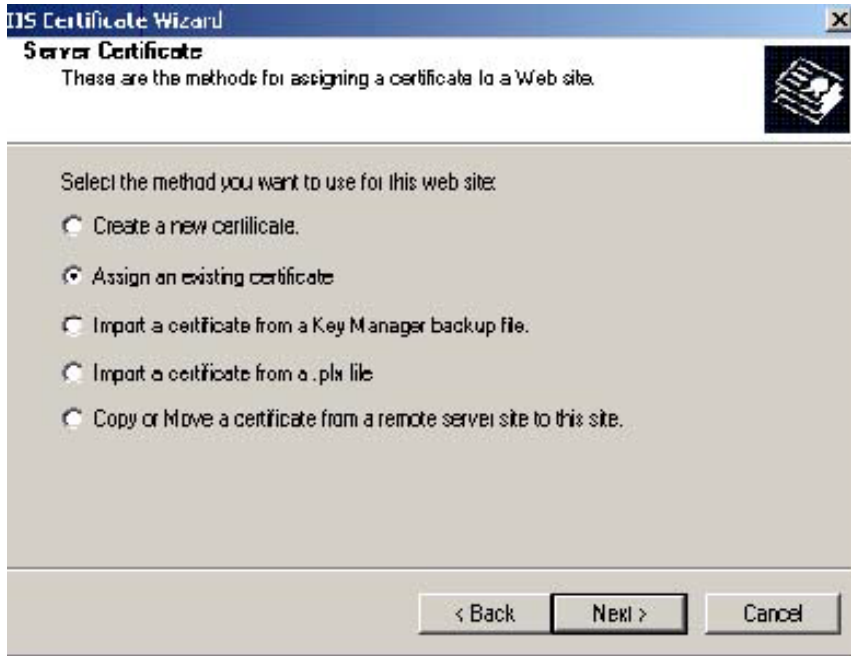
Using the Web Server Certification wizard:

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

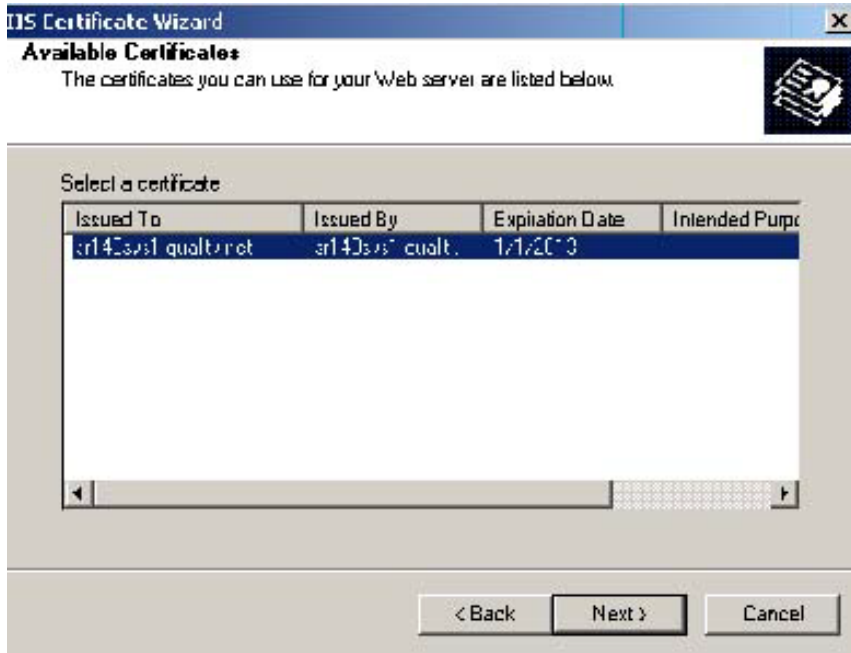


- 2 Click the **Server Certificate** button. The **Welcome to the Web Server Certification Wizard** page is displayed.

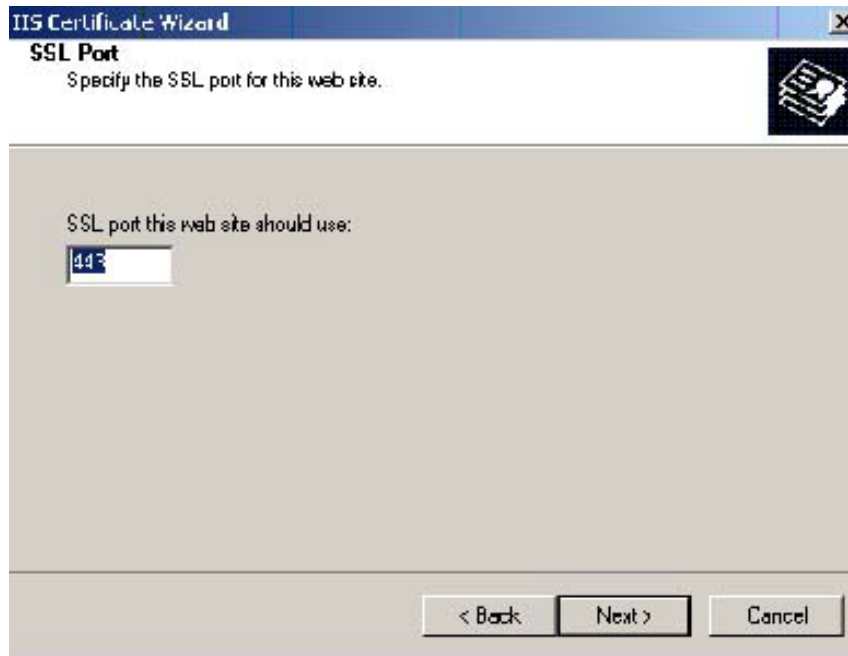
- 3 Click **Next**. The **IIS Certification Wizard** is displayed.



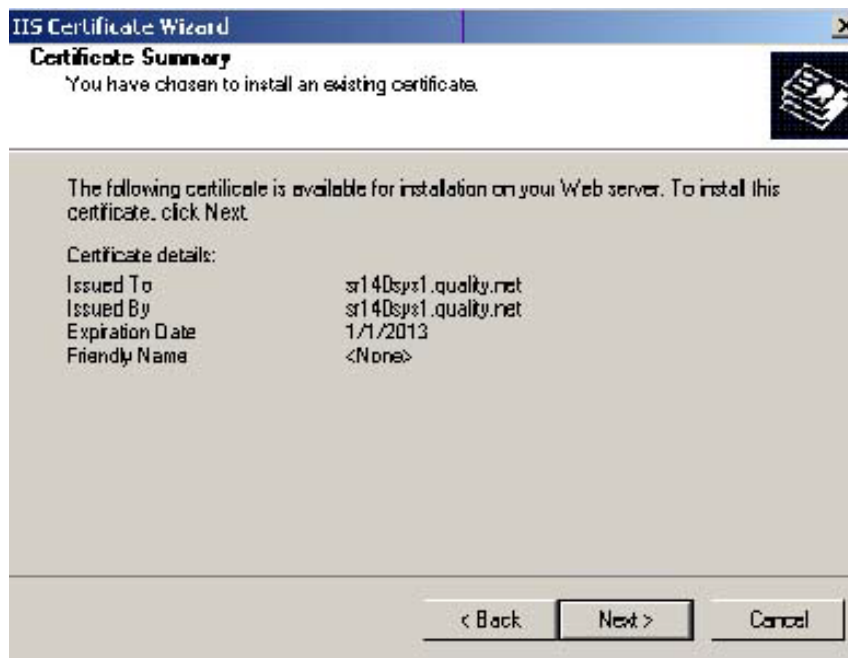
- 4 Select **Assign an existing certificate**. Click **Next**. The certificate created using MakeCert.exe is displayed.



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

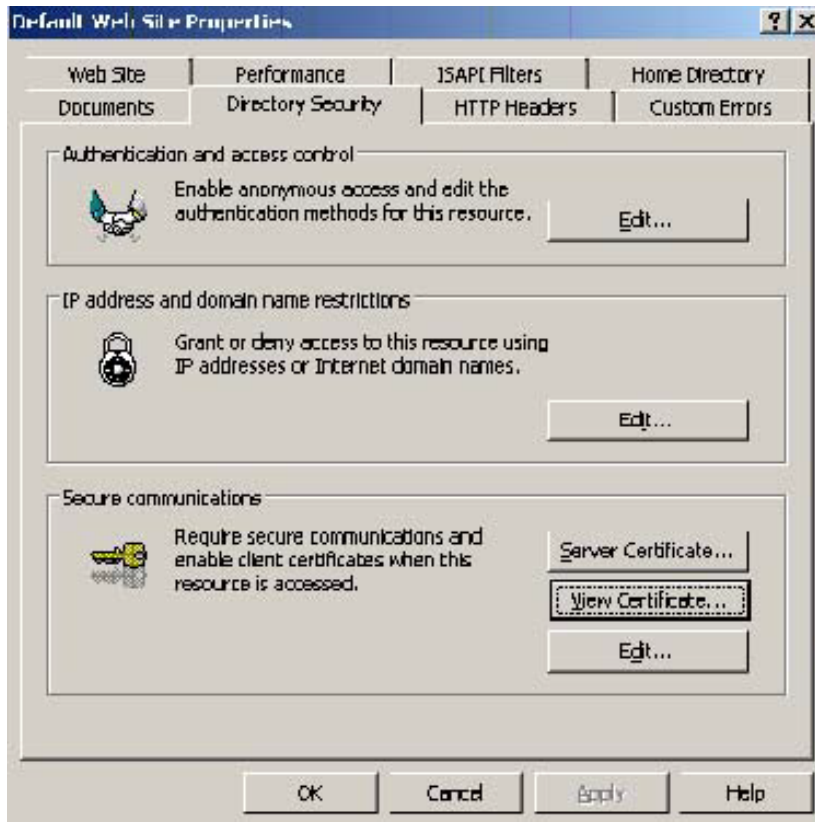


- 6 The port selected should be **443**. Click **Next**. The **Certificate Summary** is displayed.



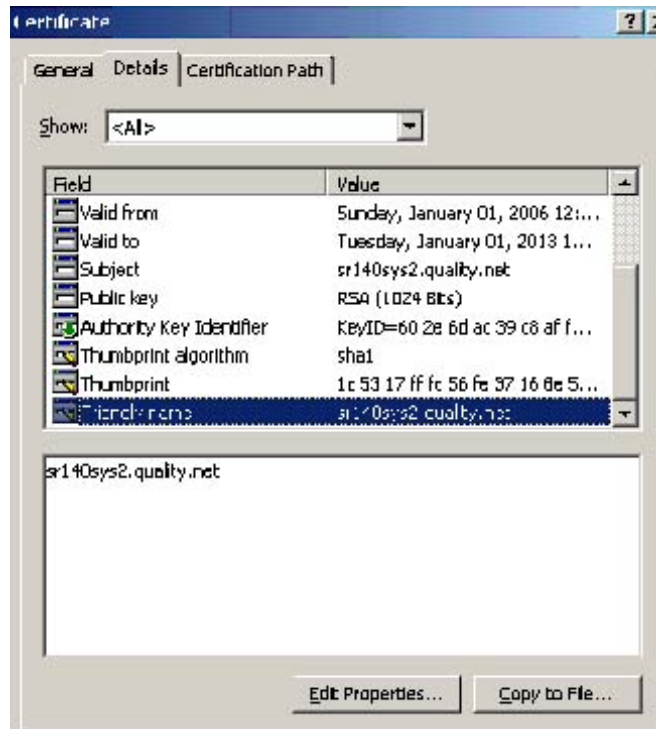
- 7 Click **Next**. A message indicates that the Web Server Certificate wizard is completed.
- 8 Click **Finish**. You are returned to the **Directory Security** page.
- 9 Export the certificate:
 - a Open IIS\local machine and navigate to the **Default Web Site** node.

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

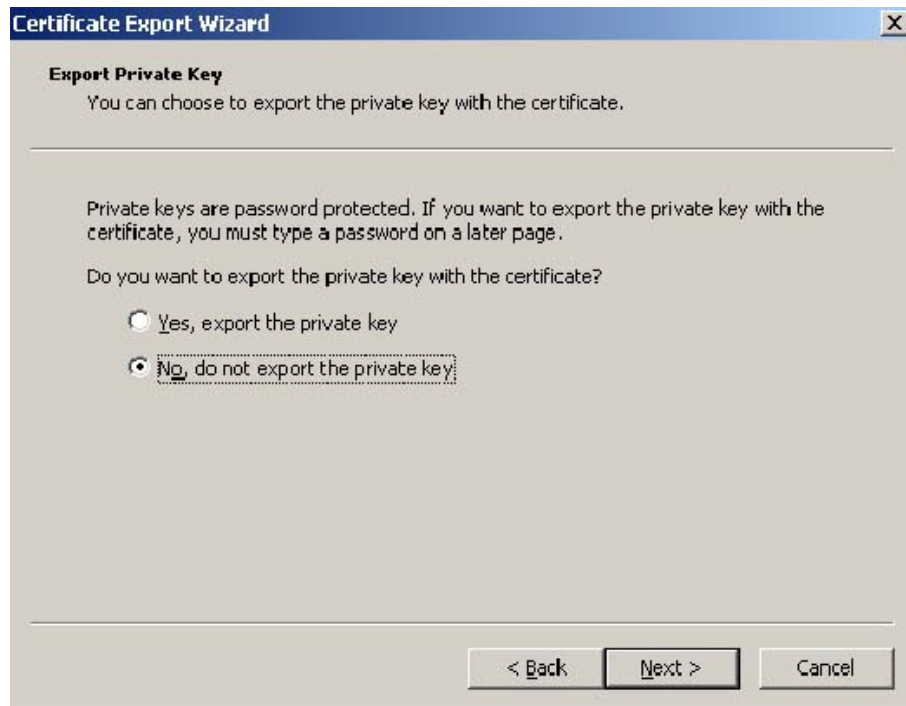


- e In the **Secure communications** section, click the **View Certificate** button.

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



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



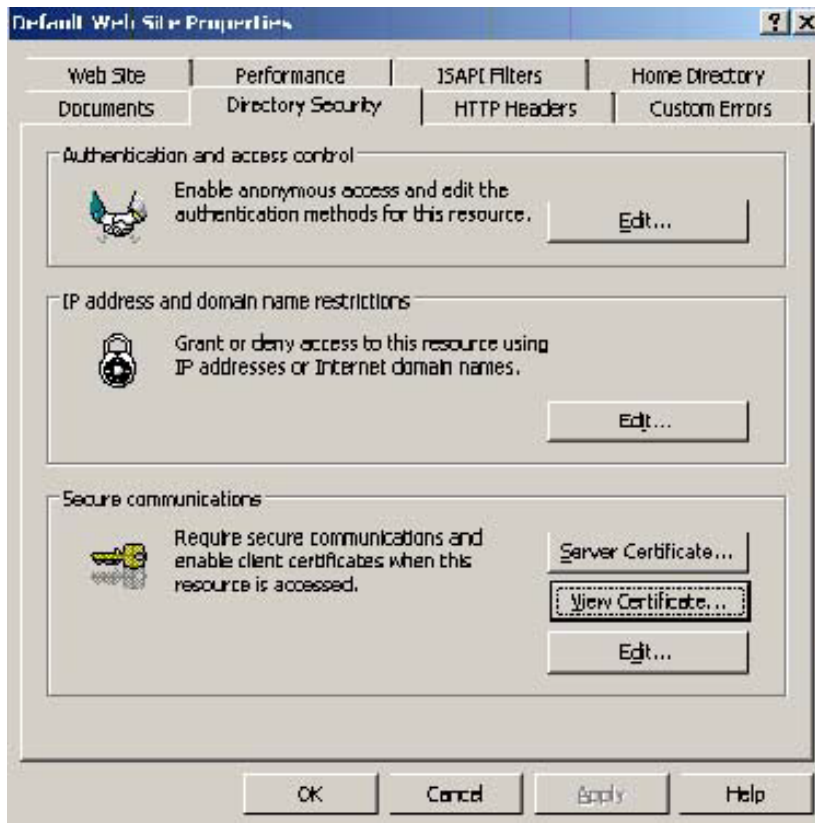
- i Select **No, do not export the private key** and click **Next**. The **Export File Format** page is displayed.



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

Requiring SSL for web sites

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



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



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

Editing the OmISAPIU.xml file

- 1 Navigate to the following path.
`C:\Program Files (x86)\Omtool\Omtool Server\WebAPI\WebAPI\Scripts`
- 2 In OmISAPIU.xml, find the FileTransfer node. Replace the IP address with the fully qualified domain name. Also, change `http` to `https`.

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

Note XML files can be edited using Microsoft Notepad.

- 3 Save the file.

Editing the Bootstrap.xml file

- 1 Navigate to the following path.

For HP OXPd v1.6:

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

For HP OXPd v1.4:

```
C:\Program Files (x86)\Omtool\OXPl.4\Configuration
```

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

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

- 3 Save the file.
- 4 Reset IIS.

Appendix B: Configuration for HTTPS Support