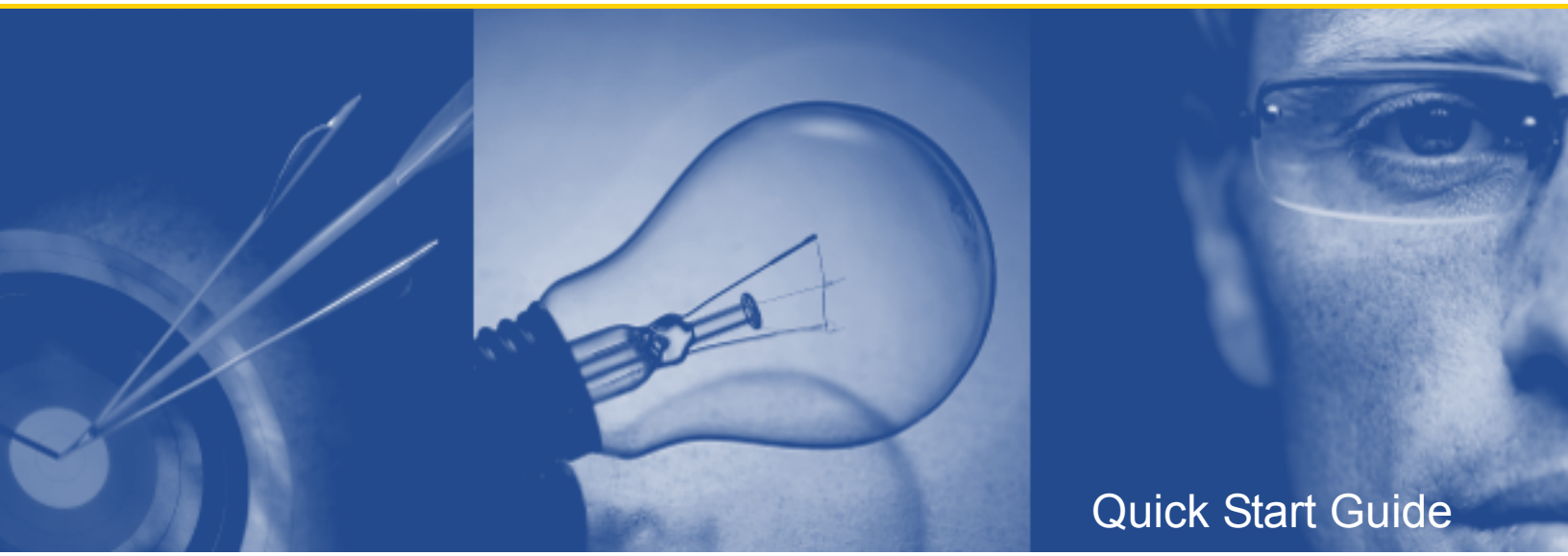
QUEST SOFTWARE®

# Quest® ActiveRoles Server 6.1



## Quick Start Guide

Quest ActiveRoles Server - Quick Start Guide
Updated - October 10, 2008
Software Version - 6.1

# CONTENTS

# Intended Audience

This document has been prepared to assist you in becoming familiar with the Quest ActiveRoles Server. The Quick Start Guide contains the information required to install and use the Quest ActiveRoles Server. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

# Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

| ELEMENT | CONVENTION |
|---|---|
| Select | This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons. |
| **Bolded text** | Interface elements that appear in Quest Software products, such as menus and commands. |
| *Italic text* | Used for comments. |
| ***Bold Italic text*** | Used for emphasis. |
| Blue text | Indicates a cross-reference. When viewed in Adobe® Reader®, this format can be used as a hyperlink. |
|  | Used to highlight additional information pertinent to the process being described. |
|  | Used to provide Best Practice information. A best practice details the recommended course of action for the best result. |
|  | Used to highlight processes that should be performed with care. |
| + | A plus sign between two keystrokes means that you must press them at the same time. |
| \| | A pipe sign between elements means that you must select the elements in that particular sequence. |

# About Quest Software

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases, and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate, and secure Active Directory, Exchange and Windows, as well as integrate Unix and Linux into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

## Contacting Quest Software

| | |
|---|---|
| Email | info@quest.com |
| Mail | Quest Software, Inc.<br>World Headquarters<br>5 Polaris Way<br>Aliso Viejo, CA 92656<br>USA |
| Web site | www.quest.com |

Please refer to our Web site for regional and international office information.

## Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.

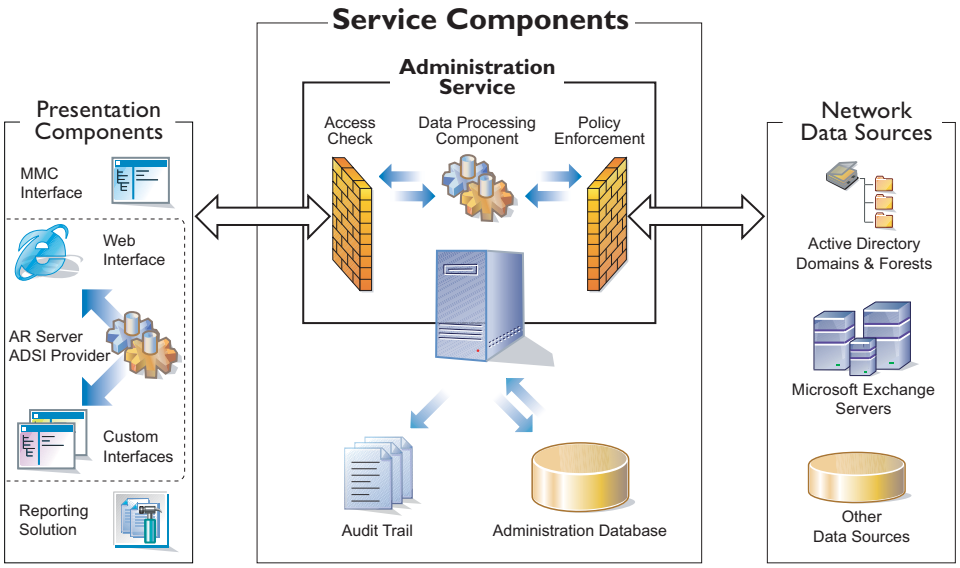
# Introduction

Quest ActiveRoles Server is an advanced administrative platform that facilitates administration and provisioning for Active Directory and Exchange. ActiveRoles Server enables organizations to implement a flexible administration framework that suits their needs, while ensuring secure delegation of tasks, reduced workload, and lower costs. It also enables the integration of diverse corporate data sources and provisioning processes, which can expedite business workflow and eliminate data inconsistencies.

This document is for individuals responsible for deploying ActiveRoles Server in their organization. It provides step-by-step instructions for preparing the environment and installing the ActiveRoles Server components.

## ActiveRoles Server Components

ActiveRoles Server divides the workload of directory administration into three functional layers: presentation components, service components, and network data sources.




The presentation components include client interfaces for the Windows platform and the Web, which allow users with appropriate rights (delegated administrators) to perform a precisely defined set of administrative activities. ActiveRoles Server also includes the reporting solution to generate reports on the administrative activities.

The service components constitute a secure layer between administrators and managed data sources. It ensures consistent policy enforcement, provides automation capabilities, and enables the integration of business processes for administration of Active Directory, Exchange and other corporate data sources.

The main component of ActiveRoles Server is the Administration Service—a powerful rules-based proxy for the management of network data sources. The Administration Service features advanced delegation capabilities and provides the ability to enforce administrative policies that keep data current and accurate. The Administration Service acts as a bridge between the presentation components and network data sources. In large networks, multiple Administration Services can be deployed to improve performance and ensure fault tolerance.

The Administration Service uses the Administration Database to store configuration data. The configuration data includes definitions of objects specific to ActiveRoles Server, assignments of administrative roles and policies, and procedures used to enforce policies.

The Administration Service provides a complete audit trail by creating records in ActiveRoles Server's event log. The log shows all actions performed and by whom, including actions that were not permitted. The log entries display the success or failure of each action, as well as which attributes were changed while managing objects in data sources.

# System Requirements

ActiveRoles Server includes the following components:

- Administration Service
- Console (MMC Interface)
- Web Interface
- Collector
- Report Pack

The ActiveRoles Server Release Notes document, included on the ActiveRoles Server distribution CD, provides information on hardware and software requirements for each of these components.

# Licensing

The ActiveRoles Server license specifies the maximum number of enabled user accounts in all managed domains. When starting, adding a managed domain, or removing a managed domain, the Administration Service counts the actual number of enabled user accounts, and compares it to the maximum number specified by the license. If the actual number exceeds the maximum number, a license violation occurs.

ActiveRoles Server bases its used license count by calculating the number of enabled user accounts in your managed domains. Once the license count exceeds the maximum number of user accounts specified in your license, a license violation occurs. In this case, a warning message is displayed on every start of the ActiveRoles Server console or connection to the Web Interface.

In the event of a license violation, you have the following options:

- Disable a sufficient number of user accounts to bring your license count under the licensed value. After that, restart the Administration Service (*net stop arssvc*, then *net start arssvc*) to recalculate the license count.
- Remove one or more managed domain to decrease your license count.
- Purchase a new license, with a greater number of user accounts. Then, update your license using the instructions provided later in this section.

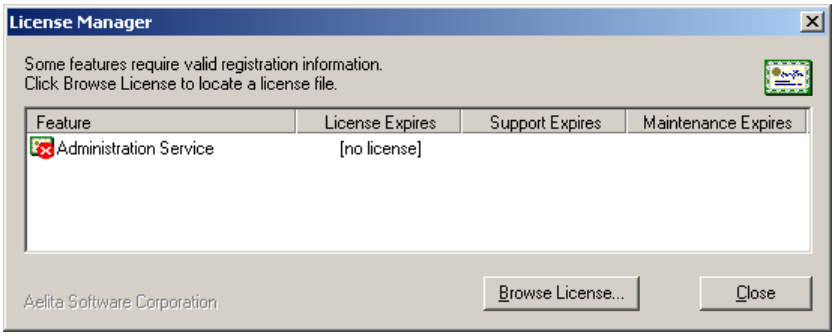
Note that the following items are not limited by the license:

- The number of delegated administrators (Trustees).
- The number of computers running the ActiveRoles Server user interfaces.
- The number of Administration Services—in a large enterprise, the Administration Service can be installed on multiple computers for enhanced performance and fault tolerance.

# Installing the License

The license is initially installed when you install the Administration Service:

1. In the Installation Wizard, click **Licenses** to display the **License Manager** dialog box:




2. Click **Browse License**, locate and open your license key file using the **Open** dialog box, and then click **Close**.

# Updating the License

If you have purchased a new license, you need to update the license by installing the new license key file. You can use the ActiveRoles Server console to install the file.

***To update the license***

1. Right-click the console tree root, click **About**, and then click **Update License**.
2. Use the **Open** dialog box to locate and open your license key file.

# Installing the Administration Service

Use the following checklist to ensure that you are ready to install the Administration Service.

| ITEM TO CHECK | DESCRIPTION |
|---|---|
| Administration Service computer | The Administration Service can be installed on any computer that meets the hardware and software requirements.<br><br>It is not mandatory to install the Administration Service on a domain controller. However, the Administration Service computer must have reliable network connections with at least one of the domain controllers for each managed domain. |
| SQL Server | The Administration Service requires Microsoft SQL Server. It is possible to use SQL Server on the Administration Service computer or on a different network computer. |
| Administration Service account | The Administration Service logs on with the account that you specify during installation. The account must have sufficient rights for ActiveRoles Server to function properly.<br><br>ActiveRoles Server uses the Administration Service account when accessing a managed domain unless an override account is specified when registering the domain with ActiveRoles Server. Therefore, the Administration Service account must have the appropriate rights in any domain for which an override account is not specified.<br><br>Additionally, the Administration Service account must have sufficient permissions to publish the Administration Service in Active Directory.<br><br>Information about how to configure the Administration Service account and an override account can be found later in this document. |
| Account used for connection to SQL Server | When installing the Administration Service you may configure it to use Windows authentication or SQL Server authentication for connection to SQL Server.<br><br>If you choose Windows authentication, the connection is established using the Administration Service account. In this case, the service account must be a member of the **sysadmin** role on SQL Server.<br><br>If you choose SQL Server authentication, the connection is established with the login you are prompted to specify when installing the Administration Service. This login must be a member of the **sysadmin** role on SQL Server.<br><br>For more information on what permissions must be granted to the account for connection to SQL Server, refer to the "Access to SQL Server" section later in this document. |
| AR Server Admin | AR Server Admin is a group for which ActiveRoles Server does not perform permission checking. If the Administration Service itself has sufficient rights to perform a certain task, then AR Server Admin can also perform that task using ActiveRoles Server.<br><br>In addition, AR Server Admin is authorized to perform any task related to the ActiveRoles Server configuration, such as adding managed domains and managing replication settings. Therefore, the membership in the AR Server Admin group should be restricted to highly trusted individuals.<br><br>By default, AR Server Admin is the Administrators local group on the computer running the Administration Service. You can change this setting when installing the Administration Service. |
| License key file | The Administration Service requires a valid license key file issued by Quest Software. This file contains the license information, and defines the maximum number of enabled user accounts in all domains registered with ActiveRoles Server (managed domains). |

# Configuring the Administration Service Account

When installing the Administration Service, you are prompted for the name and password of the Administration Service account—the account the Administration Service logs on to. This account must have sufficient permissions to:

- Gain administrative access to the computer running the Administration Service.
- Publish the Administration Service in Active Directory.
- Access any managed domain for which an override account is not specified.

When registering a domain with ActiveRoles Server, an override account may be specified. If an override account is specified, this account rather than the service account is used to access the domain.

## Access to the Administration Service Computer

The service account must be a member of the Administrators group on the computer running the Administration Service. Because of this requirement, installing the Administration Service on a domain controller effectively grants the service account administrator rights in the entire domain.

## Service Publication in Active Directory

The Administration Service must be able to publish itself in Active Directory. This enables ActiveRoles Server clients to automatically discover the Administration Service. Service publication requires that the service account have the following permissions on the **Aelita** sub-container of the **System** container in the domain of the computer running the Administration Service:

- Create Container Objects
- Create serviceConnectionPoint Objects

In addition, the service account, or the override account, if specified, must have these permissions on the **Aelita** sub-container of the **System** container in every managed domain. If an account has the domain administrator rights, then it has the required permissions by default. Otherwise, you must give these permissions to the account using the ADSI Edit tool.

***To grant permissions for Administration Service publication in Active Directory***

1. Open the ADSI Edit tool and connect to the Domain naming context.
2. In the console tree, expand the **System** container, right-click the **Aelita** sub-container, and then click **Properties**.

   *If the **Aelita** container does not exist, create it: right-click **System**, point to **New**, click **Object**, and then, in the Create Object wizard, select the Container class and specify **Aelita** as **cn**.*
3. On the **Security** tab in the **Properties** dialog box, click **Advanced**.
4. On the **Permissions** tab in the **Advanced Security Settings** dialog box, click **Add**.
5. In the **Select User, Computer, or Group** window, enter the name of the account.
6. On the **Object** tab in the **Permission Entry** dialog box, ensure that the **Apply onto** box indicates **This object and all child objects**, and then, in the **Permissions** box, select the check boxes next to **Create Container Objects** and **Create serviceConnectionPoint Objects** in the **Allow** column.
7. In the **Permission Entry** dialog box, click **OK**.

## Access to Managed Domains

ActiveRoles Server access to a domain is limited by the access rights of the service account, or the override account, if specified. For all managed domains with no override accounts specified, you should configure the service account to have permissions you want ActiveRoles Server to have in those domains.

For example, you may configure the service account to have full control of specified organizational units. In this way, ActiveRoles Server's administrative scope is limited to those units. Another option is to give ActiveRoles Server administrative access to a domain by adding the account to the Domain Admins group of that domain, or give ActiveRoles Server administrative access to an entire forest by adding the account to the Domain Admins group of the forest root domain.

In addition, the service account must meet the following requirements:

- Unless the domain functional level of the managed domain is raised to Windows Server 2003 or higher, the account must have the **Replicate Directory Changes** permission on both the Domain and Configuration naming contexts—this permission can be granted using the ADSI Edit tool (see later in this section).

  If the domain functional level of the managed domain is Windows Server 2003 or higher, and the Administration Service is running on Windows Server 2003 or later, then ActiveRoles Server retains its functionality regardless of whether the service account has the **Replicate Directory Changes** permission.
- The account must be allowed have the **Read Permissions** and **Modify Permissions** rights on the Active Directory objects and containers where you are planning to use the ActiveRoles Server security synchronization feature.

If you use an override account when registering a domain with ActiveRoles Server, ensure that the override account has these permissions for the domain. The service account does not need these permissions for the domains with override accounts specified.

If the domain functional level of the managed domain is lower than Windows Server 2003, you need to ensure that the service account has the **Replicate Directory Changes** permission regardless of whether an override account is used to access that domain.

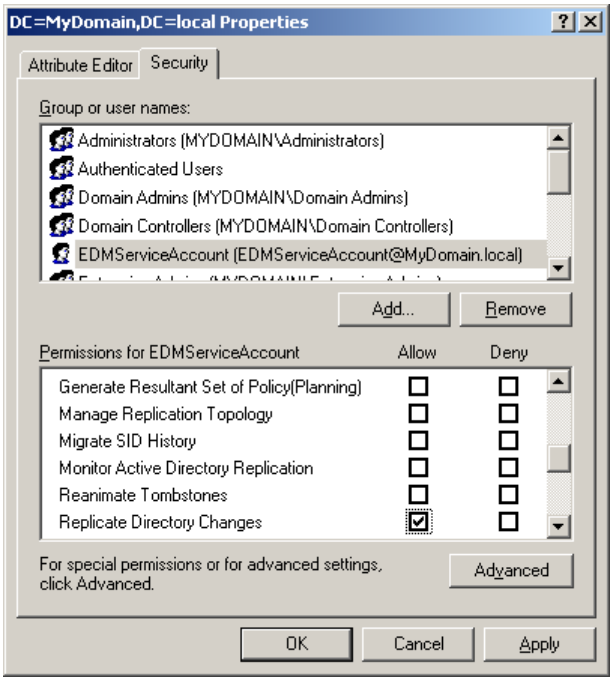
By default, the **Replicate Directory Changes** permission on the Domain and Configuration naming contexts is granted to the Enterprise Admins group of any domain, and to the Administrators and Domain Admins groups of the forest root domain. The Administrators and Domain Admins groups of a domain other than the forest root domain have this permission only on the Domain naming context. If the account is not a member of any group that has the **Replicate Directory Changes** permission by default, you should manually give that permission to the account.

You can give an account the **Replicate Directory Changes** permission using the ADSI Edit tool as follows.

***To grant the Replicate Directory Changes permission***

1. Open the ADSI Edit tool and connect to the Domain naming context and to the Configuration naming context of the domain.
2. In the console tree, select **Domain**.
3. In the details pane, right-click the domain object, and then click **Properties**.
4. On the **Security** tab in the **Properties** dialog box, click **Add**.
5. In the **Select Users, Computers, or Groups** window, enter the name of the account, and then click **OK**.

6. In the **Permissions** box, select the **Replicate Directory Changes** check box (in Windows 2000 Server, the **Replicating Directory Changes** check box), as shown in the following figure.




7. In the **Properties** dialog box, click **OK**.
8. In the console tree, select **Configuration**.
9. Repeat Steps 3–7.

## Access to Exchange Organization

### Exchange Server 2000/2003

The **Move Mailbox** task requires the Exchange System Management Tools on the computer running the Administration Service. The other Exchange tasks do not require the System Management Tools. To install the System Management Tools, run **Setup.exe** located on the Exchange Server 2003 CD, click **Exchange Deployment Tools**, and then click **Install Exchange System Management Tools Only** in the **Welcome to the Exchange Server Deployment Tools** dialog box.

To enable ActiveRoles Server to perform Exchange-related tasks in an Exchange Server 2000/2003 organization, the **Exchange View-only Administrator** role must be assigned to the service account if an override account is not used. With an override account, the role must be assigned to the override account. The **Move Mailbox** task requires that the **Exchange Administrator** role be assigned either to the service account (if no override account is used) or to the override account.

A role can be assigned using the Exchange Administration Delegation wizard. To start the wizard, select the Exchange organization in the Exchange System Manager tool, and then, on the **Action** menu, click **Delegate Control**.

The service account (or the override account) must also have Read and Write access to certain attributes in Active Directory, depending on the task. You can use the following links to view the comprehensive lists of those attributes grouped by task:

- Mailbox-enabling user objects (http://technet.microsoft.com/en-us/library/aa997743.aspx)
- Moving mailboxes (http://technet.microsoft.com/en-us/library/aa998937.aspx)
- Mailbox-disabling user objects (http://technet.microsoft.com/en-us/library/bb123963.aspx)
- Mail-enabling user objects (http://technet.microsoft.com/en-us/library/aa997755.aspx)
- Mail-disabling user objects (http://technet.microsoft.com/en-us/library/aa998758.aspx)
- Removing Exchange attributes on user objects (http://technet.microsoft.com/en-us/library/bb124311.aspx)
- Mail-enabling group objects (http://technet.microsoft.com/en-us/library/bb124806.aspx)
- Mail-disabling group objects (http://technet.microsoft.com/en-us/library/aa997217.aspx)
- Hiding group membership (http://technet.microsoft.com/en-us/library/bb124033.aspx)
- Removing Exchange attributes on group objects (http://technet.microsoft.com/en-us/library/aa998951.aspx)
- Mail-enabling contact objects (http://technet.microsoft.com/en-us/library/bb123562.aspx)
- Mail-disabling contact objects (http://technet.microsoft.com/en-us/library/bb123846.aspx)
- Removing Exchange attributes on contact objects (http://technet.microsoft.com/en-us/library/aa996633.aspx)

For more information, refer to the "Working with Active Directory Permissions in Exchange Server 2003" guide at http://technet.microsoft.com/en-us/library/bb124223.aspx

### Exchange Server 2007

In order to manage Exchange recipients (users, groups, or contacts) in an Exchange Server 2007 Organization, the Administration Service must:

- Run in the Active Directory forest in which the Exchange Organization is deployed. Install the Administration Service on a server belonging to any domain in that forest.
- Use the service account rather than an override account to access every domain that holds the Exchange recipients to manage. When registering such a domain with ActiveRoles Server, choose the option to access the domain using the service account information that the Administration Service uses to log on.

In addition, the Exchange Server management tools must be installed on the computer running the Administration Service, and the service account must be configured so that it has the appropriate rights in the Exchange Organization.

***To install the Exchange management tools***

1. Insert the Exchange Server 2007 DVD into the DVD drive. If Setup.exe does not start automatically, navigate to the DVD drive and double-click **Setup.exe**.
2. Follow the instructions on the Exchange Server 2007 Setup pages.
3. On the **Installation Type** page, click **Custom Exchange Server Installation**.
4. On the **Server Role Selection** page, select the **Management Tools** check box. Leave the other check boxes cleared.
5. Follow the instructions on the Exchange Server 2007 Setup pages to complete the installation.

Next, you need to configure the service account. If the Administration Service is already installed and running, you should restart it after you have changed the configuration of the account: at a command prompt, enter **net stop arssvc** to stop the service, and then enter **net start arssvc**.

***To configure the service account***

1. Delegate **Exchange Recipient Administrator** role to the account on every Exchange Server.
2. If you plan to perform the Move Mailbox task using ActiveRoles Server, delegate **Exchange Server Administrator** role to the account and add the account to the **Administrators** local group on every Exchange Server.

   *For instructions on how to delegate an administrator role to a user or group, see help topics in the Exchange Management Console.*
3. Ensure that the account has read/write permission on the attributes listed in the following table. For example, you might add the account to a domain privileged security group, such as the **Account Operators** group.

The attributes in the table below are the data that is provided to end-users via Outlook in the Global Address List (GAL).

| APPLIES TO | ATTRIBUTE | DESCRIPTION |
|---|---|---|
| User, Contact | givenName | First name |
| User, Contact | initials | Middle initial |
| User, Contact | sn | Last name |
| User, Contact | info | Notes field |
| User, Contact | streetAddress | Street address |
| User, Contact | l | City |
| User, Contact | st | State/Province |
| User, Contact | postalCode | ZIP/Postal code |
| User, Contact | countryCode | Country/Region |
| User, Contact | telephoneNumber | Business phone |
| User, Contact | otherTelephoneNumber | Alternative business phone |
| User, Contact | pager | Pager |
| User, Contact | facsimileTelephoneNumber | Fax |
| User, Contact | homePhone | Home phone |
| User, Contact | otherHomePhone | Alternative home phone |
| User, Contact | mobile | Mobile phone |
| User, Contact | otherfacsimileTelephoneNumber | Alternative fax |
| Contact | telephoneAssistant | Assistant phone |
| Contact | telephoneAssistant | Assistant phone |
| User, Contact | title | Title |
| User, Contact | company | Company |

| | | |
|---|---|---|
| User, Contact | department | Department |
| User, Contact | physicalDeliveryOfficeName | Office |
| User, Contact | manager | Manager |
| User, Contact | directReports | Direct reports |
| User, Contact | msExchAssistantName | Assistant name |
| Group | managedBy | Group owner |
| Group | info | Notes field |

## Access to File Servers

To enable ActiveRoles Server to perform the provisioning and deprovisioning tasks related to user home folders and home shares, the service account (or the override account, if specified) must belong to the Server Operators or Administrators group on each file server that hosts the user home folders to be administered by ActiveRoles Server.

ActiveRoles Server provides the following policy categories to automate the management of user home folders and home shares:

- **Home Folder AutoProvisioning** Performs the provisioning actions needed to assign home folders and home shares to user accounts, including the creation of home folders for newly created user accounts and renaming home folders upon renaming of user accounts. Specifies the server on which to create home folders and shares, and configures access rights to the newly created home folders and shares.
- **Home Folder Deprovisioning** Makes the changes needed to prevent deprovisioned users from accessing their home folders, including the removal of the user's permissions on the home folder, changing the ownership of the home folder, and deleting the home folder when the user account is deleted.

The service account or override account must be configured so that it has sufficient rights to perform the operations provided for by those policies: create, modify (including the ability to change permission settings and ownership), and delete folders and shares on the designated file servers.

You can give the required permissions to the service account or override account by adding that account to the appropriate administrative group (Administrators or Server Operators) on each file server where you are planning ActiveRoles Server to manage user home folders.

## Access to SQL Server

In some scenarios, you may want to grant the Administration Service the minimum permissions on SQL Server that are required for the ActiveRoles Server to operate properly. This section describes the necessary permissions, depending on the following factors:

- Authentication mode used by the Administration Service when connecting to SQL Server
- SQL Server’s role in the ActiveRoles Server replication environment—Publisher or Subscriber

The section also provides a reference to Microsoft’s documentation with recommendations on setting up Windows service accounts for the SQL Server and SQL Server Agent services. You should follow those recommendations when installing and configuring Microsoft SQL Server for use with ActiveRoles Server.

The following recommendations are applicable regardless of the authentication mode (SQL Server or Windows) that the Administration Service uses when connecting to SQL Server:

- The SQL Server service may be configured to log on as the Local System account—this setting is applied by default when installing SQL Server.
- If SQL Server is designated as the Publisher, the SQL Server Agent service must be up and running on that SQL Server.
- If SQL Server is designated as a Subscriber, the SQL Server Agent service may be stopped, disabled, or removed altogether from that SQL Server.
- Service account privileges and registry-related permissions are to be assigned following Microsoft's recommendations, outlined in SQL Server Books Online (see Setting up Windows Services Accounts in SQL Server Books Online).

The following sections elaborate on the requirements that vary depending on the authentication mode and replication-related role of SQL Server.

### Administration Service Permissions on SQL Server

The Administration Service may be configured to use either SQL Server authentication or Windows authentication:

- With SQL Server authentication, the Administration Service provides the SQL Server login and password when connecting to SQL Server. The name and password of that login are specified when installing the Administration Service.
- With Windows authentication, the Administration Service connects to SQL Server in the security context of the Administration Service account. The name and password of that account is specified when installing the Administration Service.

If the Administration Service uses SQL Server authentication, the SQL Server login must belong to the **sysadmin** fixed server role on SQL Server used by that Administration Service.

If the Administration Service uses Windows authentication, the Administration Service account must belong to the **sysadmin** fixed server role on SQL Server used by that Administration Service.

### Publisher Permissions on Subscriber SQL Server

If the Administration Service uses SQL Server that is designated as the Publisher, the Administration Service account may need certain permissions on SQL Server that is designated as a Subscriber. This depends on whether a Subscriber uses Windows authentication or SQL Server authentication.

If a Subscriber uses SQL Server authentication, the Administration Service account of the Publisher does not need any permissions on the Subscriber SQL Server.

If a Subscriber uses Windows authentication, the Administration Service account of the Publisher needs certain permissions on that Subscriber:

- On the Subscriber SQL Server, the Administration Service account must belong to the **db_owner** database role of the Subscriber database.
- Alternatively, the Administration Service account may belong to the **sysadmin** fixed server role on the Subscriber SQL Server.

The Administration Service account of the Publisher must meet this requirement on each Subscriber that uses Windows authentication.

### SQL Server Agent Permissions

If SQL Server is designated as the Publisher, the SQL Server Agent service must be up and running on that SQL Server.

If all of the Publisher's Subscribers use SQL Server authentication, the SQL Server Agent service may be configured to log on as Local System.

The situation changes if the Publisher has Subscribers that use Windows authentication. In this case, the SQL Server Agent service must be configured to log on as a domain user account that meets the following requirement:

- On the Subscriber SQL Server, the account must belong to the **db_owner** database role of the Subscriber database.
- Alternatively, the account may belong to the **sysadmin** fixed server role on the Subscriber SQL Server.

The logon account of the Publisher SQL Server Agent service must meet this requirement on each Subscriber that uses Windows authentication.

# Steps to Install the Administration Service

ActiveRoles Server requires Microsoft .NET Framework 3.5 or later. You can use the following instructions to update Microsoft .NET Framework on your server.

***To update Microsoft .NET Framework***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **Redistributables**.
3. On the **Redistributables** page, click **.NET Framework 3.5 SP1**.
4. Follow the instructions in the Installation Wizard.

The Administration Service requires Microsoft SQL Server. SQL Server may be installed on the Administration Service computer or on a different network computer. If you do not have Microsoft SQL Server deployed in your environment, you can install Microsoft SQL Server 2005 Express Edition from the ActiveRoles Server CD.

***To install Microsoft SQL Server 2005 Express Edition***

1. On the **Redistributables** page in the ActiveRoles Server CD **Autorun** window, click **SQL Server Express**.
2. Follow the instructions in the Installation Wizard.

Now that you have access to SQL Server, you can install the Administration Service. The installation procedure depends on whether your computer already has the Administration Service installed.

The following steps provide the guidance on how to install the Administration Service on a computer with no Administration Service installed. If you have the Administration Service installed on your computer, you should use the instructions given later in this document (see "Upgrading the Administration Service").

***To install the Administration Service***

1. In the ActiveRoles Server CD **Autorun** window, click **ActiveRoles Server**, and then click **Administration Service (with Resource Kit)** in the **ActiveRoles Server Components** list.
2. Follow the instructions in the Installation Wizard.
3. On the **User Information** page, click **Licenses** to install the license key file (see "Installing the License" earlier in this document).
4. On the **Select Features** page, ensure that the **Administration Service** feature is selected for installation.
5. On the **Service Account Information** page, enter the name and password of the domain user account to be used as the Administration Service account.
6. On the **AR Server Admin Account** page, accept the default account, or click **Browse** and select the group or user to be designated as AR Server Admin.
7. If the **Distributed COM Security Configuration** page appears, click either **Yes** or **No**.

   *This page may appear if the computer is running Windows Server 2003 SP1 or later, indicating that remote clients will not be able to access the Administration Service unless they have local administrator rights or belong to the Distributed COM Users group on this computer.*

   *If you click **Yes**, Setup adds Authenticated Users to the Distributed COM Users group, thereby enabling any authenticated client to remotely access the Administration Service on this computer.*

   *If you click **No**, you will have to manually add the appropriate user accounts to the Distributed COM Users group on this computer as needed. Remote clients that do not have local administrator rights must run in the security context of a member of that group in order to access the Administration Service.*
8. On the **Service Deployment Options** page, select the appropriate option, and then follow the instructions in the Installation Wizard.

The deployment options along with the remaining steps of the Installation Wizard are related to setting up the database that will hold configuration data of the Administration Service you are installing. These options and the corresponding steps are discussed in the sections that follow.

## Installing Initial Service

This section discusses the database-related steps of the Installation Wizard in the assumption that you are installing the first Administration Service in your environment.

***To install initial Service***

1. On the **Service Deployment Options** page, click **Install initial Service**.
2. On the **Database and Connection Settings** page, complete the **Database** area:
   a) In **SQL Server**, type the name of SQL Server in the form <*Computer*>\<*Instance*> (for named instance) or <*Computer*> (for default instance). Setup will create the database on the SQL Server instance you specify.
   b) In **Database name**, type a name for the database to be created.
3. Complete the **Connection** area:
   - To have the new Administration Service connect to SQL Server using the Administration Service account, click **Use Windows authentication**.
   - To have the new Administration Service connect to SQL Server using a SQL Server login, click **Use SQL Server authentication** and type the login name and password.

4. On the **Configuration Database Summary** page, review the database and connection settings you are going to use.
5. Complete the **Backup of Encryption Keys** page, as described later in this section (see "Backup of Encryption Keys").
6. Follow the instructions in the wizard to complete the installation.

### Backup of Encryption Keys

When creating the database, the Setup program generates a key set that the Administration Service will use to encrypt data in the database. The key set is specific to the database.

You should save a backup copy of the encryption keys to a file and keep it in a secure location for database reuse, and for maintenance and troubleshooting procedures. You need a backup copy of the encryption keys when moving the Administration Service to another environment while preserving its configuration, or when restoring the database from a backup.

On the **Backup of Encryption Keys** page, the Installation Wizard prompts you to specify a file in which to save a copy of the encryption keys. You have the option to use password protection for that file.

***To create a backup copy of encryption keys***

1. On the **Backup of Encryption Keys** page, click the **Browse** button to specify the file name and location.

   *When creating the database, the Installation Wizard will export the database encryption keys to that file.*

2. Optionally, select the **Use password protection for this file** check box, and then type and confirm a password.

   *You will have to enter the specified password whenever you need to restore the keys from the file. If you lose or forget the password, it cannot be recovered.*

## Installing Additional Service

This section discusses the database-related steps of the Installation Wizard in the following assumptions:

- You have at least one Administration Service version 6.1 up and running in your environment.
- You are installing one more Administration Service for load distribution and fault tolerance.

***To install additional Service***

1. On the **Service Deployment Options** page, click **Install additional Service**.
2. On the **Configuration Synchronization Options** page, click one of the following options, depending on how you want to synchronize the configuration of the new Administration Service with the configuration of the existing Administration Services:
   - **Share common configuration database** Lets the new Administration Service use the database of an existing Administration Service so that the new Administration Service has the same configuration as the existing one.
   - **Create new database, to be synchronized via replication** After installing the Administration Service, you will need to set up ActiveRoles Server replication for the new Administration Service to have the same configuration as existing ones.

3. If you have selected the option **Share common configuration database**, follow the instructions provided later in this section (see "Using Common Configuration Database").
4. If you have selected the option **Create new database, to be synchronized via replication**, use the instruction provided in the previous section (see "Installing Initial Service") to complete the wizard.

   *The database created by this option holds the pristine configuration of the Administration Service. To update and synchronize the new database with the configuration data of the Administration Services that were earlier deployed in your environment, you need to use the replication function. For instructions on how to set up replication of configuration data, refer to the ActiveRoles Server Administrator Guide.*

## Using Common Configuration Database

By selecting the option **Share common configuration database** you set up the new Administration Service so that it connects to the database of an existing Administration Service. The newly installed Administration Service automatically becomes a replica of the existing one.

This option makes it possible to centralize configuration storage. You can deploy multiple Administration Services of the same configuration without having to synchronize multiple databases via replication. Rather, you have the option for multiple Administration Services to share configuration data held in a single database on centrally deployed SQL Server.

This option also ensures that the newly installed Administration Service can immediately be used as a replacement for the existing Administration Service. Switching between Administration Services is transparent to ActiveRoles Server users since both Administration Services have the same configuration.

***To have Administration Services use common configuration database***

1. On the **Configuration Synchronization Options** page, click **Share common configuration database**.
2. On the **Database and Connection Settings** page, in the **Database** area, specify the SQL Server and database being used by an existing Administration Service version 6.1.
3. On the **Database and Connection Settings** page, in the **Connection** area, select the appropriate authentication option:
   - To have the new Administration Service connect to SQL Server using the Administration Service account, click **Use Windows authentication**.
   - To have the new Administration Service connect to SQL Server using a SQL Server login, click **Use SQL Server authentication**, and type the login name and password.
4. On the **Configuration Database Summary** page, review the database and connection settings you are going to use.
5. Complete the **Provision of Encryption Keys** page, as described later in this section (see "Encryption Keys Provisioning").
6. Follow the instructions in the wizard to complete the installation.

## Encryption Keys Provisioning

In the configuration database, certain data is encrypted. For example, if an override account is specified for a managed domain, the credentials of that account are encrypted. To gain access to encrypted data, the newly installed Administration Service needs encryption keys.

The **Provision of Encryption Keys** page prompts you to choose how you want the new Administration Service to obtain the keys that are used to encrypt data in the specified database. You can choose from these options:

- **Retrieve keys from existing Service** The Setup program retrieves the keys and passes them to the Administration Service you are installing. You need to have at least one Administration Service up and running that uses the specified database.
- **Restore keys from a backup copy** You must provide the file to which the encryption keys were exported (see "Backup of Encryption Keys" in the "Installing Initial Service" section, earlier in this document).
- **Generate new keys** The Setup program generates new encryption keys for the database and passes them to the Administration Service you are installing. The encrypted data that was previously stored in the database is lost.

***To automatically provision encryption keys***

- On the **Provision of Encryption Keys** page, click **Retrieve keys from existing Service**.

***To restore encryption keys from a backup***

1. On the **Provision of Encryption Keys** page, click **Restore keys from a backup copy**.
2. On the **Restore of Encryption Keys** page, specify the file containing a backup copy of the encryption keys you need. If the file is password-protected, type the password.

***To generate new encryption keys***

1. On the **Provision of Encryption Keys** page, click **Generate new keys**.
2. On the **Backup of Encryption Keys** page, click the **Browse** button to specify the file name and location: a backup copy of the new encryption keys will be saved in that file.
3. Optionally, select the **Use password protection for this file** check box, and then type and confirm a password.

The new encryption keys are passed only to the Administration Service you are installing. The other Administration Services are not provided with the new keys, and therefore may need to be reconfigured. For example, generating new keys causes the existing Administration Services that use the database in question to lose the credentials of the override accounts for access to managed domains. As a result, you would have to re-register Active Directory domains with those Administration Services.

## Importing Configuration Data

When installing the Administration Service, you may need to import configuration data from an existing database in order to ensure that the newly installed Administration Service has the same configuration as the existing one. Importing configuration data to a newly created database instead of attaching the Administration Service to the existing database is necessary if the version of the Administration Service you are installing is greater than the version of the database you want to use. Some examples of such a situation are as follows:

- Restoring configuration data from a backup copy of the database whose version does not match the version of the Administration Service.
- Upgrading the Administration Service while preserving its configuration (see "Upgrading the Administration Service 5.2" later in this document).

The following instructions on how to import configuration data are applicable to any situation where you choose to create a new database when installing the Administration Service. In this case, the **Database and Connection Settings** page includes the option **Import data from this database** that is intended to direct the Setup program to copy the configuration data to the newly created database.

***To import configuration data***

1. In the **Database** area on the **Database and Connection Settings** page, select the **Import data from this database** check box.
2. In the box next to **Import data from this database**, type the name of the database from which you want to import data.

   *The source database must be located on SQL Server that hosts the database for the new Administration Service installation.*
3. In the **Connection** area, select the authentication mode you want the Administration Service to use on SQL Server.
4. On the **Configuration Database Summary** page, review the database and connection settings you are going to use.
5. On the **Import of Encrypted Data** page, choose whether to import the encrypted data from the source database.

   *Importing the encrypted data requires a backup copy of the encryption keys of the source database.*
6. If you have chosen to import the encrypted data, on the **Restore of Encryption Keys** page, specify the file containing a backup copy of the source database encryption keys. If the file is password-protected, type the password.
7. On the **Backup of Encryption Keys** page, specify where to store a backup copy of the encryption keys for the new database.
8. Follow the instructions in the wizard to complete the installation.

## Advanced Scenarios

This section discusses the database-related steps of the Installation Wizard in the following scenarios:

- Using the database of an earlier Administration Service installation
- Using a pre-created, blank database

To implement any of these scenarios, you should select the **Perform custom installation** option on the **Service Deployment Options** page in the Installation Wizard.

### Using the Database of an Earlier Administration Service Installation

When installing the Administration Service, you may need to have it use the database of an earlier installation of the Administration Service instead of creating a new database. The situations where the need arises to re-use an existing database include the following scenarios:

- Repairing the Administration Service installation by using **Add or Remove Programs** in Control Panel.
- Restoring the configuration database from a backup, and then reinstalling the Administration Service so that it uses the restored database.
- Installing a maintenance release of the Administration Service to update the existing Administration Service installation.

All of these scenarios presuppose that the database has the same version as the Administration Service you are installing. If the Administration Service version is greater than the database version, you should choose the option to create a new database and import data from the existing database (see "Importing Configuration Data" earlier in this document).

Assuming that the database has the same version as the Administration Service you are installing, you can use the following instructions to make the Administration Service use that database.

***To use the database of an earlier Administration Service installation***

1. On the **Service Deployment Options** page, click **Perform custom installation**.
2. On the **Configuration Storage Options** page, click **Database of an earlier installed Service**.
3. On the **Database and Connection Settings** page, specify SQL Server and the name of the database, and select the authentication mode you want the Administration Service to use on SQL Server.
4. On the **Configuration Database Summary** page, review the database and connection settings you are going to use.
5. Complete the **Provision of Encryption Keys** page by using the instructions given in the "Installing Additional Service" section earlier in this document (see "Encryption Keys Provisioning").
6. If you have chosen the option to generate new keys, use the **Backup of Encryption Keys** page to specify where to store a backup copy of the newly generated keys.
7. Follow the instructions in the wizard to complete the installation.

## Using a Pre-created, Blank Database

When creating a database, the Setup program uses default values for database properties, such as the location and other parameters of the database files and transaction log files. If you need to adjust these properties, you should first create a blank database with the parameters that meet your requirements, and then have the Setup program attach the database to the Administration Service you are installing. Assuming that the database is already created, you can use the following instructions to implement this scenario.

***To use a pre-created, blank database***

1. On the **Service Deployment Options** page, click **Perform custom installation**.
2. On the **Configuration Storage Options** page, click **Existing blank database**.
3. On the **Database and Connection Settings** page, specify SQL Server and the name of the database, and select the authentication mode you want the Administration Service to use on SQL Server.
4. On the **Configuration Database Summary** page, review the database and connection settings you are going to use.
5. On the **Backup of Encryption Keys** page, specify where to store a backup copy of the encryption keys that the Setup program will generate for the database.
6. Follow the instructions in the wizard to complete the installation.

## Verifying the Service Installation

To make certain that the Administration Service is up and running you might enter **net start arssvc** at a command prompt. Normally, this command should return the following message: "The requested service has already been started."

The Setup program tries to grant the following privileges on the Administration Service computer to the Administration Service account:

- **SeServiceLogonRight** Log on as a service
- **SeTcbPrivilege** Act as part of the operating system
- **SeAssignPrimaryTokenPrivilege** Replace a process level token

If the Setup program fails to grant these privileges, it cannot install the Administration Service. You need to grant these privileges with User Rights Assignment in Group Policy, and then run the Installation Wizard again.

# Installing User Interfaces

ActiveRoles Server provides user interfaces for the Windows system and the Web, allowing users with appropriate rights to perform administrative activities. The user interfaces include:

- **MMC Interface**, also referred to as the **ActiveRoles Server console** An MMC snap-in that provides full access to the capabilities and functions of ActiveRoles Server.

  MMC Interface can be used to specify administrative roles and delegate control, define security policies, business rules and automation scripts, and administer Active Directory data and Microsoft Exchange recipients.

- **Web Interface** A customizable Web application for performing day-to-day administrative tasks through the use of ActiveRoles Server.

  Different Web Interface sites can be deployed for administrators, help desk operators, and business users. Administrators use a Web Interface site that supports a wide range of tasks, whereas help desk operators use a tailored, dedicated site to expedite the resolution of trouble tickets. Business users have access to a special Web Interface site for self-administration.

## Steps to Install the Console

The ActiveRoles Server console can be installed on any computer that meets the system requirements and has a reliable network connection to a computer running the Administration Service. It can also be installed on the Administration Service computer.

***To install the ActiveRoles Server console***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In **Autorun** window, click **ActiveRoles Server**, and then click **Console (MMC Interface)** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard to complete the installation.

# Steps to Install the Web Interface

The ActiveRoles Server Web Interface can be installed on any computer that meets the system requirements and is running Internet Information Services (IIS) 6.0 or later. It is not necessary to install the Web Interface on the computer running the Administration Service. However, the computer that hosts the Web Interface must have a reliable network connection to a computer running the Administration Service.

If you plan to deploy the Web Interface on a Windows Server 2003 based computer, then you first need to ensure that IIS and ASP.NET are installed on that computer. Go to **Add or Remove Programs** in Control Panel, click **Add/Remove Windows Components**, select **Application Server**, click **Details**, and verify that the **Internet Information Services (IIS)** and **ASP.NET** check boxes are selected.

If you plan to install the Web Interface on a Windows Server 2008 based computer, then you first need to deploy the ASP.NET server on that computer. For instructions, see the "IIS 7.0: Deploying an ASP.NET Server" topic in Microsoft's documentation on Windows Server 2008 at http://technet.microsoft.com/en-us/library/cc731252.aspx

ActiveRoles Server Setup allows you to configure the Web Interface to use:

- Administration Service that runs on the same computer as the Web Interface
- Administration Service that runs on a specified computer
- Any available Administration Service that belongs to a specified replication group

Unless you choose the first option (Local Administration Service), you should ensure that the Web Interface users have the "Log on locally" privilege on the computer running the Web Interface. By default, all domain users have this privilege on workstations and member servers. However, for domain controllers, only domain administrators have this privilege by default.

Before installing the Web Interface, ensure that the Administration Service is up and running. Otherwise, Setup will fail to install the Web Interface. You might use the **net start arssvc** syntax to check the health of the Administration Service.

The procedure for deploying the Web Interface includes two stages:

- **Installing the Web Interface** At this stage, the files are copied to the computer, and three Web Interface sites are created based on the default configuration templates.
- **Creating, modifying or deleting Web Interface sites** At this stage, you can create additional sites, and modify or delete existing sites.

When creating Web Interface sites, you have the option to apply the configuration of an existing Web Interface site to the newly created one. If you have the Web Interface site tailored to meet your requirements, and need to deploy its instance on another Web server, this option ensures that the new Web Interface site has the same set of menus, commands and pages as the existing one.

Initially, the Installation Wizard creates three Web Interface sites based on the following configuration templates that are available out of the box:

- **Default Site for Administrators** Supports a broad range of tasks, including the management of directory objects and computer resources.
- **Default Site for Help Desk** Handles typical tasks performed by Help Desk operators, such as enabling/disabling accounts, resetting passwords, and modifying select properties of users and groups.
- **Default Site for Self-Administration** Provides self-service management capabilities, allowing users to accomplish certain IT-related tasks without assistance from the Help Desk or IT administrators.

Each configuration template provides an individual set of commands installed by default. Once a Web Interface site has been created, you can customize its configuration by adding or removing commands, and by modifying Web pages (forms) associated with commands. The relevant procedures are outlined in the *ActiveRoles Server Web Interface Administrator Guide*.

***To install the Web Interface***

1. In the ActiveRoles Server CD **Autorun** window, click **ActiveRoles Server**, and then click **Web Interface** in the **ActiveRoles Server Components** list.
2. Follow the instructions in the Installation Wizard.
3. On the **Administration Service Selection** page, choose from the following options to specify what Administration Service you want the Web Interface to use:
   - **Administration Service on this computer** Use the Administration Service running on the computer where you are installing the Web Interface.
   - **Administration Service on the specified computer** Enter the name of the computer running the Administration Service you want the Web Interface to use.
   - **Any Administration Service from the specified replication group** Specify any Administration Service whose SQL Server holds the Publisher role in ActiveRoles Server replication, by typing the fully qualified DNS name of the computer running that Administration Service.
4. On the **Ready to Install the Application** page, click **Next** to start the installation process.
5. Wait while the wizard completes the installation.

The Installation Wizard creates three Web Interface sites based on the default configuration templates. Once installation has been completed, you can modify the Web server-related parameters, such as the virtual directory name, for these Web Interface sites, or delete Web Interface sites. You can also create additional Web Interface sites.

***To create, modify or delete a Web Interface site***

1. Start the Web Interface Sites Configuration wizard: click **Start**, and select **All Programs | Quest Software | ActiveRoles Server | Web Interface Sites Configuration**.
2. Follow the instructions in the wizard.
3. On the **Web Interface Configuration** page, do one of the following:
   - To create a site, click **New**.
   - To modify a site, select it from the list and click **Edit**.
   - To delete a site, select it from the list and click **Delete**.

4. If you have selected **New** or **Edit**, set up the following parameters:
   - **Location** The Web site where the Web Interface site (virtual directory) is located.
   - **Virtual directory** The name of the IIS virtual directory to which the Web Interface site is installed.
   - **Application name** This name is used to help identify the Web Interface site.
   - **Configuration settings** Create a new configuration based on a template and apply it to the Web Interface site, or use the configuration of an existing Web Interface site.

Configuration specifies customizable settings of user interface elements, such as menus, commands, and Web pages (forms), displayed by the Web Interface. The configuration of a Web Interface site is stored as part of ActiveRoles Server configuration data. Multiple sites may use the same configuration.

5. Once you have completed the **Web Interface Configuration** page, click **Next** to continue.
6. On the **Begin Configuration Process** page, click **Next** for the wizard to start configuring the Web Interface site.

During the configuration process, the wizard restarts the World Wide Web Publishing Service. While that service is being restarted, all Web applications deployed on this Web server are unavailable.

7. On the **Configuration Results** page, review the summary of the operations performed by the wizard, and check for success or failure of each operation. When you have done, click **Finish** to close the wizard.

Each Web Interface site can be accessed using the URL based the name of the site's virtual directory:

`http://<WebSite>/<Directory>`

In this notation, <*WebSite*> identifies the Web site where the virtual directory is located. For example, if the virtual directory is located under the default Web site, the URL is http://<*Computer*>/<*Directory*>, where <*Computer*> stands for the network name of the computer running the Web Interface and <*Directory*> stands for the name of the Web Interface site's virtual directory, as specified in the Web Interface Sites Configuration wizard.

Normally, Web Interface users connect to the Web Interface using an HTTP transport. An HTTP transport does not encrypt the data transferred from a Web browser to the Web Interface. If your business process requires a secure transport for passing data to the Web Interface, you should use an HTTPS transport.

The secure hypertext transfer protocol (HTTPS) is designed to transfer encrypted information between computers over the Web. HTTPS is HTTP using a Secure Sockets Layer (SSL). SSL is an encryption protocol invoked on a Web server that uses HTTPS. For instructions on how to enable SSL on a Web server, refer to Microsoft's documentation. The instructions depend upon the version of the Web server, which can be either IIS 6.0 (Web server in Microsoft Windows Server 2003) or IIS 7.0 (Web server role in Microsoft Windows Server 2008):

- **Configuring Secure Sockets Layer (IIS 6.0)** at http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/d70e2bb7-9693-485e-a5e1-7196d7e655b3.mspx
- **Configuring Secure Sockets Layer in IIS 7.0** at http://technet2.microsoft.com/windowsserver2008/en/library/70c33ea8-4192-4110-be70-a11e11984f1e1033.mspx

If SSL is enabled, users specify an HTTPS prefix rather than an HTTP prefix when connecting to the Web Interface.

# Installing Additional Features

In addition to the Administration Service, MMC Interface and Web Interface, ActiveRoles Server Setup allows you to install the following features:

- **Language Pack** Installs the support files for the languages other than English. Provides the ability to select the user interface language in the Web Interface, and makes it possible to have the Administration Service and the Console behave in accordance with the computer locale.
- **SDK and Resource Kit** Provides developers with documentation and samples to help them customize ActiveRoles Server by creating custom client applications and user interfaces, and implementing business rules nd policies based on custom scripts.
- **ADSI Provider** Enables custom applications and scripts to access directory data via ActiveRoles Server by using standard COM interfaces.
- **Collector** Gathers data required for reporting. When scheduled to run automatically, the Collector retrieves data, accessing specified data sources through the Administration Service, and stores the data on SQL Server.
- **Report Pack** A comprehensive suite of report definitions that cover all administrative actions available in ActiveRoles Server.

## Steps to Install the Language Pack

The Language Pack for ActiveRoles Server provides the language support files for the following components of ActiveRoles Server:

- Web Interface
- Administration Service and ADSI Provider
- MMC Interface (Console)

By installing the Language Pack, you can switch ActiveRoles Server to a language other than English.

***To install the Language Pack***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **ActiveRoles Server**, and then click **Language Pack for ActiveRoles Server** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard until you reach the **Select Features** step.
4. On the **Select Features** page, choose the ActiveRoles Server components for which you want to install the language support files.

   *The Setup program detects the presence of ActiveRoles Server components, and makes the default selection of the language support files accordingly. It is advisable to install only the support files specific to the components that are present on the computer where you are installing the Language Pack. Thus, on a Web server running the Web Interface, the default selection is the Web Interface. On a computer running the Administration Service or MMC Interface (Console), the default selection is the Service or MMC, respectively.*
5. Follow the instructions in the Installation Wizard to complete the installation of the Language Pack.

Once you have installed the Language Pack on a particular computer, the behavior of the ActiveRoles Server components on that computer changes as follows:

- A user who connects to the Web Interface running on that computer has the option to choose a user interface language other than English in the **Settings** section of the Web Interface site.
- The Administration Service (along with the ADSI Provider) is localized in accordance with the computer locale. This means that all language-sensitive data that flows to the clients, such as error or warning messages, is represented in the language determined by the computer locale. For example, on the computer running the German version of Windows, installing the Language Pack causes the Administration Service to switch to the German language.
- The MMC Interface (Console) is localized in accordance with the computer locale. This means that when you open the Console after installing the Language Pack, all the Console menus, dialog boxes, error messages, and help files are represented in the language determined by the computer locale. For example, on the computer running the German version of Windows, installing the Language Pack causes the Console to switch to the German language.

The following registry values determine which support files are to be used:

- HKLM\SOFTWARE\Aelita\Enterprise Directory Manager\Language
  (for Administration Service)
- HKLM\SOFTWARE\Aelita\ActiveRoles Server ADSI Provider\6.1\Settings\Language
  (for ADSI Provider)
- HKLM\SOFTWARE\Aelita\ActiveRoles Server\6.1\Settings\Language
  (for MMC Interface)

You can modify the Language value in those locations in order to switch the Administration Service, ADSI Provider, or MMC Interface (Console) to a different language. However, this only makes sense if the Language Pack contains the support files for the language you want to use.

The Language value conforms to the *culture name* syntax. The format for the culture name is "<language code>-<country/region code>", where <language code> is an ISO 639 language code and <country/region code> is an ISO 3166 subculture code. Examples include "de-DE" for German in Germany and "en-US" for English in U.S. Thus, by setting the Language value to "de-DE" or "en-US" you can switch the Service and Console to the German or English language, respectively. Note that the Service must be restarted and the Console must be re-opened in order for your changes to the Language value to take effect.

# Steps to Install SDK and ADSI Provider

When installing the Administration Service, you have the option to also install SDK and Resource Kit. This feature installs documentation and samples to help customize ActiveRoles Server. Once installed, SDK and Resource Kit can be accessed from the **Start** menu: **All Programs | Quest Software | ActiveRoles Server | SDK and Resource Kit**.

The ADSI Provider is automatically installed when you install any of these features:

- Administration Service
- SDK and Resource Kit
- Web Interface

The ADSI Provider enables custom scripts and applications to access the Administration Service using standard ADSI COM interfaces. The ADSI Provider documentation is included in SDK and Resource Kit.

***To install the ActiveRoles Server SDK and ADSI Provider***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **ActiveRoles Server**, and then click **Administration Service (with Resource Kit)** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard.
4. On the **Feature Selection** page, ensure that the **SDK and Resource Kit** feature is selected for installation.

   *You may install SDK and ADSI Provider without installing the Administration Service. To do so, unselect the **Administration Service** feature.*
5. Follow the instructions in the wizard to complete the installation.

The ADSI Provider can also be installed from a separate installation package. The package file is located in the folder **ADSI Provider** on the ActiveRoles Server CD. To install the ADSI Provider, run **setup.exe**, located in that folder. You can also install the ADSI Provider from the **Free Tools** area on the **Solutions** page in the ActiveRoles Server CD **Autorun** window.

# Steps to Install the Reporting Components

ActiveRoles Server comes with a comprehensive suite of report definitions, contained in the ActiveRoles Server Report Pack. To work with reports, you must install the following features:

- Collector
- Report Pack

## Installing the ActiveRoles Server Collector

The ActiveRoles Server Collector is used to prepare data for reporting, allowing you to configure, schedule, and execute data collection jobs.

***To install the Collector***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window:
   a) Click **ActiveRoles Server**.
   b) In the **Reporting Components** area, click **Data Collector**.
3. Follow the instructions in the Installation Wizard.

The ActiveRoles Server Collector stores report data in a database on SQL Server, and requires Microsoft SQL Server 2005. Beginning with version 6.1, ActiveRoles Server Collector cannot use Microsoft SQL Server 2000 to host the database for report data.

## Installing the ActiveRoles Server Report Pack

The Report Pack requires Microsoft SQL Server 2005 Reporting Services (SSRS). Make sure that you have SSRS deployed in your environment. The Report Pack Installation Wizard prompts you for the address (URL) of the Report Server Web service. You can check for this address using the **Report Server Virtual Directory Settings** page in the Reporting Services Configuration Manager tool on the server where you have SSRS installed.

***To instal the Report Pack***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window:
   a) Click **ActiveRoles Server**.
   b) In the **Reporting Components** area, click **Report Pack**.
3. Follow instructions in the Installation Wizard.
4. When prompted for the address of the Report Server Web service, type the URL of your SSRS report server.
   *By default, the URL is http://<ComputerName>/reportserver where <ComputerName> stands for the name of the computer on which SSRS is installed.*
5. When prompted to configure the data source, do the following:
   a) Click the **Configure** button.
   b) Select the name of the data source from the list, and click **Modify**.
   c) Use the wizard to specify the SQL Server instance that hosts the database you have prepared by using the ActiveRoles Server Collector, the name of the database, and the authentication method to use for connection to the database.

   *Configuring the data source is an optional step. You may simply click **Next** in the Installation Wizard. If you do so, you will have to configure the data source after installing the Report Pack. For instructions, see the "Working with Reports" section in the ActiveRoles Server Administrator Guide.*
6. Follow the instructions in the wizard to complete the installation.

ActiveRoles Server reports can be administered using Report Manager, a Web-based tool included with SSRS. Another option is to use Quest Knowledge Portal. For information on how to install, configure and use Quest Knowledge Portal, refer to Quest Knowledge Portal documentation that is included on the ActiveRoles Server CD.

# Silent Installation

The ActiveRoles Server setup program provides for silent installation of the following components:

- ActiveRoles Server console
- Web Interface
- ActiveRoles Server ADSI Provider

You can perform a silent installation of these components on a computer that meets the system requirements for the component being installed. For example, prior to installing the console or Web Interface, you must ensure that Microsoft .NET Framework 2.0 is installed on the computer. A silent installation is done entirely from the command line, and requires no interaction.

Use the following instructions to perform silent installations of ActiveRoles Server components. A basic command-line syntax is provided for each component, along with the component-specific arguments. Depending on your requirements, you can also configure the standard Windows Installer (Msiexec.exe) command-line options. For more information about Windows Installer command-line options, see "Command-Line Options" at http://msdn.microsoft.com/en-us/library/aa367988.aspx

Use the following Windows Installer command-line syntax for silent installations of the ActiveRoles Server components:

```
msiexec /i "<Path to setup.msi>" /qn arguments
```

To have Windows Installer write information to a log file, thus documenting the installation process, you might alter this syntax as follows:

```
msiexec /i "<Path to setup.msi>" /qn /l*v "C:\Log.txt" arguments
```

The .msi file is specific to the component you want to install. For each component, you can find the respective .msi file on the ActiveRoles Server CD using the path specified in the following table.

| COMPONENT | PATH TO THE FOLDER CONTAINING .MSI ON THE ACTIVEROLES SERVER CD |
|---|---|
| Console | <*root*>\ActiveRoles Server 6.1\MMC Interface\ |
| Web Interface | <*root*>\ActiveRoles Server 6.1\Web Interface\ |
| ADSI Provider | <*root*>\Solutions\Free Tools\ADSI Provider\ |

The following two tables list the component-specific arguments you can use to complete the syntax.

### Arguments for silent installation of the ActiveRoles Server console

| ARGUMENT | DESCRIPTION |
|---|---|
| **PF_ARS_MMC=***Path* | Use this argument to specify the location where you want to install the console (installation folder). If this argument is omitted, the default value is the following path:<br>*%ProgramFiles%*\Quest Software\ActiveRoles Server\ |

### Arguments for silent installation of the Web Interface

| ARGUMENT | DESCRIPTION |
|---|---|
| **PF_ARS_WI**=*Path* | Use this argument to specify the location where you want to install the Web Interface (installation folder). If this argument is omitted, the default value is the following path:<br>*%ProgramFiles%*\Quest Software\ActiveRoles Server\Web Interface 6.1\ |

| | |
|---|---|
| **SERVICE_LOCATION**=<br>LOCAL \| REMOTE \| ANYREPGROUP | Use this argument to choose the Administration Service to which the Web Interface will connect. Specify one of the following:<br><br>**SERVICE_LOCATION=LOCAL** for the Web Interface to connect to the Administration Service running on the same computer as the Web Interface.<br><br>**SERVICE_LOCATION=REMOTE** for the Web Interface to connect to a certain Administration Service running on a different computer; the name of the computer must be specified by using **REMOTE_SERVICE_NAME**.<br><br>**SERVICE_LOCATION=ANYREPGROUP** for the Web Interface to connect to any available Administration Service from a certain replication group; the Publisher of the replication group must be specified by using **REMOTE_SERVICE_NAME**.<br><br>If this argument is omitted, the default value is **SERVICE_LOCATION=LOCAL**. |
| **REMOTE_SERVICE_NAME**=<br>*Servername* | If **SERVICE_LOCATION=REMOTE**, the *Servername* value specifies the fully qualified DNS name of the computer running the Administration Service you want the Web Interface to connect to.<br><br>If **SERVICE_LOCATION=ANYREPGROUP**, the *Servername* value specifies the fully qualified DNS name of the computer running the Administration Service whose SQL Server is the Publisher of the replication group you want the Web Interface to use.<br><br>In both cases, this argument is required. If **SERVICE_LOCATION=LOCAL**, this argument is ignored. |
| **ENABLEWEBLOG**=0 \| 1 | Use this argument to enable diagnostic logging in the Web Interface Sites Configuration utility, which might be helpful in isolating problems, if any, with the creation of Web Interface sites. Specify either **ENABLEWEBLOG=1** to enable or **ENABLEWEBLOG=0** to disable diagnostic logging.<br><br>If this argument is omitted, the default value is **ENABLEWEBLOG=0**. |
| **WEBLOGURL**=*Path**Filename* | If **ENABLEWEBLOG=1**, the *Path**Filename* value specifies the path and name of the file where you want the diagnostic records to be written. If this argument is omitted, the default value is the following path and file name:<br><br>"C:\Quest.ArspWI.WebSitesConfigurationConsole.log"<br><br>If **ENABLEWEBLOG=0**, this argument is ignored. |

# Upgrading from an Earlier Version

If an earlier version of the product is already installed, the Setup program first uninstalls the features of the old version, and then installs the features you have selected from the new version.

Setup allows you to import configuration data stored by the previous version. When upgrading the Administration Service, you have the option to copy all data from the old database to the new one. In this way, Setup ensures that the configuration settings, including all permission and policy definitions and assignments, are identical to those used in the earlier installation.

# Components Compatibility

When upgrading the Administration Service, you should check that the user interfaces are compatible with the new version of the Administration Service. The new Administration Service is only compatible with the ActiveRoles Server console (MMC Interface) and Web Interface version 6.0 or 6.1. Earlier versions of the user interfaces will not work with the new Administration Service and thus need to be upgraded. The user interfaces of ActiveRoles Server 6.1 are only compatible with the Administration Service version 6.1. Therefore, to use the ActiveRoles Server console or Web Interface version 6.1, you first need to upgrade the Administration Service.

# Upgrade Issues

## Impact on ActiveRoles Server Replication

The upgrade process of the Administration Service version 5.2 or 6.0.0 does not preserve the replication settings. In this case, an upgrade can only be performed if the Administration Service is not configured for replication. Before upgrading the Administration Service version 5.2 or 6.0.0, you should ensure that it is not configured as a Subscriber or Publisher. Replication for the new Administration Service needs to be configured after the upgrade.

## Impact on Custom Solutions

An upgrade of ActiveRoles Server components may affect custom solutions, if any, that rely on the functions of ActiveRoles Server. Custom solutions (such as scripts or other modifications) that work fine with the earlier version of ActiveRoles Server may cease to work after the upgrade. Prior to attempting an upgrade, you should test the existing solutions with the new version of ActiveRoles Server in a lab environment to verify that the solutions continue to work. Should any compatibility issues arise during the test process, you can contact Quest Professional Services for paid assistance with those solutions.

## Impact on Dynamic Groups

Beginning with version 6.0, the Administration Service uses a new mechanism for managing Dynamic Groups, so you must upgrade your existing Dynamic Groups after upgrading the Administration Service from version 5.2. For that purpose, the script **DGUpgrade6x.vbs** must be executed on the computer running the Administration Service upgraded to version 6.1. You can find the **DGUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder.

## Impact on Mailbox Policies

Beginning with version 6.0, the Administration Service uses a new mechanism for managing mailbox policies, so you must upgrade your existing mailbox policies after upgrading the Administration Service from version 5.2. For that purpose, the script **ExchangePolicyUpgrade6x.vbs** must be executed on the computer running the Administration Service you have upgraded to version 6.1. You can find the **ExchangePolicyUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder.

## Impact on Credentials of Override Accounts

Beginning with version 6.0, the Administration Service uses a new, improved algorithm for encrypting security-sensitive data, such as credentials of override accounts. After an upgrade of the Administration Service from version 5.2, ActiveRoles Server cannot read the data that was encrypted earlier. As a result, if a managed domain was registered so that ActiveRoles Server uses an override account rather than the service account to access the domain, the credentials of the override account are lost. You have to re-enter the passwords of the override accounts (if any) after the upgrade. For instructions, refer to the "Upgrading the Administration Service 5.2" section later in this document.

# Upgrading the Administration Service

The process of upgrading the Administration Service depends upon the version you are going to upgrade. When upgrading the Administration Service, you have the option to preserve the ActiveRoles Server configuration settings.

## Moving ActiveRoles Server Databases from SQL Server 2000

Beginning with version 6.1, ActiveRoles Server requires Microsoft SQL Server 2005 to host the ActiveRoles Server databases. So, when upgrading the Administration Service that uses Microsoft SQL Server 2000, you need to move the ActiveRoles Server databases from SQL Server 2000. This section provides instructions on how to move a database from to SQL Server 2005 during the upgrade.

Prior to the upgrade, ensure that the Administration Service you are going to upgrade has no replication partners. You can do this using the ActiveRoles Server console:

- If the Administration Service is configured as a Subscriber, connect to its Publisher and remove the Administration Service from the list of Subscribers.
- If the Administration Service is configured as the Publisher, connect to that Administration Service, remove all of its Subscribers, and then demote the Publisher.

Once the Administration Service is configured not to participate in ActiveRoles Server replication, you can use the following instructions to perform the upgrade. After the upgrade, configure ActiveRoles Server replication as appropriate.

First, create a full backup of the database in use by the Administration Service you are going to upgrade. The database is assumed to be hosted by SQL Server 2000. For instructions, refer to Microsoft's documentation at http://msdn.microsoft.com/en-us/library/aa176763.aspx - "How to create a database backup (Enterprise Manager)".

Next, restore the database from the backup to the SQL Server 2005 instance you want to host the ActiveRoles Server database after the upgrade. For instructions, refer to Microsoft's documentation at http://msdn.microsoft.com/en-us/library/ms177429.aspx - "How to restore a database backup (SQL Server Management Studio)".

Then, use the Administration Service Installation Wizard to perform the upgrade:

1. On the **Service Deployment Options** page in the Installation Wizard, select the **Install initial Service** option.
2. On the **Database and Connection Settings** page, set the **Database** options as follows:
   a) In **SQL Server**, specify the SQL Server 2005 instance to which you have restored the database backup.
   b) In **Database name**, specify a name for the new database that will be created by the Setup program.
   c) Select the **Import data from this database** check box.
   d) In **Import data from this database**, type the name of the database you have restored from the backup.
3. Follow the instructions in the wizard to complete the installation.

Since the import operation during Administration Service setup does not transfer the Management History data, you need to use the Management History Migration wizard after installing the Administration Service with the new database. Using this wizard, you can transfer the Management History data from the restored database to the database of the newly installed Administration Service. For instructions on how to use the Management History Migration wizard, refer to the "Importing Management History Data" section later in this document.

## Upgrading the Administration Service 5.2

If you are upgrading the Administration Service 5.2, you must first ensure that the Administration Service has no replication partners. You can do this using the ActiveRoles Server console:

- If the Administration Service is configured as a Subscriber, connect to its Publisher and remove the Administration Service from the list of Subscribers.
- If the Administration Service is configured as the Publisher, connect to that Administration Service, remove all of its Subscribers, and then demote the Publisher.

Once the Administration Service is configured not to participate in ActiveRoles Server replication, you can use the following steps to perform the upgrade. After upgrade, configure ActiveRoles Server replication as appropriate.

***To upgrade the Administration Service 5.2***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **ActiveRoles Server**, and then click **Administration Service (with Resource Kit)** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard.
4. On the **User Information** page, click **Licenses** to install the license key file (see "Installing the License" earlier in this document).
5. On the **Service Account Information** page, enter the name and password of the user account to be used as the Administration Service account.
6. On the **AR Server Admin Account** page, accept the default setting, or click **Browse** and select the group or user to be designated as AR Server Admin.
7. On the **Service Deployment Options** page, select the **Install initial Service** option.
   *With this option, Setup creates a database for the new Administration Service and, optionally, imports data from the database used by the Administration Service you are upgrading.*

8. On the **Database and Connection Settings** page, in the **Database** area, configure the following settings:
   - **SQL Server** Identifies the SQL Server instance on which the database for the new Administration Service will be created.
   - **Database name** The name of the database to be created for the new Administration Service. Setup will create a database with this name on the SQL Server instance specified in **SQL Server**.
   - **Import data from this database** Identifies the database of the Administration Service you are upgrading. To import data from that database to the database of the new Administration Service, select the **Import data from this database** check box.

     *The database from which to import data must be located on the SQL Server instance specified in the **SQL Server** box. If necessary, you can transfer the database to the desired SQL Server instance by using the instructions given earlier in this document (see "Moving ActiveRoles Server Databases from SQL Server 2000").*
9. On the **Database and Connection Settings** page, in the **Connection** area, select one of these options:
   - **Use Windows authentication** Configures the Administration Service to connect to SQL Server using the Administration Service account.
   - **Use SQL Server authentication** Configures the Administration Service to connect to SQL Server using a SQL Server login. Type in the login name and password.
10. Follow the instructions in the wizard to complete the installation.

After upgrading the Administration Service from version 5.2, you need to run the **DGUpgrade6x.vbs** and **ExchangePolicyUpgrade6x.vbs** scripts in order for the new Administration Service to recognize the Dynamic Groups and Exchange mailbox-related policies that were created using the earlier version of ActiveRoles Server. You can run each of those scripts by double-clicking the script file in Windows Explorer. The script files are located on the ActiveRoles Server CD, in the **Misc** folder.

The scripts can be successfully executed only after the Administration Service has finished building its internal data structures. To ensure that this process is completed, try to connect to the Administration Service with the ActiveRoles Server console (MMC Interface). If a connection can be established, the Administration Service is ready to execute the script.

## Re-entering passwords of override accounts

If you have performed the upgrade with the option to import the configuration data from the database of version 5.2, then you may need to perform some additional steps to ensure that the Administration Service can access managed domains. Namely, you have to re-enter the passwords of the override accounts (if any) that are used to access managed domains. You can do this by using the ActiveRoles Server console as follows.

***To re-enter the passwords of the override accounts***

1. Open the ActiveRoles Server console and connect to the Administration Service you have upgraded.
2. In the console tree, navigate to the **Configuration/Server Configuration/Managed Domains** container.

3. In the details pane, double-click an object in that container and examine the settings in the **Access the domain using** area on the **General** tab in the **Properties** dialog box for that object:
   - If the first option (**The service account information the Administration Service uses to log on**) is selected, click **Cancel** to close the **Properties** dialog box.
   - If the second option (**The Windows user account information specified below**) is selected, type the password of the override account in the **Password** box and click **OK**.
4. Repeat Step 3 for each object in the **Managed Domains** container.

## Upgrading the Administration Service 6.0

If you are upgrading the Administration Service 6.0, the use of the **Database of an earlier installed Service** option is the most straightforward way to preserve configuration data. This option causes the Administration Service to use the database that was created during the earlier installation of the Administration Service. However, this option cannot be used for upgrading the Administration Service of version 6.0.0.

This section provides instructions on how to upgrade:

- **Administration Service 6.0.0** In this case, you must use the upgrade process that transfers configuration data to a new database instead of re-using the existing database. Before upgrade, ensure that the Administration Service has no replication partners:
  - If the Administration Service is configured as a Subscriber, connect to its Publisher and remove the Administration Service from the list of Subscribers.
  - If the Service is configured as the Publisher, connect to that Administration Service, remove all of its Subscribers, and then demote the Publisher.
- **Administration Service 6.0.1 or later** In this case, the recommended option is to re-use the existing database of the earlier version. With this option, the Administration Service you are upgrading need not be removed from ActiveRoles Server replication.

Use one of the following procedures to perform the upgrade depending upon the version of the Administration Service you are upgrading.

***To upgrade the Administration Service 6.0.0***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **ActiveRoles Server**, and then click **Administration Service (with Resource Kit)** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard.
4. On the **Service Account Information** page, enter the name and password of the user account to be used as the Administration Service account.
5. On the **AR Server Admin Account** page, accept the default setting, or click **Browse** and select the group or user to be designated as AR Server Admin.
6. On the **Configuration Storage Options** page, verify that the **New database, to be created by this setup** option is selected.

7. On the **Database and Connection Settings** page, in the **Database** area, configure the following settings:
   - **SQL Server** Identifies the SQL Server instance on which the database for the new Administration Service will be created.
   - **Database name** The name of the database to be created for the new Administration Service.
   - **Import data from this database** Identifies the database of the Administration Service you are upgrading. To import data from that database to the database of the new Administration Service, select the **Import data from this database** check box.

     *The database from which to import data must be located on the SQL Server instance specified in the **SQL Server** box. If necessary, you can transfer the database to the desired SQL Server instance by using the instructions given earlier in this document (see "Moving ActiveRoles Server Databases from SQL Server 2000").*
8. On the **Database and Connection Settings** page, in the **Connection** area, select one of these options:
   - **Use Windows authentication** Configures the Administration Service to connect to SQL Server using the Administration Service account.
   - **Use SQL Server authentication** Configures the Administration Service to connect to SQL Server using a SQL Server login. Type in the login name and password.
9. Follow the instructions in the wizard to complete the installation.

***To upgrade the Administration Service 6.0.1 or later***

1. Run **autorun.exe**, located in the root folder of the ActiveRoles Server CD.
2. In the **Autorun** window, click **ActiveRoles Server**, and then click **Administration Service (with Resource Kit)** in the **ActiveRoles Server Components** list.
3. Follow the instructions in the Installation Wizard.
4. On the **Service Account Information** page, enter the name and password of the user account to be used as the Administration Service account.
5. On the **AR Server Admin Account** page, accept the default setting, or click **Browse** and select the group or user to be designated as AR Server Admin.
6. On the **Configuration Storage Options** page, verify that the **Database of an earlier installed Service** option is selected.
7. On the **Database and Connection Settings** page, in the **Database** area, examine these settings:
   - **SQL Server** Identifies the SQL Server instance that hosts the database of the Administration Service you are upgrading.
   - **Database name** Identifies the database of the Administration Service you are upgrading.
8. On the **Database and Connection Settings** page, in the **Connection** area, select one of these options:
   - **Use Windows authentication** Configures the Administration Service to connect to SQL Server using the Administration Service account.
   - **Use SQL Server authentication** Configures the Administration Service to connect to SQL Server using a SQL Server login. Type in the login name and password.
9. Follow the instructions in the wizard to complete the installation.

## Importing Management History Data

A part of the ActiveRoles Server database, the Management History data storage is empty after the upgrade of the Administration Service if you choose the option to import data from the database of your existing installation. This behavior is due to the fact that the import operation performed by the Installation Wizard transfers only the configuration data—administrative right assignments, rule-based policy definitions, administrative view settings, and other parameters that determine the ActiveRoles Server work environment. The Management History data is excluded from the import operation in order to reduce the time it takes for the Installation Wizard to upgrade the Administration Service.

The Management History data describes the changes that were made to directory data via ActiveRoles Server. This includes information on who did what and when it was done as applied to the directory data management tasks. In ActiveRoles Server, the Management History data is used as a source of information for the Change History and User Activity reports.

After you have upgraded the Administration Service using the option to import data from the existing database, you need to take some additional steps to transfer the Management History data from your old ActiveRoles Server database to the new ActiveRoles Server database.The Administration Service installation includes the Management History Migration Wizard to help you perform this task.

***To start the Management History Migration Wizard***

- On the computer on which you have installed the new version of the Administration Service, click **Start**, and select **All Programs | Quest Software | ActiveRoles Server | Management History Migration Wizard**.

The wizard is intended to populate a new storage of Management History data with your existing Management History data, to make the data available to the ActiveRoles Server user interfaces after your upgrade to the new version of the Administration Service. The wizard merges the Management History data found in the source database with the data stored in the destination database. Note that the wizard only adds new data, keeping intact any data that already exists in the destination database. You may import your old data at any time after you have upgraded the Administration Service, without being afraid of losing any data.

***To import Management History data***

1. Start the Management History Migration Wizard, and follow the instructions on the wizard pages.
2. On the **Choose the Source Database** page, specify the database from which you want to import data (normally, this should be the database that was in use by your earlier version of the Administration Service):
   a) Type the name of the SQL Server instance that hosts the database. Specify the name in the form *computername* for the default instance or *computrname**instancename* for a named instance.
   b) Type the name of the database.
   c) Specify the authentication mode. Depending on the option you select, either your Windows account or the SQL Server login you provide must have sufficient rights to retrieve data from the database.

3. On the **Choose the Destination Database** page, specify the database to which you want to import data (normally, this should be the database that is in use by the newly installed Administration Service, which is the default setting on this page):
   a) Verify the name of the SQL Server instance that hosts the database. If necessary, type a different name. The name should be in the form *computername* for the default instance or *computrname**instancename* for a named instance.
   b) Verify the name of the database. If necessary, type a different name.
   c) Specify the authentication mode. Depending on the option you select, either your Windows account or the SQL Server login you provide must have sufficient rights to update data in the database.
4. On the **Records to Migrate** page, specify whether you want to import all the data records or a certain range of data records. You may choose not to import all the data records since importing a large volume of data may take hours or more.
5. On the **Ready to Start** page, click **Next** to start the import operation.

# Upgrading Other Components

For any component other than the Administration Service, ActiveRoles Server enables automatic upgrade from earlier versions. To upgrade, install the component on the computer with the old version installed, as described earlier in this document. Setup first uninstalls the old version, and then installs the new version of the component.

When upgrading the ActiveRoles Server Collector, you may be prompted to uninstall the earlier version prior to installing the new version.

# Performing a Pilot Deployment

In a large enterprise environment, a pilot project may need to be conducted before upgrading to the new version of the product. In a pilot project, you deploy components of the new version in your production environment side-by-side with the existing installation of the components you are going to upgrade, evaluate the results, and fix problems.

Normally, a pilot project is conducted with a small group of users in the production environment where select individuals perform particular tasks using the new version of the product. This demonstrates that the new version works as expected and that it meets the organization's requirements.

A pilot project is a deployment of the new product version to a subset of the user group. Those who do not participate in the pilot project perform their regular, daily work using the old version of the product. This requires that the old version be up and running in the production environment side-by-side with the pilot deployment.

When the pilot project is deemed successful and ready for production, you can upgrade your existing production components to the new version.

Deploying a pilot project involves the following steps:

1. **Installing the pilot Administration Service** Install a new Administration Service instance of the version that you have in your production ActiveRoles Server environment, and update the new instance with the configuration data from your production Administration Service.
2. **Installing the pilot Web Interface** Install a new Web Interface instance of your production ActiveRoles Server version so that the new instance connects to the Administration Service you installed in Step 1.

   *If any non-default Web Interface sites are created in your production environment, you need to create the corresponding site or sites in the newly installed Web Interface. You also have to ensure that each site in the newly installed Web Interface uses the same configuration as the respective site in your production Web Interface.*
3. **Upgrading the pilot Administration Service** Upgrade the Administration Service you installed in Step 1, with the option to preserve the configuration data.
4. **Upgrading the pilot Web Interface** Upgrade the Web Interface you installed in Step 2, with the option to connect to the Administration Service you upgraded in Step 3.
5. **Installing the console** Install the Active Roles Server console of the new version.

To successfully deploy a pilot project, you have to perform these steps in exactly the same order as they are listed above.

# Installing the Pilot Administration Service

When creating your pilot instance of the Administration Service, you need to ensure that it has the same configuration as your production instances of the Administration Service. This can be achieved as follows:

1. Install an additional Administration Service of the same version as you have in your production environment, with the option to create a new, separate configuration database for that Administration Service. Use the installation instructions included in the *Quick Start Guide* for the respective version of ActiveRoles Server. This Administration Service instance will become your pilot Administration Service.

   *Since the latest version of the Administration Service requires Microsoft SQL Server 2005, it is highly advisable to create the database for the Administration Service version 6.0 on SQL Server 2005 rather than SQL Server 2000. This will simplify the upgrade process.*

2. Have the newly installed Administration Service replicate configuration data from your existing instances of the Administration Service. For instructions on how to configure ActiveRoles Server replication, refer to the *Administrator Guide* for the respective version of ActiveRoles Server.

   If ActiveRoles Server replication is already set up in your environment, simply add the newly installed Administration Service as a Subscriber for the Administration Service acting as the Publisher in the ActiveRoles Server replication group. Otherwise, make your production Administration Service the Publisher, and then add the newly installed Administration Service as a Subscriber.

   Once the ActiveRoles Server replication function has completed copying the data to the new Subscriber, remove the newly installed Administration Service from the ActiveRoles Server replication group. In this way you ensure that your pilot Administration Service has the same configuration as your production Administration Service, while isolating the configuration of your pilot ActiveRoles Server deployment.

# Installing the Pilot Web Interface

Once you have installed your pilot Administration Service and updated its configuration, you are ready to install the Web Interface for your pilot project. Install a new Web Interface instance of the same version as you have in your production environment. Use the installation instructions included in the Quick Start Guide for the respective version of the Administration Service. This Web Interface instance will become your pilot Web Interface.

When prompted by the Installation Wizard to specify the Administration Service, choose one of these options depending upon the location of your pilot Administration Service:

- If the Administration Service is installed on the computer on which you are installing the Web Interface, then choose the option to use the local Administration Service.
- If the Administration Service is installed on a different computer, then choose the option to use the Administration Service running on a specific computer and supply the name of that computer.

After you have installed the Web Interface, you need to ensure that the sites of the newly installed Web Interface match the sites of your production Web Interface. Use the Web Interface Sites Configuration tool to examine and compare the production Web Interface sites and the newly installed Web Interface sites, and, if necessary, create additional sites or delete the unwanted sites for your pilot Web Interface. To start the tool, select **Start | All Programs | Quest Software | ActiveRoles Server | Web Interface Sites Configuration**.

Start the Web Interface Sites Configuration tool on the computer running your production Web Interface. If the Welcome page appears, click **Next**. Examine the list on the **Web Interface Configuration** page: each entry in the list identifies a certain Web Interface site in you production ActiveRoles Server environment. For each list entry, note down the name displayed in the **Configuration** column.

Start the Web Interface Sites Configuration tool on the computer running your pilot Web Interface and proceed to the **Web Interface Configuration** page. Examine the list on that page and compare the names in the **Configuration** column with the names you noted down earlier. Use the Web Interface Sites Configuration tool to create additional sites and delete unwanted sites as needed:

- If a list entry with a certain configuration name exists on the production Web Interface but is missing from the pilot Web Interface, then you need to create an additional site: click **New**, choose the **Use existing configuration** option, and select the same configuration name as in the respective list entry on the production Web Interface. Repeat this for each list entry that is missing from your pilot Web Interface.
- If a list entry with a certain configuration name exists on your pilot Web Interface but does not exist on the production Web Interface, then you should delete the respective site from the pilot Web Interface: select that entry from the list and click **Delete**. Repeat this for each list entry that does not exist on the production Web Interface.

Now that you have installed and configured the Web Interface for your pilot project, you can upgrade the pilot Administration Service, and then upgrade the pilot Web Interface to the new version.

# Upgrading the Pilot Administration Service

When performing the upgrade, you need to preserve the existing configuration of the Administration Service. Depending on the version you are upgrading, this can be done either by importing the existing configuration data (in case of upgrading from version 5.2 or 6.0.0) or by reusing the configuration database of the earlier installed Administration Service (in case of upgrading from the 6.0.1 or later releases of version 6.0). For instructions, see the "Upgrading the Administration Service" section earlier in this document.

# Upgrading the Pilot Web Interface

Once you have upgraded the pilot Administration Service, upgrading the Web Interface is straightforward. Install the new version of the Web Interface on the computer on which you have installed your pilot Web Interface.

When the Installation Wizard prompts you for the Administration Service, ensure that the Web Interface is configured to use your pilot Administration Service. Select the option to use the Administration Service either on the local computer or on the specified computer, depending on where your pilot Administration Service is installed.

# Installing the ActiveRoles Server Console

You need the latest version of the ActiveRoles Server console if you want to connect to the latest version of the Administration Service. Since the latest version of the console does not connect to the Administration Service of an earlier version, the use of the latest console version for your pilot project assures automatic connection to the pilot Administration Service. For installation instructions, see the "Steps to Install the Console" section earlier in this document.

# Deployment Considerations

This section addresses issues concerning the deployment of ActiveRoles Server's Administration Service. Information for this section was collected from:

- Interviews and feedback from current ActiveRoles Server customers who have enterprise class deployments with multiple sites/locations
- Extensive testing of ActiveRoles Server in Quest Software's labs
- Comparisons and testing of ActiveRoles Server to competitors' solutions

There are no technical requirements for installing many Administration Services in a location or in different locations. The number of Administration Services in a location and the number of locations with Administration Services depends on an organization's needs and expectations, the current infrastructure and hardware, and the business workflow. When considering an ActiveRoles Server deployment, administrators should consider the following issues:

- Business workflow
- ActiveRoles Server resource usage
- Hardware requirements
- Need for availability
- Replication traffic

When an organization has gathered and assessed the information above, it will be able to determine the locations and number of Administration Services to be installed. The last sub-section provides network diagrams that illustrate potential ActiveRoles Server deployments.

## Business Workflow

This factor focuses on Active Directory (AD) data management processes and practices, including who will perform these tasks and from where they access the management services. Generally, these tasks will be divided among several groups, which might include both high- and low-level administrators, a Help Desk, HR personnel, and work group managers.

Possible business workflows for AD data management processes might be:

- Centralized at one location and performed by one group
- Centralized at one location or LAN site and performed by multiple groups
- Distributed at multiple sites but performed by one business group
- Distributed at multiple sites and performed by multiple independent business groups

Organizations should diagram the locations/sites at which AD data management is done, their network connections, the number of users performing tasks, the type of work they do. For example, Help Desk personnel will make more use of the Administration Service than regular employees who are occasionally changing their personal information.

Finally, the number of users at each site should be added to the diagram. Current customers report that there has been no need to install additional services in order to improve ActiveRoles Server performance. Adding the number of users is not intended to indicate the workload on or the performance of the Administration Service. The number of users is intended to help organizations to estimate and understand their own administration workload and how ActiveRoles Server will fit into that workload.

# Resource Usage

Organizations should begin their deployment analysis by determining the resources needed for one Administration Service. This information is relevant to assessing locations for Services, hardware needs, and replication traffic. For an Administration Service, the ActiveRoles Server Resource Usage Calculator enables organizations to determine:

- Memory used by the Administration Service
- Size of an Administration Service's log file during a period of time (e.g., week or month)
- Size of the Administration Database

The Administration Database is normally used to store only the Access Templates, Policy Objects, Managed Unit specifications, and object links. It does not store any Active Directory information. Consequently, the Administration Database is rather small.

The ActiveRoles Server Resource Usage Calculator is available from any Quest Software sales person, and any prospective customer can use it and their own data to project resource usage. The Resource Usage Calculator is also included on the ActiveRoles Server distribution CD.

# Hardware Requirements

After calculating the resource usage of an Administration Service and mapping the business workflow of the network sites, an organization will have the necessary information to start assessing any need for additional hardware.

There is no technical need for installing the Administration Service on dedicated hardware. In fact, current customers do not use only dedicated hardware. They use a combination of dedicated and shared hardware to host the Administration Service. For example, a current customer manages 2,000,000 AD objects in a global deployment with a total of five Administration Services, two of which are dedicated and the other three are shared with other applications.

An organization's current infrastructure, including existing servers, sites and connections, will greatly determine the need for additional hardware to run ActiveRoles Server. The Administration Service can be installed on any server, although organizations should consider these two guidelines:

- It is not recommended that the Administration Service be installed on a domain controller.
- Typically, organizations install the Administration Service on other application, file, or print servers.

Depending on service level agreements or goals, if existing servers are currently fully loaded or overloaded, then a new server should be purchased, and the Administration Service and additional services should be moved onto the new equipment. Not only will this enable ActiveRoles Server deployment, it will also improve the performance of the currently deployed services. Since ActiveRoles Server is often deployed during migration to Active Directory, ActiveRoles Server deployment can be included in planning for new hardware and server consolidation.

The need for redundancy and availability also will affect the hardware requirements. See the sub-section "Availability and Redundancy" for further details.

## Web Interface: IIS Server Required

If an organization plans to use the ActiveRoles Server Web Interface, IIS must be installed on the server running the Web Interface.

It is recommended that organizations use the ActiveRoles Server Web Interface because it offers more flexibility than the MMC Interface. Users can access it from almost anywhere on the network. It shows administrators only the data they can administer and the tasks they can perform, which makes it easy to learn and highly secure.

# Availability and Redundancy

One of the benefits of ActiveRoles Server is that administrators do not need permissions on Active Directory to perform user management and other tasks. This forces administrators to use ActiveRoles Server and assures secure administration with the enforcement of ActiveRoles Server's "Rules and Roles." However, this lack of AD permissions might be a problem if the Administration Service becomes unavailable. The impact of this potential problem depends on the specifics of the situation, but the problem can be addressed with the following guidelines.

## Major Sites

Two guidelines should be followed for major sites:

- Current ActiveRoles Server customers typically deploy two Administration Services per major location/site where AD data administration and user management is performed. This redundant service solution would be effective if both the primary Administration Service and all connections to other sites failed.

  Again, organizations should use their administration framework and their experience with other management services, such as SMS, to determine the need for an Administration Service at a site.

- Most current customers do not place all of their Administration Services at one location/site. If access to that one location/site should fail, all Administration Service of AD would stop. Instead, they install Administration Services at two or sometimes more sites.

  In most scenarios, even if the server hosting the Administration Service fails, connections to other sites will be maintained. Administrators can access Administration Services at another site and force AD replication to make the changes appear on the local domain controller as soon as possible.

## Remote Sites

Three approaches can be used for remote sites where either no or only a low level of administration work is performed (e.g., creating a few users, updating employee information, or unlocking accounts). One or more approaches can be used, and they should eliminate the possible problem of administrators not having AD permissions and an Administration Service failing. The approaches used depend on business workflow.

- If few AD administration tasks are performed at a site, then local administrators might access a remote Administration Service. Administrators at remote sites can access an Administration Service at a major location/site. If necessary, native Windows administrative tools can be used to force AD to replicate the changes so that they appear on the local domain controller as soon as possible.

- If local administrators at a site do not normally need access to AD, then an Administration Service would not have to be installed in that site. An administrator at a major site can make changes for a user at a remote site, and if necessary forced replication can cause the changes to appear quickly at the user's local domain controller.

With ActiveRoles Server user interfaces, the administrator can deliberately choose the domain controller where to apply the changes, thus eliminating data replication delays.

- An organization might provide one or more administrators at each site with permissions to AD. For example, if a site has five administrators, one administrator would be given permissions to AD. This solution would be acceptable for most sites, except for small sites managed by very low-level administrators.

ActiveRoles Server allows administrators to push (synchronize) permissions from ActiveRoles Server to Active Directory, thus making it easier to manage permissions to AD.

# Replication Traffic

Current ActiveRoles Server customers report that replication traffic is negligible and that connection type (i.e., LAN or WAN) is not a factor.

For prospective customers, replication traffic can be judged by considering what is replicated and what is not. In ActiveRoles Server, only ActiveRoles Server configuration information is replicated and only if it is changed. This means that if administrators are not creating Managed Units, Access Templates, Policies and delegating permissions that often, there is not much replication traffic. Unlike AD replication, typically ActiveRoles Server configuration changes occur infrequently. In short, once ActiveRoles Server is setup, if it is not changing much, it does not replicate much data.

A rough estimate of the amount of ActiveRoles Server configuration data that needs to be replicated can be calculated with the ActiveRoles Server Resource Usage Calculator. An organization can calculate an initial size for the Administration Database. Then, estimate the number of changes (i.e., new Access Templates, Managed Units, links, etc.) that will be created during a time period—typically, a day—and enter these values into the Resource Usage Calculator to determine a second database size. The difference between the initial size and the second size will be the amount of data that will need to be replicated.

Typically, changes to the ActiveRoles Server configuration information will be controlled by a select group of administrators and made from one Administration Database. Consequently, the estimate from the method described above should be reasonably accurate. However, ActiveRoles Server uses a multi-master database, and changes to ActiveRoles Server configuration data can be made on each Administration Service. If changes are made at different Administration Databases, the estimate from the ActiveRoles Server Resource Usage Calculator will not be exact, and the total replication impact increases slightly.

ActiveRoles Server employs the Microsoft SQL Server to maintain the Administration Database. The replication capabilities of SQL Server facilitate the implementation of multiple equivalent configuration databases used by different Administration Services.

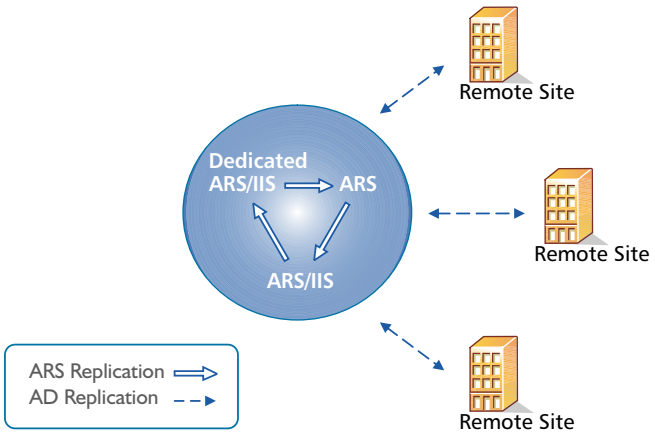
# Locations and Number of Services—Sample Network Diagrams

After considering the major factors that might influence the locations and number of ActiveRoles Server's Administration Services, organizations should have a network diagram that illustrates a high-level design for the ActiveRoles Server deployment.

The following high-level sample network diagrams illustrate potential ActiveRoles Server deployments using the guidelines described earlier.

## Centralized

This diagram shows a centralized network and workflow (the ARS abbreviation refers to ActiveRoles Server's Administration Service).




In this centralized structure, all AD data management is done from the corporate headquarters by a group of network administrators and the Help Desk staff. The headquarters is a large campus location with several well-connected sites. Most employees work at the headquarters. Large remote sites will have networking personnel who are responsible for the tasks such as hardware and software setup and maintenance. Small remote sites are staffed by non-technical employees. Network maintenance for these sites is done by IT staff that travels to them or by contractors.

The number of Administration Services depends on the number of managed objects and administrators. In the diagram, there is one dedicated Administration Service (ARS Service) and two Administration Services on shared hardware. This number should assure both availability and redundancy. Other services on the shared hardware include printing and applications.

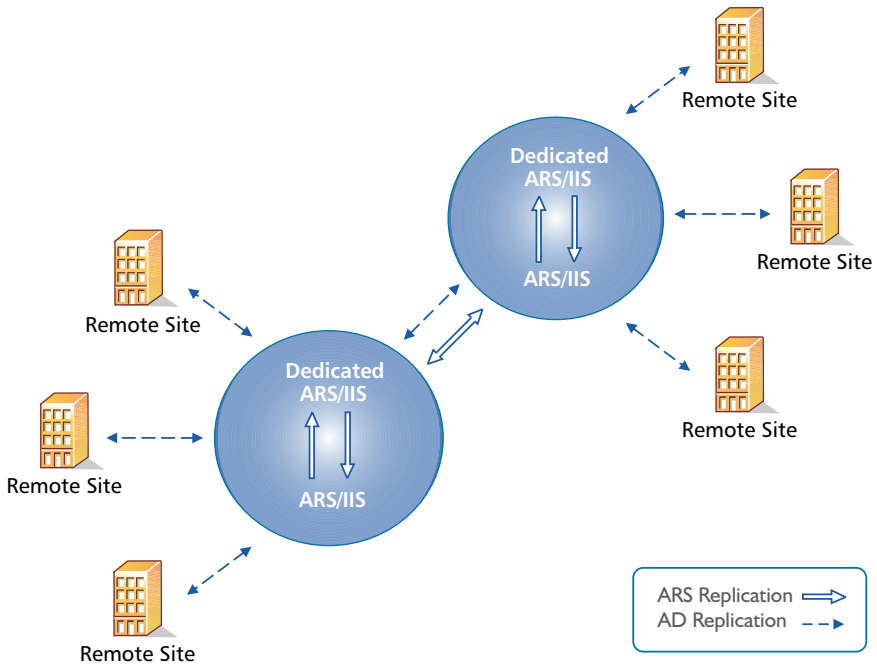
A small number of administrators use the ActiveRoles Server MMC Interface, while the majority of administrators and all Help Desk personnel use the Web Interface.

Typically, customers do not install all Administration Services at one location, but in this case, one or both of the following business workflow and technical factors over rule that guideline:

- The remote sites are lightly populated and require very little AD data management work.
- It is determined that if the connection to the central site fails, the organization's primary concern would be restoring the connection, not managing AD.

## Distributed with No Remote Management

This diagram shows a distributed network and workflow (the ARS abbreviation refers to ActiveRoles Server's Administration Service).




In this scenario, AD data management is performed at major locations by a group of network administrators and the Help Desk staff. These locations can be campuses or single locations connected by LAN/WAN connections.

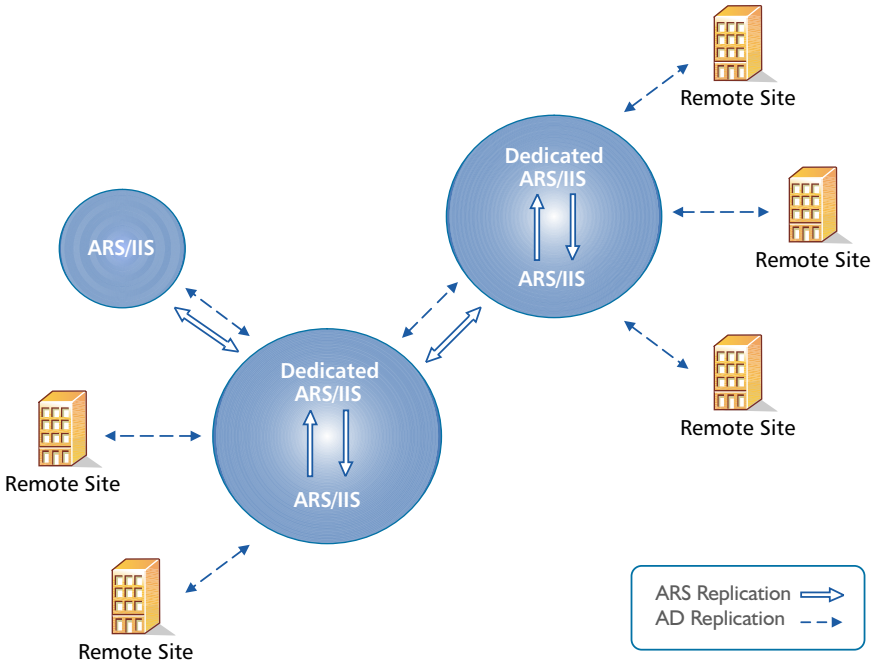
Large remote sites have networking personnel who are responsible for tasks such as hardware and software setup and maintenance. Small remote sites are staffed by non-technical employees. Network maintenance for these sites is done by IT staff that travels to them or by contractors.

Again, the number of Administration Services depends on the number of managed objects and administrators. In the diagram, there is one dedicated and one shared Administration Service per location. This setup assures both redundancy and availability at each major location and through out the network. If one Administration Service fails, the other Service at the location can be used. If both services at a location fail, AD data management can be done at the other location. As long as the connections function, administrators at the failed location can access the Administration Services at the functioning location.

At both locations a small number of administrators use the ActiveRoles Server MMC Interface, while the majority of administrators and all Help Desk personnel use the Web Interface.

## Distributed with Remote Management

This diagram illustrates a highly distributed network and workflow (the ARS abbreviation refers to ActiveRoles Server's Administration Service).




In this scenario, AD data management is performed at all locations. These locations can be campuses or single locations connected by LAN/WAN connections. The work is done by a group of network administrators and the Help Desk staff. Work group managers perform very low-level work such as access to specific file directories and distribution lists.

The number of Administration Services depends on the number of managed objects, administrators, and locations. In the diagram, there is one dedicated and one shared Administration Service at the large locations. This setup assures both redundancy and availability at each major location and through out the network. If one Administration Service fails, the other server at the location can be used. If both Administration Services at a location fail, AD management can be done at the other location. As long as the connections function, administrators at the failed location can access the Administration Services at the functioning location.

A third, midsize location has an Administration Service installed on shared hardware. Administrators at this location use a Web interface, so the hardware also hosts IIS. An Administration Service was installed at this location because the location had a significant number of users that needed AD management work and Help Desk support. Placing an Administration Service in this location balances the load on the services while improving redundancy and availability. If this location and the network grow, the need might develop for establishing connections and replication between the three largest sites.

Administrators at the smallest locations access the Administration Services at the large locations via the Web Interface. The reason for this is the number of users and administrators and their workload.

At both large locations a small number of administrators use the ActiveRoles Server MMC Interface, while the majority of administrators and all Help Desk personnel and work group managers use the Web Interface.