One Identity Active Roles

Quick Start Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Active Roles Quick Start Guide
Updated - September 2022
Version - 7.5.4

Contents

1

Introduction

Active Roles simplifies and streamlines creation and ongoing management of user accounts and groups in Windows Active Directory (AD) environments by automating user and group account creation in AD, Azure AD, mailbox creation in Exchange and Exchange Online, group population, and resource assignment in Windows.

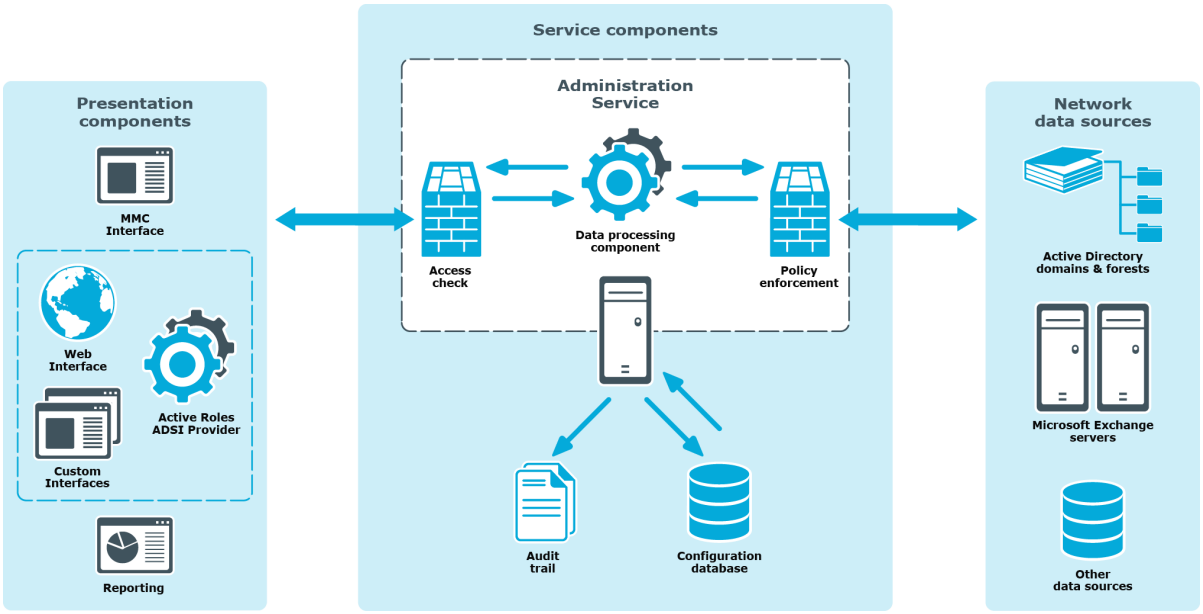
It provides strictly enforced security, rich capabilities for automating directory management tasks, change approval and easy-to-use Web interfaces, to achieve practical user and group account management for the Windows enterprise.

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

Active Roles components

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

Figure 1: Active Roles Components



The presentation components include client interfaces for the Windows platform and the Web, which allow users with appropriate rights to perform a precisely defined set of administrative activities. Active Roles 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 Active Roles 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 instances of the Administration Services can be deployed to improve performance and ensure fault tolerance.

The Administration Service uses the configuration database to store configuration data that includes definitions of objects specific to Active Roles, assignments of administrative roles and policies, and procedures used to enforce policies.

The Administration Service provides a complete audit trail by creating records in the Active Roles 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.

Active Roles Setup package

The Active Roles distribution Media folder constitutes the following:

- ActiveRoles.exe
- Components
- Documentation
- Redistributables
- Solutions
- Active Roles Release Notes

Table 1: Active Roles Media contents and description

Media content	Description
ActiveRoles.exe	The executable file allows you to start the Setup wizard and install the Active Roles components.
Components	Provides separate installer files for the following Active Roles components which enables you to install the default Active Roles components individually: • ADSI Provider • Configuration Center • Management Shell • MMC Console • Administration Service • Web Interface • ActiveRoles Synchronization Service
Documentation	Provides the product documentation including the Resource Usage calculation file.
Redistributables	Provides the pre-requisite redistributables for the latest Active Roles version
Solutions	Provides the installer files for the following additional components: • Add-in for Outlook • Add-on Manager • Collector and Report Pack • Configuration Transfer Wizard • Diagnostic Tools

Media content	Description
	• Management Pack for SCOM • SPML Provider • Sync Service Capture Agent • Administrative Template
Release Notes	Provides information about the latest Active Roles release and the hardware and software requirements for Active Roles and its components.

Active Roles installation

The Active Roles distribution Media folder contains the executable file and installers for the default and additional components that enable you to install Active Roles and its components on your computer.

To install Active Roles and its components

1. Before installing Active Roles and its components, make sure that all installation prerequisites are met. For information on the hardware and software requirements for each component, see System Requirements in the *Active Roles Release Notes*.

   NOTE: Installing the requisite Active Roles components to an offline Active Roles server (with no internet connection available) requires manual installation steps. For more information, see Knowledge Base Article 299533.

2. Navigate to the location of the Active Roles distribution package, double-click **ActiveRoles.exe** and start the Setup wizard.
3. Follow the instructions in the Setup wizard.

   Based on the components selected, the Administration Service, Configuration Center, Web Interface, Management Shell, MMC Console, and ADSI Provider are installed on the system.

   Alternatively, you can also download the installer file and install individual components manually from the respective component folder.
4. Configure the Administration Service and other installed components.

   NOTE: The Administration Service must be configured and running to configure and start any other Active Roles components.

   For information on installing and configuring the Administration Service see Deploying the Administration Servicesection.

   For information on installing and configuring the user interfaces see the Deploying user interfaces section.
5. In addition to Active Roles default components, you can install and configure the following additional solutions components provided by Active Roles:

- Add-in for Outlook
- Add-on Manager
- Collector and Report Pack
- Configuration Transfer Wizard
- Diagnostic Tools
- Management Pack for SCOM
- SPML Provider
- Sync Service Capture Agent
- Administrative Template

For information on installing and configuring the additional solutions components, see Installing additional components.

NOTE: For more information on extending the Active Roles provisioning and account administration capabilities to your cloud applications, click **Learn More** in the **Setup Progress** window.

Active Roles uninstallation

To uninstall Active Roles and its components

1. On the system where Active Roles is installed, go to the **Control Panel**, and navigate to **Programs**| **Programs and Features**.
2. In the list of installed programs, right-click on **One Identity Active Roles**, and click **Uninstall/Change**.

   The Active Roles Setup window is displayed.
3. Click **Remove**.

   The Active Roles Setup - Ready to Remove dialog box is displayed.
4. Click **Remove**, to uninstall Active Roles.

NOTE: Alternatively, click **Modify** to add or remove the Active Roles components. Click **Repair** to re-install the corrupt files in Active Roles.

2

System requirements

Active Roles Setup includes the following components:

- Administration Service
- Console (MMC Interface)
- Web Interface
- Management Tools
- Synchronization Service

The Active Roles Release Notes document, included on the Active Roles distribution media, provides information about the hardware and software requirements for each of these components.

The Active Roles distribution media includes separate installation packages for additional components, such as Add-in for Outlook, Collector and Report Pack. The system requirements for these components are as follows:

Table 2:
Active Roles Add-in for Outlook requirements

Requirement	Details
Microsoft Office Outlook	Microsoft Office Outlook 2010 or later (32-bit) NOTE: The Active Roles Add-in for Outlook does not support the 64-bit version of Microsoft Office Outlook.
Other Microsoft Office features	• .NET Programmability Support for Microsoft Office Outlook • Microsoft Forms 2.0.NET Programmability Support
Microsoft .NET Framework	Microsoft .NET Framework 4.7.2

Table 3:
Active Roles Collector and Report Pack requirements

Requirement	Details
Operating system	Any operating system listed in requirements for Active Roles Console
SQL Server	Any SQL Server version listed in requirements for Administration Service
SQL Server Reporting Services	Any SQL Server version listed in requirements for Administration Service
Microsoft .NET Framework	Microsoft .NET Framework 4.7.2
Active Roles ADSI Provider	Management Tools of the current Active Roles version must be installed

3

Deploying the Administration Service

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

Table 4: Checklist: Deploying 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. 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. One Identity recommends to have SQL Server and the Administration Service on different systems with reliable network connection. Administration Service can now be configured on Azure databases namely Azure SQL database, Azure SQL Managed Instance and Azure SQL Elastic Pool. One Identity recommends to have proper network topology to allow the Azure database configuration.
Administration Service account	The Administration Service logs on with the account that you specify during installation. The account must have sufficient rights for Active Roles to function properly. Active Roles uses the Administration Service account when accessing a managed domain unless an override account is specified when registering the domain with Active Roles. Therefore, the Administration Service account must have the appropriate rights in any domain for which an override account is not specified. Additionally, the Administration Service account must have sufficient permissions to publish the Administration Service in Active Directory. Information about how to configure the Administration Service

Item to Check	Description
	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 or Azure AD authentication. If you choose Windows authentication, the connection is established using the Administration Service account. In this case, the service account must at minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in the Active Roles database. 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 at minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in the Active Roles database. For connecting to Azure SQL database variants like SQL database and Elastic Pool database using SQL server authentication,the login must be a member of the **dbmanager** fixed database role and have the default schema of **dbo** in the Active Roles database. If you choose Azure Active Directory authentication, the connection is established with the login you are prompted to specify when installing the Administration Service. For more information on what permissions must be granted to the account for connection to SQL Server, see SQL Server permissions later in this document.
Active Roles Admin	Active Roles Admin is a group for which Active Roles does not perform permission checking. If the Administration Service itself has sufficient rights to perform a certain task, then Active Roles Admin can also perform that task using Active Roles. In addition, Active Roles Admin is authorized to perform any task related to the Active Roles configuration, such as adding managed domains and managing replication settings. Therefore, the membership in the Active Roles Admin group should be restricted to highly trusted individuals. By default, Active Roles Admin is the Administrators local group on the computer running the Administration Service. You can change this setting when installing the Administration Service.

Active Roles service account minimum permissions

As Active Roles performs operations on objects on behalf of delegated users, the Active Roles service account requires adequate permissions. It is recommended that the Active Roles proxy account be given the Domain Admin membership to ensure that Active Roles has all the required access.

It is possible to separate the tasks managed by the service account from Domain management by specifying different accounts for the service and for managing the Domain.

The service account credential has five main roles, two of the roles are optional:

- Accessing local resources on the Active Roles Administration Service host.
- Creating the Service Connection Point in Active Directory- This functionality is non-critical and do not prevent the service from functioning as expected. Active Roles clients do not automatically discover the Active Roles Administration Service. Active Roles Clients will still be able to connect if the service name or IP address is available.
- All script modules are executed under the security context of the Active Roles Service Account.
- Connecting to the Microsoft SQL database- This is optional, as an SQL Authentication credential may also be specified.
- Synchronizing native permissions to Active Directory- This is required only if Active Roles is configured to do so.

Access to the Administration Service computer

The service account must be a member of the Administrators group on the computer running the Administration Service.

Service publication in Active Directory

The Administration Service attempts to publish itself in the Active Directory. This enables Active Roles clients to automatically discover the Administration Service. This functionality is non-critical and if permissions are not granted, this will not prevent the service from functioning as expected, instead Active Roles clients won't automatically discover the Active Roles Administration Service. They will still be able to connect if the service name or IP address is available. 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
- Delete the **serviceConnectionPoint** objects in the System container
- Write permission for the keywords attribute of the **serviceConnectionPoint** objects in the System container

Along with the mentioned permissions, 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, provide the permissions to the account by using the ADSI Edit console. The following instructions apply to the ADSI Edit console that ships with Windows Server 2016, Windows Server 2019, or Windows Server 2022.

To grant permissions for Administration Service publication in Active Directory

1. Open the ADSI Edit console and connect to the Domain naming context.
2. In the console tree, expand the System container, right-click the Aelita subcontainer, 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 for the cn value.
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. On the Permission Entry page, configure the permission entry:
    - Click the Select a principal link, and select the desired account.
    - Verify that the Type box indicates Allow.
    - Verify that the Applies onto box indicates This object and all descendant objects.
    - In the Permissions area, select the Create container objects and Create serviceConnectionPoint objects check boxes.
    - Click OK
6. Click OK to close the Advanced Security Settings dialog box, and then click OK to close the Properties dialog box.

All script modules are executed under the security context of the Active Roles Service Account

The permissions needed by custom scripts will vary according to the needs of the scripts, and ideally should be reviewed on a case-by-case basis as a Best Practice security model.

Connecting to the Microsoft SQL database

In some configurations, assigning these permissions to the service account are optional, as a SQL Authentication credential may also be specified and the necessary permissions then be assigned to that SQL Authentication credential. For more information on the necessary SQL Server permissions, see *SQL Server Permissions* topic.

Synchronizing native permissions to Active Directory

The service account must have the Read Permissions and Modify Permissions rights on the Active Directory objects and containers where it is desired to use the Active Roles security synchronization feature.

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.

NOTE: When registering a domain with Active Roles, you can specify an override account. If you specify an override account, the Administration Service uses the override account rather than the service account to access the domain.

Access to managed domains

Active Roles 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 account specified, you should configure the service account to have permissions you want Active Roles to have in those domains. If you use an override account when registering a domain with Active Roles, ensure that the override account (rather than the service account) has these permissions for the domain. In addition, the service account (or the override account, if any) must have the **Read Permissions** and **Modify Permissions** rights on the Active Directory objects and containers where you are planning to use the Active Roles security synchronization feature.

For more information, see Active Roles service account minimum permissions.

Access to Exchange Organizations

To manage Exchange recipients on Exchange Server 2019, 2016, or 2013, the service account or the override account must be configured to have sufficient rights in the Exchange organization. The rights must be delegated to the service account if an override account is not used; otherwise, the rights must be delegated to the override account. See the following steps for details.

To configure the service account or the override account

1. Add the account to the **Recipient Management** role group.

   For instructions for Exchange 2019, see "Add Members to a Role Group" at https://technet.microsoft.com/en-in/library/jj657492(v=exchg.160).aspx.

2. Add the account to the **Account Operators** domain security group.
3. Enable the account to use remote Exchange Management Shell.

   For instructions for Exchange 2019, see "Enable Remote Exchange Management Shell for a User" at https://technet.microsoft.com/en-us/library/dd335083(v=exchg.160).aspx.

4. Ensure that the account can read Exchange configuration data (see Configuring the Administration Service account).
5. Restart the Administration Service after you have changed the configuration of the account: Start Active Roles Configuration Center (see "Running Configuration Center" in the Active Roles Administration Guide), go to the **Administration Service** page in the Configuration Center main window, and then click the **Restart** button at the top of the **Administration Service** page.

NOTE:

- For instructions for Exchange 2013, 2016, and 2019, see the relevant Microsoft Exchange pages at https://technet.microsoft.com/en-us/library.
- ARS service account must be a part of **Recipient Management group** to run exchange hybrid commands.

The Exchange 2016 management tools are not required on the computer running the Administration Service.

Permission to read Exchange configuration data

To perform Exchange recipient management tasks, Active Roles requires read access to Exchange configuration data in Active Directory. This requirement is met if the service account (or the override account, if specified) has administrator rights (for example, is a member of the **Domain Admins** or **Organization Management** group). Otherwise, you should give the account the Read permission in the **Microsoft Exchange** container. You can do this by using the ADSI Edit console as follows (these instructions apply to the ADSI Edit console that ships with Windows Server 2016, Windows Server 2019, or Windows Server 2022):

1. Open the ADSI Edit console and connect to the Configuration naming context.
2. In the ADSI Edit console, navigate to the **Configuration | Services** container, right-click **Microsoft Exchange** in that container, and then click **Properties**.
3. On the **Security** tab in the **Properties** dialog box that appears, click **Advanced**.
4. On the **Permissions** tab in the **Advanced Security Settings** dialog box, click **Add**.
5. On the **Permission Entry** page, configure the permission entry:
    a. Click the **Select a principal** link, and select the desired account.
    b. Verify that the **Type** box indicates **Allow**.
    c. Verify that the **Applies onto** box indicates **This object and all descendant objects**.
    d. In the **Permissions** area, select the **List contents** and **Read all properties** check boxes.
    e. Click **OK**.
6. Click **OK** to close the **Advanced Security Settings** dialog box, and then click **OK** to close the **Properties** dialog box.

Support for remote Exchange Management Shell

When performing Exchange recipient management tasks on Exchange Server 2013 or later, Active Roles uses remote Exchange Management Shell to communicate with Exchange Server, so you do not need to install the Exchange management tools on the computer running the Administration Service.

To use remote Exchange Management Shell, the Administration Service must be running on a computer that has:

- Windows Server 2016 or a later.
- Microsoft .NET Framework 4.7.2 installed see https://www.microsoft.com/en-us/download/details.aspx?id=53321).
- Windows Management Framework 5.1 installed (see "Windows Management Framework 5.1" at https://www.microsoft.com/en-us/download/details.aspx?id=54616).

Remote Shell also requires the following:

- TCP port 80 must be open between the computer running the Administration Service and the remote Exchange server.
- The user account the Administration Service uses to connect to the remote Exchange server (the service account or the override account) must be enabled for remote Shell. To enable a user account for remote Shell, update that user account by using the `Set-User` cmdlet with the `RemotePowerShellEnabled` parameter set to `$True`.
- Windows PowerShell script execution must be enabled on the computer running the Administration Service. To enable script execution for signed scripts, run the `Set-ExecutionPolicy RemoteSigned` command in an elevated Windows PowerShell window.

Access to managed AD LDS instances

Active Roles access to Active Directory Lightweight Directory Services (AD LDS) instances is limited by the access rights of the service account, or the override account, if specified. For all managed AD LDS instances with no override account specified, you should configure the service account to have permissions you want Active Roles to have in those instances. If you use an override account when registering an AD LDS instance with Active Roles, ensure that the override account (rather than the service account) has these permissions for that instance.

To control access to directory data, AD LDS provides four default, role-based groups: **Administrators**, **Instances**, **Readers**, and **Users**. These groups reside in the configuration partition and in each application partition, but not in the schema partition. To register an AD LDS instance with Active Roles, the service account or, if specified, the override account must, at a minimum, be a member of the following groups:

- **Instances** (CN=Instances,CN=Roles) in the configuration partition
- **Readers** (CN=Readers,CN=Roles) in the configuration partition and in each application partition

To allow Active Roles full access to the AD LDS instance, add the account to the following group:

- **Administrators** (CN=Administrators,CN=Roles) in the configuration partition

If you add the account to the **Administrators** group, you don't need to add it to the **Instances** or **Readers** group.

Access to file servers

To enable Active Roles 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 Active Roles.

Active Roles 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 Active Roles to manage user home folders.

Access to BitLocker recovery information

Viewing BitLocker recovery passwords in Active Roles requires the domain administrator rights for the account being used by the Active Roles Administration Service to access the domain. Ensure that the service account or, if specified, the override account is a member of the Domain Admins group in each managed domain where you want to use Active Roles for viewing BitLocker recovery passwords.

With the domain administrator rights given to the Active Roles Administration Service, Active Roles allows delegated administrators to locate and view BitLocker recovery passwords held in the Active Directory domain. To view BitLocker recovery passwords, the delegated administrator must be granted the appropriate permissions in Active Roles. The following Access Template provides sufficient permissions to view BitLocker recovery passwords:

- Computer Objects - View BitLocker Recovery Keys

In addition, viewing BitLocker recovery passwords in a given domain requires the following:

- The domain must be configured to store BitLocker recovery information (see http://technet.microsoft.com/en-us/library/dd875529.aspx).
- The computers protected by BitLocker must be joined to the domain.
- BitLocker Drive Encryption must be enabled on the computers.

The BitLocker recovery information is displayed on the **BitLocker Recovery** tab in the computer object's **Properties** dialog box, in the Active Roles console. It is also possible to perform domain-wide searches for BitLocker recovery passwords.

SQL Server permissions

This section discusses the SQL Server permissions required to:

- Configure the Active Roles Administration Service (configuration permissions)
- Run the Active Roles Administration Service (operation permissions)
- Configure replication in Active Roles (replication configuration permissions)
- Run Active Roles replication (replication agent permissions)

Configuration permissions

The account that you use when configuring the Administration Service must have sufficient rights on SQL Server to perform the configuration tasks.

Which account is used to access SQL Server during configuration of the Administration Service depends upon the SQL Server connection option you select in the wizard for configuring the Administration Service. If you select the option to use Windows authentication, the wizard accesses SQL Server with the Windows user account under which the wizard is running. If you select the option to use SQL Server authentication, then the wizard accesses SQL Server with the SQL login and password that you specify in the wizard.

NOTE: Windows authentication is not applicable for configuring Active Roles on Azure database server.

The required rights of the account that is used to access SQL Server during configuration vary depending on your configuration scenario:

- If you want the wizard to create a new database for the Administration Service, then the account must be a member of the **dbcreator** fixed server role.
- For Azure SQL database variants, Azure SQL database and Azure SQL on elastic pool **dbmanager** role should be provided to create databases.
- However, for variant Azure SQL Managed instance, the **dbcreator** fixed server role should be provided.
- If you want the wizard to import data from the Active Roles database of an earlier version, then the account must be a member of the **db_datareader** fixed database role in the source database.
- If you want the wizard to configure the Administration Service to use an existing database of the current version, then the account must be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.
- If you want the wizard to use an existing blank database for the Administration Service, then the account must be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.

Operation permissions

The Administration Service accesses its database with the account specified during configuration:

- If the option to use Windows authentication is selected in the wizard for configuring the Administration Service, then the Administration Service uses its service account to access the database.
- If the option to use SQL Server authentication is selected, then the Administration Service accesses the database with the SQL login and password supplied in the configuration wizard.

In either case, the account must have sufficient rights on SQL Server to retrieve data from, and make changes to, the database. The required rights vary depending on the role of the Administration Service's database server in the Active Roles replication environment.

NOTE: Active Roles does not support replication on Azure SQL databases.

Standalone mode

When initially installed, the Administration Service's database is configured not to participate in Active Roles replication. This configuration is referred to as *standalone Administration Service*. The account that the standalone Administration Service uses to access the database must at a minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.

Publisher mode

If the Administration Service's database server holds the role of the Publisher in Active Roles replication, then the account the Administration Service uses to access the database must at a minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database. Additional rights are required if you want to see the replication status information and error messages in the Active Roles console. These additional rights are as follows:

- Default schema of **dbo** in the **msdb** system database.
- **SELECT** permission on the **sysjobs**, **sysjobsteps** and **MSagent_parameters** system tables in the **msdb** system database.
- **SELECT** permission on the **sysservers** system view in the **master** system database.
- **EXECUTE** permission on the **xp_sqlagent_enum_jobs** system extended stored procedure in the **master** system database.
- **SELECT** permission on the **MSmerge_agents**, **MSmerge_history**, **MSmerge_sessions**, **MSsnapshot_agents** and **MSsnapshot_history** system tables in the distribution database (**AelitaDistributionDB** database by default).

Subscriber mode

If the Administration Service's database server holds the role of a Subscriber in Active Roles replication, then the account that the Administration Service uses to access the database requires the same rights as in standalone mode: The account must at a minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.

Replication configuration permissions

After you install and configure two or more Administration Service instances, each with its own database, you can deploy replication, if necessary, to synchronize the databases so that all your Administration Service instances have the same configuration and management history. Replication deployment begins when you configure the Publisher. Once the Publisher has been configured, the next step is to configure Subscribers. The task of configuring the Publisher or a Subscriber requires more rights on SQL Server than the Administration Service needs for normal operation. To elevate the rights of the Administration Service, Active Roles prompts for an alternative account. The following topics elaborate on the permissions needed to create the Publisher or add a Subscriber.

Permissions for creating or removing the Publisher

To create the Publisher, the Administration Service needs **sysadmin** rights on SQL Server. If the Administration Service's account for database access does not belong to the **sysadmin** role, then Active Roles prompts you to supply an alternative account. The alternative account must:

- Be a member of the **sysadmin** fixed server role on the database server you are going to make the Publisher.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Publisher.

The same permissions are required for removing (demoting) the Publisher.

Permissions for adding or removing a Subscriber

To add a Subscriber, the Administration Service's database server must hold the Publisher role. When adding a Subscriber, the Administration Service makes changes on the Publisher database server and on the database server being configured as a Subscriber (Subscriber database server). Therefore, the Administration Service needs sufficient rights on both database servers.

On the Publisher database server, the Administration Service needs **sysadmin** rights. If the Administration Service's account for database access does not belong to the **sysadmin** role, then Active Roles prompts you to supply an alternative account for connection to the Publisher database server. The alternative account must:

- Be a member of the **sysadmin** fixed server role on the Publisher database server.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Subscriber.

On the database server you are going to make a Subscriber, the Administration Service needs **db_owner** rights in the Active Roles database. If the Administration Service's

account for database access does not have sufficient rights on the Subscriber database server, then Active Roles prompts you to supply an alternative account for connection to the Subscriber database server. The alternative account must:

- Be a member of the **db_owner** fixed database role in the Active Roles database on the database server you are going to make a Subscriber.
- Have the default schema of **dbo** in that database.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Subscriber.

The same permissions are required for removing a Subscriber.

Replication agent permissions

In Active Roles replication, SQL Server replication agents (Merge Agents) are used to synchronize data between the Publisher and Subscriber databases. Each Subscriber has a dedicated replication agent running on SQL Server that hosts the Publisher database. Since the agent's role is to maintain the Publisher and Subscriber databases in sync with each other, the agent needs sufficient rights to access both the Publisher and Subscriber database servers.

The Administration Service creates and configures a replication agent when adding a Subscriber. In terms of SQL Server, this is a Merge Agent for a push subscription. According to SQL Server Books Online (see "Replication Agent Security Model" at msdn.microsoft.com/en-us/library/ms151868.aspx), Merge Agent for a push subscription requires the following permissions.

The Windows account under which the agent runs is used when it makes connections to the Publisher and Distributor. This account must:

- At a minimum be a member of the **db_owner** fixed database role in the distribution database (**AelitaDistributionDB** database by default).
- Be a member of the publication access list (PAL).
- Be a login that is associated with a user in the publication database (the Active Roles database on the Publisher).
- Have read permissions on the snapshot share (by default, this is the **ReplData** folder on the administrative share C$).

The account used to connect to the Subscriber must at minimum be a member of the **db_owner** fixed database role in the subscription database (the Active Roles database on the Subscriber).

By default, the security settings of a Merge Agent configured by Active Roles are as follows:

- The account under which the Merge Agent runs and makes connections to the Publisher and Distributor is the Windows service account of the SQL Server Agent service.
- The account the Merge Agent uses to connect to the Subscriber is the account under which the Merge Agent runs.

This means that, by default, Active Roles requires that the account of the SQL Server Agent service have all permissions the Merge Agent needs to make connections both to the Publisher/Distributor and to the Subscriber.

When adding a Subscriber, you have the option to supply a separate login for connection to the Subscriber. If you choose that option, the Merge Agent will use the login you supply (rather than the account of the SQL Server Agent service) to make connections to the Subscriber. In this case, it is the login you supply that must have **db_owner** rights in the subscription database. The SQL Server Agent service does not need to have any rights in the subscription database. However, it still must have all permissions the Merge Agent needs to make connections to the Publisher and Distributor.

Steps to deploy the Administration Service

Active Roles requires Microsoft .NET Framework 4.7.2. See https://www.microsoft.com/en-us/download/details.aspx?id=53345 for instructions on how to update .NET Framework.

The Administration Service requires Microsoft SQL Server or Azure SQL database 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 Microsoft SQL Server 2012 Express from "Microsoft SQL Server 2012 Service Pack 1 (SP1) Express" at http://go.microsoft.com/fwlink/?LinkID=267905.

Azure SQL Database variants supported in Active Roles are Azure SQL database, Azure SQL Managed Instance, and Azure SQL Elastic Pool.

Now that you have access to SQL Server, you can install the Administration Service.

This section provides a guidance on how to install and configure a new instance of the Administration Service. for instructions on how to upgrade an existing Administration Service instance of an earlier version, see Upgrading the Administration Service later in this document.

To install the Administration Service files

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, ensure that the **Administration Service** component is selected, and click **Next**.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page, confirm that the **I want to perform configuration** check box is selected, and click **Finish**.

The Setup wizard only installs the files. After you have completed the Setup wizard, you need to configure the newly installed Administration Service instance by using Active Roles Configuration Center that opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the Setup wizard. Another way to open Configuration Center is by selecting **Active Roles 7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

To configure the Administration Service

1. In Configuration Center, under **Administration Service**, click **Configure**.
2. Perform the following steps in the Configure Administration Service wizard that appears:
    a. On the **Service Account** page, enter the name and password of the domain user account or the service account details of the Group Managed Service Account (gMSA), to be used as the Administration Service account.
    b. On the **Active Roles Admin** page, accept the default account, or click **Browse** and select the group or user to be designated as Active Roles Admin.
    c. On the **Database Options** page, select the appropriate option, and then follow the instructions in the wizard.

The database options are related to setting up the database for the Administration Service you are configuring. These options and the corresponding wizard steps are discussed in the sections that follow.

Configuring the initial Administration Service

This section covers the database-related steps of the Configure Administration Service wizard in a scenario where you are configuring the first Administration Service in your environment.

To configure the initial Administration Service

1. On the Configure Administration Service wizard, on the **Database Options** page, select the **New Active Roles database** or the **Existing Active Roles database** option, and then click **Next**.
2. On the **Connection to Database** page, specify a database type, database server instance, database name, and select the authentication option for the Configuration database:
    a. In the **Database Server name** box, specify a SQL Server instance in the form <*Computer*>\<*Instance*> (for named instance) or <*Computer*> (for default instance), where <*Computer*> stands for the short name of the computer running SQL Server. The wizard will create the database on the SQL Server instance you specify.
    b. In the **Database** box, enter a name for the database that will be created.
    c. Under **Connect using**, select the appropriate authentication option:

- To have the Administration Service connect to the database using the service account, click **Windows authentication**.

  NOTE: Windows authentication is not applicable for configuring Active Roles in Azure database server.

- To have the Administration Service connect to the database using an SQL Server login, click **SQL Server authentication** and enter the login name and password.
- To have the Administration Service connect to the database using an Azure AD login, click Azure Active Directory authentication and provide the login name and password.

d. (Optional) To configure advanced database settings (connection timeout intervals, failover instances and SQL database auto-shrinking), open the **Advanced Database Properties** dialog by clicking the **Configure advanced database properties** link. Configure any of the available advanced settings.

- In the **Connection Timeout** text box, enter the timeout interval in seconds. This value specifies the time to wait while trying to establish a connection before terminating the attempt and generating an error. The minimum value is 1 second.

  NOTE:

  - The default connection timeout value corresponds to the SQL OLEDB connection timeout.
  - This setting is not applicable to Azure databases.

- (Optional) Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to enable MultiSubnetFailOver, providing faster detection and connection times to active servers. For more information, see SqlClient Support for High Availability, Disaster Recovery in the *Microsoft ADO.NET* documentation.
- (Optional) Select the check box **Enable SQL auto shrink** to allow background tasks to shrink the SQL database.

  NOTE: Consider the following when using this setting:

  - Frequent grow and shrink operations can result in performance and fragmentation issues. Therefore, the **Enable SQL auto shrink** setting is not selected by default. One Identity recommends selecting this setting only if your database is already pre-configured and pre-grown to the required size, as this can prevent frequent shrink and growth operations on the database file. For more information on the potential performance issues, see Recommendations and guidelines for setting the AUTO_SHRINK database option in SQL Server in the *Microsoft SQL Server 2008 Enterprise* documentation.

- The **Enable SQL auto shrink** option is displayed only if the Administration Service is configured with the new Active Roles database option for Configuration Databases or Management History databases.
- This option is not available if you select the **Existing database** or the **New Active Roles database** > **Use pre-created blank database** option during configuration.
- This setting is not applicable to Azure databases.

3. On the Connection to MH Database page, perform the steps a to d for the Management history database.
4. Click **Next**, and then complete the **Encryption Key Backup** page as described in Steps to deploy the Administration Service, later in this document.

   NOTE: This <name of window> window is displayed only if the Administration Service is configured with the **New Active Roles database** option for either the configuration or management history database.
5. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Backup of encryption key

When you configure the initial Administration Service, Configuration Centers creates a database along with a secret key that the Administration Service will use to encrypt and decrypt sensitive data in the database, such as the credentials of the override accounts for managed domains, Azure administrator user password.

The secret key, also referred to as encryption key, is stored in the database using asymmetric cryptography so that it can only be retrieved and decrypted by the Administration Service that knows the private portion of the asymmetric key pair. Storing the secret key in this way ensures the optimal level of protection for security-sensitive data in the Active Roles database.

As the retrieval of the secret key requires knowing the private key related to the public key that was used to encrypt the secret key, you may encounter a situation where a new Administration Service instance attached to an existing Active Roles database is unable to retrieve the secret key. Typically, this is the case when you:

- Attach a new Administration Service instance to an Active Roles database that is used by other instances of the Administration Service while there is no running instance that could decrypt the secret key.
- Import Active Roles configuration data from another database (for example, a databases of an earlier Active Roles version). In this case, you need the secret key that is used for data encryption in the source database; otherwise, the encrypted data cannot be imported.

If the Administration Service cannot retrieve the secret key from the database, you need a backup copy of the secret key. Configuration Center prompts you to create a backup of the secret key whenever you perform initial configuration of the Administration Service with the option to create a new database.

On the **Encryption Key Backup** page, the Configure Administration Service wizard specifies a file to store a backup copy of the secret key. You can encrypt the backup by protecting the file with a password.

NOTE:

- The encryption key is only used to encrypt passwords for domain override accounts (including AD LDS instances). Other than passwords, we do not encrypt any other data.
- By default, the encryption key will be created in the following folder: **C:\ProgramData\One Identity\Active Roles** with a default name of:**ARServiceEncryptionKey-dj-ars<*version*>.bin**.
- If you lose your encryption key, you can still use Active Roles using one of the following:
  - Since the encryption key is used for the Managed Domain password encryption, you can simply install Active Roles and use a new database and import the settings from the old database. You will be prompted to create a new encryption key file.
  - Another method is to bring up an additional Active Roles service. It can retrieve the encryption key from an already running Active Roles service machine (you will be presented with the option to do so during installation).
  - In case you do not have the encryption file for your original Active Roles service, you can still upgrade to 6.9 from 6.x. You must create a new key if required.
  - If you have multiple Active Roles services sharing one database, you really do not need the encryption key as Active Roles can pull the encryption information from the existing running system.
  - Encryption key file is not used during upgrade.
- You need Active Roles encryption key in the following cases:
  - To add another Active Roles service to existing shared database
  - There are no services connected to the same database up and running
  - You cannot afford re-typing passwords for managed domains

Additional Information

Active Roles encrypts some data, stored in the Active Roles database. Encryption is performed using a symmetric cypher. To use the encrypted data you need the encryption key as the file is password protected. Active Roles stores the encryption key inside the Active Roles database using asymmetric cypher. Thus Active Roles can get the value of this key from the database. Active Roles also has logic that allows the service to share this key with other services (like several services per single database). In case the key is lost, you need to re-type passwords for the managed domains. The only situation when you would need this file, would be when you want to use existing Active Roles database but cannot afford retyping passwords for Managed Domains.

To complete the Encryption Key Backup page

1. If you want to change the name or location of the backup file, click the **Browse** button and specify the desired file name and location. The wizard will save a copy of the secret key to the file specified.
2. If you want to encrypt the backup, select the **Protect the backup file with a password** check box, and then type and confirm a password. You will have to enter the specified password to retrieve the key from the backup file. If you lose or forget the password, it cannot be recovered.

Configuring an additional Administration Service

This section covers the database-related steps of the Configure Administration Service wizard in a scenario where:

- At least one instance of the Administration Service version Active Roles is up and running in your environment.
- You are installing one more Administration Service instance for load distribution and fault tolerance.

To configure an additional Administration Service

1. On the **Database Options** page in the Configure Administration Service wizard, select one of the following options, depending upon how you want to synchronize the configuration of the new Administration Service instance with the configuration of the existing Administration Service instances:
    - **Existing Active Roles database** Configures the new Administration Service instance to use the database of an existing Administration Service instance so that the new Administration Service instance has the same configuration as the existing instance.
    - **New Active Roles database** After configuring the new Administration Service instance, you will need to set up Active Roles replication for the new Administration Service instance to have the same configuration as the existing instances.
2. If you have selected the **Existing Active Roles database** option, follow the instructions provided later in this section (see Steps to deploy the Administration Service).
3. If you have selected the **New Active Roles database** option, use the instruction provided in the previous section (see Steps to deploy the Administration 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 Service instances 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, see the Active Roles Administration Guide.

Using common database

If you select the **Existing Active Roles database** option on the **Database Options** page, the Configure Administration Service wizard causes the new Administration Service instance to connect to the database of an existing Administration Service instance. The new instance automatically becomes a replica of the existing one.

This option allows you to centralize the Active Roles configuration storage. You can deploy multiple Administration Service instances of the same configuration without having to synchronize them via replication. Rather, you have the option for multiple Administration Service instances to share configuration data held in a single database on centrally deployed SQL Server.

This option also ensures that the newly deployed Administration Service instance can immediately be used as a replacement for the existing one. Switching between Administration Service instances is transparent to Active Roles users as both instances of the Administration Service have the same configuration.

To configure the Administration Service to share a database

1. On the **Database Options** page in the Configure Administration Service wizard, select the **Existing Active Roles database** option, and then click **Next**.
2. On the **Connection to Database** page, specify Database type, Database Server name, and Database fields. Specify the SQL Server instance and the name of the database being used by an existing instance of the Administration Service version Active Roles.

   Specify the SQL Server instance in the form <*Computer*>\<*Instance*> (for named instance) or <*Computer*> (for default instance), where <*Computer*> stands for the short name of the computer running SQL Server.
3. On the **Connection to Database** page, under **Connect using**, select the appropriate authentication option:
   - To have the Administration Service connect to the database using the service account, click **Windows authentication**.
   - To have the Administration Service connect to the database using an SQL Server login, click **SQL Server authentication** and enter the login name and password.
4. On the **Connection to MH Database** page, specify the database type, database server name, and the name of the database, and select the desired authentication option for the Administration Service connection to the management history database.
5. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply.**:
   - On the **Advanced Database Properties** dialog box, in the **Connection Timeout** text box, enter the time in seconds. This value indicates the amount of time trying to establish a connection before terminating the attempt and generating an error.

NOTE:

- Default connection time out is as per the SQL OLEDB connection timeout.
- A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
- If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.

  If you enter a value less outside the specified range, an error is displayed.
- Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to enable MultiSubnetFailOver.
- The settings available on Advanced Database properties are not applicable for Azure databases.

6. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Advanced scenarios

This section covers the database-related steps of the Configure Administration Service wizard in the following scenarios:

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

Using the database of an earlier Administration Service installation

When you deploy the Administration Service, you may need to configure it to use the database of an earlier installation of the Administration Service instead of creating a new database. You may need to do so in the following scenarios:

- Restoring the Active Roles database from a backup, and then configuring the Administration Service to use the restored database.
- Repairing the Active Roles installation by using **Programs and Features** in Control Panel.
- Installing a maintenance release of Active Roles to update the existing Administration Service instance.

NOTE: All these scenarios assume that the database has the same version as the Administration Service you are configuring. 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 Steps to deploy the Administration Service later in this document).

Provided that the database is of the same Active Roles version as the Administration Service you are configuring, you can use the following steps to make the Administration Service use that database.

To use the database of an earlier Administration Service installation

1. On the **Database Options** page in the Configure Administration Service wizard, select the **Existing Active Roles database** option, and then click **Next**.
2. On the **Connection to Database** page, specify the Database type, Database Server name, and the name of the database. Select the desired authentication option for the Administration Service connection to the configuration database.
3. On the **Connection to MH Database** page, specify the Database type, Database Server name, and the name of the database. Select the desired authentication option for the Administration Service connection to the management history database.
4. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply.**:
    - On the Advanced Database Properties dialog box, in the **Connection Timeout** text box, enter the time in seconds for the database connection to get timed out.

      If you enter a value less outside the specified range, an error is displayed.
    - Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to eable MultiSubnetFailOver.

    NOTE:
    - Default connection time out is as per the SQL OLEDB connection timeout.
    - A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
    - If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.
5. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Using a pre-created blank database

When you choose the option to create a new Active Roles database, the Configure Administration Service wizard uses default values for database properties, such as the location and other parameters of the database files and transaction log files. If you need specific database properties, then you can use SQL Server tools to create a blank database with the properties that meet your requirements, and have the wizard create the new Active Roles database by adding the Active Roles tables and data to that blank database. The following steps assume that you have a blank database already created.

To use a pre-created blank database

1. On the **Database Options** page in the Configure Administration Service wizard, select the **New Active Roles database** option, select the **Use a pre-created blank database** check box, and then click **Next**.
2. On the **Connection to Database** page, specify the Database type, Database Server name and the name of the database. Select the desired authentication option for the Administration Service connection to the configuration database.

3. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply.**:
    - On the Advanced Database Properties dialog box, in the **Connection Timeout** text box, enter the time in seconds. This value indicates the time to wait while trying to establish a connection before terminating the attempt and generating an error.

    NOTE:
    - Default connection time out is as per the SQL OLEDB connection timeout.
    - A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
    - If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.

If you enter a value less outside the specified range, an error is displayed.

4. Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to enable MultiSubnetFailOver.
5. On the **MHDatabase Options** page, select the **New Active Roles database** option, select the **Use a pre-created blank database** check box, and then click **Next**.
6. On the **Connection to MH Database** page, specify the Database type, Database Server name and the name of the database. Select the desired authentication option for the Administration Service connection to the management history database.
7. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Importing configuration data

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

- Upgrading the Administration Service while preserving its configuration.
- Restoring configuration data from a backup copy of the database whose version does not match the version of the Administration Service.

During import configuration, the import configuration page notifies you to select a tenant from the list of tenants configured in the source database, from the **Azure Tenant association** section and the selected tenant is associated with all Azure objects in the destination database. You can also choose to **Run Azure Tenant association immediately** or **Schedule Azure Tenant Association**, where you select the date and time from the Calendar to run the tenant association.

NOTE: If Azure Tenant association is scheduled at a certain time and the upgrade/import operation is still in progress or completes after the Azure Tenant association scheduled time, the tenants are not associated. You have to run the built-in scheduled task **Update Azure Objects Associated Tenant Id** from the Active Roles console to manually associate the Azure Tenants.

For in-place upgrade , in upgrade configuration page notifies you to select a tenant from the list of tenant configured in the Source database, from the **Azure Tenant association** section and the selected tenant is associated with all Azure objects in the destination database. You can also choose to **Run Azure Tenant association immediately** or **Schedule Azure Tenant Association**, where you select the date and time from the Calendar to run the tenant association.

NOTE:

- Alternatively, Azure Tenant association can be run at any time using the template workflow Update Azure Objects Associated Tenant Id available in the Built-in Workflow Container. The parameter in the script used by the workflow can be configured with the required tenant ID. You can use the drop-down to select a default Azure Tenant from the list of available Azure Tenants. The script used by the workflow can be modified to Search Azure objects based on the requirement.
- Depending on the infrastructure, the import operation may take several minutes to complete.

The **Services association** page allows you to configure the Administration services for executing Dynamic Groups, Group Families, and Scheduled tasks from the drop-down list.

The available options in the drop-down list are **This Server** and **Other**, where choosing **Other** allows to specify any other Administration Service in fully qualified domain name (FQDN) format. If the value is empty, then the current administration service is used.

NOTE: Services association does not update certain scheduled tasks, For example, scheduled tasks that cannot be edited (Managed Object Counter) or scheduled tasks that are set to **All servers** option.

You can choose to run the Services association immediately or schedule service association.

NOTE: Alternatively, Services association can be performed any time using the template workflow **Update Services To Execute On** available in the built-in Workflow Container. The parameters in the script used by the workflow can be configured to the required administration services, such as, **Dynamic Group Service**, **Group Family Service**, **Scheduled Task Service**. You can select the administration service from the drop-down list. The drop-down list displays all the currently running administration services that are connected to the current configuration database. If the parameter value is not selected, then the current administration service is used.

To ensure Dynamic Groups, Group Families, and Scheduled tasks continue to function after an import the installation configures the new Active Roles server as the executing server for the tasks mentioned above. The configuration mentioned here runs after an upgrade.

The following instructions on how to import configuration data are applicable to any situation where you choose to create a new database when configuring the Administration Service. In this case, after you have initially configured the Administration Service

instance, Active Roles Configuration Center enables you to import the configuration data to the newly created database.

To import configuration data

1. In the Configuration Center main window, under **Administration Service**, click **Manage Settings**.

   You can start Configuration Center by selecting **Active Roles 7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. On the **Settings** page, in the **Active Roles database** area, click **Import configuration**.
3. On the **Source database** page in the Import configuration wizard that appears, specify the database from which you want to import the configuration data (source database):
   a. Select the required Database Type. In the **Database Server name** box, specify the SQL Server instance that hosts the source database.
   b. In the **Database** box, specify the name of the source database.
4. Under **Connect using**, select the appropriate authentication option:
   - If your Windows logon account has sufficient rights to write data to the destination database, click **Windows authentication**.
   - If you have a SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.
   - If you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.
5. Click **Next** to proceed to the **Destination database** page.

   The **Destination database** page identifies the database of the Administration Service to which you are going to import data (destination database), and allows you to select the authentication option.

5. On the **Destination database** page, under **Connect using**, select the appropriate authentication option:
   - If your Windows logon account has sufficient rights to write data to the destination database, click **Windows authentication**.
   - If you have a SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.
   - If you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.
6. Click **Next**.
7. On the **Add-on advisor** page, the add-ons for the earlier version of Active Roles are displayed.

   NOTE: The Add-ons must be uninstalled manually from the earlier version using the Active Roles Add-on Manager and from the system where ever applicable, before

continuing configuration import.

8. Click **Next**, and then, on the **Import of Encrypted Data** page, choose from the following options:
   - If you have a backup of the secret key for the source database (see Steps to deploy the Administration Service), click **Use a backup of encryption key to import encrypted data** and then click **Browse** to specify the backup file. If the backup file is password-protected, type the password in the **Password** box.
   - If you don't have a backup of the secret key for the source database, click **Do not import encrypted data**. In this case, the encrypted data from the source database, such as the override account's password for managed domain registrations, will not be available in the destination database, so you will need to re-enter the override account's password in the managed domain registrations with the Administration Service that uses the destination database.
9. The **Azure Tenant association** page displays the lists of configured Azure tenants in the source database and options for association.

   NOTE: This page is visible only if the tenants are present in the source database.
10. The **Services association** page allows you to configure the Administration services for executing Dynamic Groups, Group Families, and Scheduled tasks from the drop-down list.
11. View the Summary page to review database configuration, Azure Tenant association and Service association details.
12. Click **Next**, and follow the instructions in the wizard to complete the import operation.

Importing management history data

A part of the Active Roles database, the management history data storage is empty after you have configured the Administration Service with the option to create a new database. During import of configuration data (see Steps to deploy the Administration Service), Configuration Center transfers only the administrative right assignments, policy definitions, administrative view settings, workflow definitions and other parameters that determine the Active Roles work environment. Management history data is excluded from the import operation in order to reduce the time it takes to upgrade the configuration of the Administration Service.

The management history data describes the changes that were made to directory data via Active Roles. This includes information about who did what and when it was done as applied to the directory data management tasks. The management history data is used as a source of information for the change history and user activity reports. In addition, the management history data storage holds information about various tasks related to approval workflow and temporal group membership.

After you have configured the Administration Service with the option to create a new database, and imported the configuration data from an existing database, you need to take additional steps to transfer the management history data from that database to the new

database. Configuration Center provides the Import Management History wizard to perform this task.

The wizard is intended to populate a new storage of management history data with the data found in an existing Active Roles database, to make the data available to the Active Roles user interfaces after your configure a new Administration Service instance. The wizard merges the management history data from 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 legacy management history data at any time after you have configured the Administration Service, without being afraid of losing any data.

To import Management History data

1. In the **Configuration Center** main window, under **Administration Service**, click **Manage Settings**.

   Start the Configuration Center by selecting **Active Roles7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending on the version of your Windows operating system.
2. On the **Administration Service** page, click **Import Management History** to open the Import Management History wizard.
3. On the **Source database** page, specify the database from which you want to import the management history data (source database):
   a. **Database Type**: Select the required database type from the drop-down (on premises or Azure SQL).
   b. **Database Server name**: Enter the name of the SQL Server instance that hosts the source database.
   c. **Database**: Enter the name of the source database.
4. Under **Connect using**, select the authentication option:
   - If your Windows logon account has sufficient rights to write data to the destination database, click **Windows authentication**.
   - If you have a SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.
   - If you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.

   NOTE: Azure databases can be connected using SQL Server authentication and Azure AD authentication. Windows authentication is applicable only for on-premises databases.

   NOTE: Azure AD authentication currently does not support Multi-Factor Authentication (MFA).
5. Click **Next**.

   The **Destination database** page identifies the database of the Administration Service to which you are going to import data (destination database), and allows you to select the authentication option.

6. Under **Connect using**, select the authentication option:
    - If your Windows logon account has sufficient rights to write data to the destination database, click **Windows authentication**.
    - If you have a SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.
    - If you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.

    NOTE: Azure databases can be connected using SQL Server authentication and Azure AD authentication. Windows authentication is applicable only for on-premises databases.

    NOTE: Azure AD authentication currently does not support Multi-Factor Authentication (MFA).
7. Click **Next**.
8. On the **Records to Import** page, specify whether you want to import all data records or only a certain range of the data records.

    NOTE: The data for unfinished temporal group membership is imported when the management history data is imported for a selected date range.

    You can choose not to import all the data records as importing a large volume of data can take hours. Later, you can import additional data by choosing a different range of data records. During subsequent import sessions, the wizard only imports the data records that were not imported earlier.
9. Click **Next** and follow the instructions in the wizard to complete the import operation.

Deploying user interfaces

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

- **Web Interface** A customizable Web application for directory administration.
- **MMC Interface** A desktop console for Active Roles configuration and directory administration.

By default, the Active Roles Setup wizard installs all core Active Roles components, including the console (MMC Interface) and Web Interface. You can choose to install individual components, if needed.

Steps to install the console

The Active Roles 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 Active Roles console

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, ensure that the **Console (MMC Interface)** component is selected, and click **Next**.

   By default, all components are selected. If you only want to install the console, clear the check boxes that denote unwanted components.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page click **Finish**.

Once you have installed the console, you can start it by selecting **Active Roles 7.5.4 Console** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

Steps to deploy the Web Interface

The Active Roles Web Interface can be installed on any computer that meets the system requirements and is running Internet Information Services (IIS) 7.5 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.

Checking Web Interface prerequisites

Windows Server 2016 and Windows Server 2019

On a Windows Server 2016 or Windows Server 2019 based computer, ensure that the **Web Server (IIS)** sever role is installed, including:

- Web Server/Common HTTP Features/
    - Default Document
    - HTTP Errors
    - Static Content
    - HTTP Redirection
- Web Server/Security/
    - Request Filtering
    - Basic Authentication
    - Windows Authentication
- Web Server/Application Development/
    - .NET Extensibility 4.7.2
    - ASP
    - ASP.NET 4.7.2
    - ISAPI Extensions
    - ISAPI Filters
- Management Tools/IIS 6 Management Compatibility/
    - IIS 6 Metabase Compatibility

The Web Interface Setup program configures the **Web Server (IIS)** server role to meet the Web Interface requirements. You can use Server Manager to verify that the server role is configured properly.

Feature delegation

Web Interface requires Internet Information Services to provide **Read/Write** delegation for the following features:

- Handler Mappings
- Modules

Use **Feature Delegation** in the Internet Information Services (IIS) Manager tool to confirm that these features have delegation set to **Read/Write**.

Installing and configuring the Web Interface

When installing and initially configuring the Web Interface, you first use the Setup wizard to install the Web Interface files and then use Active Roles Configuration Center to choose the Administration Service and create the Web Interface sites.

To install the Web Interface files

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, ensure that the **Web Interface** component is selected, and click **Next**.

   By default, all components are selected. If you only want to install the Web Interface, clear the check boxes that denote unwanted components.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page, verify that the **I want to perform configuration** check box is selected, and click **Finish**.

The Setup wizard only installs the files. After you have completed the Setup wizard, you need to configure the newly installed Web Interface by using Active Roles Configuration Center.

The procedure for configuring the Web Interface includes two stages:

- Steps to deploy the Web Interface During initial configuration, the Administration Service is selected, and three Web Interface sites are created based on the default configuration templates.
- Steps to deploy the Web Interface You can create additional sites, and modify or delete existing sites.

Initial configuration

Configuration Center 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

Before configuring the Web Interface, ensure that the Administration Service is configured and started. Otherwise, Configuration Center will fail to configure the Web Interface. You can view the state of the Administration Service on the **Administration Service** page in the Configuration Center main window.

To perform initial configuration of the Web Interface

1. Log on with a user account that has administrator rights on the computer.
2. Open Active Roles Configuration Center.

   Configuration Center opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the Setup wizard. Another way to open Configuration Center is by selecting **Active Roles 7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.
3. In the Configuration Center main window, under **Web Interface**, click **Configure**.

   This starts the wizard that will perform initial configuration of the Web Interface.
4. On the **Administration Service** page, specify how you want the Web Interface to select the Active Roles Administration Service. You can choose from the following options:
   - **Administration Service on the computer running the Web Interface**
   - **Administration Service on this computer**

     Supply the fully qualified domain name of the computer running the desired Administration Service instance.
   - **Any Administration Service of the same configuration as this one**

   Specify any Administration Service whose database holds the desired configuration, by supplying in the fully qualified domain name of the computer running that Administration Service. If Active Roles replication is used to synchronize configuration data, this must be any Administration Service whose database server acts as the Publisher for the configuration database.
5. Click the **Configure** button to start the configuration process.
6. Wait while the wizard completes the configuration.

Configuration Center creates three Web Interface sites based on the following configuration templates:

- **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 User Profile Editor, allowing end users to manage personal or emergency data through a simple-to-use Web interface.

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 customization procedures are covered in the Active Roles Web Interface Administration Guide.

After initial configuration, you can modify Web Interface site parameters, such as the Web application alias, create new Web Interface sites, or delete existing Web Interface sites.

Additional configuration

After initial configuration, you can use Configuration Center to create additional Web Interface sites, as well as modify or delete existing Web Interface 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.

To create, modify or delete a Web Interface site

1. Open Configuration Center.

   You can open Configuration Center by selecting **Active Roles Active Roles Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. In the Configuration Center main window, under **Web Interface**, click **Manage Sites**.
3. On the **Sites** page, do one of the following:
   - To create a new site, click **Create**.
   - To modify an existing site, select the site from the list and click **Modify**.
   - To delete a site, select the site from the list and click **Delete**.
4. View or change the following settings in the wizard that appears if click **Create** or **Modify**:
   - **IIS Web site** Specifies the IIS Web site containing the Web application that implements the Web Interface site. You can select the desired Web site from a list of all Web sites defined on the Web server.

- **Alias** Specifies the alias of the Web application that implements the Web Interface site. The alias defines the virtual path used in the address of the Web Interface site on the Web server.
- **Configuration** Specifies customizable settings of user interface elements, such as menus, commands, and Web pages (forms), displayed by the Web Interface. The configuration of each Web Interface site is stored by the Active Roles Administration Service. Multiple sites may use the same configuration. You can choose from the following options:
  - **Keep the current configuration** Choose this option when modifying an existing Web Interface site if you do not want to assign a different configuration to that site.
  - **Create from a template** Create a new configuration for the Web Interface site based on a template. With this option, you need to supply a unique name for the new configuration and select the desired template.

  Choose this option if you want the Web Interface site to use a separate configuration that is initially populated with the template data.

- **Use an existing configuration** Assign an existing configuration to the Web Interface site. With this option, you need to select the desired configuration from a list of configurations found on the Administration Service. The list includes the configurations of the current Active Roles version only.

  Choose this option if you want the Web Interface site to share its configuration with other Web Interface sites. For example, when creating a new instance of a given site for load balancing, you should assign the configuration of that site to the new Web Interface site.

- **Import from an existing configuration** Create a new configuration for the Web Interface site by importing data from an existing configuration. With this option, you need to supply a unique name for the new configuration and select the desired existing configuration from a list of all supported configurations found on the Administration Service. The list includes the configurations of both the current and earlier Active Roles versions.

  Choose this option if you want the Web Interface site to use a separate configuration that is populated with the data imported from a configuration of an earlier Active Roles version or copied from a configuration of the current Active Roles version.

- **Import from a file** Create a new configuration for the Web Interface site by importing data from an export file. With this option, you need to supply a unique name for the new configuration and select the export file. This can be an export file created by the current Active Roles version or an earlier, supported Active Roles version.

  Choose this option if you want the Web Interface site to use a separate configuration that is populated with the data found in an export file. You could create an export file from the **Web Interface** page in Configuration Center, by selecting a site and then selecting **Export Configuration**. Earlier Active Roles versions used the Web Interface Sites Configuration wizard to export Web Interface site configuration data.

Each Web Interface site can be accessed from a Web browser using the address based the Web application alias:

`http://<WebSite>/<Alias>`

Here, <*WebSite*> identifies the IIS Web site containing the Web application that implements the Web Interface site and <*Alias*> stands for the alias of that Web application, as specified in Configuration Center. For example, if the Web application is contained in the default Web site, the address is http://<*Computer*>/<*Alias*>, where <*Computer*> stands for the network name of the computer (Web server) running the Web Interface.

By default, Web Interface users connect to the Web Interface using a HTTPs transport, which encrypts the data transferred from a Web browser to the Web Interface. If your business process does not require a secure transport for passing data to the Web interface, you can disable the HTTPs option using the Configuration Center and use the HTTP transport.

The secure hypertext transfer protocol (HTTPS) uses Secure Sockets Layer (SSL) provided by the Web server for data encryption. For instructions on how to enable SSL on your Web server, see "Configuring Secure Sockets Layer in IIS 7" at http://go.microsoft.com/fwlink/?LinkID=108544.

Configure Web interface for secure communication

By default, Active Roles users connect to the Web interface using a HTTP protocol, which does not encrypt the data during communication. However, it is recommended to use a HTTPS protocol to transfer data securely over the web. You can use the **Force SSL Redirection** option in the Configuration Center to enable secure communication over HTTPS for the Web interface on local or remote servers.

To configure the Web interface for secure communication for the first time

1. In the Configuration Center main window, click **Web Interface**.

   The Web Interface page lists all the Web interface sites that are deployed on the Web server running the Web interface.

2. To modify the secure communication settings for the sites, click **Force SSL Redirection**.

   The **Manage Force SSL Redirection Settings** for sites window is displayed.

3. In the **Available Websites** field, select the required web site from the drop-down list.

   The configuration status of the website is displayed.

4. To enable the force SSL redirection, switch between the **Enable Force SSL Redirection** states. Turn it on.

   NOTE:

   - If the website is not configured earlier for secure communication, the **Enable Force SSL Redirection** option is not selected by default and the HTTPS configuration status is shown as **Not configured**.

- If the website is configured earlier for secure communication, then the **Enable Force SSL Redirection** option is selected by default and the HTTPS configuration status shows as **Configured**.
- If the website is configured earlier for secure communication, and the SSL bindings was deleted in the IIS site, the **Enable Force SSL Redirection** option is selected by default. The status **Binding Deleted** is displayed. In this case, the secure communication must be configured again for the web site.

5. In the **Available HTTPS Bindings** field, click the drop-down list and select the required binding for the web site.
6. Click **Modify**.

   After successful completion of configuration changes, in the Web Interface window, the Force SSL Redirection configuration state for the selected web site is displayed as green and enabled.
7. Click **Finish**.

   NOTE: The browser cache must be cleared after any changes are made to SSL settings.

   For the configured web site, any HTTP communication is now redirected to HTTPS automatically.

Disabling secure communication for Web interface sites

By default, Active Roles users connect to the Web interface using a HTTP protocol, which does not encrypt the data during communication. However, it is recommended to use a HTTPS protocol to transfer data securely over the web. You can use the **Force SSL Redirection** option in the Configuration Center to enable secure communication over HTTPS for Web interface on local or remote servers.

In case you do not want a secure communication enabled for transferring data over the web, you can disable the HTTPS option using the **Force SSL Redirection** option in the Configuration Center.

To disable the secure communication for Web interface sites

1. In the Configuration Center main window, click **Web Interface**.

   The Web Interface page displays all the Web interface sites that are deployed on the Web server running the Web interface.
2. To modify the secure communication settings for the sites, click **Force SSL Redirection**.

   The Manage Force SSL Redirection Settings for sites window is displayed. The **Enable Force SSL Redirection** option is enabled after HTTPS configuration.

3. In the **IIS Web site** field, select the required web site from the drop-down list.
4. To disable the force SSL redirection, switch between the **Enable Force SSL Redirection** states. Turn it off.
5. Click **Modify** , and then **Finish**.

   NOTE: The browser cache must be cleared after any changes are made to the SSL settings.

   After successful completion of the configuration changes, in the Web Interface window, the Force SSL Redirection configuration state for the selected web site is displayed as not configured.

   After disabling the Force SSL Redirection, all communication is now redirected to HTTP.

For more information on secure communication and Federated Authentication, see Working with Federated Authentication.

Installing additional components

In addition to the Administration Service, MMC Interface and Web Interface, Active Roles allows you to install the following components:

- **Active Roles Management Shell** Provides commands based on the Windows PowerShell platform for managing users, group, computers and other objects in Active Directory via Active Roles; administering certain Active Roles objects; and configuring Active Roles Administration Service instances and Web Interface sites.
- **ADSI Provider** Enables custom applications and scripts to access directory data via Active Roles by using standard COM interfaces. Documentation for ADSI Provider can be found in the Active Roles SDK.
- **Active Roles SDK** Provides developers with documentation and samples to help them customize Active Roles by creating custom client applications and user interfaces, and implementing business rules and policies based on custom scripts.
- **Collector** Gathers data required for reporting. Retrieves data from specified data sources through the Administration Service, and stores the data on database server.
- **Report Pack** A comprehensive suite of report definitions that cover various administrative actions available in Active Roles.

Steps to install only the Shell, ADSI Provider and SDK

Active Roles Management Shell, SDK and ADSI Provider are collectively referred to as management tools. On the **Component Selection** page, the Active Roles Setup wizard selects the **Management Tools** component if you have selected any core component such as **Administration Service**, **Console (MMC Interface)** or **Web Interface**. This means that Setup installs the Shell, SDK and ADSI Provider together with any core component. However, it is possible to install solely the Shell, SDK and ADSI Provider by selecting the **Management Shell** component only.

To install only the Shell, SDK and ADSI Provider

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, clear all check boxes except the **Management Tools** check box, and then click **Next**.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page click **Finish**.

Once you have installed the management tools, you can open Management Shell or view SDK topics (including documentation for ADSI Provider). Depending upon the version of your Windows operating system, select the following on the **Apps** page or **Start** menu:

- To open Management Shell, select **Active Roles 7.5.4 Management Shell**
- To view SDK topics, select **Active Roles 7.5.4 SDK**

After you have opened Management Shell, you can view a reference manual by typing **QuickRef**. The manual contains documentation for all commands provided by Management Shell.

Steps to install Collector and Report Pack

Active Roles comes with a comprehensive suite of report definitions, contained in the Active Roles Report Pack. To work with reports, you need to:

- Install the Active Roles Collector
- Use the Collector wizard to deploy the Report Pack

Installing Collector

The Active Roles Collector is used to prepare data for reporting, allowing you to configure, schedule, and run data collection jobs. Collector stores report data in a database on an on-premises SQL Server or Azure SQL database. For best results, use Microsoft SQL Server 2012 or a later version of SQL Server to host the Collector's database.

NOTE: Collector can now store data in Azure database.

To install the Collector

1. Install Active Roles Management Tools. For installation instructions, see Steps to install only the Shell, ADSI Provider and SDK earlier in this document.
2. In the Active Roles distribution package, navigate to the **Solutions/Collector and Report Pack** folder, and double-click the .msi file held in that folder.
3. Follow the instructions in the Setup wizard.
4. Wait while the wizard completes the installation.

Once you have installed Collector, you can start the Collector wizard by selecting **Active Roles 7.5.4 Collector and Report Pack** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

Deploying Report Pack

Report Pack requires Microsoft SQL Server Reporting Services (SSRS). Make sure that you have SSRS deployed in your environment. When deploying Report Pack, the Collector wizard prompts you for the address (URL) of the Report Server Web service. You can find this address on the **Web Service URL** page in the Reporting Services Configuration Manager tool on the server where SSRS is installed.

To deploy the Report Pack

1. Start the Collector wizard.

   You can start the Collector wizard by selecting **Active Roles 7.5.4 Collector and Report Pack** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. On the **Select Task** page, click **Deploy reports to Report Server**, and then click **Next**.
3. On the **Report Server** page, type the URL of your SSRS Report Server in the **Report Server Web Service URL** box. Click **Next**.

   By default, the URL is http://*<serverName>*/ReportServer. You can use the Reporting Services Configuration Manager tool to confirm the server name and URL. For more information about URLs used in Reporting Services, see the topic "Configure Report Server URLs (SSRS Configuration Manager)" at http://msdn.microsoft.com/library/ms159261.aspx.

4. Optionally, on the **Data Source** page, configure the data source for the Active Roles reports:
   a. Click the **Configure Data Source** button.
   b. Use the **Configure Data Source** dialog box to specify the database server instance that hosts the database you have prepared by using Collector, the name of the database, database type, and the authentication method to use for connection to the database.

Configuring the data source is an optional step. If you do not have a database prepared by Collector, you can configure the data source later, after you have deployed the Report Pack. For instructions, see "Working with reports" in the Active Roles Administration Guide.

5. Click **Next** and wait while the wizard deploys the Report Pack.

You can create and view Active Roles reports using Report Manager, a Web-based tool included with SSRS. For instructions, see "Generating and viewing a report" in the Active Roles Administration Guide.

Upgrade of an earlier version

You can upgrade from Active Roles 7.0.x or later to Active Roles 7.x using one of the following methods:

- In-place upgrade: Install the latest version of Active Roles on the computer without removing the earlier version.
- New installation with import of database from earlier version: Install the latest version of Active Roles and import the database from the earlier version of Active Roles.

NOTE:

- To perform a clean installation of Active Roles, uninstall the currently installed version before installing Active Roles 7.5.4.
- Active Roles supports selection of custom installation path only during a fresh installation. During an in-place upgrade, Active Roles does not support changing the custom installation path.

For information on importing configuration data from the database of an earlier version of Active Roles, see *Import Configuration* under Upgrading the Administration Service.

NOTE: Before upgrading to the latest version of Active Roles, the add-ons of the earlier versions must be uninstalled.

Upgrading from Active Roles 6.9 version to 7.x version is a side-by-side upgrade, which does not interrupt operations or affect the configuration of your earlier Active Roles version. To ensure smooth upgrade to the new Active Roles version, first upgrade the Administration Service and then upgrade the Web Interface.

Active Roles 6.x components are not used in the upgrade and neither are any components from the earlier version uninstalled.

IMPORTANT:
During in-place upgrade, when importing from the source database (Configuration and Management History database), the following database permissions are automatically migrated from the previously used (source) SQL database to the new (destination) SQL database:

- ARS database users with associated permissions.
- SQL logins mapped to ARS database users.

- Roles.

The service account that is used for performing the in-place upgrade or the import or migration operation should have the following permissions in the SQL Server to perform the operation:

- **db_datareader** fixed database role in the source database.
- **db_owner** fixed database role and the default schema of **dbo** in the destination database.
- **sysadmin** fixed server role in the destination database.

By default, the database users, permissions, logins, and roles are imported to the destination database. You can clear the **Copy database users, permissions, logins, and roles** check box in the following locations depending on the operation:

- During in-place upgrade: in the **Upgrade configuration** window.
- Importing configuration: **Import Configuration > Source Database > Configure advanced database properties**.
- Importing management history: **Import Management History > Source database > Configure advanced database properties**.

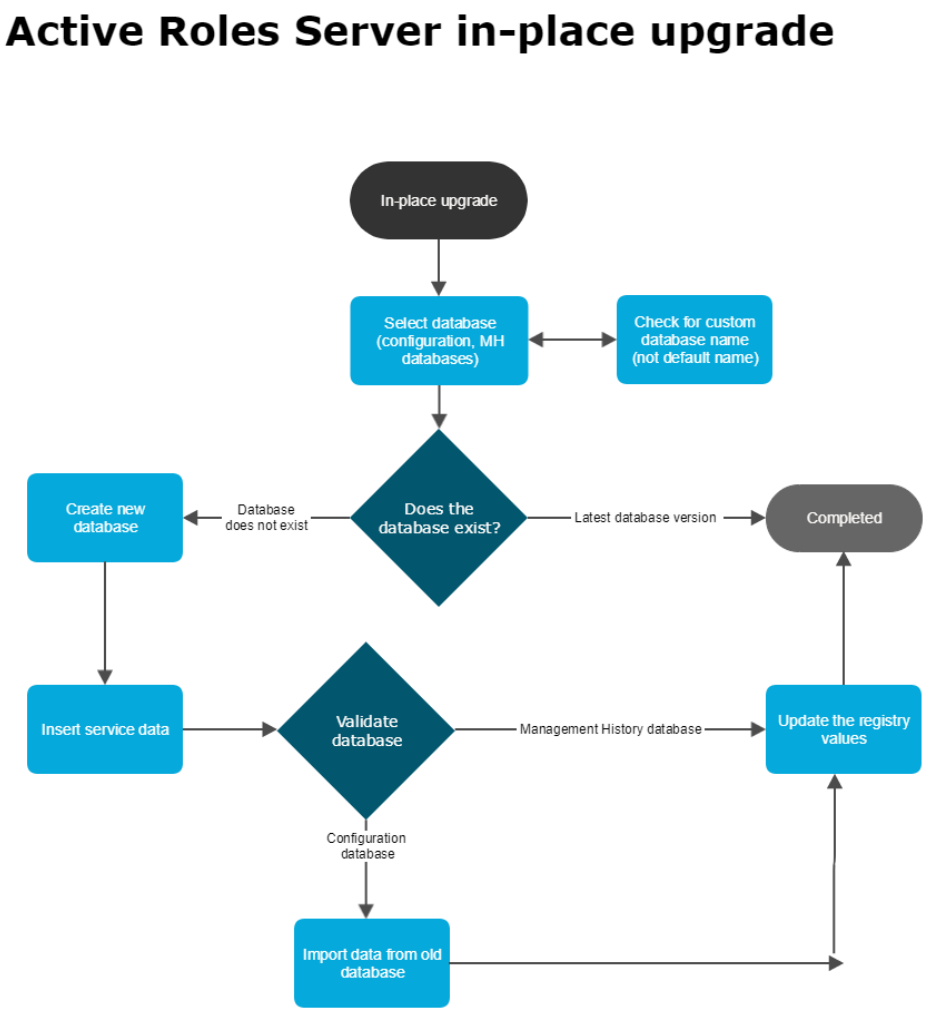
Impact on Office 365 add-on

After an upgrade of Active Roles components to Active Roles 7.5.4, the Office 365 add-on which was supported in the earlier versions of Active Roles, ceases to work. Hence, it is recommended to uninstall the Office 365 add-on prior to the upgrade of Active Roles.

NOTE:

- Uninstall the Office 365 add-on before installing the latest version of Active Roles as the add-on is not supported.
- The latest version of Active Roles manages Office 365 and Azure AD natively. However, Active Roles does not support the following feature of Office 365 add-on that was supported in earlier versions:
    - Ability to manage and select Office 365 domains through policies.

Upgrading to Active Roles 7.5.4 from 7.0.x or later using in-place upgrade method



To upgrade existing Active Roles 7.0.x or later version to the latest version, perform the following steps.

NOTE: One Identity recommends to approve all pending approval activities before performing the in-place upgrade.

To upgrade the Active Roles package using in-place upgrade

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.

4. On the **Ready to Upgrade** page, click **Upgrade** to perform upgrade.
5. On the **Completion** page, click **Finish**.

NOTE: After upgrading the Active Roles package to 7.5.4, perform Configuring Active Roles during in-place upgrade.

NOTE: By default, during in-place upgrade, the **Copy database users, permissions, logins, and roles** check box is selected in the **Upgrade configuration** window.

Configuring Active Roles 7.5.4 during in-place upgrade

NOTE: Before upgrading to the latest version of Active Roles:

- Uninstall the add-ons of the earlier versions.
- Remove replication partners (if there are any).

The in-place upgrade of Active Roles 7.4 upgrades the Active Roles 7.4 Administration Service and Web Interface components.

The in-place upgrade of Active Roles 7.4 does not upgrade the Active Roles solution components such as SPML Provider, Add-on Manager, Add-ins for Outlook, Diagnostic Tools, and so on. To upgrade the solution components installed with Active Roles, use the respective installers available in the Active Roles installation package.

During Active Roles upgrade, if the Active Roles database is not split into configuration and management history databases, then the upgrade process creates a management history database by default.

The following steps describe the in-place upgrade scenario for Active Roles 7.5.4

1. After upgrading the Active Roles package to 7.5.4, restart the operating system.

   NOTE: When upgrading from Active Roles version 7.4.1 or 7.4.3 to 7.5.4, you must restart the operating system

2. After the system restarts, the Configuration Center opens by default, displaying the Upgrade configuration wizard.

   As part of this upgrade, Active Roles creates new databases with default names. The Upgrade configuration wizard displays the new databases information.

   Optional step: To change the default names of the new databases, click **Click here to change or provide existing database names**.

3. On the Upgrade configuration wizard, select the check box to confirm that you have read the instructions in the *Quick Start guide* regarding "Configuring Active Roles for in-place upgrade".

4. The **Azure Tenant association** page displays the lists of configured Azure tenants in the source database and options for association.

   The Azure Tenant association section notifies you to select an Azure tenant from the drop-down list of the Azure tenants configured in the source database, and the selected Azure tenant is associated with all Azure objects in the destination database. You can also choose to **Run Azure Tenant association immediately** or **Schedule Azure Tenant association**, where you select the date and time from the Calendar to run the Azure tenant association.

   NOTE:

   - This page is visible only if the Azure tenants association are present in the source database.
   - If Azure Tenant association is scheduled at a certain time and the upgrade/import operation is still in progress or completes after the Azure Tenant association scheduled time, the tenants are not associated. You have to run the built-in scheduled task **Update Azure Objects Associated Tenant Id** from the Active Roles console to manually associate the Azure Tenants.
   - Alternatively, Azure Tenant association can be run at any time using the template workflow Update Azure Objects Associated Tenant Id available in the Built-in Workflow Container. The parameter in the script used by the workflow can be configured with the required tenant ID. You can use the drop-down to select a default Azure Tenant from the list of available Azure Tenants. The script used by the workflow can be modified to Search Azure objects based on the requirement.

5. The **Services association** page allows you to configure the Administration services for executing Dynamic Groups, Group Families, and Scheduled tasks from the drop-down list.

   The available options in the drop-down list are **This Server** and **Other**, where choosing **Other** allows to specify any other Administration Service in a fully qualified domain name (FQDN) format. If the value is empty, then the current administration service is used.

   NOTE: Services association does not update certain scheduled tasks, For example, scheduled tasks that cannot be edited (Managed Object Counter) or scheduled tasks that are set to **All servers** option.

   You can choose to run the Services association immediately or schedule Services association.

   NOTE: If Services association is scheduled at a certain time and the upgrade/import operation is still in progress or completes after the Services association scheduled time, the services are not associated. You have to run the built-in scheduled task **Update Services To ExecuteOn** from the Active Roles console to manually associate the Services.

   To ensure Dynamic Groups, Group Families, and Scheduled tasks continue to function after an import the installation configures the new Active Roles server as the

executing server for the tasks mentioned above. The configuration mentioned here runs after an upgrade.

NOTE: Alternatively, Services association can be performed any time using the template workflow **Update Services To Execute On** available in the built-in Workflow Container. The parameters in the script used by the workflow can be configured to the required administration services, such as, **Dynamic Group Service**, **Group Family Service**, **Scheduled Task Service**. You can select the Administration Service from the drop-down list. The drop-down list displays all the currently running Administration Services that are connected to the current configuration database. If the parameter value is not selected, then the current Administration Service is used.

6. Click **Next**.

   NOTE: If the disk space in SQL server is insufficient, then an error is displayed prompting you to increase the disk space.

   In case of any errors during the in-place upgrade, you must resolve the errors and re-open the Configuration Center to continue the in-place upgrade.

   The upgrade starts and the **Execution** tab displays the progress bar for the upgrade.

7. After the database upgrade, stop and then restart the Active Roles Service.

After the database upgrade is complete, the Active Roles Service is ready for use.

NOTE: To upgrade multiple Active Roles Service instances, log in to the individual systems where Active Roles Service was upgraded, and perform the in-place upgrade steps for each Service.

Compatibility of Active Roles components

The new Administration Service is only compatible with the Active Roles user interfaces (Web Interface and console) of version 7.5.4. Earlier versions of the user interfaces may not work with the new Administration Service. The user interfaces of Active Roles 7.5.4 are only compatible with the Administration Service of version 7.5.4. Therefore, to use the Active Roles console or Web Interface of version 7.5.4, you must first upgrade the Administration Service.

Impact on custom solutions

An upgrade of Active Roles may affect custom solutions (such as scripts or other modifications), if any, that rely on the Active Roles functions. Custom solutions that work fine with an earlier Active Roles version may cease to work after the upgrade. Prior to attempting an upgrade, you should test the existing solutions with the new Active Roles version in a lab environment to verify that the solutions continue to work.

Upgrading the Administration Service

To upgrade Active Roles Administration Service from a version earlier than 6.9 to 7.x, you must first upgrade to version 6.9.

You can upgrade the Administration Service from version 6.9 through 7.4 to 7.5.4.

Upgrading the Administration Service implies creation of a new Administration Service instance of the latest version, with the configuration and management history data imported from your Administration Service of an earlier version. As a result, the new Administration Service instance inherits all of your existing Active Roles configuration settings, such as managed domains, managed units, permission assignments, policies, workflows, virtual attributes and so on. By importing management history data, you transfer change history, approval tasks, and temporal group membership tasks from your Administration Service of an earlier version to the new Administration Service instance.

To upgrade the new Administration Service instance from 7.0.x or later to 7.5.4 perform the following steps:

> NOTE: Before upgrading to the latest version of Active Roles, the add-ons of the earlier versions must be uninstalled.

1. After upgrading the Active Roles package to 7.5.4, you are prompted to restart the system.
2. After the system restarts, the Configuration Center opens by default, displaying the Upgrade configuration wizard.

   The fields in the wizard are auto-populated. The database name for Configuration and Management history are suggested, by default. However. if you want to update the database name, click **Click here to change or provide existing database names** link.
3. Select the check box on the Upgrade configuration wizard, to confirm that you have read the instructions in the *Quick Start guide* regarding "Configuring Active Role for in-place upgrade".
4. Click **Next**.

   > NOTE: If you click **Next** without selecting the check box, an error is displayed prompting you to follow the instructions given against the check box and select the check box.

   The upgrade starts and the **Execution** tab displays the Progress bar for the upgrade.

After the database upgrade is complete, the Active Roles Service is automatically started and ready for use.

You can upgrade from Active Roles 7.0.x or later to Active Roles 7.x using in-place upgrade or a new installation of Active Roles with import of database from an earlier version.

Upgrading from Active Roles 6.9 version to 7.x version is a side-by-side upgrade, which does not interrupt operations or affect the configuration of your earlier Active Roles version. To ensure smooth upgrade to the new Active Roles version, you must first upgrade the Administration Service and then upgrade the Web Interface.

If you no longer need the Administration Service of the earlier version, you can uninstall it using **Programs and Features** in Control Panel: Right-click **Administration Service** in the list of installed programs, and then click **Uninstall**.

Install and configure the Administration Service

To create a new Administration Service instance, you first install Administration Service files and then perform initial configuration.

To install the Administration Service files

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, ensure that the **Administration Service** component is selected, and click **Next**.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page, select the **I want to perform configuration** check box, and click **Finish**.

The Setup wizard only installs the files. After you have completed the Setup wizard, you need to configure the newly installed Administration Service instance by using Active Roles Configuration Center. The Configuration Center opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the Setup wizard. Another way to open Configuration Center is by selecting **Active Roles Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

To perform initial configuration

1. In Configuration Center, under **Administration Service**, click **Configure**.
2. On the **Service Account** page in the Configure Administration Service wizard that appears, enter the name and password of the domain user account or the service account details of the Group Managed Service Account to be used as the Administration Service account, and then click **Next**.
3. On the **Active Roles Admin** page, accept the default account, or click **Browse** and select the group or user to be designated as Active Roles Admin. When finished, click **Next**.
4. On the **Configuration Database Options** page, select the **New Active Roles database** option, and then click **Next**.
5. On the **Connection to Database** page, specify a SQL Server instance and database name, and select the authentication option:

a. Select the required Database Type, in the Database Server name. Specify an SQL Server instance in the form <*Computer*>\<*Instance*> (for named instance) or <*Computer*> (for default instance), where <*Computer*> stands for the short name of the computer running SQL server or name of the Azure SQL database server. The wizard will create the database on the SQL Server instance you specify.

b. In the **Database** box, type a name for the database that will be created.

c. Under **Connect using**, select the appropriate authentication option:

- To have the Administration Service connect to the database using the service account, click **Windows authentication**.
- To have the Administration Service connect to the database using a SQL Server login, click **SQL Server authentication** and type the login name and password.
- To have the Administration Service connect to the database using Azure AD login, click **Azure Active Directory authentication** and type the login name and password.

6. On the **Management History Database Options** page in the Configure Administration Service wizard, select the New Active Roles database option, and then click Next.
7. On the Connection to Database page, perform the steps a to c for Management history database.
8. Click **Next**, and then complete the **Encryption Key Backup** page as described in Steps to deploy the Administration Service, earlier in this document.
9. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Import configuration

After you have installed and initially configured the Administration Service of the new version, import the configuration data from the database used by your Administration Service of the earlier version. To import configurations, you must identify that database. To identify the database:

1. Open the Active Roles console and connect to your Administration Service of the earlier version (see "Connecting to the Administration Service" in the Active Roles Administration Guide).
2. Select the console tree root, and then, on the page in the details pane, expand the **Configuration Databases and Replication** area.

   You can identify the database name, SQL Server name, and database type from the first string in the **Configuration Databases and Replication** area that has the following format: Database <*name*> on SQL Server <*name*> Database Type <type>.

After identifying the database, perform the import using the Import configuration wizard provided by Configuration Center. On the **Source database** page in the Import

configuration wizard, supply the database name and SQL Server name that you have identified. For detailed instructions, see Steps to deploy the Administration Service earlier in this document.

> NOTE: When an import configuration is performed from Active Roles version 7.0 to 7.5.4, the Web Interface does not get upgraded. However, the Configuration Center or any client report the Active Roles Web interface version incorrectly as 7.5.4. To upgrade the Web interface to the latest version see Upgrading the Web Interface.

Import management history

After you have imported configuration of your earlier Active Roles version, import the management history data from the database used by your Administration Service of the earlier version. First, identify that database:

1. Open the Active Roles console and connect to your Administration Service of the earlier version (see "Connecting to the Administration Service" in the Active Roles Administration Guide).
2. Select the console tree root, and then, on the page in the details pane, expand the **Management History Databases and Replication** area.

   Identify the database name, SQL Server, database type name from the first string in the **Management History Databases and Replication** area that has the following format: Database <*name*> on SQL Server <*name*> Database Type <type>.

After identifying the database, perform the import. You can do this using the Import Management History wizard provided by Configuration Center. On the **Source database** page in the Import Management History wizard, supply the database name and SQL Server name you have identified. For detailed instructions, see Steps to deploy the Administration Service earlier in this document.

Upgrade in case of shared database

If multiple instances of the Administration Service use a single database, then you can perform the upgrade as follows:

1. Upgrade one of the Administration Service instances as described earlier (see Upgrading the Administration Service).

   As a result of this step, you have an Administration Service instance of the new version connected to the new database containing the data imported from the old database. The other instances of the Administration Service are not upgraded at this point; they continue to use the old database.
2. Now that you have the database of the new version, you can upgrade the remaining instances of the Administration Service, one by one.

3. In the Configure Administration Service wizard, select the **Existing Active Roles database** option on the **Configuration Database Options** page, and then, on the **Connection to Database** page, specify the database created during upgrade of the first Administration Service instance. You need not import configuration as the database already has that data imported.
4. In the Configure Administration Service wizard, select the **Existing Active Roles database** option on the **Management History Database Options** page, and then, on the **Connection to Database** page, specify the database created during upgrade of the first Administration Service instance. You need not import the management history as the database already has that data imported.

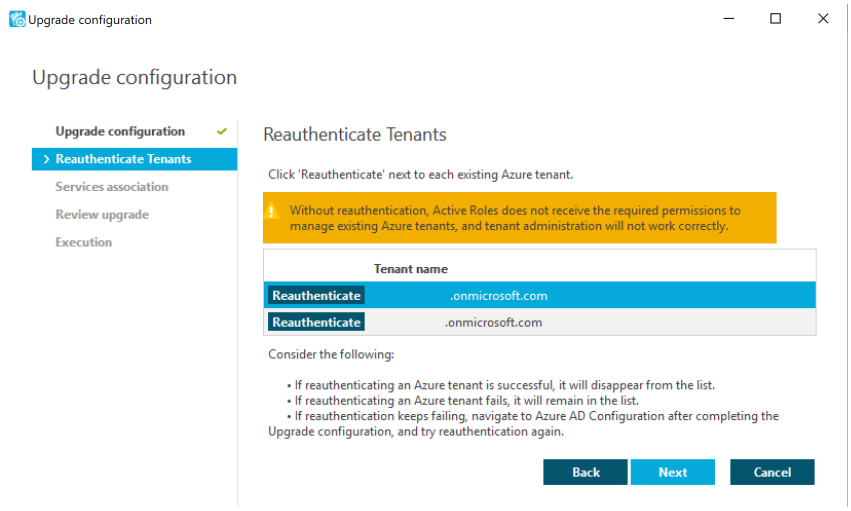
As a result of these steps, multiple Administration Service instances of the new version use a single database updated with the configuration and management history data of your earlier Active Roles version.

Reconfiguring Azure tenants during upgrade configuration

If your organization has any Azure tenants managed in Active Roles, you will need to reauthenticate and reconsent each Azure tenant after installing a new version of Active Roles. Otherwise, you may experience difficulties with Exchange Online connectivity and managing Azure AD resources (for example, assigning Azure AD roles).

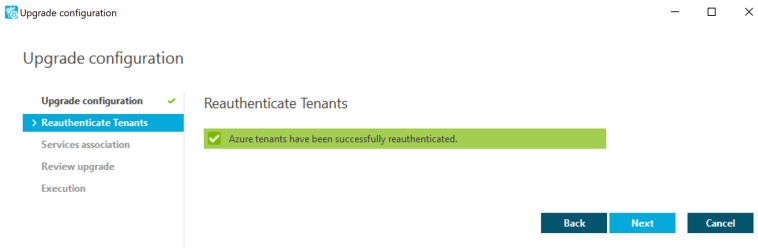
To reauthenticate and reconsent Azure tenants after installing Active Roles

1. Once Active Roles is installed, open the Active Roles Configuration Center in Windows. The **Upgrade configuration** wizard will automatically appear.
2. To reauthenticate existing Azure tenants, proceed to the **Reauthenticate tenants** step and click **Reauthenticate** next to each Azure tenant.



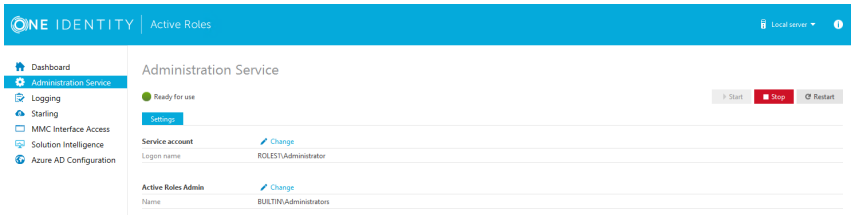
NOTE: Consider the following when reauthenticating existing Azure tenants:

- If reauthentication is successful, the Azure tenant will disappear from the list, and the **Reauthenticate tenants** step shows a confirmation message.

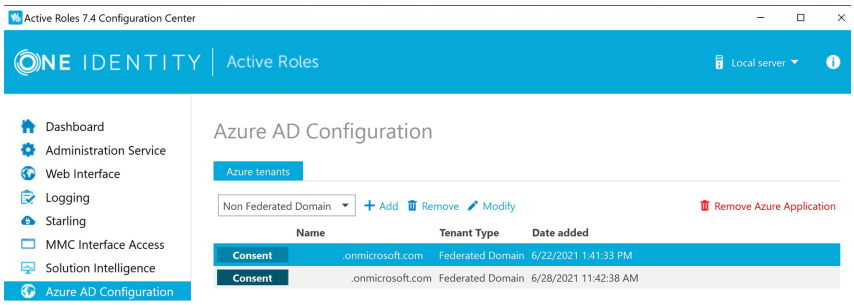


- If reauthentication fails, the Azure tenant will remain in the list. Reauthentication can typically fail if there is a service outage in Azure AD, or in case of internet connectivity issues in your network. If reauthentication keeps failing, try performing it later after completing the **Upgrade configuration** wizard by removing, readding and consenting the Azure tenants to Active Roles via the **Azure AD Configuration** tab of the Active Roles Configuration Center. For more information, see Reconfiguring Azure tenants manually.

3. Complete the rest of the steps in the **Upgrade configuration** wizard.
4. To make the reauthenticated Azure tenants appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.

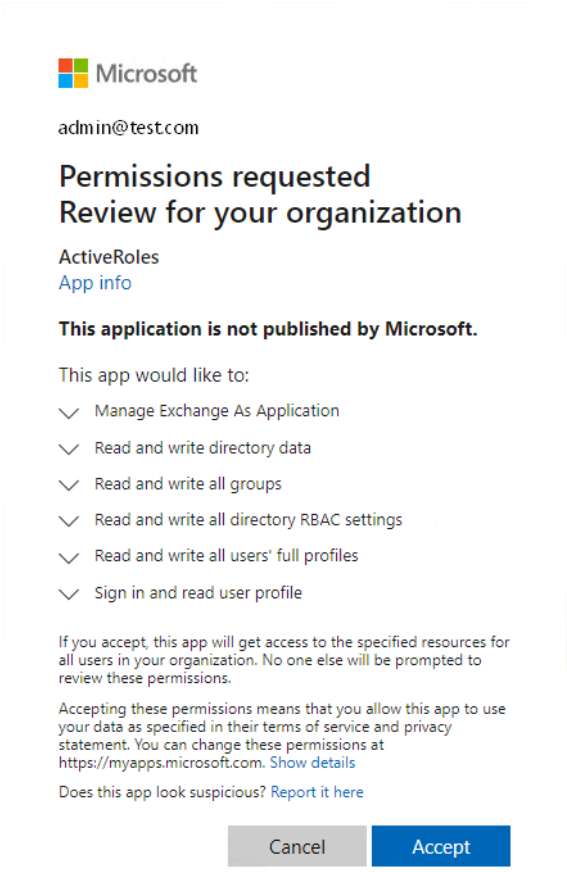


5. Once the Active Roles Configuration Center successfully restarted, navigate to **Azure AD Configuration**.



6. To reconsent Active Roles as an Azure application for the reauthenticated Azure tenants, click **Consent** in each tenant row.

7. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.



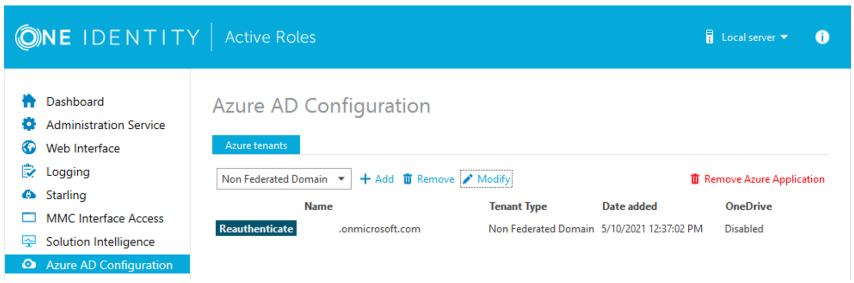
Reconfiguring Azure tenants manually

If your organization has any Azure tenants managed in Active Roles, you will need to reauthenticate and reconsent each Azure tenant after installing a new version of Active Roles. Otherwise, you may experience difficulties with Exchange Online connectivity and managing Azure AD resources (for example, assigning Azure AD roles).

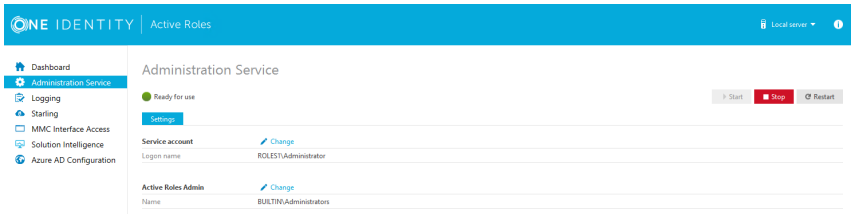
Azure tenant reauthentication is part of the in-place **Upgrade configuration** process by default (for more information, see Reconfiguring Azure tenants during upgrade configuration). However, if reauthentication fails during that process for any reason, you can complete the reauthentication and reconsenting of existing Azure tenants with the following manual steps later.

To reconfigure Azure tenants after upgrading from Active Roles 7.4.1 or 7.4.3 to Active Roles 7.5.4

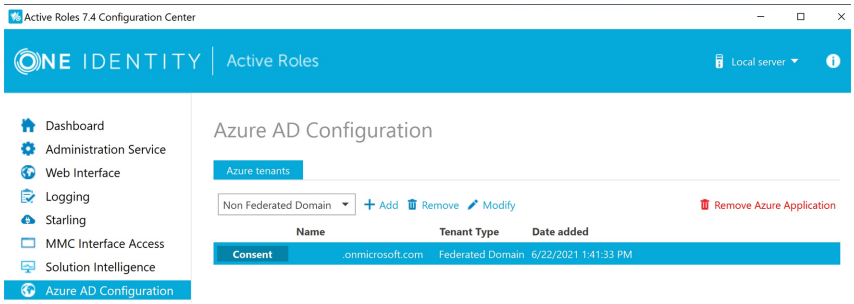
1. In the Active Roles Configuration Center, navigate to **Azure AD Configuration**.
2. To reconfigure the existing Azure tenants, select a tenant and click **Reauthenticate** in its row. Repeat the process for each existing Azure tenant.



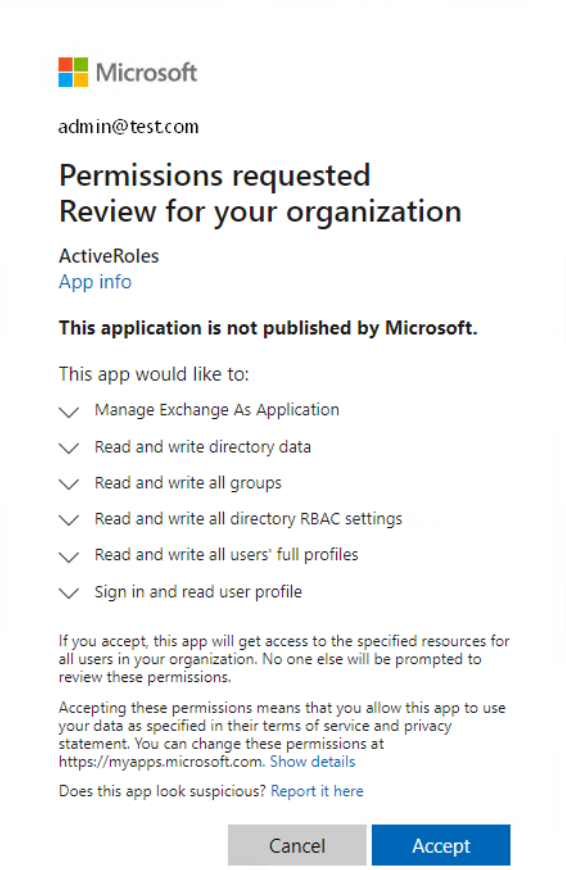
3. To make the configured Azure tenant appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



4. Once the Administration Service is restarted, consent Active Roles as an Azure application for each reconfigured Azure tenant. To do so, navigate again to **Azure AD Configuration**, select the Azure tenant and click **Consent**.



5. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.

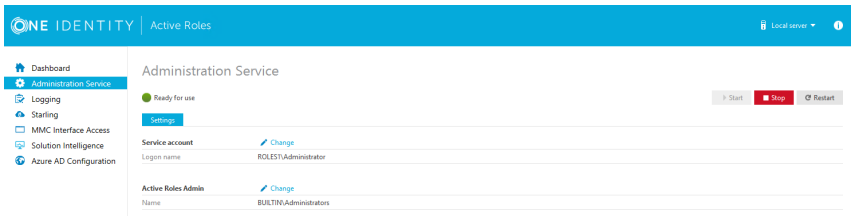


6. Repeat the previous two steps for each Azure tenant.

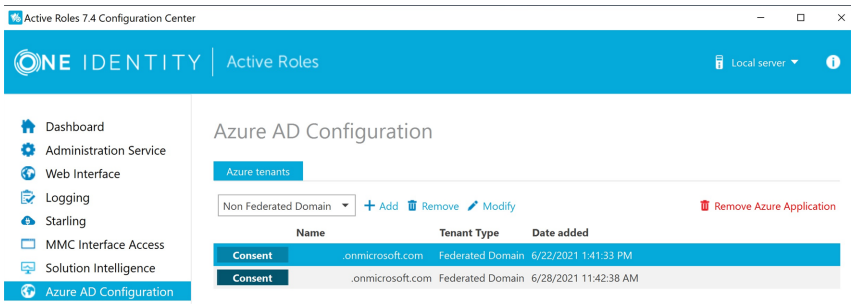
To reconfigure Azure tenants when upgrading from Active Roles 7.4.4 to 7.5.4

1. In the Active Roles Configuration Center, navigate to **Azure AD Configuration**.
2. Remove all Azure tenants. To do so, select an Azure tenant and first click **Remove Azure Application**, and then click **Remove**.
3. Repeat the previous step for each remaining Azure tenant.
4. Add the removed Azure tenants again to the list. To do so, use the drop-down box to select the type of domain assigned to the Azure tenant (**Non-Federated Domain**, **Federated Domain**, **Synchronized Identity Domain**), and click **Add**.

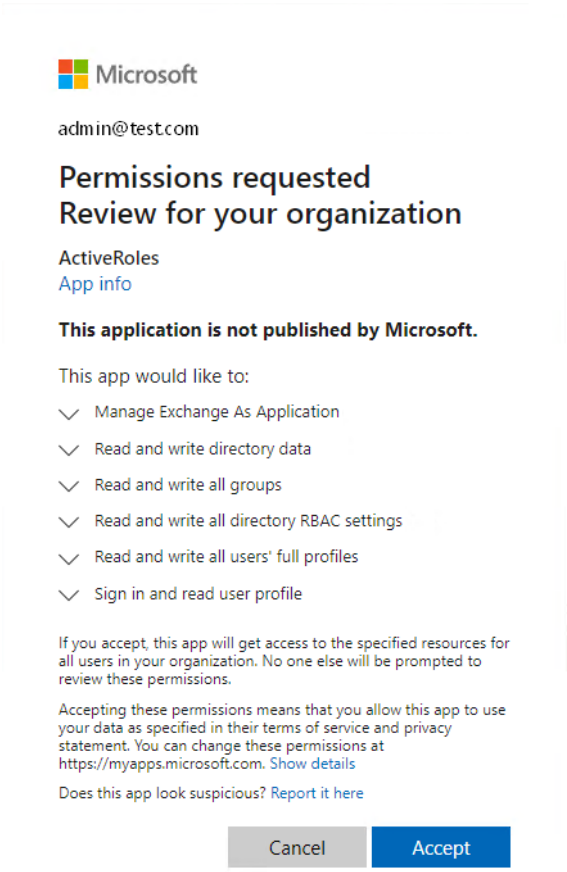
   Upon successful authentication, the new Azure tenant appears in the list.
5. Repeat the previous step for each Azure tenant that you previously removed.
6. To make the configured Azure tenants appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



7. Once the Administration Service is restarted, consent Active Roles as an Azure application for the reconfigured Azure tenants. To do so, navigate to **Azure AD Configuration**, select an Azure tenant and click **Consent**.



8. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.



9. Repeat the previous two steps for each Azure tenant.

Upgrading the Web Interface

You can upgrade the Web Interface of version 7.0, 7.1, 7.2, or 7.3 to version 7.4.x.

Upgrading the Web Interface implies creation of a new Web Interface instance of the latest version that has the same Web Interface sites as your Web Interface of an earlier version, with the site configuration data imported from your Active Roles configuration of the earlier version. As a result, the new Web Interface sites inherit all customizations that were made to the menus, commands, forms, and other elements of your Web Interface sites of the earlier version.

When an import configuration is performed from Active Roles version 7.3 to 7.5.4, the web interface does not get upgraded. However, the Configuration Center or any client report the Active Roles Web interface version incorrectly as 7.5.4. To upgrade the Web interface to the latest version see Upgrading the Web Interface.

Creating Web interface sites and importing configuration

To create a new Web interface instance of the latest version and import the site configurations perform the following steps:

1. For each Web Interface site of your earlier Active Roles version, identify and note down the name of the configuration object that the Administration Service uses to store the site's configuration data.
2. Install and configure the Web Interface instance of the latest Active Roles version, choosing the new Administration Service to which you have imported configuration of your earlier Active Roles version (see Upgrading the Administration Service earlier in this document).
3. On the new Web Interface instance that you installed and configured in Step 2, create sites based on information you noted down in Step 1, importing data from the configuration objects used by your earlier Web Interface version. Those configuration objects were copied to the new Administration Service during configuration data import (see Upgrading the Administration Service earlier in this document).
4. Optionally, delete the default sites that were created when you configured the Web Interface in Step 2. The default sites are unaware of your existing site customizations, and have the default configuration of menus, command, forms and other elements.

These steps are covered in the topics that follow.

You can install the Web Interface of version Active Roles side-by-side with the Web Interface of version 6.9 on the same computer, and perform the upgrade without interrupting operations or affecting the configuration of your Web Interface sites of the earlier Active Roles version.

If you no longer need the Web Interface of the earlier version, you can uninstall it using **Programs and Features** in Control Panel: Right-click **Web Interface** in the list of installed programs, and then click **Uninstall**.

Identify configuration objects

When creating Web Interface sites of the new Active Roles version, you need to know which configuration objects are used by your Web Interface sites of the earlier version. Each site stores its configuration in a certain object on the Administration Service, referred to as the *site configuration object*. Upgrade of the Administration Service copies the existing site configuration objects to the new Administration Service, retaining the name of each object.

To create a Web Interface site of the new Active Roles version that inherits your existing site customizations, you need to specify the name of the corresponding site configuration object of the earlier version. Then, Active Roles creates a site configuration object of the new version, imports the site configuration data to that object, and causes the new Web

Interface site to use that object. As a result, the new Web Interface site has the same configuration as the Web Interface site of the earlier version.

To identify the configuration object of the Web Interface site of an earlier Active Roles version

1. On the Web server running your Web Interface of the earlier Active Roles version, start the Web Interface Sites Configuration wizard.

   To start the wizard, select **Web Interface Sites Configuration** on the **Apps** page or **Start** menu, depending upon the version of the Windows operating system on the Web server.

2. Proceed to the **Web Interface Configuration** page in the Web Interface Sites Configuration wizard.

   The page lists your Web Interface sites of the earlier Active Roles version.

3. On the **Web Interface Configuration** page, click the list item representing the desired site, and then click the **Edit** button.

   You can distinguish sites by alias, shown in the **Virtual Directory** column on the **Web Interface Configuration** page. The alias defines the virtual path used in the address of the Web Interface site on the Web server.

4. Note down the name of the site's configuration object shown in the **Configuration settings** area of the dialog box that appears.

   The name of the object is displayed in the **Name** box under the **Use existing configuration** option, and includes the version number.

5. Click **Cancel** to close the dialog box.

To identify the configuration object of the Web Interface site of the current Active Roles version

1. Start the **Configuration Center** on the computer running the **Administration Service** instance on which you want to identify the web interface sites.

   You can start Configuration Center by selecting Active Roles 7.4 Configuration Center on the Apps page or Start menu, depending upon the version of your Windows operating system.

2. On the Configuration Settings main window, on the left pane, click Web Interface.

   The Web Interface page is displayed, which lists the Web Interface sites of the current Active Roles version that are deployed on the Web server running the Web Interface.

   For each Web Interface site, the list provides the following information:

   - IIS Web site The name of the Web site that holds the Web application implementing the Web Interface site

- Web app alias The alias of the Web application that implements the Web Interface site, which defines the virtual path of that application on the Web server.
- Configuration Identifies the object that holds the Web Interface site's configuration and customization data on the Active Roles Administration Service.

3. From the Web Interface page, you can open Web Interface sites in your Web browser:
    a. Click an entry in the list of Web Interface sites.
    b. Click Open in Browser on toolbar.

You can also use Configuration Center to:

- Create, modify or delete Web Interface sites
- Export a Web Interface site's configuration object to a file

For more information, see the Web Interface management tasks section in the *One Identity Active Roles Administration Guide*.

Identify the configuration object for each of your existing Web Interface sites, and note down the name of each object. You will need these names when creating the Web Interface sites of the new Active Roles version.

Install and configure the Web Interface

To create a new Web Interface instance, you first install Web Interface files and then perform initial configuration.

To install the Web Interface files

1. Log on with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles distribution package, and start the Setup wizard by double-clicking `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
4. On the **Component Selection** page, ensure that the **Web Interface** component is selected, and click **Next**.
5. On the **Ready to Install** page, click **Install** to perform installation.
6. On the **Completion** page, confirm that the **I want to perform configuration** check box is selected, and click **Finish**.

The Setup wizard only installs the files. After you have completed the Setup wizard, you need to configure the newly installed Web Interface instance by using Active Roles Configuration Center that opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the Setup wizard. Another way to open Configuration Center is by selecting **Active Roles 7.5.4 Configuration Center** on

the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

To perform initial configuration

1. In Configuration Center, under **Web Interface**, click **Configure**.

   This starts the wizard that will perform initial configuration of the Web Interface.

2. On the **Administration Service** page, specify the new Administration Service instance created during upgrade (see Upgrading the Administration Service earlier in this document).

   If the new Administration Service instance runs on the computer on which you are installing the new Web Interface, choose the option **Administration Service on the computer running the Web Interface**. Otherwise, choose the option **Administration Service on this computer**, and supply the fully qualified domain name of the computer running the new Administration Service instance.

3. Click the **Configure** button, and wait while the wizard completes the configuration.

Create sites based on old configuration objects

After you have installed and configured the Web Interface instance of the new Active Roles version, you can use Configuration Center to create Web Interface sites of the new version, importing site configuration data from the configuration objects used by your existing Web Interface sites of the earlier Active Roles version (see Upgrading the Web Interface earlier in this document). As a result, the new Web Interface sites will inherit all customizations that were made to the menus, commands, forms and other elements of your Web Interface sites of the earlier version.

To create a Web Interface site based on an old configuration object

1. Open Configuration Center.

   You can open Configuration Center by selecting **Active Roles 7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. In the Configuration Center main window, under **Web Interface**, click **Manage Sites**.
3. On the **Sites** page, click **Create**.
4. On the **Web Application** page in the Create Web Interface Site that appears, choose the IIS Web site to contain the Web application that implements the Web Interface site, and specify an alias for that application.

   The alias defines the virtual path that is a part of the Web Interface site's address. You can view the resulting address on the **Web Application** page.

5. Click **Next** to proceed to the **Configuration** page.
6. From the list on the **Configuration** page, select the **Import from an existing configuration** option.
7. Complete the fields on the **Configuration** page:
    a. In the **Configuration name** field, supply the name of the configuration object for the new Web Interface site. You can accept the default name.
    b. The wizard will create a configuration object with the specified name, and import configuration data to that object.
    c. From the list in the **Configuration to import** box, select the name of the configuration object from which to import the configuration data.

    This must be the name of the configuration object used by one of your existing Web Interface sites of the earlier Active Roles version (see Upgrading the Web Interface earlier in this document).
8. Click the **Create** button, and wait while the wizard creates the new Web Interface site.

Perform these steps for each of your Web Interface sites of the earlier version, selecting the appropriate object name in Step 7b.

Delete default sites

After you have created the Web Interface sites of the new version that inherit the configuration of your Web Interface sites of the earlier version, you might delete the default Web Interface sites that were created by initial configuration of the Web Interface (see Upgrading the Web Interface earlier in this document).

To delete the default Web Interface sites

1. Open Configuration Center.

    You can open Configuration Center by selecting **Active Roles 7.5.4 Configuration Center** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.
2. In the Configuration Center main window, under **Web Interface**, click **Manage Sites**.
3. On the **Sites** page, identify list entries representing default Web Interface sites, and use the **Delete** button to delete them one by one.

    You can distinguish list entries representing default Web Interface sites by the name in the **Configuration** column:

- **Site for Administrators (7.5.4)** indicates the default site for administrators
- **Site for HelpDesk (7.5.4)** indicates the default site for Help Desk
- **Site for Self-Administration (7.5.4)** indicates the default site for self-administration

Upgrading other components

This section covers upgrade options for the following components of Active Roles:

- Console (MMC Interface)
- Management Shell
- ADSI Provider
- SDK
- Collector and Report Pack
- Synchronization Service

Upgrade of the Active Roles console

You can install the Active Roles console of version 7.5.4 side-by-side with the Active Roles console of version 6.9, on the same computer. Alternatively, you can install the new console on a different computer. For installation instructions, see Steps to install the console earlier in the document.

To upgrade from Active Roles console of version 7.x to the latest Active Roles version, perform an in-place upgrade or a new installation with import configuration from the earlier Active Roles version. In case of an in-place upgrade, the Active Roles console is upgraded automatically to the console of latest version of Active Roles.

If you no longer need the console of version 6.9 or earlier, you can uninstall it using **Programs and Features** in Control Panel: Right-click **MMC Interface** in the list of installed programs, and then click **Uninstall**.

Upgrade of the Shell, ADSI Provider and SDK

The Active Roles Management Shell, ADSI Provider and SDK of version 7.5.4 are packaged into a single component referred to as *management tools*. You can install management tools side-by-side with Active Roles version 6.9, on the same computer. Alternatively, you can install management tools on a different computer. Active Roles Setup installs management tools by default. You can install management tools without installing other components (see Steps to install only the Shell, ADSI Provider and SDK earlier in this document).

To upgrade from Active Roles Management Shell, ADSI Provider and SDK of version 7.x to the latest Active Roles version, perform an in-place upgrade. In case of an in-place upgrade, the Active Roles Management Shell, ADSI Provider and SDK is upgraded automatically to the components of the latest version of Active Roles.

If you no longer need the Management Shell that ships with Active Roles 6.9, you can uninstall it using **Programs and Features** in Control Panel: Right-click **Management**

Shell in the list of installed programs, and then click **Uninstall**. Note that the Administration Service requires the Management Shell. Do not uninstall the earlier version of Management Shell from the computer running the Administration Service of version 6.9.

The Active Roles SDK is packaged as a feature of the Administration Service installation. You can uninstall it by using the Administration Service Setup wizard in maintenance mode: In **Programs and Features**, right-click **Administration Service**, and then click **Change** to start the Setup wizard. On the **Select Features** page in the wizard, choose the option to remove the **SDK and Resource Kit** feature.

The Active Roles ADSI Provider of version 6.9 is normally installed together with any of the Active Roles core components, such as the Administration Service, Web Interface or MMC Interface, and is removed once you have uninstalled the core components.

Upgrade of Collector and Report Pack

The Active Roles reporting components should be upgraded in the following order:

- Collector
- Report Pack
- Collector's database

Collector

To upgrade, first uninstall your earlier version of Collector and then install the new version. You can uninstall Collector by using **Programs and Features** in Control Panel. Once you have uninstalled your earlier version of Collector, install the new version. For installation instructions, see Steps to install Collector and Report Pack earlier in this document.

Report Pack

To upgrade, first uninstall your earlier version of the Report Pack and then install the new version. The Report Pack should be uninstalled on the computer that was initially used to install the Report Pack. You can uninstall the Report Pack by using **Programs and Features** in Control Panel.

Once you have uninstalled your earlier version of the Report Pack, deploy the new version. For instructions, see Steps to install Collector and Report Pack earlier in this document.

Collector's database

The new version of the Report Pack is incompatible with the database of an earlier Collector version. To create reports based on the events held in that database, you need to import

the events to the database of the new Collector version, and then specify the database of the new Collector version as the data source for the reports of the new Report Pack version. For instructions on how to configure the data source, see "Working with reports" in the Active Roles Administration Guide.

To import events from the database of an earlier Collector version

1. Start the Collector wizard.

   You can start the Collector wizard by selecting **Active Roles 7.5.4 Collector and Report Pack** on the **Apps** page or **Start** menu, depending upon the version of your Windows operating system.

2. On the **Select Task** page, click **Import events from an earlier database version**, and then click **Next**.
3. On the **Source database** page, click **Specify**, and supply the name, database type and the database server of the database used by your Collector of an earlier version. Click **Next**.
4. On the **Target Database** page, click **Specify**, and supply the database type, database server, and database name of the database used by your Collector of the current version.
5. Click **Next**, and wait while the wizard performs the import.

Synchronization Service

If you have synchronization workflows configured and run by Quick Connect (predecessor of Synchronization Service), or earlier versions of Synchronization Service, then you can transfer those synchronization workflows to Active Roles and have them run by Synchronization Service.

You can transfer synchronization workflows from the following Quick Connect or Synchronization Service versions:

- Quick Connect Sync Engine 5.2.0, 5.3.0, 5.4.0, 5.4.1, or 5.5.0
- Quick Connect Express for Active Directory 5.3.0, 5.4.0, 5.4.1, 5.5.0, or 5.6.0
- Quick Connect for Cloud Services 3.3.0, 3.4.0, 3.5.0, 3.6.0, 3.6.1, 3.6.2, or 3.7.0
- Quick Connect for Base Systems 2.2.0, 2.3.0, or 2.4.0
- Synchronization Service 7.0, 7.1, 7.2, or 7.3

Performing a pilot deployment

In a large enterprise environment, a pilot project may need to be conducted before upgrading to the new Active Roles. 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 Active Roles version. 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 Active Roles version to a subset of the user group. Those who do not participate in the pilot project perform their regular, daily work using the earlier Active Roles version. This requires that the earlier 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. **Deploying the pilot Administration Service** Deploy an instance of the Administration Service of the new Active Roles version, and update that instance with the configuration data from the database used by your production Administration Service of the earlier Active Roles version.
2. **Deploying the pilot Web Interface** Deploy an instance of the Web Interface of the new Active Roles version so that the new instance uses the Administration Service you deployed in the previous step, and create the Web Interface sites on that Web Interface instance by importing the configuration data used by your production Web Interface sites of the earlier Active Roles version.
3. **Installing the console** Install the Active Roles console of the new version.

These steps are discussed in the sections that follow.

Deploying the pilot Administration Service

When deploying 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. You can achieve this as follows:

1. Create an instance of the new Administration Service. For instructions, see Upgrading the Administration Service earlier in this document.

   You can install the Administration Service of version Active Roles side-by-side with the Administration Service of version 6.9, on the same computer. Another option is to install the new Administration Service on a different computer.

2. Import the configuration data from the database used by your production Administration Service of the earlier Active Roles version, to the new Administration Service you created in the previous step.

   You can import the configuration data using the Import configuration wizard provided by Configuration Center. On the **Source database** page in the Import configuration wizard, specify the database used by your production Administration Service of the earlier Active Roles version. For detailed instructions, see Steps to deploy the Administration Service earlier in this document.

Optionally, you can import the management history data from the database of your production Administration Service, in addition to the configuration data (see Steps to deploy the Administration Service earlier in this document).

Transfer to new operating system or SQL Server version

When performing a pilot deployment, you may want to have the new Administration Service version installed on a server running a newer version of the Windows operating system. Additionally, you may need the database of the new Administration Service to be hosted on a newer SQL Server version. You can meet these requirements as follows:

1. Install and configure the new Administration Service on a computer running the operating system you want. When performing initial configuration, specify the desired SQL Server instance. You are not required to specify the SQL Server instance that hosts the database of your production Administration Service of the earlier Active Roles version. You can choose any SQL Server version that meets the system requirements for the new Active Roles version.
2. Import the configuration data and, optionally, management history data, from the database of your production Administration Service of the earlier Active Roles version to the new Administration Service you created in the previous step.

Deploying the pilot Web Interface

Once you have deployed the pilot Administration Service and updated its configuration, you can deploy the Web Interface for your pilot project. You have to ensure that your pilot instance of the Web Interface meets the following conditions:

- Uses the Administration Service instance you have deployed for your pilot project (see Deploying the pilot Administration Service earlier in this document).
- For each of your production Web Interface sites of the earlier Active Roles version, holds a site with the same customizations of the menus, commands, forms and other elements as the production site.

You can address these conditions as follows:

1. For each of your production Web Interface sites of the earlier Active Roles version, identify and note down the name of the configuration object used by that site.

   You can identify your existing site configuration objects by using the Web Interface Sites Configuration wizard on the computer running your production Web Interface. For detailed instructions, see Upgrading the Web Interface earlier in this document.
2. Create an instance of the new Web Interface, and configure it to use the Administration Service instance you have deployed for your pilot project. For details, see Upgrading the Web Interface earlier in this document.

   You can install the Web Interface of version Active Roles side-by-side with the Web Interface of version 6.9, on the same computer. Another option is to install the new Web Interface on a different computer.
3. On the Web Interface instance you have created in Step 2, create Web Interface sites, importing site configuration data from the configuration objects you have identified in Step 1. For instructions, see Upgrading the Web Interface earlier in this document.

Optionally, delete the default sites that were created when you configured the Web Interface in Step 2. The default sites are unaware of your existing site customizations, and have the default configuration of menus, command, forms and other elements. For instructions on how to delete the default Web Interface sites, see Upgrading the Web Interface earlier in this document.

Installing the Active Roles console

You need the Active Roles console of version 7.5.4 if you want the console to connect to the Administration Service of version Active Roles. As the console of version 7.5.4 does not connect to the Administration Service of earlier versions, the use of the console version Active Roles for your pilot project ensures that the console automatically connects to the pilot Administration Service.

For installation instructions, see Steps to install the console earlier in this document.

Deployment considerations

This section addresses issues concerning the deployment of the Active Roles Administration Service. Information for this section was collected from:

- Feedback from our current customers who have enterprise class deployments with multiple sites/locations
- Extensive testing of Active Roles in our software development labs
- Comparisons and testing of Active Roles 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 To add the Active Roles console (MMC Interface) to the pilot deployment, simply install the new version of the console on an appropriate server and have the console connect to your pilot Administration Service. deployment, administrators should consider the following issues:

- Business workflow
- 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 Active Roles 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 Active Roles 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 Active Roles will fit into that workload.

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 Active Roles. 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 Active Roles deployment, it will also improve the performance of the currently deployed services. Since Active Roles is often deployed during migration to Active Directory, Active Roles 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 Active Roles Web Interface, IIS must be installed on the server running the Web Interface.

It is recommended that organizations use the Active Roles 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 Active Roles is that administrators do not need permissions on Active Directory to perform user management and other tasks. This forces administrators to use Active Roles and assures secure administration with the enforcement of "Rules and Roles" provided by Active 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:

- Our 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 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.

  NOTE: With Active Roles 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.

  NOTE: Active Roles allows administrators to push (synchronize) permissions from Active Roles to Active Directory, thus making it easier to manage permissions to AD.

Replication traffic

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

Replication traffic can be judged by considering what is replicated and what is not. Active Roles configuration information is replicated 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.

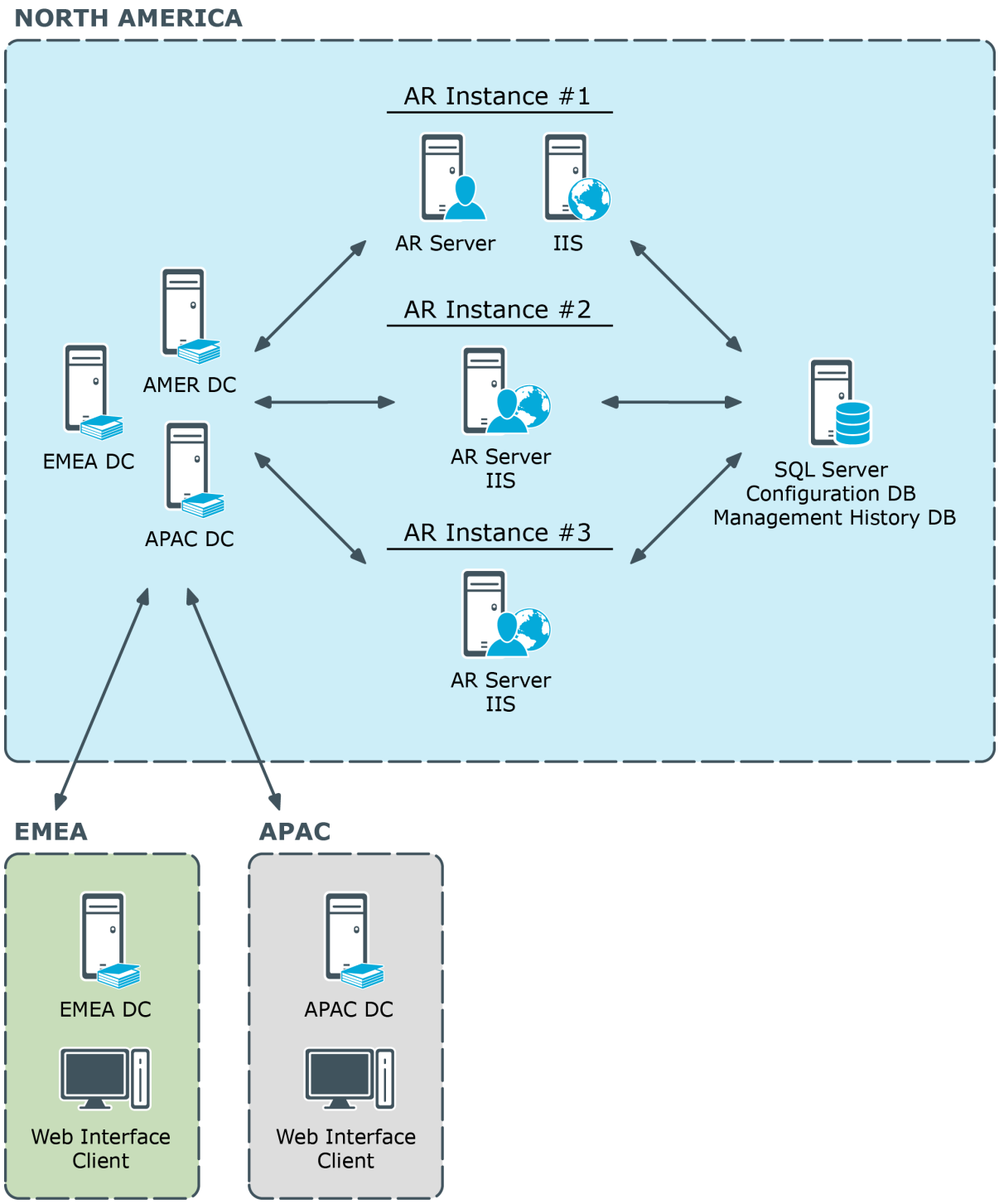
Locations and number of services

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

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

Centralized

This diagram shows a centralized network and workflow (the ARS abbreviation refers to the Active Roles 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 Active Roles Administration Service (Dedicated ARS) 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 Active Roles console, while the majority of administrators and all Help Desk personnel use the Web Interface.

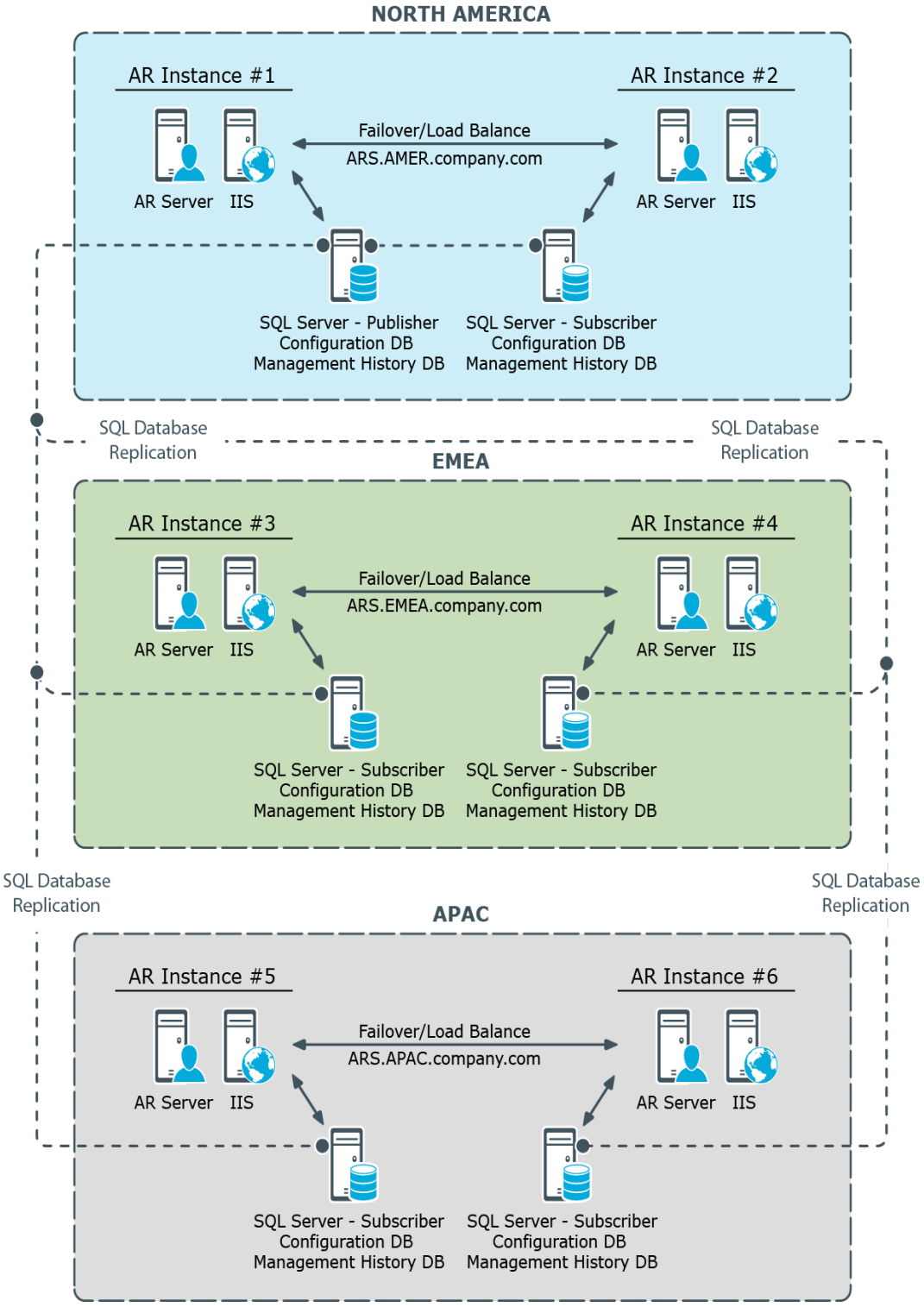
Typically, customers do not install all Administration Services at one location, but in this case, one or both of the following business workflow and technical factors over rule that guideline:

- 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 the Active Roles Administration Service).

Figure 2: Distributed network and workflow



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.

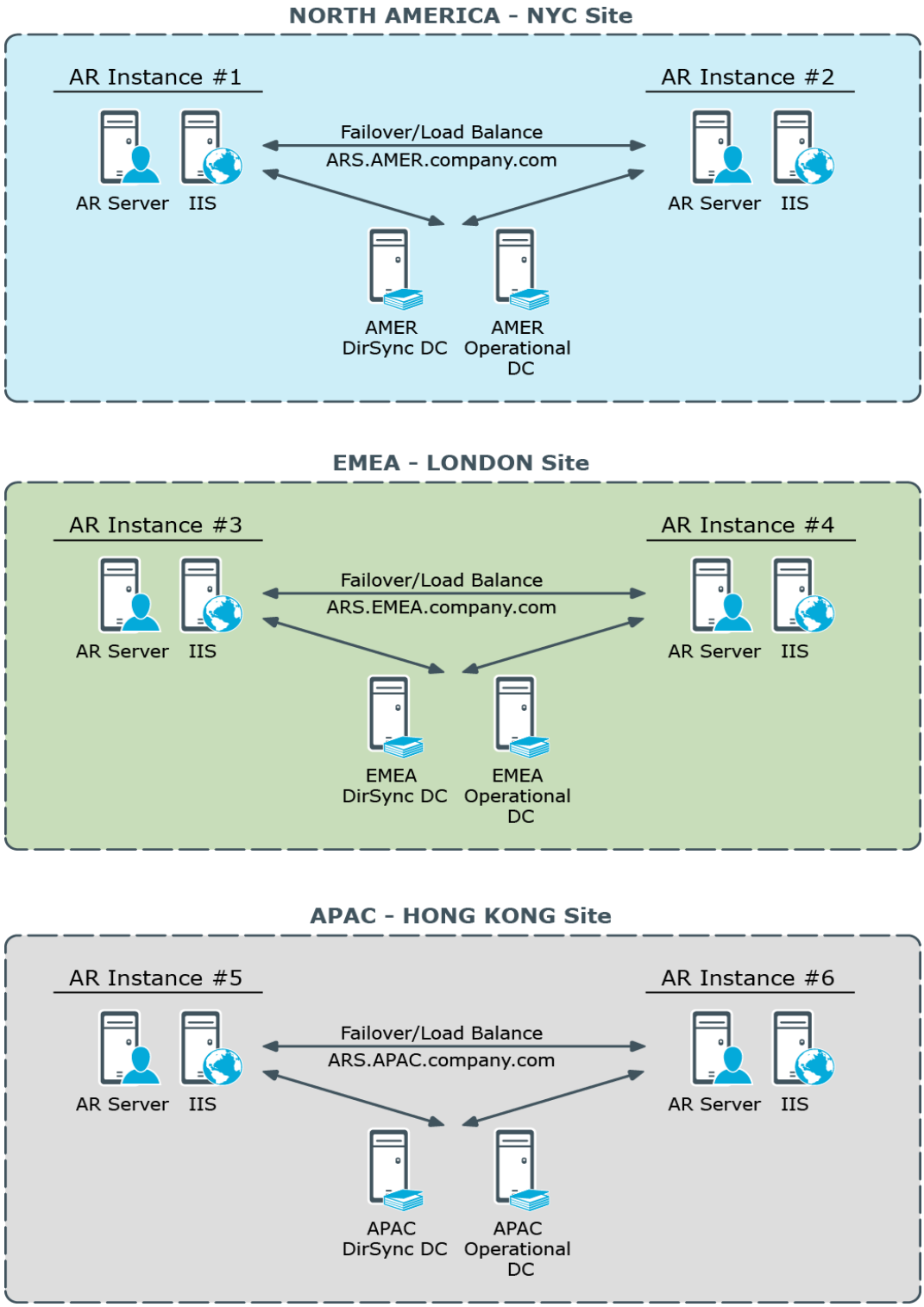
Again, the number of Administration Services depends on the number of managed objects and administrators. In the diagram, there is one dedicated and one shared Administration Service per location. This setup assures both redundancy and availability at each major location and through out the network. 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 Active Roles console, 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 the Active Roles Administration Service).

Figure 3: Highly distributed network and workflow



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 Active Roles console, while the majority of administrators and all Help Desk personnel and work group managers use the Web Interface.

Physical design

This section covers two typical installation configurations for Active Roles. In both installations the architecture is designed to maximize the effectiveness of the Active Roles software based on how the network is configured and how administrative duties are assigned.

Several software components must be considered when deploying Active Roles:

- **AR Service** The Active Roles Administration Service (AR Service) communicates directly with an Active Directory domain controller (DC), and is responsible for making all changes to Active Directory. The DC to which the AR Service speaks is selected automatically and can be changed by the Active Roles user. The ARS Service is also responsible for performing access checks to prevent non-authorized users from connecting to Active Roles interfaces and to ensure that authorized users are performing tasks according to the role they hold and the rules that have been put in place.
- **Console** the Active Roles console provides an MMC-based interface to configure Active Roles as well as perform administration of Active Directory. The Console only connects to the AR Service and is not capable of making changes directly in Active Directory.

- **Web Interface** Three Web Interfaces are provided with Active Roles out of the box: the Web Interface for Administrators; the Web Interface for Help Desk; and the Web Interface for Self-administration. During the setup of the Web Interfaces the administrator must make a decision to connect the Web Interface to a specific AR Service or allow the AR Service to be selected dynamically. All of the Web Interfaces connect only to the AR Service and are not capable of making changes directly in Active Directory.

The decision where to place servers running the Active Roles software components should leverage the strengths of the existing network and the associated IT Service structure.

Deploying for fault tolerance and load balancing

In the same way Active Directory is not fault tolerant with a single domain controller Active Roles would not be fault tolerant when a single server running the AR Service is deployed. It is critical that at least two servers running the AR Service be deployed to have a fault-tolerant Active Roles environment. None the less, even in the worst case scenario where all AR Service instances fail, Active Directory will continue to function normally. The only result of a complete failure is that day-to-day administration or help desk functions may be interrupted until a server running the AR Service is brought back on-line.

An additional benefit of deploying multiple AR Service instances is that both the Console and the Web Interfaces will fail-over to a new AR Service if the first one becomes unresponsive. The user experience is slightly different depending upon which interface the user is using when the AR Service fails. Within the Console the user will notice the AR Service has failed and will only have to use the **Connect** command to get automatically connected to the next available AR Service. Users of the Web Interface will have a more seamless transition as the Web Interface fails over automatically to the next AR Service. One important item to note is that automatic failover only works if the option to use any available Administration Service was selected during the Web Interface setup.

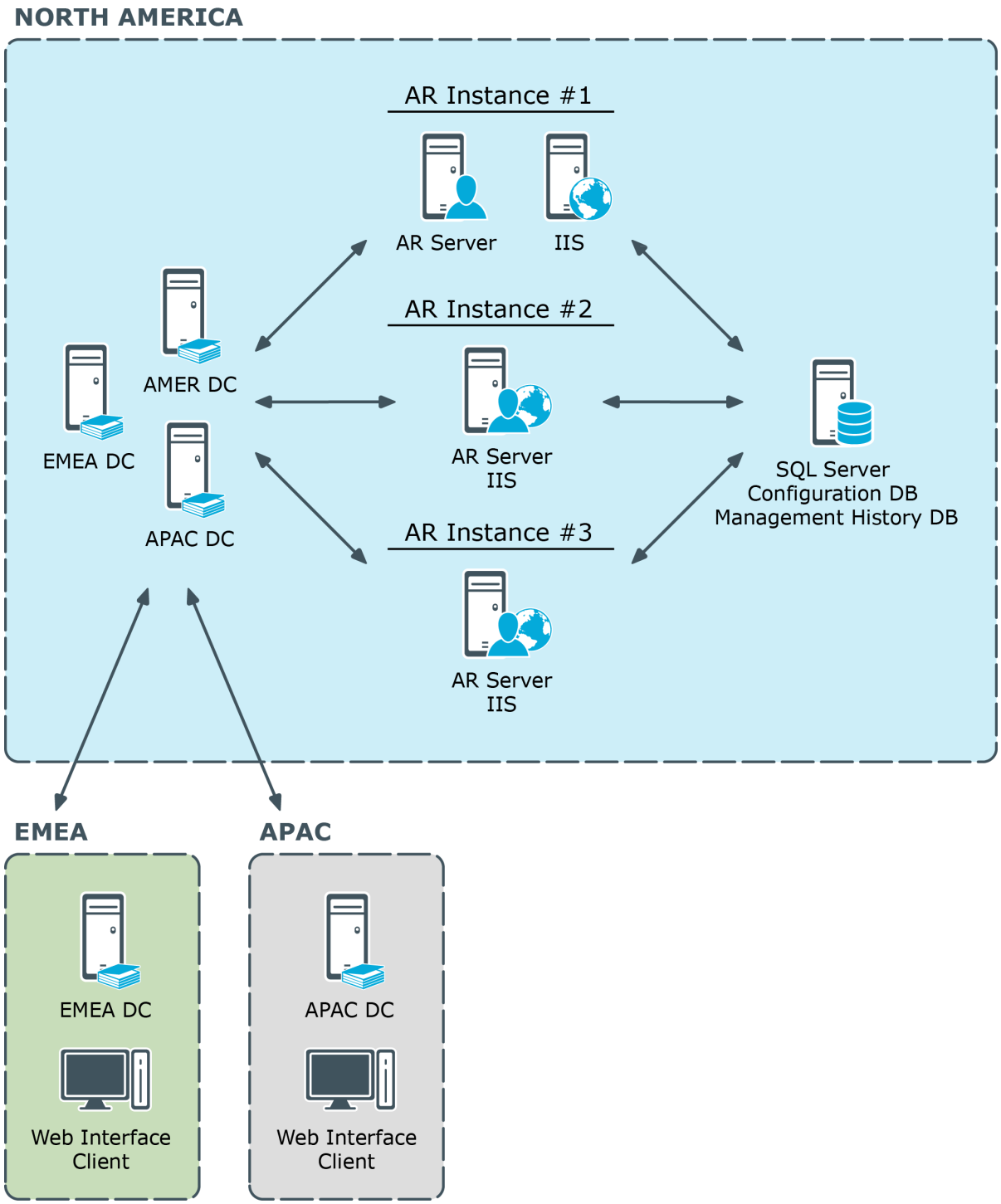
It is possible to deploy the Web Interface and AR Service components on separate servers, for security concerns or business reasons. However, when the Web Interface and AR Service are deployed on separate servers, basic authentication is normally used to authenticate the Web Interface users, causing the user credentials to be transferred over the network in clear text. In this case we highly recommend that a secure (SSL) channel be configured on the server running the Web Interface to encrypt traffic between the server and the Web browser. However it is best to keep the AR Service and Web Interface components together, on the same server, for integrated authentication and better performance.

Centralized deployment

The first installation configuration is known as the *Centralized model*. In this model administration is controlled from a single larger site. In the centralized model the deployment places servers in one physical location. This allows all the AR Service instances to share a single configuration and management history database, or replicate their

configuration changes to a partner, providing a fault tolerant configuration. While a centralized deployment may involve smaller physical locations or branch offices, administration is probably not usually performed from those locations.

Figure 4: Centralized deployment of Active Roles



This diagram illustrates a centralized deployment of Active Roles with the following characteristics:

- All the Active Roles (AR) instances are placed in a single location. Each instance is hosted on a server running the AR Service along with a Web server (IIS) running the Web Interfaces.
- All Active Roles instances share the same database for storing the configuration and management history data (Configuration DB and Management History DB).
- The EMEA and APAC branch offices use the Web Interface to perform administrative tasks, help desk operations or self-service actions.

DC focusing

Normally, the Active Roles Administration Service (AR Service) itself chooses the Active Directory domain controller (DC) to communicate with, which is the nearest DC by default. With a centralized deployment model, this means that the AR Service will select DC found in the same location where the corresponding AR instance resides, so even the regionally local changes calls (those submitted from the EMEA or APAC location) are performed against DC located in North America (rather than a locally-placed DC) thereby causing an additional slow-down due to Active Directory replication latency.

The preferred behavior would be as follows:

- Regionally local changes calls are executed against locally-placed DC.
- Cross-site changes calls are executed against DC located at the target site.

The appropriate choice of DC would ensure that the changes appear on the target site without an Active Directory replication related slow-down. Active Roles users can choose an appropriate DC by using the **Change Operational DC** command on the menu for the domain object, in the Active Roles console or Web Interface. If operational DC is explicitly specified by the user, the AR Service submits the change requests to that DC instead of the nearest DC.

Distributed deployment

The second installation configuration is the *Distributed model* where servers are deployed by analysis of how the network is configured and how administrative duties are assigned and performed.

In a distributed environment there are three primary criteria for the determination of the placement of Active Roles:

1. Where will administration be performed?
2. How are domain controllers placed?
3. What is the interface of choice for the administrators?

If both administrators and domain controllers reside in the same physical location, the AR Service should be placed in that location. In this situation either the Console or the Web Interface could be used by the administrators. However, if the Web Interface is the primary interface of choice, it is important to ensure that the AR Service the Web Interface connects to points to a domain controller in the same location so that changes are not passed over a WAN connection.

If the administrators reside in one location and domain controllers reside in another, the determining factor would be WAN reliability.

It is important to understand that the AR Service writes all administrative changes to a domain controller to which it has been associated. The critical point here is that Active Roles client applications never interface directly with a domain controller. Consequently it is more important that the AR Service be located close to its associated domain controller than where the client application is deployed in relation to the domain controller.

However, from either the Console or the Web Interfaces it is possible to choose a specific domain controller to which the AR Service writes the changes.

This diagram illustrates a distributed deployment of Active Roles with the following characteristics:

- Each of the three sites has two Active Roles (AR) instances deployed, for the sake of fault tolerance and load balancing.
- Each Active Roles instance is hosted on a server running the AR Service along with a Web server (IIS) running the Web Interface.
- Each Active Roles instance has a separate database for storing the configuration and management history data (Configuration DB and Management History DB).
- The databases are synchronized by means of SQL Server replication function. One of the database servers holds the Publisher role while the others are Subscribers to that Published (in terms of SQL Server replication).
- Administration is performed using the Web Interface on a per-site basis, by connecting Web Interface clients (Web browsers) to any of the two AR instances deployed within the site.

Total of six Active Roles instances are deployed across the world-wide enterprise, with two instances located in each of three major regions—North America, EMEA (Europe, Middle East and Africa), and APAC (Asia Pacific). This per-site deployment model provides an efficient way for Active Directory data changes initiated via Active Roles to take effect by minimizing wait time for cross-site Active Directory replication.

All Active Roles instances provide the same Active Directory access delegation workflow and can be treated as a single delegation mechanism. Sharing the same configuration settings between instances is achieved by means of SQL replication.

Each region has two Active Roles instances for failover and load balancing purposes. For failover purposes each instance is independent from a hardware and software standpoint by having its own dedicated AR Service, Web Interface (IIS) and SQL Server. This deployment is flexible in regards to hardware extension: new hardware can be added into the project for load balancing or troubleshooting purposes without changing the deployment.

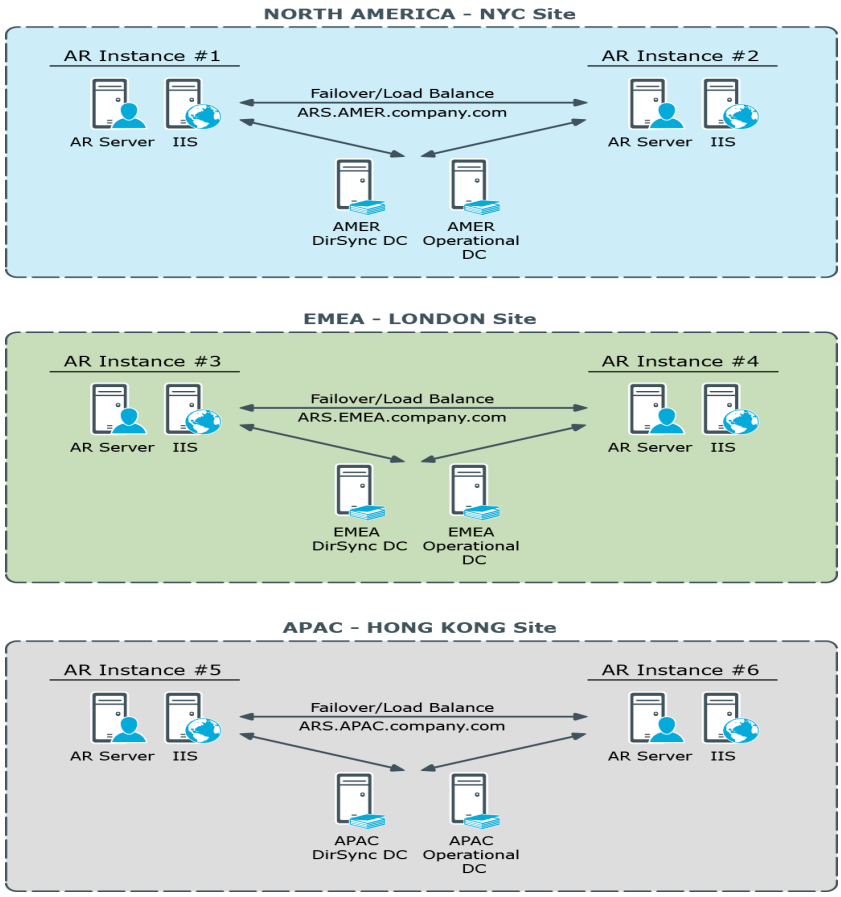
DC focusing

The AR Service normally selects the nearest Active Directory domain controller (DC) to communicate with. Therefore, the AR instance located in a given site normally communicates with a DC found in than site. This has the following implications:

- The AR instance normally applies Active Directory data changes to a DC found in the local site. This DC is referred to as *Operational DC*.
- The AR instance normally retrieves the data changes that occur in Active Directory from a DC found in the local site. This DC is referred to as *DirSync DC*.

By default, the AR Service chooses the same domain controller to hold the role of both the Operational DC and DirSync DC.

Figure 5: Active Roles Service - DC focusing



The AR Service is permanently listening to the DirSync DC for changes related to Active Roles dynamic configuration objects, such as Dynamic Groups and Managed Units. Every operation that involves the retrieval or modification of Active Directory data, requested by Active Roles client interfaces or by AR Service internal logic, is performed against this DC. The user can specify another DC for the client operations, by using the **Change Operational DC** command in the Active Roles console or Web Interface.

Each 10 minutes the AR Service validates the availability of the selected DirSync DC. If the AR Service identifies that the DC is not available, it selects another DC. Until the AR Service selects another DC, every user of Active Roles who does not explicitly specify the Operational DC will receive an error when trying to perform any operation with Active Directory.

If you have a single DC in the same site with the AR Service, and that DC becomes unavailable for some reason (for example, it was restarted), then the AR Service will select a DC from other site. After the DC in its home site becomes available, the AR Service will switch back to DC in its home site.

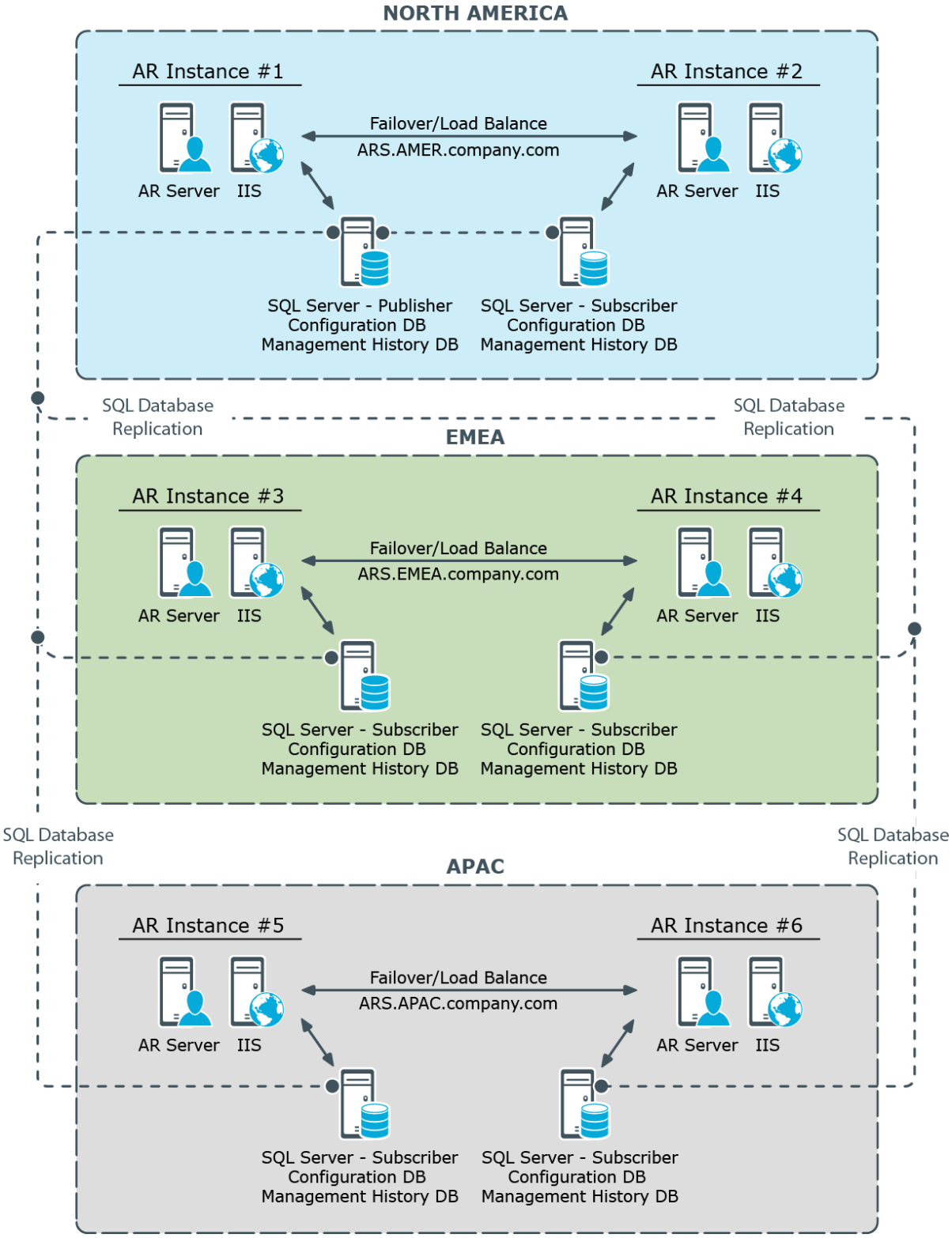
If you have multiple DCs in the same site with the AR Service, it will not randomly switch from one DC to other each 10 minutes. When other than the current DC is identified as the nearest DC, the AR Service will switch to the new DC only if the new one is in its home site and the current DC is located in another site, so the AR Service never switches between 2 available DCs in the same site.

By default, the AR Service selects any nearest available DC for a managed domain. This behavior can be configured on a per-Service or per-domain basis. To configure this behavior, use the **DirSync Servers** tab, on the property sheet for a Managed Domain object in the **Configuration/Server Configuration/Managed Domains** folder on the property sheet for an Administration Service object in the **Configuration/Server Configuration/Administration Services** folder, in the Active Roles console). If you choose the **Only specified domain controller** option and the specified DC becomes unavailable, the AR Service will not switch to other DC and the domain will be unavailable for management. For more information, refer to Active Roles Help: click **Help** on the **DirSync Servers** tab, or press F1 in the **DirSync Server Selection** dialog box that appears when you click **Change** on the **DirSync Servers** tab.

SQL database

Total of six SQL Server instances are deployed across the world-wide enterprise to host the Active Roles database, with two instances located in each of three major regions—North America, EMEA, and APAC. Each AR instance has a separate SQL database. The databases are synchronized by means of SQL Server replication function. One of the database servers holds the Publisher role while the others are Subscribers to that Published.

Figure 6: Active Roles using SQL database



Active Roles normally uses the same database to store both the Configuration and Management History data. The Configuration data applies to the delegation and workflow

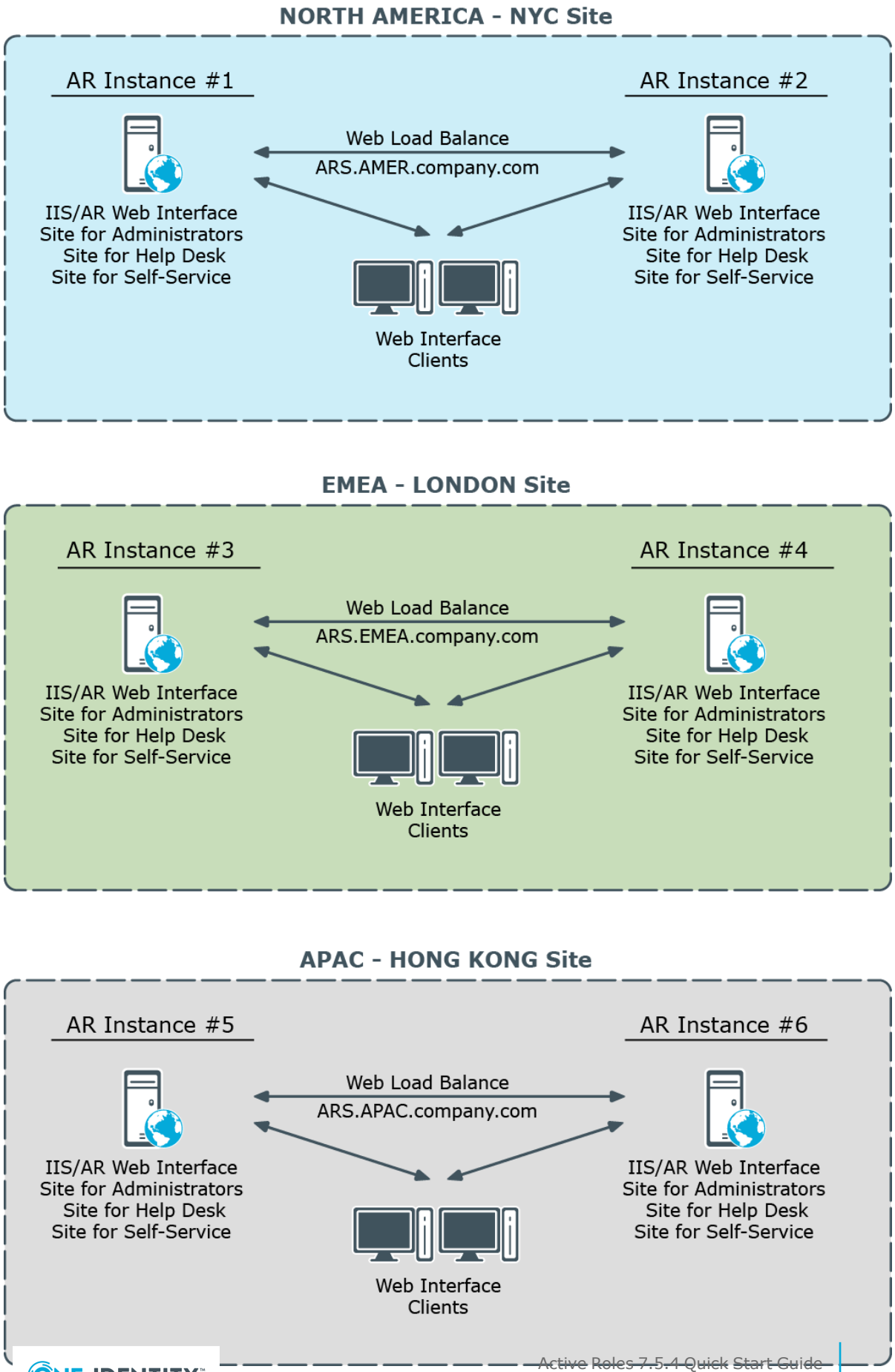
related objects, such as Access Templates, Police Objects and Managed Units. The virtual attributes created with Active Roles are also stored as part of the Configuration data. The Management History data comprises history of changes that were made to directory objects via Active Roles. In addition, the approval, temporal group membership, and deprovisioning tasks are stored as part of the Management History data. Given a large volume of Management History data, it may be advisable to create a separate Management History database (see "Centralized Management History Storage" in the Active Roles Administration Guide).

Active Roles uses SQL Server merge replication to synchronize the Configuration and Management History data among the databases. One of the databases is configured on the SQL Server instance that holds the Publisher role; the remaining databases are configured as Subscriber role holders. The instructions on how to configure replication can be found in the Active Roles Administration Guide (see the "Configuring Replication" chapter). Separate instructions are provided in connection with replication of the Management History data (see "Replication of Management History Data" in the Active Roles Administration Guide). To successfully configure replication, ensure that all your SQL Server instances run the same version of SQL Server. If a SQL Server Service Pack is installed on one of the instances, the same Service Pack must be installed on all the instances.

Web Interface

Each of the six AR instances has a separate Web Interface installation, with the AR Service and Web Interface components running together, on the same server. A design where both the AR Service and Web Interface are installed on a single server takes advantage of integrated authentication, which allows domain users to access the Web Interface without being prompted for their user name and password.

Figure 7: Active Roles Web interface deployment


NORTH AMERICA - NYC Site
AR Instance #1
AR Instance #2
Web Load Balance
ARS.AMER.company.com
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
Web Interface
Clients
EMEA - LONDON Site
AR Instance #3
AR Instance #4
Web Load Balance
ARS.EMEA.company.com
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
Web Interface
Clients
APAC - HONG KONG Site
AR Instance #5
AR Instance #6
Web Load Balance
ARS.APAC.company.com
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
IIS/AR Web Interface
Site for Administrators
Site for Help Desk
Site for Self-Service
Web Interface
Clients

Total of six Web Interface instances are deployed across the world-wide company enterprise, with two instances installed in each of three major regions. In each region two Web Interface instances provide load balancing and failover capabilities. Initially, each AR Service has one dedicated Web Interface instance; later it will be possible to introduce another Web Interface instance for the same AR Service if performance needs to be increased.

Each Web Interface instance comprises several websites. The website configuration is synchronized among the Web Interface instances by means of SQL database replication (the website configuration settings are stored as a part of Active Roles configuration data). This allows you to customize a website on a single Web Interface instance and be sure that the replication function will apply the customization changes across all Web Interface instances.

The Web Interface provides rich customization capabilities out of the box, so Web Interface sites can be easily configured to show or hide certain fields or attributes to the end-user, including custom (extended) schema attributes. It is also possible to add or remove commands, create new forms or customize existing pages by adding forms (tabs) and form fields (entries).

The Web Interface ships with three built-in website templates:

- Default site for Administrators
- Default site for Help Desk
- Default site for Self-administration

You can use these templates to create new Web Interface sites and then customize each of the new sites as needed. Thus, you may deploy multiple Help Desk sites, having each customized individually. To create new Web Interface sites and site configurations Active Roles provides the Web Interface Sites Configuration wizard. You can open the wizard from the Start menu on any server running the Web Interface. The wizard is mainly intended to:

- Create a new Web Interface site with an existing configuration. This option only allows you to select a Web Interface site configuration that already exists in your Active Roles environment. Use this option when deploying a new Web Interface instance to add an existing custom Web Interface site to that instance.
- Create a new Web Interface site with a new configuration. This option only allows you to select one of the three built-in website templates, and creates a new Web Interface site configuration based on the template you select. Use this option to create a new Web Interface site on one of your Web Interface instances. On the other instances the new site should be deployed by selecting the site configuration you have created.

When deploying a new Web Interface instance, it is important to understand that only three default Web Interface sites are installed out of the box. To add a custom Web Interface site to a newly installed Web Interface instance, you should use the Web Interface Sites Configuration wizard.

Unattended installation of Active Roles components

Active Roles supports Command line options for the installation of Active Roles Server. The following is a list of command line options available with Active Roles Server 7.5.4:

- ActiveRoles.exe

  Launches the Setup wizard.

- ActiveRoles.exe /quiet [parameters]

  Quiet mode, no user interaction. Also known as a silent or unattended installation.

- Parameter syntax

  /parameter [*properties*]

  Use a space character to separate properties.

- Properties

  ADDLOCAL=

  Comma-separated list of Active Roles components to install.

  REMOVE=

  Comma-separated list of Active Roles components to remove.

  TARGETDIR=

  Path to the desired install folder.

- Component names
  - ALL - all components
  - Service - Administration Service
  - Web - Web Interface
  - Console - Console (MMC Interface)
  - Tools - Management Tools
  - SyncService - Synchronization Service

- Parameters
  - /**IAcceptActiveRolesLicenseTerms**
    - Required when both the /quiet and /install parameters are specified.
    - By specifying this parameter, you acknowledge that you have read and understand the terms in the Active Roles license agreement.
  - /**install [optional properties]**
    - Takes effect if no Active Roles components installed; otherwise, disregarded.
    - Installs components specified by ADDLOCAL property to TARGETDIR folder.
    - If ADDLOCAL omitted, installs all components except Synchronization Service.
    - To install Synchronization Service, you have to specify ADDLOCAL=SyncService.
    - If TARGETDIR omitted, installs to %programfiles%\One Identity\Active Roles\.

  Examples:

  ActiveRoles.exe /quiet /install */IAcceptActiveRolesLicenseTerms*

  ActiveRoles.exe /quiet /install *ADDLOCAL=Service,Console /IAcceptActiveRolesLicenseTerms*

  ActiveRoles.exe /quiet /install *ADDLOCAL=Console TARGETDIR=D:\Active Roles\ /IAcceptActiveRolesLicenseTerms*

- /modify ADDLOCAL=| REMOVE=
  - Takes effect if any Active Roles components installed; otherwise, disregarded.
  - Installs components specified by ADDLOCAL property or
  - Removes components specified by REMOVE property.

  Examples:

  ActiveRoles.exe /quiet /modify *ADDLOCAL=Web*

  ActiveRoles.exe /quiet /modify *REMOVE=Console*

- /repair
  - Takes effect if any Active Roles components installed; otherwise, disregarded.
  - Repairs all installed components.

  Example:

  ActiveRoles.exe /quiet /repair

- /uninstall
  - Takes effect if any Active Roles components installed; otherwise, disregarded.
  - Uninstalls all components. Error conditions may terminate uninstall.

Example:

ActiveRoles.exe /quiet /uninstall

- /forceuninstall
  - Takes effect if any Active Roles components are installed; otherwise, disregarded.
  - Use this parameter to uninstall all components if errors prevent normal uninstall.

  Example:

  ActiveRoles.exe /quiet /forceuninstall
- /forcerestart
  - Auto-restarts the computer when a restart is required to complete the requested
  - setup actions. Without this parameter, you may have to restart the computer manually
  - after running Setup (for example, if Setup needs to update any files that are in use).

  Examples:

  ActiveRoles.exe /quiet /uninstall /forcerestart

  ActiveRoles.exe /quiet /repair /forcerestart

10

Configuring Active Roles to Manage Hybrid AD Objects

When a user signs up for a Microsoft cloud service such as Azure Active Directory, details about the user's organization and the organization's Internet domain name registration are provided to Microsoft. This information is then used to create a new Azure AD instance for the organization. The same directory is used to authenticate sign in attempts when you subscribe to multiple Microsoft cloud services.

The Azure AD instance of the organization, also called the Azure AD tenant, stores the users, groups, applications, and other information pertaining to an organization and its security. To access the Azure AD tenant, we need an application that is registered with the tenant. Active Roles uses this application, also called the Azure AD application, to communicate to Azure AD tenant after providing the required consent.

The Active Roles Web Interface and Management Shell can be used to perform the Azure AD configuration tasks. The new feature in Active Roles enables you to add or modify existing tenants to the management scope through the web interface and Management Shell.

The latest release of Active Roles supports Multiple tenants model.

NOTE: Administrative users or users with sufficient privileges only can view Azure configuration.

The following section guides you through the Active Roles web interface and Management Shell to configure Azure AD tenants and applications and synchronize existing AD objects to Azure AD.

- Configuring Active Roles to manage Azure AD using the GUI
- Configuring Active Roles to manage Hybrid AD using Management Shell
- Active Roles Configuration steps to manage Hybrid AD objects
- Active Roles Configuration to synchronize existing AD objects to Azure AD
- Changes to Azure O365 Policies in Active Roles after 7.4.1

Configuring Active Roles to manage Azure AD using the GUI

Use the Active Roles Web Interface and the Active Roles Configuration Center to perform the following actions and configure Azure AD deployments:

- Configuring a new Azure tenant and consenting Active Roles as an Azure application
- Importing an Azure tenant and consenting Active Roles as an Azure application
- Viewing or modifying the Azure AD tenant type
- Removing an Azure AD tenant
- Delete an Azure AD Application
- View Azure Health for Azure AD tenants and applications
- View Azure Licenses Report

Configuring a new Azure tenant and consenting Active Roles as an Azure application

When installing Active Roles out-of-the-box, the **Directory Management** > **Tree** > **Azure** node of the Active Roles Web Interface only contains an empty **Azure Configuration** sub-node by default.

To manage Azure AD directory objects (Azure users, guest users, contacts, O365 groups and Azure Security groups, and so on), you must specify an Azure tenant and configure Active Roles as a consented Azure application for it in the Active Roles Configuration Center.

NOTE: If you have already used an Azure tenant (or tenants) in a previous version of Active Roles, you can import and reconfigure them in two ways:

- If you perform an in-place upgrade of Active Roles (that is, you install the latest version without uninstalling the previous version of Active Roles first in one of the supported upgrade paths), you can reauthenticate the existing Azure tenants with the **Upgrade configuration** wizard upon launching the Active Roles Configuration Center after installation.

  For more information on reauthenticating Azure tenants this way, see *Reconfiguring Azure tenants during upgrade configuration* in the *Active Roles 7.5.4 Quick Start Guide*. For more information on the supported upgrade paths, see *Version upgrade compatibility chart* in the *Active Roles 7.5.4 Release Notes*.
- If you install a new version of Active Roles to a machine that does not have any earlier versions of the software installed (either because it has been already

uninstalled, or it has been installed on another machine), you can import your existing Azure tenant(s) by importing your Azure AD configuration. Following the import, you can reconsent your Azure tenants manually.

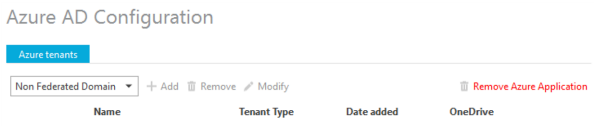
For more information on importing existing Azure tenants this way, see Importing an Azure tenant and consenting Active Roles as an Azure application.

Prerequisites

The Active Roles Administration Service must be already running. If the service is not running, then:

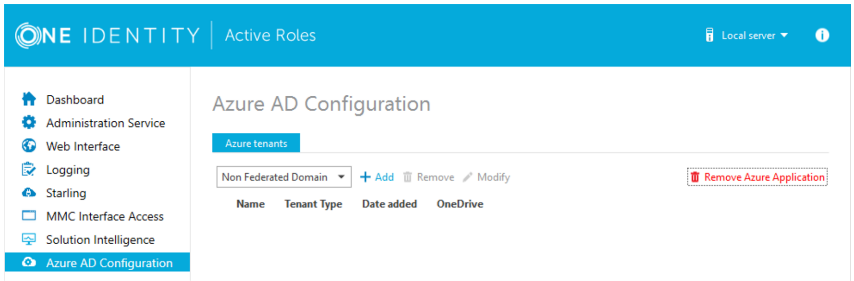
1. Open the Active Roles Configuration Center.
2. Navigate to the **Administration Service** page.
3. Click **Start**.

TIP: If the Active Roles Administration Service is not running, the **Azure AD Configuration** page indicates it with an on-screen warning.



To configure a new Azure tenant (or tenants) and set Active Roles as a consented Azure application

1. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.

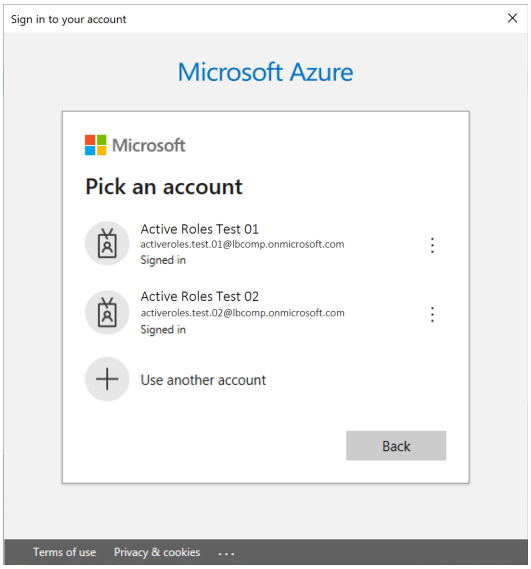


2. From the drop-down list, select the type of domain assigned to the new Azure AD tenant:
   - **Non-Federated Domain**: When selected, on-premises domains are not registered in Azure AD, and Azure AD Connect is not configured. Azure users and Azure guest users are typically created with the `onmicrosoft.com` UPN suffix.
   - **Federated Domain**: On-premises domains are registered in Azure AD and Azure AD Connect. Also, Active Directory Federation Services (ADFS) is configured. Azure users and Azure guest users are typically created with the

UPN suffix of the selected on-premises domain.

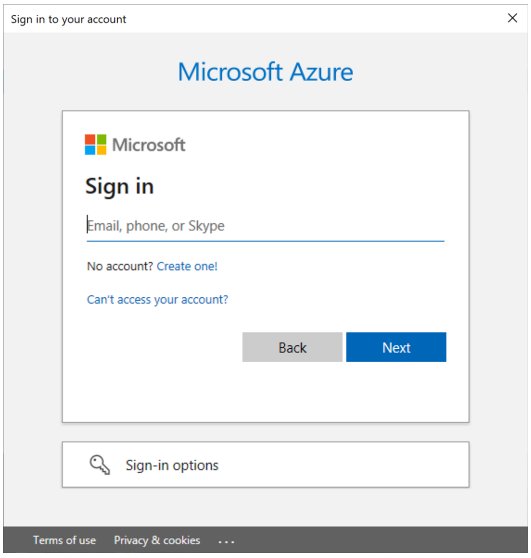
- **Synchronized Identity Domain**: On-premises domains may or may not be registered in Azure AD. Azure AD Connect is configured. Azure users and Azure guest users can be created either with the selected on-premises domain, or with the `onmicrosoft.com` UPN suffix.

3. To configure a new Azure tenant, click **Add**.
4. Authenticate your Azure AD administrator account.
    - If you already used one or more Azure AD administrator accounts on your PC, select your account from the **Pick an account** list, then provide the account password. If you do not find your account in the list, specify your account by clicking **Use another account**.



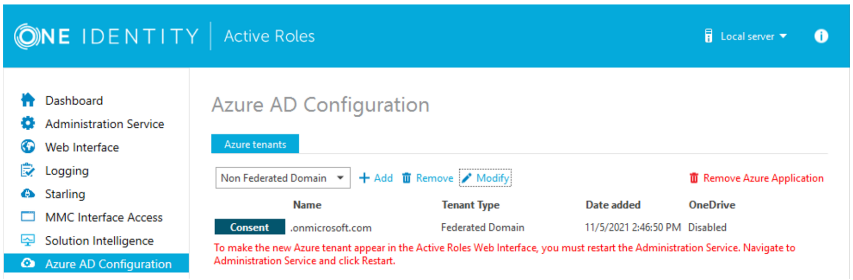
    - If you have not used any Azure AD administrator accounts yet on the PC (for example, because you are configuring a fresh Active Roles installation), specify

your account user name in the **Sign in** field, then provide your password.



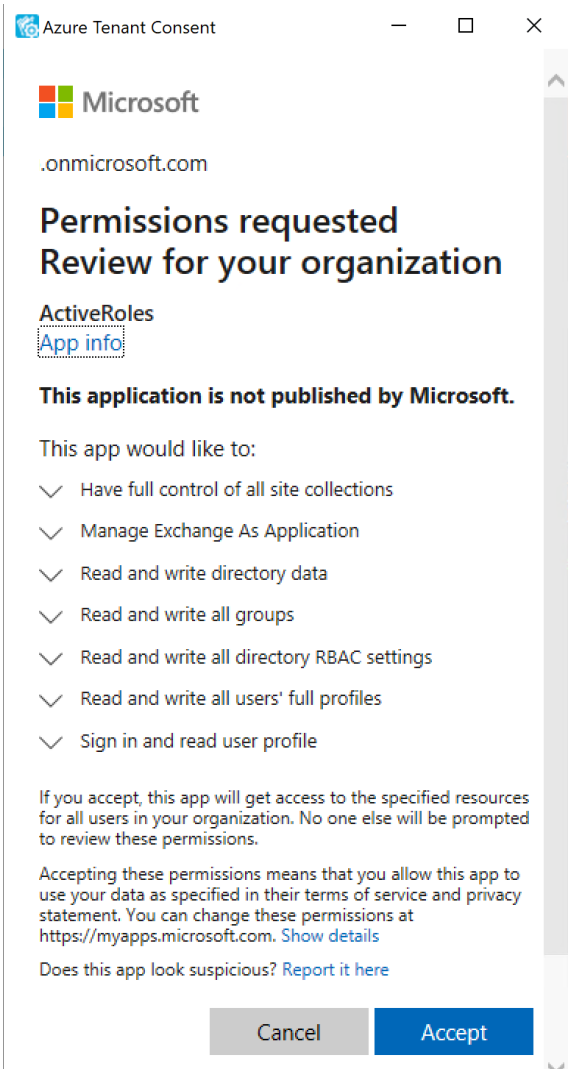
NOTE: Do not specify an account that has already been used to add an Azure tenant. You can only add a single Azure tenant with the same Azure AD account. Specifying an administrator account that is already linked to an Azure tenant will result in an error.

Upon successful authentication, the new Azure tenant appears in the list.



5. To manage the Azure tenant and its contents in the Active Roles Web Interface, you must consent Active Roles as an Azure application. To do so, click **Consent** next to the Azure tenant.
6. Authenticate your Azure AD administration account again. Depending on the type of Microsoft pop-up that appears (**Pick an account** or **Sign in**), either select the Azure AD account you used for adding the Azure tenant, or specify its user name and password again.

   NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.
7. The standard Microsoft **Permissions requested** pop-up appears, listing all the permissions required for configuring Active Roles as an Azure application. To finish creating the Azure application, click **Accept**.



Active Roles then authenticates every Azure AD administrative operation performed in the Azure tenant with a set of generated client ID and client secret.

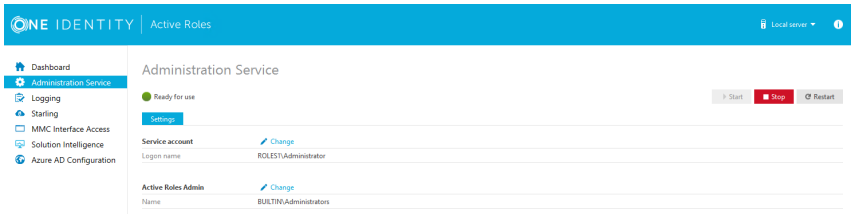
NOTE: Once you click **Accept**, Windows may show a **Security Warning** pop-up with the following message:

```
The current webpage is trying to open a site on your intranet. Do you
want to allow this?
```

In such cases, clicking either **Yes** or **No** could freeze the pop-up dialog, but consenting the Azure tenant will finish without problem.

This issue can occur in case the computer running Active Roles has incorrect browser settings. As a workaround, to get an up-to-date status of the state of the Azure tenant, close and restart the Active Roles Configuration Center after clicking **Yes** in the **Security Warning** pop-up.

8. If you have additional Azure tenants to add and consent, configure them as described in the previous steps of this procedure.
9. To make the configured Azure tenant(s) appear in the Active Roles Web Interface, you must restart the Administration Service, as indicated on the user interface. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



TIP: Once the Azure tenant or tenants are configured, and Active Roles is also set as a consented Azure AD application for it, you can view and modify the configured tenant(s) and their settings at the following locations:

- To change the domain type or OneDrive provisioning settings of an Azure tenant, in the Active Roles Configuration Center, navigate to **Azure AD Configuration**, select the Azure tenant, and click **Modify**. For more information, see Viewing or modifying the Azure AD tenant type.
- To check the connectivity status of the Azure configuration, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Azure Health Check**. For more information, see View Azure Health for Azure AD tenants and applications.
- To check the Azure Licenses Report, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Azure Licenses Report**. For more information, see View Azure Licenses Report.
- To check the Office 365 Roles Report, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Office 365 Roles Report**. For more information, see View Office 365 Roles Report.

NOTE: Consider the following when configuring an Azure tenant:

- When Active Roles is registered as a consented Azure AD application, minimal permissions are assigned to it by default. To add additional permissions to the Azure application, sign in to the Azure Portal and add your required permissions there.
- Azure Multi-Factor Authentication (MFA) is automatically enforced for Azure users and Azure guest users added to the configured Azure tenant. To disable Azure MFA for the Azure tenant, sign in to the Azure Portal and navigate to **Tenant** > **Properties** > **Manage Security defaults** and set **Enable Security defaults** to **No**.

Importing an Azure tenant and consenting Active Roles as an Azure application

If you have previously managed an Azure AD deployment, but you are not upgrading from a previous version of Active Roles via in-place upgrade (for example, because the previous version of Active Roles has been uninstalled before installing the new version), you can import, reauthenticate and consent existing Azure tenants via the Active Roles Configuration Center.

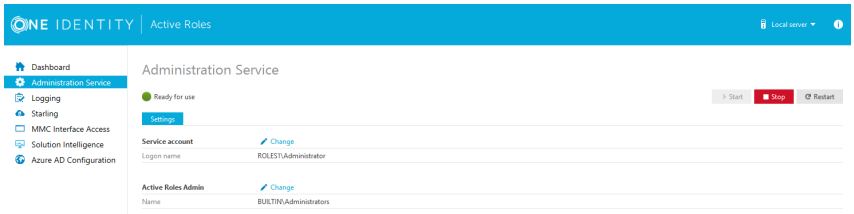
NOTE: Consider the following if you have not used any Azure tenants earlier, or if you installed the latest version of Active Roles via in-place upgrade:

- If you have installed Active Roles out-of-the-box, and no Azure AD environment has been used previously in your organization, you must specify a new Azure tenant to manage Azure directory objects (such as Azure users, guest users, contacts, O365 groups or Azure Security groups). For more information, see Configuring a new Azure tenant and consenting Active Roles as an Azure application.
- If you perform an in-place upgrade of Active Roles (that is, you install the latest version without uninstalling the previous version of Active Roles first in one of the supported upgrade paths), you can reauthenticate the existing Azure tenants with the **Upgrade configuration** wizard upon launching the Active Roles Configuration Center after installation.

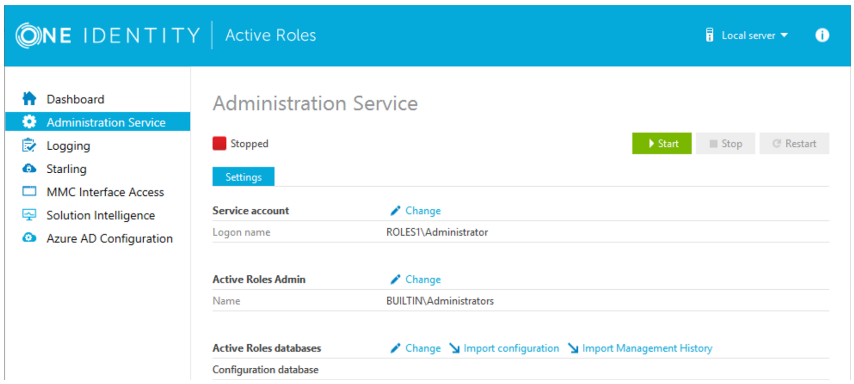
  For more information on reauthenticating Azure tenants this way, see *Reconfiguring Azure tenants during upgrade configuration* in the *Active Roles 7.5.4 Quick Start Guide*. For more information on the supported upgrade paths, see *Version upgrade compatibility chart* in the *Active Roles 7.5.4 Release Notes*.

To import and reauthenticate an Azure tenant and set Active Roles as a consented Azure application

1. Stop the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, on the left pane, navigate to **Administration Service** and click **Stop**.



2. Once the Active Roles Administration Service stopped, open the **Import configuration** wizard by clicking **Active Roles databases** > **Import configuration**.

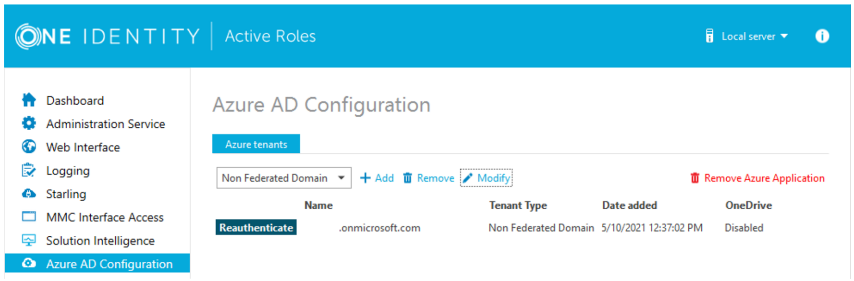


3. Perform the steps of the wizard. For more information, see Import configuration data or *Steps to deploy the Administration Service* in the *Active Roles Quick Start Guide*.

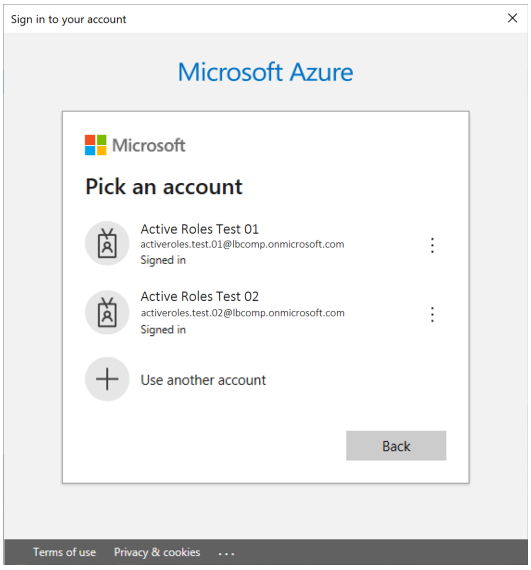
   CAUTION: Importing a configuration will overwrite every Azure tenant currently listed in the Azure AD Configuration page with those included in the imported configuration.

4. Once the import procedure finished, start the Active Roles Administration Service by clicking **Start** in the **Administration Service** page.
5. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.

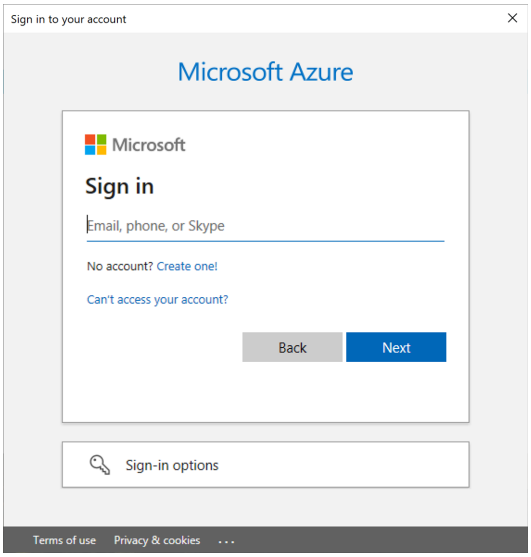
   The list of imported Azure tenants appears.



6. To configure an imported Azure tenant, click **Reauthenticate**.
7. Authenticate your Azure AD administrator account.
   - If you already used one or more Azure AD administrator accounts on your PC, select your account from the **Pick an account** list, then provide the account password. If you do not find your account in the list, specify your account by clicking **Use another account**.



- If you have not used any Azure AD administrator accounts yet on the PC (for example, because you are configuring a fresh Active Roles installation), specify your account user name in the **Sign in** field, then provide your password.



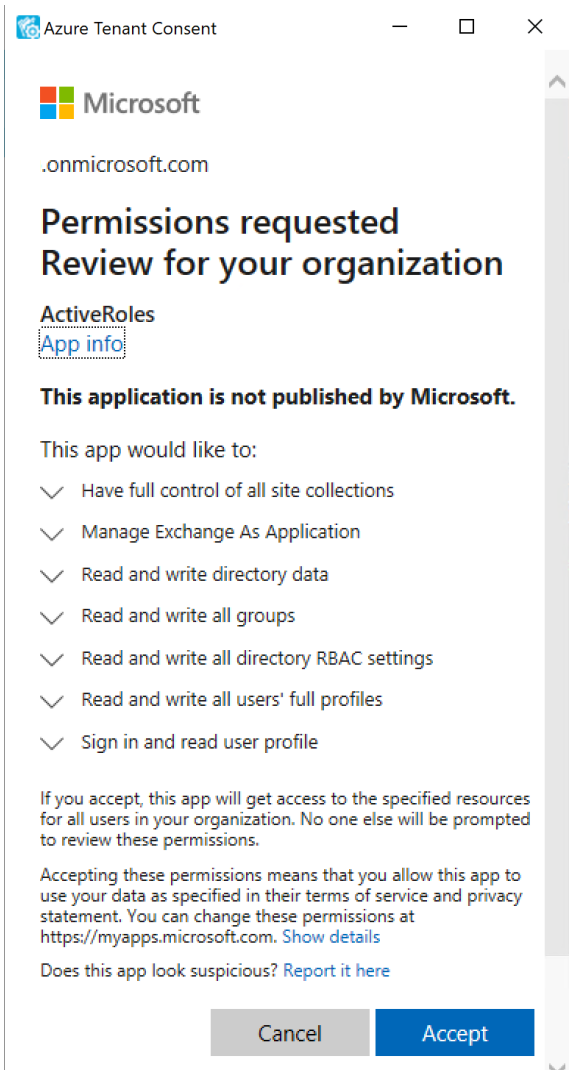
NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.

8. To manage the Azure tenant and its contents in the Active Roles Web Interface, you must consent Active Roles as an Azure application. To do so, click **Consent** next to the Azure tenant.
9. Authenticate your Azure AD administration account again. Depending on the type of Microsoft pop-up that appears (**Pick an account** or **Sign in**), either select the Azure

AD account you used for adding the Azure tenant, or specify its user name and password again.

NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.

10. The standard Microsoft **Permissions requested** pop-up appears, listing all the permissions required for configuring Active Roles as an Azure application. To finish creating the Azure application, click **Accept**.



Active Roles then authenticates every Azure AD administrative operation performed in the Azure tenant with a set of generated client ID and client secret.

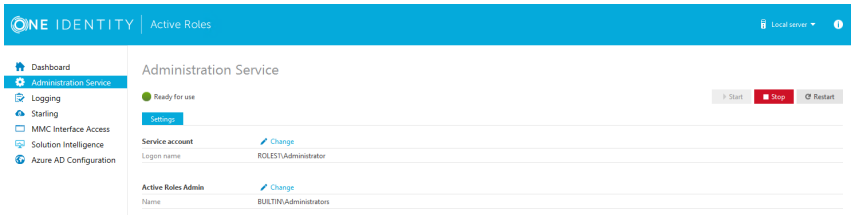
NOTE: Once you click **Accept**, Windows may show a **Security Warning** pop-up with the following message:

```
The current webpage is trying to open a site on your intranet. Do you
want to allow this?
```

In such cases, clicking either **Yes** or **No** could freeze the pop-up dialog, but consenting the Azure tenant will finish without problem.

This issue can occur in case the computer running Active Roles has incorrect browser settings. As a workaround, to get an up-to-date status of the state of the Azure tenant, close and restart the Active Roles Configuration Center after clicking **Yes** in the **Security Warning** pop-up.

11. To make the configured Azure tenant(s) appear in the Active Roles Web Interface, you must restart the Administration Service, as indicated on the user interface. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



TIP: Once the Azure tenant or tenants are configured, and Active Roles is also set as a consented Azure AD application for it, you can view and modify the configured tenant(s) and their settings at the following locations:

- To change the domain type or OneDrive provisioning settings of an Azure tenant, in the Active Roles Configuration Center, navigate to **Azure AD Configuration**, select the Azure tenant, and click **Modify**. For more information, see Viewing or modifying the Azure AD tenant type.
- To check the connectivity status of the Azure configuration, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Azure Health Check**. For more information, see View Azure Health for Azure AD tenants and applications.
- To check the Azure Licenses Report, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Azure Licenses Report**. For more information, see View Azure Licenses Report.
- To check the Office 365 Roles Report, in the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **Azure Configuration** > **Office 365 Roles Report**. For more information, see View Office 365 Roles Report.

NOTE: Consider the following when configuring an Azure tenant:

- When Active Roles is registered as a consented Azure AD application, minimal permissions are assigned to it by default. To add additional permissions to the Azure application, sign in to the Azure Portal and add your required permissions there.

- Azure Multi-Factor Authentication (MFA) is automatically enforced for Azure users and Azure guest users added to the configured Azure tenant. To disable Azure MFA for the Azure tenant, sign in to the Azure Portal and navigate to **Tenant** > **Properties** > **Manage Security defaults** and set **Enable Security defaults** to **No**.

Viewing or modifying the Azure AD tenant type

Use the Active Roles Administration Center to view or modify the tenant type of an existing Azure AD tenant. This is useful if you need to change the default domain settings of an Azure tenant due to an IT or organizational change.

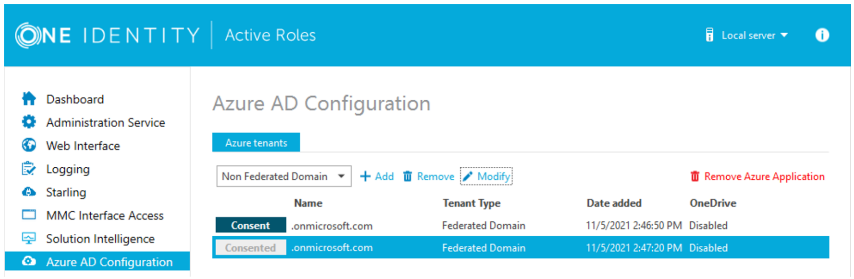
NOTE: Consider the following limitations when modifying the properties of the selected Azure AD tenant:

- If you set the tenant type of an on-premises or hybrid Azure AD to **Federated Domain** or **Synchronized Identity Domain**, then the **Azure properties** fields of the objects (Azure users, Azure guest users, groups and contacts) in the Azure tenant will be disabled and cannot be edited in the Active Roles Web Interface.
- You cannot modify the tenant ID and the authentication settings of the Azure AD tenant.

To view or modify the Azure AD tenant properties

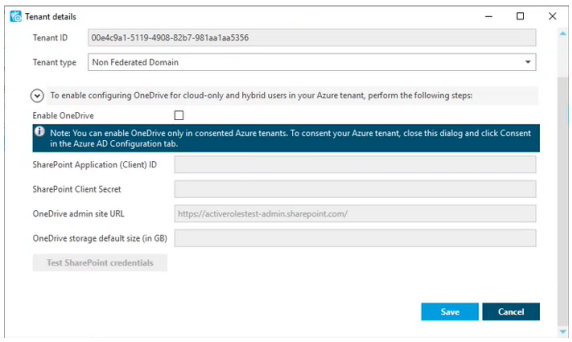
1. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.

   The list of existing Azure AD tenants appears.



2. Select the Azure AD tenant you want to view or modify, then click **Modify**.

   The **Tenant details** window appears.



3. (Optional) To change the domain type of the Azure tenant, select the applicable type from the **Tenant type** drop-down list.
    - **Non-Federated Domain**: When selected, on-premises domains are not registered in Azure AD, and Azure AD Connect is not configured. Azure users and Azure guest users are typically created with the `onmicrosoft.com` UPN suffix.
    - **Federated Domain**: On-premises domains are registered in Azure AD and Azure AD Connect. Also, Active Directory Federation Services (ADFS) is configured. Azure users and Azure guest users are typically created with the UPN suffix of the selected on-premises domain.
    - **Synchronized Identity Domain**: On-premises domains may or may not be registered in Azure AD. Azure AD Connect is configured. Azure users and Azure guest users can be created either with the selected on-premises domain, or with the `onmicrosoft.com` UPN suffix.
4. (Optional) To enable, disable or modify the provisioned OneDrive storage of the Azure tenant, select or deselect **Enable OneDrive**, and (when selected), configure the SharePoint and OneDrive settings listed in the **Tenant details** window. For more information on configuring OneDrive storage in an Azure tenant, see Enabling OneDrive in an Azure tenant.
5. To close the **Tenant details** window without any changes, click **Cancel**. To apply your changes, click **Save**.

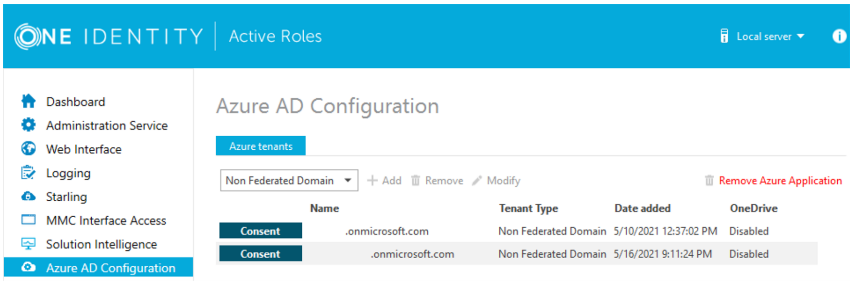
Removing an Azure AD tenant

You can use the Active Roles Configuration Center to delete an Azure AD tenant. This is typically required when an Azure tenant and its directory objects become obsolete because of organizational reasons.

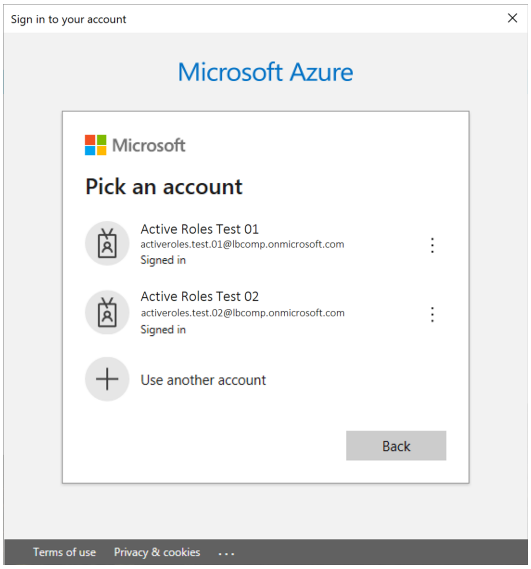
To remove an Azure AD tenant

1. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.

    The list of existing Azure tenants appears.

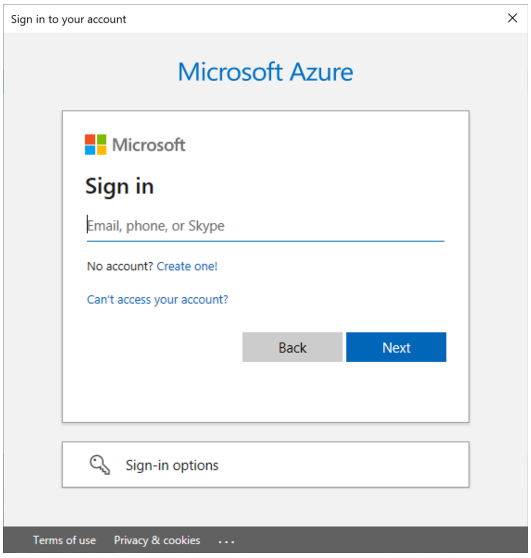


2. On the **Azure AD Configuration** page, from the list of Azure tenants, select the tenant that you want to remove.
3. Click **Remove**.
4. Authenticate your Azure AD administrator account.
    - If you already used one or more Azure AD administrator accounts on your PC, select your account from the **Pick an account** list, then provide the account password. If you do not find your account in the list, specify your account by clicking **Use another account**.



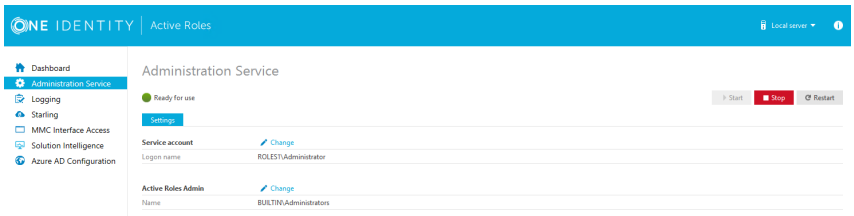
    - If you have not used any Azure AD administrator accounts yet on the PC (for example, because you are configuring a fresh Active Roles installation), specify

your account user name in the **Sign in** field, then provide your password.



NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.

5. The Azure tenant and all the related domains and applications are then deleted upon successful login.
6. To apply the changes, you must restart the Administration Service, as indicated on the user interface. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



7. (Optional) If you want to force the deletion of the Active Roles Azure application on the Azure Portal for the removed Azure tenant, click **Remove Azure Application** and log in with the credentials of the removed Azure tenant.

   This is typically recommended as an extra housekeeping and security measure if the removed Azure tenant has been previously managed either in earlier Active Roles versions or on other machines as well, but the Azure tenant has not been removed from those Active Roles installations prior to uninstalling them (leaving their client secret intact on the Azure Portal).

CAUTION: Using the Remove Azure Application option will result in all Active Roles installations losing access to the specified Azure tenant. If this happens, users managing the Azure tenant in another Active Roles installation (for example, on another machine) can regain access to the Azure tenant if they:

1. **Remove the Azure tenant in the Azure AD Configuration tab of their Active Roles Configuration Center.**
2. **Add the Azure tenant again, as described in Configuring a new Azure tenant and consenting Active Roles as an Azure application.**

8. To confirm removal, check if the removed Azure tenant has disappeared from the list of Azure tenants in the **Azure AD Configuration** page of the Active Roles Configuration Center, and from the **Directory Management** > **Tree** > **Azure** node of the Active Roles Web Interface.

Configuring Active Roles to manage Hybrid AD using Management Shell

Active Roles Management Shell enables you to perform the following configuration tasks to manage Hybrid AD:

- Adding an Azure AD tenant
- Add an Azure AD Application

Adding an Azure AD tenant

Use the Active Roles Management Shell to add an Azure AD tenant. To do so, run the `New-QADAzureConfigObject` cmdlet on the Management Shell interface.

Description

`New-QADAzureConfigObject` lets you add an Azure AD tenant to Active Directory.

Usage Recommendations

Use `New-QADAzureConfigObject` to add an Azure AD tenant using the tenant ID provided by Microsoft for the default tenant (created at the time of the Microsoft Azure subscription).

Syntax

```
New-QADAzureConfigObject -type 'AzureTenant' -name 'Azuretenantname' -
AzureTenantId 'AzureTenantGUID' -AzureTenantDescription 'AzureTenantDescription'
-AzureAdminUserID 'AzureGlobalAdminUserID' -AzureAdminPassword
'AzureGlobalIDPassword' -AzureADTenantType 'AzureTenantType'
```

Parameters

The `New-QADAzureConfigObject` cmdlet has the following parameters.

- `type (string)`: Specifies the object class of the directory object to be created (such as User or Group). The cmdlet creates a directory object of the object class specified with this parameter.

  Table 5: Parameter: type (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `name (string)`: Sets the `name` attribute to the value of this parameter on the new object created by **`New-QADAzureConfigObject`** in the directory.

  Table 6: Parameter: name (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `AzureTenantId (string)`: Specifies the Azure AD tenant ID obtained from the default tenant (created after subscribing to Microsoft Azure).

  NOTE: The Azure AD ID value configured for this parameter must match the tenant ID configured on the Azure AD side. Otherwise, attempts to create an Azure AD application or manage Azure AD objects will fail.

Table 7: Parameters: AzureTenantId (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `AzureTenantDescription`: Specifies the required description of the Azure AD tenant.

Table 8: AzureTenantDescription

Required	false
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `AzureAdminUserID`: Specifies the administrative user name for Microsoft Azure AD.

  NOTE: The administrative user must have the required privileges (for example, License Administrator, User Administrator or Groups Administrator roles) to perform license management or Azure user, guest user, and group management.

  For more information on the available privileges and for an overview of the various Azure and Azure AD administrative roles, see Azure AD built-in roles and Classic subscription administrator roles, Azure roles, and Azure AD roles in the official Microsoft documentation.

Table 9: Parameters: AzureAdminUserID

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `AzureAdminPassword`: Specifies the administrative user password for Microsoft Azure AD.

Table 10: Parameters: AzureAdminPassword

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- `AzureADTenantType`: Specifies the Azure AD tenant type (Federated, Non-Federated, or Synchronized Identity).

  NOTE: Make sure that you select the tenant type corresponding to your organization environment.

Table 11: Parameters: AzureADTenantType

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false
Accepts value	• Federated • NonFederated • SynchronizedIdentity

Examples

See the following use cases for examples on how to use this cmdlet.

Example: Creating a new Azure AD tenant with a local user

To create a new Azure AD tenant with a locally logged on user

1. Connect to any available domain controller with the credentials of your local user.
2. Create a new Azure AD tenant with the following `New-QADAzureConfigObject` cmdlet:

```
C:\PS> New-QADAzureConfigObject -type 'AzureTenant' -name
'CompanyAzuretenant' -AzureTenantId 'CompanyAzureTenantID' -
AzureTenantDescription 'Azure tenant for Company' -AzureAdminUserID
'AzureAdminUser1' -AzureAdminPassword 'AzureAdminPassword1’ -
AzureADTenantType 'AzureTenantType'
```

Example: Creating a new Azure AD tenant with a specific user and then disconnecting

To create a new Azure AD tenant with a specific user and then disconnect

1. Connect to any available domain controller:

   ```
   C:\PS> $pw = read-host "Enter password" -AsSecureString
   ```

2. Connect to the local Administration Service with a specific user of your choice:

   ```
   C:\PS> connect-qadService -service 'localhost' -proxy -
   ConnectionAccount 'company\administrator' -ConnectionPassword $pw
   ```

3. Create the new Azure AD tenant:

   ```
   C:\PS> New-QADAzureConfigObject -type 'AzureTenant' -name
   'CompanyAzuretenant' -AzureTenantId 'CompanyAzureTenantID' -
   AzureTenantDescription 'Azure tenant for Company' -AzureAdminUserID
   'AzureAdminUser1' -AzureAdminPassword 'AzureAdminPassword1’ -
   AzureADTenantType 'AzureTenantType'
   ```

4. Once the Azure AD tenant is created, disconnect your user:

   ```
   C:\PS> disconnect-qadService
   ```

Add an Azure AD Application

You can use the Active Roles Management Shell to add an Azure AD application to the Azure AD tenant.

To add an Azure AD application

On the Management Shell interface, run the **New-QADConfigObject** cmdlet.

Synopsis

This cmdlet enables you to add an Azure AD application to the Azure AD tenant.

Syntax

```
New-QADAzureConfigObject -type 'AzureApplication' -name 'AzureApplication' -
DisplayName 'ApplicationDisplayName' -AzureTenantId 'AzureTenantGUID' -
AzureAppPermissions 'ApplicationPermission'
```

Description

Use this cmdlet to add an Azure AD application.

Parameters

- type (string)

  Use this parameter to specify the object class of the directory object to be created. This is the name of a schema class object, such as User or Group. The cmdlet creates a directory object of the object class specified by the value of this parameter.

  Table 12: Parameters: type (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- name (string)

  Use this parameter to set the 'name' attribute to this parameter value on the new object created by this cmdlet in the directory.

  Table 13: Parameters: name (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- AzureTenantId (string)

  Use this parameter to enter the Azure AD tenant ID obtained from the default tenant created after subscribing for Microsoft Azure.

  NOTE: The values entered for configuring Azure AD tenant must exactly match the values configured for Azure AD, else Azure AD application creation and management of Azure AD objects fail.

Table 14: Parameters: AzureTenantId (string)

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- Displayname (string)

  Use this parameter to specify the 'displayName' attribute to this parameter value.

Table 15: Parameters: Displayname (string)

Required	false
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- AzureAppPermissions

  Use this parameter to specify the permission scope for applications for Azure AD.

Table 16: Parameters:AzureAppPermissions

Required	true
Position	named
Accepts pipeline input	false
Accepts wildcard characters	false

- AzureApplicationDescription

  Use this parameter to specify the description of the Azure AD application.

Table 17: Parameters: AzureApplicationDescription

Required	false
Position	named
Accepts pipeline input	false

Accepts wildcard characters	false

Example

Connect to any available domain controller with the credentials of the locally logged on user, and create a new Azure AD application:

```
C:\PS> New-QADAzureConfigObject -type 'AzureApplication' -name
'AzureApplication' -DisplayName 'ApplicationDisplayName' -AzureTenantId
'AzureTenantGUID' -AzureAppPermissions 'ApplicationPermission'
```

Example

Connect to the local Administration Service with the credentials of a specific user, create a new Azure AD tenant and then disconnect:

```
C:\PS> $pw = read-host "Enter password" -AsSecureString

C:\PS> connect-qadService -service 'localhost' -proxy -ConnectionAccount
'company\administrator' -ConnectionPassword $pw

C:\PS> New-QADAzureConfigObject -type 'AzureApplication' -name
'AzureApplication' -DisplayName 'ApplicationDisplayName' -AzureTenantId
'AzureTenantGUID' -AzureAppPermissions 'ApplicationPermission'

C:\PS> disconnect-qadService
```

Active Roles Configuration steps to manage Hybrid AD objects

To configure Active Roles to manage Hybrid AD objects, perform the following tasks:

1. Create an Azure AD tenant.
2. Create the Azure AD application.
3. Provide the administrator consent for the Azure AD application.
4. Enforce the **Built-in Policy - Azure - Default Rules to Generate Properties** Policy Object to the on-premises Active Directory containers, which are synchronized to Azure AD.

NOTE:

- After an upgrade the **edsvaAzureOffice365Enabled** is not available for viewing or editing from **Organizational Unit | Advanced Properties** or through the management shell command-let, however the organizational unit container continues to be an Azure enabled container as the azure policy is already applied.

For more information on Azure custom policies, see Changes to Azure O365 Policies in Active Roles after 7.4.1.

Active Roles on Windows Azure VM

This section outlines the recommended steps for deploying Active Roles in the Windows Azure Infrastructure Services environment. After you complete these steps, you have the following services deployed in Windows Azure using Windows Azure virtual machines:

- SQL Server 2012 or later to host the Active Roles database
- Active Roles Administration Service
- Active Roles Web Interface

Step 1. Prerequisites

This guide assumes that you already have the following prerequisites:

- Microsoft account with at least one valid, active Windows Azure subscription
- At least one writable replica domain controller installed in your Windows Azure account

  For instructions on how to install a replica domain controller, see Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks.

Step 2. Deploy Microsoft SQL Server 2012

Perform the following tasks to deploy SQL Server:

1. Create a virtual machine based on a SQL Server 2012 image published in Windows Azure.

   When creating the virtual machine, on the **Virtual machine configuration** page, select the **Create a new cloud service** option and choose the Virtual Network used by your replica domain controller in Windows Azure.

For instructions on how to deploy SQL Server 2012 in Windows Azure, see Provisioning a SQL Server Virtual Machine on Windows Azure.

2. Join the SQL Server 2012 virtual machine to your Active Directory domain.
3. Using SQL Server Management Studio, grant the **sysadmin** fixed server role to the domain user account that will be used as the service account for the Active Roles Administration Service.
4. Configure Windows Firewall to allow connections to TCP Port 1433 from computers in your Virtual Network.

   Because SQL Server will be accessed from within the Virtual Network, you do not need to create public endpoints in Windows Azure.

Step 3. Deploy Active Roles Administration Service

Perform the following tasks to deploy the Active Roles Administration Service:

1. Create a virtual machine based on a Windows Server 2016 image published in Windows Azure.

   When creating the virtual machine, on the **Virtual machine configuration** page, select the Cloud Service that you created for the SQL Server virtual machine in Step 2. Deploy Microsoft SQL Server 2012. This will automatically select the correct Virtual Network as this Cloud Service is already used to host the SQL Server virtual machine. For further information, see Add a Virtual Machine to a Virtual Network, section "Create Virtual Machine and Deploy to Virtual Network."

2. Join the newly created virtual machine to your Active Directory domain.
3. Connect to the virtual machine using Remote Desktop, and run the Active Roles Setup wizard to install the Active Roles Administration Service (see Steps to deploy the Administration Service earlier in this document).

   When prompted for the service account, specify the appropriate user account defined in your Active Directory domain. Ensure that this user account is a member of the Administrators local group on the virtual machine where you are installing the Administration Service. For example, this could be a domain user account that belongs to the Domain Admins group of your Active Directory domain.

   When prompted for SQL Server, specify the name of SQL Server you deployed in Step 2. Deploy Microsoft SQL Server 2012.

4. Run the following Windows PowerShell command on the virtual machine where you have installed the Active Roles Administration Service, to configure Windows Firewall:

```
$allowedClientSubnets = @('10.0.0.0/8', '172.16.0.0/12',
'192.168.0.0/16');
New-NetFirewallRule -DisplayName "Active Roles" -Direction Inbound `
-Action Allow -Service 'aradminsvc' -RemoteAddress
```

```
$allowedClientSubnets `
-Enabled True
```

Step 4. Deploy Active Roles Web Interface

Perform the following tasks to deploy the Active Roles Web Interface:

1. Create a virtual machine based on a Windows Server 2016 image published in Windows Azure.

   When creating the virtual machine, on the **Virtual machine configuration** page, select the Cloud Service that you created for the SQL Server virtual machine in Step 2. Deploy Microsoft SQL Server 2012. This will automatically select the correct Virtual Network as this Cloud Service is already used to host the Active Roles Administration Service and SQL Server virtual machines. For further information, see Add a Virtual Machine to a Virtual Network, section "Create Virtual Machine and Deploy to Virtual Network."

2. Join the newly created virtual machine to your Active Directory domain.
3. Connect to the virtual machine using Remote Desktop, and run the Active Roles Setup wizard to install the Active Roles Web Interface (see Steps to deploy the Web Interface earlier in this document).

   When prompted, choose the option to connect to the Administration Service on the specified computer, and specify the fully qualified domain name of the virtual machine you deployed in Step 3. Deploy Active Roles Administration Service.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product