Active Roles 8.2.1

Upgrade 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 Upgrade Guide
Updated - 28 November 2024, 10:55

For the most recent documents and product information, see Online product documentation.

Contents

Introduction

Active Roles simplifies creating and managing user accounts and groups in Windows Active Directory (AD) environments by automating the following:

- User and group account management in AD and Azure AD.
- Mailbox management in Exchange and Exchange Online.
- Group population, and resource assignment in Windows.

Active Roles enforces security, automates directory management tasks, and provides change approval and a Web Interface.

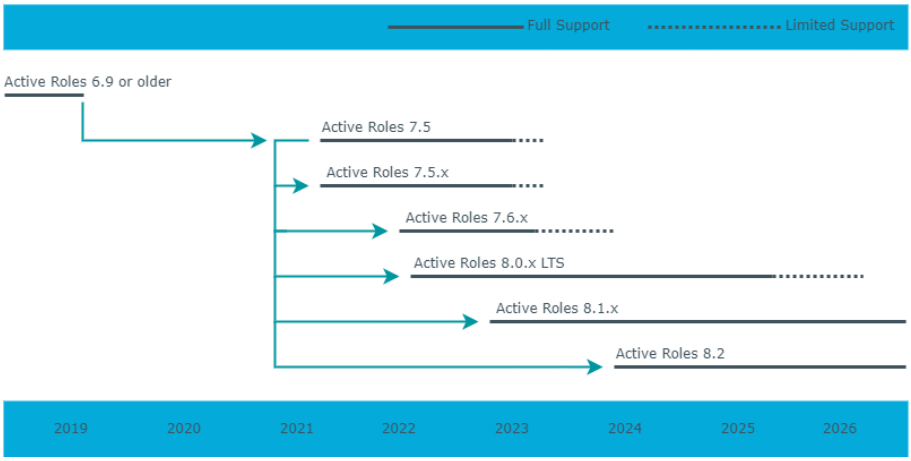
This document describes how to upgrade Active Roles and its components to a newer version.

Upgrading from an earlier version

You can upgrade from Active Roles 7.5 or later to the latest version of Active Roles 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 importing database from earlier version: Install the latest version of Active Roles and import the database from the earlier version of Active Roles.

Figure 1: Supported Active Roles upgrade path



NOTE: Consider the following when upgrading from an earlier version:

- To perform a clean installation of Active Roles, uninstall the currently installed version before installing Active Roles 8.2.1.
- Active Roles supports selecting a custom installation path only during a clean installation. During an in-place upgrade, Active Roles does not support changing the previously set installation path.

For information on importing configuration data from the database of an earlier version of Active Roles, see *Importing configuration data* in the *Active Roles Installation Guide*.

NOTE: Before upgrading to the latest version of Active Roles, you must uninstall the add-ons of the earlier versions using the Add-on Manager.

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:

- Active Roles database users with associated permissions.
- SQL logins mapped to Active Roles 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.

If the SQL access account used for performing the in-place upgrade does not have permission to create a database, then you must manually create the database for Active Roles. In the Configuration Center, during the initial configuration, select **Use a pre-created blank database**. For more information, see Knowledge Base Article 4303098 on the One Identity Support Portal.

By default, **Copy database users, permissions, logins, and roles** is selected, but you can clear it 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**.

CAUTION: Upgrading from Active Roles 6.9 to a newer version is only meant to be a temporary solution, as the side-by-side installation of two different Active Roles versions can have a negative impact on the environment.

Different versions of Active Roles are not supported in the same Active Directory (AD) domain. Different versions of Active Roles servers in the same AD domain will cause issues with dynamic groups, policies, workflows, custom scripts, and conflicts in product functionality.

When upgrading Active Roles to a later version, One Identity recommends to upgrade all servers running Active Roles components to the same version, otherwise the configuration is not supported.

For more information, see Knowledge Base Article 4307177.

Prerequisites of upgrading Active Roles using in-place upgrade

Before upgrading to the latest version of Active Roles, One Identity recommends that you complete the following prerequisite tasks.

Microsoft OLE DB Driver for SQL Server security impacts

IMPORTANT: Starting from version 8.2, Active Roles supports (and its installer is shipped with) Microsoft OLE DB Driver 19.x for SQL Server. However, Active Roles still supports earlier OLE DB Driver versions as well (18.4 or newer).

- If you upgrade to Active Roles 8.2.1 from an earlier version via in-place upgrade, and you want to keep using an earlier version of Microsoft OLE DB Driver (version 18.4 or newer), this change has no impacts on your Active Roles installation.
- If you upgrade to Active Roles 8.2.1 from an earlier version via in-place upgrade, and you want to switch to Microsoft OLE DB Driver 19.x from an earlier OLE DB Driver version due to security concerns, you must perform additional configuration steps. Otherwise, the Active Roles Administration Service might fail to start. For more information, see Configuring Active Roles for a newer Microsoft OLE DB Driver for SQL Server version.

Backing up the Active Roles database

CAUTION: Not backing up the Active Roles database and the existing Web Interface site configurations might result in data loss.

- Back up the Active Roles database. For more information on general best practices, see *Create a Full Database Backup* in the *Microsoft SQL documentation*.
- Back up the current Web Interface site configurations.

  Any Web Interface sites that were created in Active Roles 7.5 or later versions will continue to function in 8.2.1. However, One Identity recommends to thoroughly test before upgrading, as some customizations will not work in newer versions of Active Roles.

  To back up the Web Interface site configurations

  1. Open the Active Roles Configuration Center.
  2. Click **Web Interface**.
  3. Select the site(s) to back up and click **Export Configuration**.
- Verify that your SQL Server has SSL configured and the necessary trusted certificate set.
- Approve all pending approval activities.
- Uninstall the add-ons of the earlier versions in the Add-on Manager or the Active Roles Console.
- Remove replication partners, if there are any. For more information, see *Removing Subscribers from a replication group* in the *Active Roles Administration Guide*.
- Make sure you have enough disk space in SQL Server. For more information, see Disk space requirements in the *Microsoft SQL Server documentation*.

Impact on custom solutions

Custom solutions, such as scripts that rely on Active Roles functions or the Console might stop working after upgrading Active Roles.

CAUTION: Before upgrading Active Roles, test the existing custom solutions with the new Active Roles version in a lab environment to verify that they continue to work.

Impact on the Office 365 add-on

The latest version of Active Roles manages Microsoft 365 and Azure AD natively, therefore the Office 365 add-on is no longer supported and it will stop working after upgrading Active Roles. Before upgrading Active Roles, One Identity recommends uninstalling the Office 365 add-on.

NOTE: Active Roles does not support managing and selecting Microsoft 365 domains through policies, which the Office 365 add-on supported.

After completing the prerequisite tasks, to upgrade Active Roles, perform the steps in Upgrading to Active Roles 8.2.1 using in-place upgrade.

Upgrading to Active Roles 8.2.1 using in-place upgrade

Using in-place upgrade, you can install the latest version of Active Roles on the computer without removing the earlier version.

NOTE: The in-place upgrade of Active Roles automatically upgrades the following Active Roles components to the latest version:

- Administration Service
- Console (MMC Interface)
- Web Interface
- Management Tools: ADSI Provider, Management Shell, SDK
- Synchronization Service

The in-place upgrade of Active Roles does not upgrade the following Active Roles tools:

- Add-in for Outlook
- Add-on Manager
- Administrative Template
- Collector and Report Pack
- Configuration Transfer Wizard
- Diagnostic Tools

- Management Pack for SCOM
- SPML Provider
- Synchronization Service Capture Agent

To upgrade the tools installed with Active Roles, use the respective installers available in the Active Roles ISO.

Before upgrading, make sure you perform the prerequisite tasks. For more information, see Prerequisites of upgrading Active Roles using in-place upgrade.

To upgrade the existing Active Roles 7.5 or later version to the latest version, perform the following steps.

To upgrade Active Roles using in-place upgrade

1. Log in with a user account that has administrator rights on the computer.
2. Navigate to the location of the Active Roles ISO, and to start the Setup wizard, double-click `ActiveRoles.exe`.
3. Follow the instructions in the Setup wizard.
    a. Select the check box and click **Next**.
    b. Select **I accept the terms in the license agreement**, and click **Next**.
    c. Review the summary and warning, and click **Next**.
    d. Make sure that the prerequisite software are installed, then click **Upgrade**.

    NOTE: If your organization enforces the AllSigned policy, install the One Identity Certificate.

    e. Click **Finish**.
4. After upgrading to Active Roles, you are prompted to restart the system. Click **Restart Now**.
5. After the system restarts and the Configuration Center opens automatically, click **Update Service Instance**.

    Due to the update of the database schema, the 7.5 or later versions of the Web Interface sites are no longer compatible. For more information, see Upgrading the Active Roles Web Interface.

After upgrading the Active Roles package to 8.2.1, perform the steps of Configuring Active Roles 8.2.1 during in-place upgrade.

Configuring Active Roles 8.2.1 during in-place upgrade

After upgrading Active Roles to 8.2.1 and restarting the operating system, the Configuration Center opens automatically. Use the Upgrade configuration wizard to configure Active Roles.

NOTE: If the Active Roles Configuration Center does not open automatically, open it from the Windows **Start** menu.

To configure Active Roles 8.2.1 during in-place upgrade

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

   NOTE: During Active Roles upgrade, if the Active Roles database is not split into Configuration and Management History databases, the upgrade process creates a Management History database by default.

   NOTE: The names of the new databases must be unique. If a database with the same name already exists, you will get a `Verification failed` error message. To resolve the issue, rename the new database.

   IMPORTANT: Active Roles does not support pre-creating databases for in-place upgrade. If you pre-create the new Active Roles databases, then perform an in-place upgrade with those pre-created databases, the initial configuration will fail with a `Process instantly failed with the message Invalid object name 'Settings'` error message.

   CAUTION: When creating a new configuration database, you might encounter a `Verification failed` error message due to an Active Roles version mismatch. To resolve the issue, you must clear the existing Active Roles configuration. For more information, see Knowledge Base Article 4340880.

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

   b. Select the check box to confirm that you have read the instructions in this document about the in-place upgrade process, and click **Next**.

2. The **Reauthenticate Tenants** page lists the configured Azure tenants in the source database. To reauthenticate a tenant, click **Reauthenticate** next to its name.

   CAUTION: You must reauthenticate the tenant(s). Otherwise, Active Roles does not receive the required permissions to manage existing tenants, and tenant administration will not work correctly.

   NOTE: After a successful upgrade, in the Configuration Center, under **Azure AD Configuration**, you must consent the Azure tenants manually.

3. Click **Next**.

4. In the **Services association** page, configure the Administration Service instances for running the following:

   - Dynamic groups
   - Group families
   - Scheduled tasks

a. Select **This server** or **Other**. Selecting **Other** allows you to specify another Administration Service instance in a fully qualified domain name (FQDN) format. If the value is empty, 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**.

b. Select **Run Services association immediately** or **Schedule Services association**.

   NOTE: If Services association is scheduled to a specific time, but the upgrade or import operation is still in progress or completes after the scheduled Services association time, then the services will not be associated. In such cases, you must associate the Services manually by running the template workflow **Update Services To Execute On** available in the built-in workflow container.

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 initiating server for the listed tasks. This configuration runs after an upgrade.

NOTE: Alternatively, you can perform Services association any time using the template workflow **Update Services To Execute On** available in the built-in workflow container. You can configure the parameters in the script that the workflow uses to the required Administration Service instances, such as, **Dynamic Group Service**, **Group Family Service**, **Scheduled Task Service**. You can select the Administration Service instance to use from the drop-down list. The drop-down list displays all the currently running Administration Service instances connected to the current configuration database. If the parameter value is not selected, then the current Administration Service instance will be used.

5. Click **Next**.
6. In the **Review upgrade** page, review your settings and click **Upgrade**.
7. (Optional) 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. For more information on the errors, click **View log** or navigate to `C:\ProgramData\One Identity\Active Roles\Logs\Configuration Center`.
8. Click **Finish**.

NOTE: Multiple Active Roles Service instances must be upgraded one by one.

Configuring Active Roles for a newer Microsoft OLE DB Driver for SQL Server version

Starting from version 8.2, Active Roles supports (and its installer is shipped with) Microsoft OLE DB Driver 19.x for SQL Server. However, Active Roles still supports earlier OLE DB Driver versions as well (18.4 or newer).

If you have previously used an earlier supported version of Microsoft OLE DB Driver for SQL Server (18.4 or newer) with Active Roles, but you want to upgrade to 19.x due to security reasons, then perform the following steps after completing the in-place upgrade of Active Roles as described in Upgrading to Active Roles 8.2.1 using in-place upgrade.

IMPORTANT: Not completing these steps after performing the in-place upgrade might result in the Active Roles Administration Service not starting when using Microsoft OLE DB Driver 19.x for SQL Server.

To upgrade your Active Roles environment to be compatible with Microsoft OLE DB Driver 19.x for SQL Server

1. Stop the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, navigate to **Administration Service**, then click **Stop**.
2. To use SSL with your SQL Server, configure a valid certificate. For more information on installing or viewing certificates for SQL Server via SQL Server Configuration Manager, see Certificate management in the *Microsoft SQL Server documentation*.

   For general information about the encryption and certificate requirements of Microsoft OLE DB Driver 19.x, see Encryption and certificate validation in OLE DB and Certificate requirements for SQL Server in the *Microsoft SQL Server documentation*.

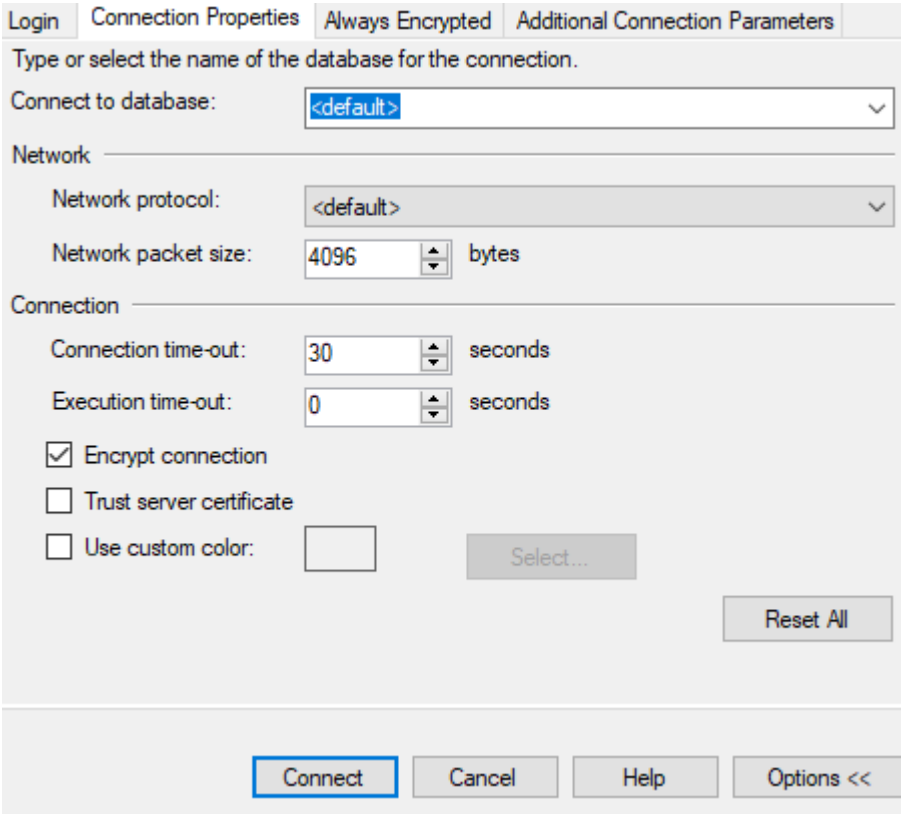
   When configuring the SSL connection, consider the following:

   - Microsoft OLE DB Driver 19.x for SQL Server requires a certificate from a Certificate Authority and no longer accepts self-signed certificates. For more information on how to access a Certificate Authority, see Certification Authority Guidance in the *Microsoft Windows Server documentation*.
   - The Service Account running the SQL Server service must have permission to view the private key from the server certificate. For more information, see Configure SQL Server Database Engine for encrypting connections in the *Microsoft SQL Server documentation*.
   - Microsoft OLE DB Driver 19.x for SQL Server requires specifying the Service Principal Names (SPNs). For more information, see the following *Microsoft SQL Server documentation* resources:
     - Service Principal Name (SPN) Support in Client Connections
     - Service Principal Names (SPNs) in Client Connections (OLE DB)

- Service Principal Names (SPNs) in Client Connections (OLE DB) in SQL Server Native Client
- You might need to change your SQL connection string to match the certificate and the SPN. For more information, see Using Connection String Keywords with OLE DB Driver for SQL Server in the *Microsoft SQL Server documentation*.

3. To commit your SSL configuration changes, restart the SQL service/instance.
4. In SQL Server Management Studio, under the **Connection Properties** tab, make sure that **Encrypt connection** is selected and **Trust server certificate** is cleared.

Figure 2: Checking the correct SSL settings in SQL Server Management Studio



5. In the **Server name** field, make sure that you specify the SQL Server by using its FQDN instead of its short name.
6. Test your connection in SQL Server Management Studio. If it connects to your database instance, then SSL is configured correctly.
7. Change your existing database names in Active Roles so that they use their FQDN instead of their short names. To do so:
   a. In the Active Roles Configuration Center, navigate to **Administration Service** > **Active Roles databases** > **Change**.

b. In the **Change Active Roles Database** wizard, in the **Configuration Database Options** step, select **Existing Active Roles database**, then click **Next**.

c. In the **Connection to Configuration Database** step, in the **Database name** field, change the short name of the server to its FQDN. To continue, click **Next**.

d. In the **Management History Database Options** step, select **Existing Active Roles database**, then click **Next**.

e. In the **Connection to Management History Database** step, in the **Database name** field, change the short name of the server to its FQDN. To continue, click **Next**.

f. In the **Ready to Change** step, to apply your changes, click **Change**.

8. Start the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, navigate to **Administration Service**, then click **Start**.

Upgrading the Active Roles Administration Service

Upgrading the Administration Service implies creating 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.

The new Administration Service is only compatible with the Active Roles 8.2.1 components. Earlier versions of the components might not work with the new Administration Service. Before upgrading the other components, upgrade the Administration Service first.

CAUTION: If you no longer need the earlier version of an Active Roles component and want to uninstall it using the `appwiz.cpl` command, make sure that you uninstall the earlier version (for example, Active Roles 6.9). In the uninstaller, select Modify, and select the components you want to uninstall.

Identifying the database to import configuration

After configuring the Administration Service of the new version, import the configuration data from the database used by the earlier version of your Administration Service. To import configurations, you must identify that database.

To identify the database

1. Open the Active Roles Console and connect to the older-version instance of the Administration Service (see *Connecting to the Administration Service* in the *Active Roles Administration Guide*).
2. Select the **Console tree** root, and 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>`. You can also find this information in the **Administration Service** pane of the Configuration Center.

NOTE: When an import configuration is performed from Active Roles version 7.5 to 8.2.1, the Web Interface does not get upgraded. However, the Configuration Center or any client reports the Active Roles Web Interface version incorrectly as 8.2.1. To upgrade the Web Interface to the latest version, see Creating Web Interface sites and importing configuration.

Importing configuration data

When deploying the Administration Service, you might need to import configuration data from an existing database 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 the following:

- 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.

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:

- Active Roles database users with associated permissions.
- SQL logins mapped to Active Roles 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.

If the SQL access account used for performing the in-place upgrade does not have permission to create a database, then you must manually create the database for Active Roles. In the Configuration Center, during the initial configuration, select **Use a pre-created blank database**. For more information, see Knowledge Base Article 4303098 on the One Identity Support Portal.

By default, **Copy database users, permissions, logins, and roles** is selected, but you can clear it 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**.

If you want to create a new database for the imported configuration data during the configuration of the Administration Service instance, perform the following procedure. After the initial configuration of the Administration Service instance, you can use the Active Roles Configuration Center to import the configuration data to the newly-created database.

To import configuration data to a new database

1. From the Windows **Start** menu, open the Active RolesConfiguration Center.
2. To open the Import configuration wizard, navigate to **Administration Service** <, **Import configuration**.
3. On the **Source database** page, specify the database from which you want to import the configuration data, and click **Next**.
    a. Select the required **Database type**.
    b. In **Database Server name**, enter the database instance that hosts the source database in the format `<Computer>\<Instance>` (for named instances) or `<Computer>` (for default instances). In these formats, `<Computer>` stands for the FQDN of the computer running SQL Server or the name of the Azure SQL database server.
    c. In **Database name**, enter the name of the source database.
    d. 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.

4. The **Destination database** page identifies the database of the Administration Service instance to which you will import data. Under **Connect using**, select the appropriate authentication option, and click **Next**.
    - 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. The **Add-on advisor** page lists the add-ons installed for the previous version of Active Roles. Uninstall the add-ons and click **Next**.

    NOTE: Before you continue importing the configuration data, uninstall the add-ons manually from the earlier version using the Active Roles Add-on Manager, and also uninstall them from the system, if applicable.
6. On the **Import of Encrypted Data** page, select one of the following options:
    - If you have a backup of the secret key for the source database, click **Use a backup of encryption key to import encrypted data**.
        - To specify the backup file, click **Browse**.
        - If the backup file is password-protected, in the **Password** field, enter the password.
    - If you do not 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 password for managed domain registrations) will not be available in the destination database. Because of this, you will need to re-enter the override account password later in the managed domain registrations with the Administration Service instance that uses the destination database.

    For more information, see *Backing up the encryption* key in the *Active Roles Installation Guide*.
7. The **Reauthenticate Tenants** page lists the configured Azure tenants in the source database. To reauthenticate a tenant, click **Reauthenticate** next to its name.

    CAUTION: You must reauthenticate the tenant(s). Otherwise, Active Roles does not receive the required permissions to manage existing tenants, and tenant administration will not work correctly.

    NOTE: After a successful upgrade, in the Configuration Center, under **Azure AD Configuration**, you must consent the Azure tenants manually.
8. In the **Services association** page, configure the Administration Service instances for running the following:
    - Dynamic groups
    - Group families

- Scheduled tasks

a. Select **This server** or **Other**. Selecting **Other** allows you to specify another Administration Service instance in a fully qualified domain name (FQDN) format. If the value is empty, 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**.

b. Select **Run Services association immediately** or **Schedule Services association**.

   NOTE: If Services association is scheduled to a specific time, but the upgrade or import operation is still in progress or completes after the scheduled Services association time, then the services will not be associated. In such cases, you must associate the Services manually by running the template workflow **Update Services To Execute On** available in the built-in workflow container.

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 initiating server for the listed tasks. This configuration runs after an upgrade.

NOTE: Alternatively, you can perform Services association any time using the template workflow **Update Services To Execute On** available in the built-in workflow container. You can configure the parameters in the script that the workflow uses to the required Administration Service instances, such as, **Dynamic Group Service**, **Group Family Service**, **Scheduled Task Service**. You can select the Administration Service instance to use from the drop-down list. The drop-down list displays all the currently running Administration Service instances connected to the current configuration database. If the parameter value is not selected, then the current Administration Service instance will be used.

9. In the **Summary** page, review your settings, then click **Next**.
10. Follow the instructions in the wizard to complete the import operation.

During the import operation, the wizard retrieves and upgrades the data from the source database, and replaces the data in the destination database with the upgraded data from the source database.

NOTE: Depending on the infrastructure, the import operation may take several minutes to complete.

Identifying the database to import Management History

After you imported the configuration of your earlier Active Roles version, import the Management History data from the database used by your Administration Service of the earlier version. To import Management History data, you must identify that database.

To identify the database

1. Open the Active Roles Console and connect to the older-version instance of the Administration Service (see *Connecting to the Administration Service* in the *Active Roles Administration Guide*).
2. Select the **Console tree** root, and 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>. You can also find this information in the **Administration Service** pane of the Configuration Center.

After identifying the database, import Management History using the Import Management History wizard of the Configuration Center. For more information, see *Importing data to the new Management History database* in the *Active Roles Administration Guide*.

Importing Management History data

After configuring the Administration Service, the Management History data storage will be empty with the option to create a new database. During the import of configuration data, the 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 to reduce the time it takes to upgrade the configuration of the Administration Service.

The Management History data describes changes that were made to directory data via Active Roles. This includes information about directory data management tasks, such as:

- The changes a user performed.
- The users performing the changes.
- The time the change was performed.

The Management History data is used for change history and user activity reports. In addition, the Management History data storage holds information about various tasks related to approval workflows and temporal group memberships.

After configuring the Administration Service and importing configuration data from an existing database, you must take additional steps to transfer the Management History data. You can do this using the **Import Management History** wizard in the Active Roles Configuration Center.

You can populate the newly-created Management History database with your existing Management History data. This ensures that the data is available in the Active Roles user interfaces after configuring the Administration Service to use the new Management History database. You can import existing Management History data with the Active Roles Configuration Center on the computer running the Administration Service instance.

IMPORTANT: The reports created by the **Change History** or **User Activity** commands (available both in the Active Roles Web Interface and the Active Roles Console components) only include information about the changes that were made using a specific Administration Service group. This group must share a common database from the connected Management History database. If the change history data is not imported from the previously available database, the data will not be included in the new database.

To import Management History data

1. From the Windows **Start** menu, open the Active RolesConfiguration Center.
2. In the Configuration Center main window, under **Administration Service**, click **Manage Settings**.
3. To open the Import Management History wizard, on the **Administration Service** page, click **Import Management History**.
4. On the **Source database** page, select the source database:
    a. **Database Type**: Select the required database type from the drop-down:
        - **On-premises**
        - **Azure SQL database**
    b. **Database Server name**: Enter the name of the database instance that hosts the source database.
    c. **Database name**: Enter the name of the source database.
5. Under **Connect using** , select the authentication option:
    - If your Windows login account has sufficient rights to write data to the destination database, click **Windows authentication**.
    - If you have an SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.
    - If you selected Azure SQL as the database type and you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.
6. (Optional) Copy SQL Server users and login data after importing Management History data. This option is enabled by default, if you selected the **On-premises** database type.

    NOTE: Due to limitations in Azure SQL, Active Roles cannot synchronize SQL Server logins to Azure SQL databases.

    To synchronize SQL Server users to Azure SQL, One Identity recommends using system-provided Microsoft tools, such as Azure Data Studio or Azure Database Migration Service (DMS) Classic.

    For more information on migrating Microsoft SQL Server users to Azure SQL, see the following Microsoft documentation resources:

- To use Azure Data Studio for migrating SQL Server logins to an Azure SQL database, see *Tutorial: Migrate SQL Server logins (preview) to Azure SQL in Azure Data Studio*.
- To use Azure DMS Classic for migrating SQL Server logins to an Azure SQL Managed Instance, see *Tutorial: Migrate SQL Server to an Azure SQL Managed Instance offline using DMS (classic)*.
- For a comparison of Azure SQL Database and Azure SQL Managed Instance, see *Features comparison: Azure SQL Database and Azure SQL Managed Instance*.
- To resolve connectivity issues with Azure SQL Database and Azure SQL Managed Instance, see *Troubleshooting connectivity issues and other errors with Azure SQL Database and Azure SQL Managed Instance*.

To skip the synchronization of users and login data:

a. Click **Configure advanced database properties**.

b. Clear the **Copy database users, permissions, logins and roles** check box.

c. Click **Apply**.

7. Click **Next**.

   On the **Destination database** page, specify the database of the Administration Service instance to which you are importing data, and select the authentication option.

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

9. Click **Next**.

   On the **Records to import** page, to import all data records, select **All records**. To import only data records from a specific time interval, select **Records in the following date range**, then specify a date range.

   NOTE: Consider the following when selecting whether to import all data records or only records from a specific date range:
   - If you select to import all data records, or specify a date range which also includes the current day, then the Management History wizard will create a timestamp for the current day to ensure that all data records created up to the point of starting the migration will be imported. This means that the wizard will import all data that existed in the source database at the time the migration started, but will not import any data records that have been

created after starting the migration.

- If you select a date range manually, you cannot select future dates.
- Data for unfinished temporal group memberships are imported only if you import Management History data for a selected date range.

10. Click **Next**.

    On the **Ready to import** page, review your settings. If needed, return to the previous pages and make adjustments.

11. To start the import process once your changes are finalized, click **Import**.

    On the **Run** page, you can see the progress of the import process. After the operation finished, the wizard shows a summary and a link that you can use to check the import log.

    NOTE: During the import process, consider the following:

    - You can cancel the import process at any time. However, the wizard will not stop the import immediately, but only after it finishes the currently performed step of the operation. Active Roles will not delete the data that the wizard has successfully imported to the destination database before canceling the operation.
    - If an SQL exception occurs during migration, the operation will not be canceled. Instead, the wizard will restart the migration of that specific batch of data. The retry policy ensures that, unless there is a persistent network or database error, you do not need to restart the import process manually.

      If the SQL exception is network-related or transient, the wizard will retry the migration of the failed batch up to 3 times. If the SQL exception occurs for other reasons, the wizard will only retry the migration once.

      Depending on the severity of the exception, one of the following events can occur:

      - If the error is resolved and the migration of the failed batch is successful, then the wizard proceeds with importing the remaining data.
      - If the error is not resolved after the maximum number of retries, the wizard cannot proceed with the migration and cancels the process. You can restart the migration manually, but if the issue persists, check the log for details and contact your network administrator or database administrator.

12. To check the detailed log of the import operation, click **View log**. To exit the wizard, click **Finish**.

NOTE: The **Import Management History** wizard only adds new data, keeping intact any data that already exists in the destination database. You can import your legacy Management History data at any time after you have configured the Administration Service, without the risk of losing any data.

Upgrading in case of shared database

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

To upgrade multiple Administration Service instances with a shared database

1. Upgrade one of the Administration Service instances as described in *Configuring the initial Administration Service* in the *Active Roles Installation Guide*.
2. Now that you have the database of the new version, upgrade the remaining instances of the Administration Service one by one.
3. In the Configure Administration Service wizard, on the **Configuration Database Options** page, select **Existing Active Roles database**.
4. On the **Connection to Database** page, specify the database created during the upgrade of the first Administration Service instance. You do not need to import configuration as the database already has that data imported.
5. On the **Management History Database Options** page, select **Existing Active Roles database**.
6. On the **Connection to Database** page, specify the database created during upgrade of the first Administration Service instance. You do not need to import the management history as the database already has that data imported.

Reconfiguring Azure tenants during upgrade configuration

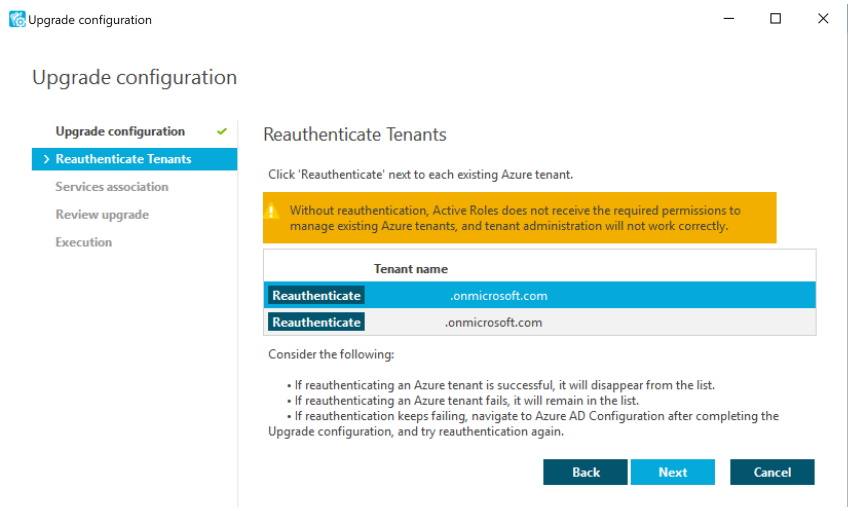
If your organization has any Azure tenants managed in Active Roles, you must reauthenticate and reconsent each Azure tenant after installing a new version of Active Roles.

CAUTION: You might experience difficulties with Exchange Online connectivity and managing resources (for example, assigning roles).

To reauthenticate and reconsent Azure tenants after installing Active Roles

1. After installing Active Roles, from the Windows **Start** menu, open the Active Roles Configuration Center. 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.

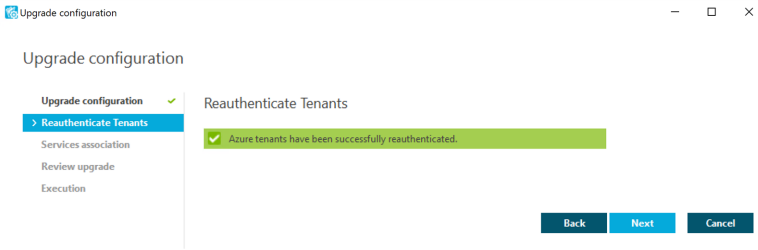
Figure 3: Reauthenticating Azure tenants



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.

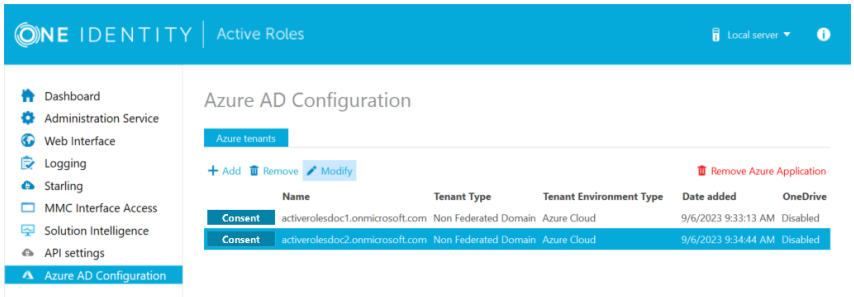
  Figure 4: Confirmation message after successfully reauthenticating tenants

- 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.

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. After the Configuration Center restarted successfully, navigate to **Azure AD Configuration**.

Figure 5: 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.

Upgrading the Active Roles Web Interface

You can upgrade the Active Roles Web Interface of version 7.5 or later to version 8.2.1.

Upgrading the Web Interface implies creating 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.

NOTE: When an import configuration is performed from Active Roles version 7.5 to 8.2.1, the Web Interface does not get upgraded. However, the Configuration Center or any client reports the Active Roles Web Interface version incorrectly as 8.2.1. To upgrade the Web Interface to the latest version, see Creating Web Interface sites and importing configuration.

Identifying configuration objects

To create Web Interface sites of the new Active Roles version, you must know which configuration objects your Web Interface sites of the earlier version use. Each site stores its configuration on the Administration Service, in a *site configuration object*. Upgrading 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, specify the name of the corresponding site configuration object of the earlier version. Active Roles creates a site configuration object of the new version, imports

the site configuration data to that object, and the new Web Interface site will use that object, inheriting the configuration of the Web Interface site of the earlier version.

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

1. From the Windows **Start** menu, open the Active Roles Configuration Center on the computer running the Administration Service instance on which you want to identify the Web Interface sites.
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 Website: The name of the website 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.

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, from the Start menu, open the Web Interface Sites Configuration wizard.
2. On the **Web Interface Configuration** page, which lists your Web Interface sites of the earlier Active Roles version, click on the site you need, and then click **Edit**.

   You can identify sites by alias, shown in the **Virtual Directory** column. The alias defines the virtual path used in the address of the Web Interface site on the Web server.
3. In the opening dialog, in the **Configuration settings** area, under **Use existing configuration**, in **Name**, the name of the site's configuration object is displayed (including the version number). Note down the name.
4. Click **Cancel** to close the dialog.

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.

You can also use the **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 *Web Interface management tasks* in the *Active Roles Administration Guide*.

Creating Web Interface sites and importing configuration

To create a new Web Interface instance of the latest version, perform the following steps.

To create a new Web Interface instance

1. For each Web Interface site of your earlier Active Roles version, create sites based on the configuration objects that your older Web Interface version used. For more information, see Identifying configuration objects.
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. For more information, see *Configuring the initial Administration Service* in the *Active Roles Installation Guide*.
3. On the new Web Interface instance that you installed and configured, create sites based on information you noted previously, 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. For more information, see Identifying the database to import configuration.
4. (Optional) Delete the default sites that were created when you configured the Web Interface in Step 2 if you no longer need to use or customize them. For more information, see Deleting default Web Interface sites.

   NOTE: The default sites have the default configuration of menus, commands, forms and other elements instead of any existing site customizations.

CAUTION: If you no longer need the earlier version of an Active Roles component and want to uninstall it using the `appwiz.cpl` command, make sure that you uninstall the earlier version (for example, Active Roles 6.9). In the uninstaller, select Modify, and select the components you want to uninstall.

Creating 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 Identifying configuration objects). 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. From the Windows **Start** menu, open the Active RolesConfiguration Center.
2. In the Configuration Center main window, under **Web Interface**, click **Manage Sites**.
3. On the **Sites** page, click **Create** to open the Web Interface Site.
4. On the **Web Application** page, 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 Identifying configuration objects).
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.

Deleting default Web Interface sites

After you created the Web Interface sites of the new version that inherit the configuration of your Web Interface sites of the earlier version, you can delete the default Web Interface sites that were created by the initial configuration of the Web Interface. For more information, see *Initial configuration of the Web Interface* in the *Active Roles Installation Guide*.

To delete the default Web Interface sites

1. From the Windows **Start** menu, open the Active RolesConfiguration Center.
2. In the Configuration Center main window, under **Web Interface**, click **Manage Sites**.
3. On the **Sites** page, select the default Web Interface sites one by one and click **Delete**.

   You can identify the default Web Interface sites by the name in the **Configuration** column:

   - **Site for Administrators (8.2.1)** indicates the default site for administrators.
   - **Site for HelpDesk (8.2.1)** indicates the default site for helpdesk.
   - **Site for Self-Administration (8.2.1)** indicates the default site for self-administration.

Upgrading the Active Roles Synchronization Service

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

You can transfer sync workflows from the following Quick Connect or Active Roles Synchronization Service versions:

- Quick Connect for Active Directory 6.1
- Quick Connect for AS400 1.4
- Quick Connect for Base Systems 2.4
- Quick Connect for Cloud Services 3.7
- Quick Connect for RACF 1.3
- Quick Connect Sync Engine 5.5 and 6.1
- Synchronization Service 7.5 and later

For more information, see *Transferring sync workflows from Quick Connect* in the *Active Roles Synchronization Service Administration Guide*.

Upgrading other components

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

- Management Shell
- ADSI Provider
- SDK
- Collector and Report Pack

Upgrading the Management Shell, ADSI Provider and SDK

The Active Roles Management Shell, ADSI Provider and SDK of version 8.2.1 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 Installing only the Management Shell, ADSI Provider and SDK in the *Active Roles Installation Guide*).

To upgrade from Active Roles Management Shell, ADSI Provider and SDK 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.

CAUTION: If you no longer need the earlier version of an Active Roles component and want to uninstall it using the `appwiz.cpl` command, make sure that you uninstall the earlier version (for example, Active Roles 6.9). In the uninstaller, select Modify, and select the components you want to uninstall.

NOTE: 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 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 Console, and is removed once you have uninstalled the core components.

Upgrading the Collector and Report Pack

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

1. Collector and Report Pack
2. Collector's database

Collector

To upgrade, first uninstall your earlier version of Collector and then install the new version. To uninstall Collector, use the **Programs and Features** list of the Windows Control Panel.

After you uninstalled your earlier version of Collector, install the new version. For more information, see *Installing the Data Collector* in the *Active Roles Installation Guide*.

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 the Control Panel.

After you uninstalled your earlier version of the Report Pack, install the new version. For more information, see *Deploying the Report Pack* in the *Active Roles Installation Guide*.

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 must import the events to the database of the new Collector version, then specify the database of the new Collector version as the data source for the reports of the new Report Pack version. For more information on how to configure the data source, see *Working with reports* in the *Active Roles Administration Service*.

To import events from the database of an earlier Collector version

1. To start the Collector wizard, in the Start menu, select **Active Roles8.2.1 Collector and Report Pack**.
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**, enter the database type, SQL Server name, and database name that your Collector of an earlier version uses, and click **Next**.
4. On the **Target Database** page, click **Specify**, enter the database type, SQL Server name, and database name that your Collector of the current version uses, and click **Next**.
5. Wait for the wizard to finish the import.

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