Active Roles 8.0.1 LTS

Feature 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 RolesFeature Guide
Updated - 13 April 2023, 17:49

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

Contents

1

Introduction

This document provides a detailed description of each major feature available in Active Roles 8.0.1 LTS.

The document describes each feature in a separate section containing the following information:

- **Feature name**: The name of the feature, indicated in the section title.
- **Description**: A detailed description of the feature.
- **Getting started**: Information on how to start using the feature. In most cases, this includes references to other Active Roles documents, such as the Administration Guide or the available User Guides, depending on the target users of the feature.

  NOTE: Consider the following regarding the **Getting started** information:

  - Unless indicated otherwise, using the described Active Roles features requires an Active Roles Admin account. By default, an Active Roles Admin is any member of the Administrators local group on the computer running the Active Roles Administration Service.
  - When attempting to use features of the Active Roles Console, make sure that the Console interface is set to "Advanced view mode". To do so, in the **View** menu, click **Mode** > **Advanced Mode**.

Administrative rules and roles

The following sections provide an overview of the Active Roles features related to:

- Workflow capabilities.
- Policies (that is, administrative rules).
- Delegation model (that is, administrative roles).

Active Roles Synchronization Service

Identity information can be stored in various data systems, such as directories, databases, or even formatted text files. However, managing and synchronizing such identity information among several different data systems have several challenges:

- The synchronization process can require considerable time and effort.
- Performing data synchronization tasks manually is error-prone and can lead to duplicate information or incompatible data formats.

Active Roles Synchronization Service helps you avoid these problems by automating the process of identity data synchronization among various data systems used in your enterprise environment.

Synchronization Service increases the efficiency of identity data management by allowing you to automate the creation, deprovisioning, and update operations between the data systems you use. For example, when an employee joins or leaves the organization, the identity information managed by Synchronization Service is automatically updated in the managed data systems, reducing administrative workload and getting the new users up and running faster.

Synchronization Service also supports scripting capabilities, providing a flexible way to automate administrative tasks and integrate the administration of managed data systems with other business processes. By automating conventional tasks, Synchronization Service helps your organization to concentrate on strategic issues, such as planning the directory, increasing enterprise security, and supporting business-critical applications.

For more information on the main features of Synchronization Service, see the following sections.

Getting started

For more information on how to install, configure and use Synchronization Service, see the *Active Roles Synchronization Service Administration Guide*.

Bidirectional synchronization

Bidirectional synchronization allows you to synchronize all changes to identity information between your data systems. Using this feature, you can prevent potential identity information conflicts between different data sources.

NOTE: This feature is only supported by certain data systems. For more information, see the relevant data connector documentation in the *Active Roles Synchronization Service Administration Guide*.

Delta processing

Delta processing allows you to synchronize identities faster by processing only data that has changed in the source and target connected systems since the last synchronization run.

By offering both full synchronization or quick delta processing methods between two data systems, Synchronization Service provides you the flexibility of choosing the appropriate method for your synchronization tasks.

NOTE: This feature is only supported by certain data systems. For more information, see the relevant data connector documentation in the *Active Roles Synchronization Service Administration Guide*.

Group membership synchronization

Synchronization Service ensures that group membership information is synchronized across all connected data systems. For example, when creating a group object from an Active Directory (AD) domain to an AD LDS (ADAM) instance, you can configure rules to synchronize the **Member** attribute from the AD domain to the AD LDS (ADAM) instance.

Windows PowerShell scripting

Synchronization Service supports Windows PowerShell-based scripting for data synchronization. The shell is implemented as a Windows PowerShell module, allowing you to automate synchronization tasks via PowerShell scripts.

For more information and examples, see the following sections of the *Active Roles Synchronization Service Administration Guide*:

- *Developing PowerShell scripts for attribute synchronization rules*
- *Using PowerShell script to transform passwords*

Attribute synchronization rules

Synchronization Service allows you to create and configure synchronization rules to generate values for target object attributes. These rules support three synchronization types:

- **Direct synchronization**: Assigns the value of a source object attribute to the target object attribute you specify.
- **Script-based synchronization**: Uses your custom Windows PowerShell script to generate the target object attribute value.
- **Rule-based synchronization**: Uses your custom synchronization rules to generate the target object attribute value you want.

Rule-based generation of Distinguished Names

Synchronization Service provides flexible rules for generating the Distinguished Names (DNs) for the created objects. These DN generation rules allow you to ensure that the created objects are named in full compliance with the naming conventions existing in your organization.

Synchronization scheduling

To meet your organizational policies and save both time and effort, you can schedule and automate the configured data synchronization tasks with Synchronization Service.

Extensive data system support

To access external data systems, Synchronization Service uses so-called "connectors", enabling Synchronization Service to read and synchronize identity data from the specific data systems.

Active Roles Synchronization Service can connect to the following data systems:

- Data sources accessible via an OLE DB provider.
- Delimited text files.

- IBM AS/400, IBM Db2, and IBM RACF systems.
- LDAP directory service.
- Micro Focus NetIQ Directory systems.
- The following Microsoft services and resources:
    - Active Directory Domain Services (AD DS) with the domain or forest functional level of Windows Server 2016 or higher.
    - Active Directory Lightweight Directory Services (AD LDS) running on any Windows Server operating system supported by Microsoft.
    - Azure Active Directory (Azure AD) using Microsoft Graph API version 1.0.
    - Exchange Online services.
    - Exchange Server with the following versions:
        - Microsoft Exchange Server 2019
        - Microsoft Exchange Server 2016

      NOTE: Microsoft Exchange 2013 and 2013 CU11 are no longer supported. For more information, refer to Knowledge Base Article 202695.
    - Lync Server version 2013 with limited support.
    - SharePoint 2019, 2016, or 2013.
    - SharePoint Online service.
    - Skype for Business 2019, 2016 or 2015.
    - Skype for Business Online service.
    - SQL Server, any version supported by Microsoft.
- One Identity Active Roles version 7.4.3, 7.4.1, 7.3, 7.2, 7.1, 7.0, and 6.9.
- One Identity Manager version 8.0 and 7.0 (D1IM 7.0).
- OpenLDAP directory service.
- Oracle Database, Oracle Database User Accounts, and Oracle Unified Directory data systems.
- MySQL databases.
- Salesforce systems.
- SCIM-based data systems.
- ServiceNow systems.

For more information on using these connectors, see *External data systems supported with built-in connectors* in the *Active Roles Synchronization Service Administration Guide*.

Exchange Resource Forest Management

The Exchange Resource Forest Management (ERFM) feature of Active Roles allows you to automate mailbox provisioning for on-premises users in environments where the mailboxes and the user accounts are managed in different Active Directory (AD) forests. Such multi-forest environments are based on the resource forest model, and mailboxes provisioned in such environments are called linked mailboxes.

Multi-forest AD deployments have higher administrative and support costs. However, they offer the highest level of security isolation between AD objects and the Exchange service. As such, One Identity recommends configuring the resource forest model for use with Active Roles in organizations that:

- Aim for an extra layer of data security.
- Frequently experience organizational changes (for example, buying companies, or consolidating and breaking off branch companies, departments and other business units).
- Abide by certain legal or regulatory requirements.

AD deployments following the resource forest model use two types of AD forests:

- **Account forests**: These AD forests store the user objects. Organizations can use one or more account forests in the resource forest model.
- **Resource forest**: This AD forest contains the Exchange server and stores the mailboxes of the user objects.

With ERFM, you can automate the **provisioning**, **synchronization** and **deprovisioning** of linked mailboxes in the resource forest for user accounts in the account forest(s).

- During **provisioning**, Active Roles can automatically create linked mailboxes for new users (if you select to create a mailbox for the user), or create linked mailboxes for existing users without a mailbox.

  In both cases, Active Roles creates a disabled **shadow user** account in the resource forest for the user, then links it to the user account of the user in the account forest (also known as the **master account**).

  > NOTE: By default, the shadow user account has the same name as the master user account in the account forest. However, if a shadow account with the same name already exists (for example, because Active Roles has already created a linked mailbox for a user in a different account forest), Active Roles uses a different shadow account name to maintain uniqueness.

- Once a linked mailbox is created, Active Roles automatically **synchronizes** the properties of the master user accounts with their shadow accounts, whenever you modify them.
- Finally, if the master user account is **deprovisioned**, Active Roles automatically deprovisions its shadow account as well, provided that you applied mailbox deprovisioning policies to the container that holds the shadow accounts in the resource forest.

NOTE: Like other AD objects, you can un-deprovision master user accounts as well. However, their shadow accounts are un-deprovisioned automatically only if the container of the deprovisioned master accounts has the **ERFM - Mailbox Management** built-in policy applied on them.

Getting started

For more information on the prerequisites and configuration of ERFM and linked mailboxes, see *Configuring linked mailboxes with Exchange Resource Forest Management* in the *Active Roles Administration Guide*.

Skype for Business Server User Management

To provision Skype for Business Server user accounts in single-forest and multi-forest Active Directory (AD) environments, Active Roles offers the Skype for Business User Management feature.

The Skype for Business Server User Management feature provides built-in Active Roles policies that synchronize user account information between Active Roles and Skype for Business Server, allowing you to perform Skype for Business Server user management tasks via the Active Roles Web Interface.

Skype for Business Server User Management lets you use Active Roles to:

- Add and enable new Skype for Business users.
- View or change Skype for Business Server user properties and policy assignments.
- Move Skype for Business Server users from one Skype for Business Server pool to another.
- Disable or re-enable user accounts for Skype for Business Server.
- Remove users from Skype for Business Server.

To perform these administration tasks, the feature adds the following elements to Active Roles:

- Built-in Policy Objects that enable Active Roles to perform user management tasks on Skype for Business Server, either in a single-forest or a multi-forest AD environment.
- Additional commands and pages in the Active Roles Web Interface for managing Skype for Business Server users.
- Access Templates (ATs) to delegate Skype for Business Server user management tasks.

The Skype for Business Server User Management policy allows you to control the following factors of creating and managing Skype for Business Server users:

- **SIP user name generation rules**. When adding and enabling a new Skype for Business Server user, Active Roles can generate a SIP user name based on other properties of the user account.
- **SIP domain selection rules**. When configuring the SIP address for a Skype for Business Server user, Active Roles can restrict the list of selectable SIP domains and suggest which SIP domain to select by default.
- **Telephony selection rules**. When configuring telephony for a Skype for Business Server user, Active Roles can restrict the list of selectable telephony options and can suggest default options to select.
- **Pool selection rules**. When adding and enabling a new Skype for Business Server user, Active Roles can restrict the list of selectable registrar pools and suggest which pool to select by default. This rule also applies to selecting the destination pool when moving a Skype for Business Server user from one pool to another.

Skype for Business Server User Management provides a number of ATs allowing you to delegate the following tasks in Active Roles:

- Add and enable new Skype for Business Server users.
- View existing Skype for Business Server users.
- View or change the SIP address for Skype for Business Server users.
- View or change the telephony option and related settings for Skype for Business Server users.
- View or change Skype for Business Server user policy assignments.
- Disable or re-enable user accounts for Skype for Business Server.
- Move users from one Skype for Business Server pool to another.
- Remove users from Skype for Business Server.

Getting started

For more information on the prerequisites and configuration of Skype for Business Server User Management, see *Skype for Business Server Solution* in the *Active Roles Administration Guide*.

Workflow features and activities

Active Roles supports the following major workflow features and activities:

- Saving object properties
- Modifying requested changes
- Using initialization scripts
- Searching for expiring users
- Sending plain-text notification messages

Getting started

To get started with workflows, see the following resources:

- For more information on the listed workflow features and activities, see the linked sections.
- For more information on workflows in general, see *Workflows* in the *Active Roles Administration Guide*.

Workflows – Saving object properties

Workflows configured in the Active Roles Console support saving object properties when running the workflow with the **Saving Object Properties** activity. The properties are saved in the workflow data context and can be retrieved by other workflow activities either before or after the object changed.

Saving object properties is useful for situations that require knowing not only the current state or properties of the changed object, but also its previous states or property values. Such earlier states or property values may be required for informational, archival or decision making purposes.

For example, to notify users and administrators of object deletions, you can create a workflow that:

1. Starts when requesting the deletion of the object.
2. Saves the name of the object to be deleted.
3. After the object is deleted, it sends a notification message with the saved name of the deleted object.

Workflow configuration options

The **Saving Object Properties** activity has the following configuration options:

- **Activity target**: Specifies the object whose properties will be saved. The available settings are the following:
    - **Workflow target object**: Specifies the target object of the request in a change workflow that started the workflow.

      For example, in case of a change workflow starting with the delete request of an object, selecting this setting will result in the activity saving the properties of the object to be deleted.
    - **Fixed object in directory**: Specifies a particular object that you select in Active Directory.
    - **Object identified by workflow parameter**: Specifies the object via the value of a certain parameter in the workflow. You can select the parameter

from the workflow definition.

- **Object from workflow data context**: When selected, the activity will select the object based on the workflow environment data collected while running the workflow. You can select the object for the activity when the workflow is initiated.
- **Object identified by DN-value rule expression**: Specifies the object via its Distinguished Name (DN) by the string value of a certain rule expression. By using a rule expression, you can compose a string value based on the properties of various objects found in the workflow environment when running the workflow. You can create the desired rule expression when you configure the activity.

- **Target properties**: Specifies the object properties you want the activity to save. The Workflow Designer contains a default list of properties; however, you can change the list as you need.

  By default, the activity saves all single-value non-constructed attributes found in the directory schema of the target object, including custom virtual attributes added to the directory schema by Active Roles.
- **Notification**: Configures notifications for the runs of the activity, and subscribes recipients to the following notification events:
  - **Activity completed successfully**: Sends a notification email if no significant errors occurred during the run of the activity.
  - **Activity encountered an error**: Sends a notification email if significant errors occurred during the run of the activity.

  The notification settings specify the notification events and recipients. When run by the workflow, the activity prepares a notification message according to the specified event. Active Roles retains the message prepared by the activity, and sends the message to the specified recipients when the event occurs.
- **Error handling**: Specifies the action to take when detecting any errors. Selecting **Continue workflow even if this activity encounters an error** will suppress any errors detected by Active Roles during the workflow run. Leaving this setting clear will result in Active Roles stopping the workflow if the activity detects any errors. By default, this setting is not selected.

Retrieving saved properties

If you use any workflows that include the **Save Object Properties** activity, you can configure additional activities to retrieve the object property information saved by the **Save Object Properties** activity. You can do this by three means:

- Using a **Script** activity with the following expression:

```
$workflow.SavedObjectProperties("activityName").get("attributeName")
```

In this expression, `activityName` is the name of the **Save Object Properties** activity, while `attributeName` is the LDAP display name of the attribute representing the property you want the script to retrieve.

NOTE: You must specify an attribute listed in the **Target properties** setting of the **Save Object Properties** activity. Otherwise, the expression will return no property value during runtime.

- Adding the **Workflow - Saved Object Properties** token to the notification message template. To do so:
  1. In the **Insert Token** dialog, in the list of tokens, click **Workflow - Saved Object Properties**, then click **OK**.
  2. In the dialog that appears, select the name of the **Save Object Properties** activity and the saved property you want the token to retrieve.

  NOTE: You must specify an attribute listed in the **Target properties** setting of the **Save Object Properties** activity. Otherwise, the token you configured will return no property value during runtime.
- If you use an **If-Else** branch condition, a **Search** filter, or a **Create**, **Update** or **Add Report Section** activity, by selecting the **Property of object from workflow data context** configuration option. To do so:
  1. In the **Object Property** dialog, click the link in the **Target object** field, then click **More choices**.
  2. In the dialog that appears, click **Saved Object Properties**. Then, in the **Activity** list, select the name of the **Save Object Properties** activity and click **OK**.
  3. In the **Object Property** dialog, click the link in the **Target property** field, then select the property you want.

  NOTE: You must specify an attribute listed in the **Target properties** setting of the **Save Object Properties** activity. Otherwise, the entry you configured will return no property value during runtime.

Getting started

For more information on how to configure object property saving in a workflow, see *Configuring a Save Object Properties activity* in the Active Roles Administration Guide.

Workflows – Modifying requested changes

Change workflows configured in the Active Roles Console support updating change requests that started a workflow with the **Modify Requested Changes** activity. This activity lets you add or remove changes to the properties of the workflow target object while the workflow is running.

For example:

- In a workflow that starts when requesting the creation of an object, you can use the **Modify Requested Changes** activity to either modify the properties that will be assigned to the new object, or change the container in which the object will be created.
- In a workflow that starts when requesting the change an object, you can use the **Modify Requested Changes** activity to modify the requested property changes of the object.

NOTE: The **Modify Requested Changes** activity is not available in automation workflows.

Workflow configuration options

The **Modify Requested Changes** activity has the following configuration options:

- **Target changes**: Specifies the property changes to add or remove from the change request. Use this setting to select:
  - The **Property** (or properties) you want the activity to change.
  - The **Action** to perform for each property (for example, adding, setting or removing the value of the property, or removing the property itself from the request).
  - The **Value** to add, remove or modify.

  You can add, remove and modify values both for single-value and multi-value properties, with the following options.

  NOTE: The various properties may only support some of the following settings.

  - **Fixed object in directory**: Specifies a particular object that you select in Active Directory.
  - **Text string**: Lets you specify the value of the property manually via a string.
  - **Workflow target object**: Specifies the target object of the request in a change workflow that started the workflow.
  - **Property of workflow target object**: Uses the value of a specific property of the target object in the request that started the workflow. When selecting this option, you can select the property from a list of object properties.
  - **Workflow initiator object**: Uses the object that initiated the workflow. When selecting this option, you can select the object from a list.
  - **Property of workflow initiator**: Uses the value of a specific property of the user who initiated the workflow. When selecting this option, you can select the property from a list of object properties.
  - **Object identified by workflow parameter**: Specifies the object via the value of a certain parameter in the workflow. You can select the parameter from the workflow definition.

- **Object from workflow data context**: When selected, the activity will select the object based on the workflow environment data collected while running the workflow. You can select the object for the activity when the workflow is initiated.
- **Object identified by DN-value rule expression**: Specifies the object via its Distinguished Name (DN) by the string value of a certain rule expression. By using a rule expression, you can compose a string value based on the properties of various objects found in the workflow environment when running the workflow. You can create the desired rule expression when you configure the activity.
- **Changed value of workflow target object property**: Uses the value that the workflow requests to be assigned to a certain property of the workflow target object. When selecting this option, you can select the property from a list of object properties.
- **Workflow parameter value**: Uses the value of a certain parameter of the workflow. When selecting this option, you can select the property from a list of workflow parameters.
- **Property of object from workflow data context**: Uses the value of a certain object property selected by the activity on the basis of the data found in the workflow run-time environment. You can choose the desired property and specify which object you want the activity to select when the workflow runs.
- **Value generated by rule expression**: Uses the string value of a certain rule expression. By using a rule expression you can compose a string value based on properties of various objects found in the workflow runtime environment. You can create the desired rule expression when you configure the activity.

- **Notification**: Configures notifications for the runs of the activity, and subscribes recipients to the following notification events:
  - **Activity completed successfully**: Sends a notification email if no significant errors occurred during the run of the activity.
  - **Activity encountered an error**: Sends a notification email if significant errors occurred during the run of the activity.

  The notification settings specify the notification events and recipients. When run by the workflow, the activity prepares a notification message according to the specified event. Active Roles retains the message prepared by the activity, and sends the message to the specified recipients when the event occurs.
- **Error handling**: Specifies the action to take when detecting any errors. Selecting **Continue workflow even if this activity encounters an error** will suppress any errors detected by Active Roles during the workflow run. Leaving this setting clear will result in Active Roles stopping the workflow if the activity detects any errors. By default, this setting is not selected.
- **Additional settings**: The **Modify Requested Changes** activity also contains the following settings:

- **Modify object creation requests so as to create objects in this container**: Allows you to change the container where Active Roles creates the new objects, while ensuring that the policies and workflows will be applied from the container where the object will be created (rather than from the container that was originally specified in the object creation request).
- **Include or exclude these controls from the change request**: Allows you to add or remove Active Roles controls from the request. "Controls" are pieces of data that provide additional information for Active Roles on how to process the request.

  If you do not specify any controls in the request, Active Roles will process the request based on the type of the request only. You can either configure the activity to add certain controls to the request (include controls) or to ensure that certain controls never occur in the request (exclude controls). For more information about adding Active Roles controls to a request, see the *Active Roles SDK documentation*.

Getting started

For more information on how to configure object property saving in a workflow, see *Configuring a Modify Requested Changes activity* in the Active Roles Administration Guide.

Workflows – Initialization scripts

When running a workflow instance, Active Roles uses a single PowerShell operating environment (called "runspace") for all script activities held in that workflow. The workflow runtime engine creates a runspace once the workflow instance started, and maintains the runspace during the run of the workflow instance.

When you configure a workflow, you can specify PowerShell commands you want the workflow runtime engine to initialize immediately after creating the runspace. These commands are part of an **initialization script** that the workflow engine runs prior to performing the script activities.

With an initialization script, you can define runspace configuration data separately from the logic of other script activities, and you can use it to initialize the environment for initializing script activities. Specifically, you can:

- Load PowerShell modules and snap-ins. All activity scripts can use the modules and snap-ins loaded in the initialization script without having to load the prerequisite modules or snap-ins on a per-activity basis.

  The modules and snap-ins loaded in the initialization script are available to all script activities at workflow runtime. For example, the `Import-Module 'SmbShare'` command added to the initialization script makes the Server Message Block (SMB) Share-specific cmdlets available to all script activities within the workflow.
- Initialize environment-specific variables, referred to as "global variables". All activity scripts can retrieve and update global variables, which makes it possible to exchange data between different activity scripts.

The global variables are visible to all script activities at workflow runtime. For example, the `$rGuid = [Guid]::NewGuid()` command added to the initialization script makes the `$rGuid` variable available to all script activities within the workflow. To reference a variable defined in the initialization script, the activity script must use the `$global:` qualifier, such as `$global:rGuid`.

> TIP: If the run of the workflow instance is suspended (for example, because it is waiting for approval), then resumed (for example, after receiving approval), the runspace is reinitialized, so the global variables may change.
>
> In such cases, if you need to preserve the value of a global variable, add the `[Persist()]` attribute to the variable name in the initialization script, such as `[Persist()]$rGuid = [Guid]::NewGuid()`. Global variables defined this way are saved to a persistent storage when the workflow instane is suspended, then restored from the storage when the workflow instance is resumed.

To save a variable, Active Roles creates and stores an XML-based representation of the object represented by the variable, similarly to the `Export-Clixml` command in Windows PowerShell. When restoring the variable, Active Roles retrieves the XML data that represents the object, and creates the object based on that data, similarly to the `Import-Clixml` command.

Getting started

You can create new initialization scripts in the Workflow Designer of the Active Roles Console.

To start creating a new initialization script

1. In the Active Roles Console, navigate to **Configuration** > **Policies** > **Workflow**.
2. To open the Workflow Designer, select the workflow you want to configure.
3. In the details pane, click **Workflow options and start conditions** > **Configure**.
4. To open the initialization script editor, click **Initialization script**.

The **Initialization script** tab then displays the currently used script (if it exists). To add a new script or modify the existing one, use the editor.

Workflows – Searching for expiring users

You can use the **Search** activity in an Active Roles workflow to search directory objects (such as users or groups), that match the criteria you specify with your search terms. Active Roles can then pass the search results to other workflow activities to perform additional actions.

The **Search** activity also supports searching for user accounts that will expire within the specified amount of time.

Getting started

To search for user accounts that expire within a certain amount of days, use the **Search** activity of the Workflow Designer in the Active Roles Console.

To search for expiring user accounts with a workflow

1. In the Active Roles Console, navigate to **Configuration** > **Policies** > **Workflow**.
2. To open the Workflow Designer, select the workflow you want to configure.
3. Add a **Search** activity to the workflow, or right-click an existing one, and select **Properties**.
4. To filter the search to user accounts that will expire, select **Retrieve only expiring user accounts**.
5. In the dialog that opens, specify the number of days to check. The **Search** activity will list user accounts that expire within the specified number of days.

Workflows – Sending plain-text notification messages

When configuring an Active Roles workflow, you can set email notification messages for the workflow based on a message template. The template specifies the format and contents of the notification message, including its subject and body.

The notification messages are created (and by default, sent) in HTML format. However, when configuring a **Notification** or **Approval** activity, you can also send them in plain-text format. Sending notification messages in plain-text format is useful for integration solutions that use mail flow for data exchange between Active Roles and other solution components in your organization.

Getting started

To configure a plain-text notification message for a **Notification** or **Approval** activity, use the Workflow Designer in the Active Roles Console.

To configure plain-text notification messages for a workflow

1. In the Active Roles Console, navigate to **Configuration** > **Policies** > **Workflow**.
2. To open the Workflow Designer, select the workflow you want to configure.
3. Right-click the **Notification** or **Approval** activity you want the notification for, or add them to the workflow from the Workflow Designer options.
4. In the **Notification Message** page, select **Format notification message as plain text**.

3

Using Active Roles

This section summarizes the major user experience features of Active Roles related to the various day-to-day administration operations you can perform with it.

Active Roles Web Interface

The Active Roles Web Interface is a highly customizable web application providing administrative coverage for all aspects of Active Directory (AD) and Azure Active Directory (Azure AD) data management. The Web Interface provides clarity, and a consistent look and feel to improve user experience and ease of use. The Web Interface also provides several several navigation options and optimized search pages, along with an enhanced point-and-click interface to create and reuse search conditions.

Key features and benefits

The key features of the Active Roles Web Interface include the following:

- **Single-page lists**: All search results are listed on a single page, making it easier to sort, filter, locate and select the objects you want to manage.
- **Enhanced search tools**: To further facilitate searches, the Web Interface features a unified toolbar for configuring search conditions and filter conditions. This includes a flexible condition builder, allowing you to choose predefined conditions, configure a wide variety of property-based conditions, or specify complex conditions using LDAP syntax.
- **Pop-up property pages**: The pages for creating, viewing or changing objects appear on the top of the object list, allowing you to keep the list visible while selecting and managing individual objects.
- **Views**: The Web Interface allows you to create, save and reuse personal views for the various AD and Azure AD containers. Each view is essentially a search query for objects contained in a particular container, and returns the list of objects matching the specified search conditions, with the specified set of list columns and list sorting order.

In addition, the Web Interface also provides the following benefits:

- Individually customizable Web Interface sites, shipping with separate Administrator, Helpdesk, and Self-Service sites by default.
- User permission-based views for each page.
- Self-administration support.
- Attractive design with superior flexibility.
- Easy navigation with a simple layout and large UI elements, with most UI elements supporting resizing, collapsing or expanding. This allows you to adapt your UI workspace to your needs.

All this results in a web application that you can tailor to any type of organizational use case and administrative personnel, regardless of whether your target users are day-to-day administrators, business data owners, helpdesk operators, or regular end-users.

Getting started

To open the Active Roles Web Interface, you must know:

- The name of the web server running the Web Interface component.
- The name of the Web Interface site you want to access.

When configuring the Web Interface, the Administration Service creates the following Web Interface sites by default:

- **ARWebAdmin**: The Administration Site, supporting a broad range of administrative tasks.
- **ARWebHelpDesk**: The Helpdesk Site, supporting the most common administrative tasks, typically performed by helpdesk personnel in an organization.
- **ARWebSelfService**: The Self-Service Site, allowing users to manage their own personal accounts.

To connect to a Web Interface site

1. In the web browser, enter the URL of the Web Interface site.

   For example, to connect to the default Administration Site, specify the following URL:

   `http://<server>/ARWebAdmin`

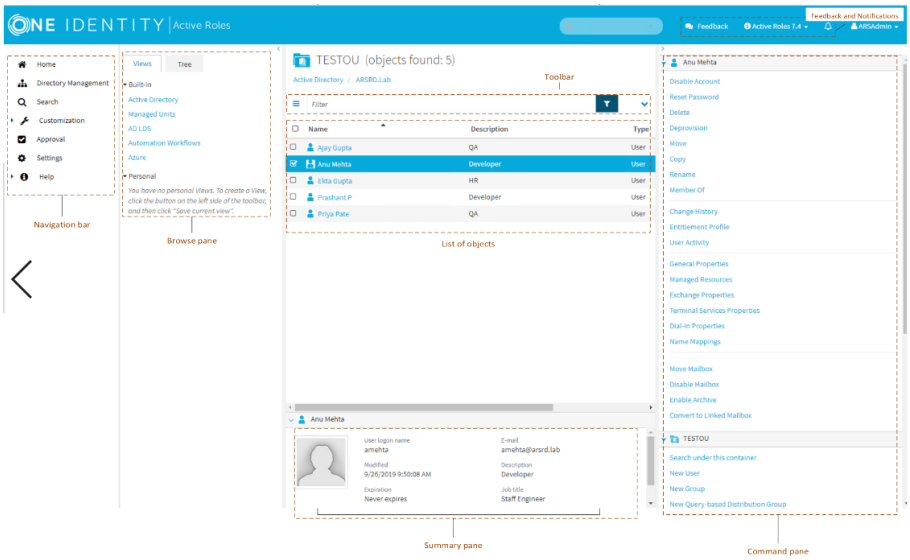
   In the above example, `<server>` is the name of the web server running the Web Interface.
2. To connect, press **Enter**.

Web Interface parts

The Web Interface UI consists of the following main parts:

- The **Header** area at the top of the page, containing the **Quick Search bar**, the **Feedback** button, the **About** button, and the **Logout** option for your currently logged-in user.
- The **Navigation bar** and the **Browse pane** on the left side. The **Navigation bar** lets you navigate between the main Web Interface components, while the **Browse pane** shows the available **View** and **Tree** settings.
- The **Object list** next to the **Browse pane**.
- The **Toolbar** above the **Object list**, allowing you to manage the loaded **Object list**.
- The **Command pane** on the right side, containing the available administration actions for the selected object(s).
- The **Summary pane** under the list of objects, containing a short summary of data about the selected object(s).

Figure 1: UI Elements



The following sub-sections describe each UI component in more detail.

Web Interface Navigation bar

Located on the left side of the Web Interface UI, the **Navigation bar** provides the first level of navigation for most of the tasks you can perform with the Web Interface. The **Navigation bar** lists all major Web Interface areas, and provides access to the following pages and features:

- **Home**: Opens the Web Interface home page.
- **Directory Management**: Allows you to browse and administer the AD and Azure AD objects in your organization.

- **Search**: Allows you to search and administer the AD and Azure AD objects in your organization.
- **Customization**: Allows you to customize your Web Interface pages.

  NOTE: This option is available for Active Roles Admin users only.
- **Approval**: Allows you to perform tasks related to the approval of administrative operations.
- **Settings**: Contains your personal settings related to displaying the Web Interface.

Web Interface Browse pane

Located next to the **Navigation bar**, the **Browse pane** lists the built-in **Views** and **Personal views**, and also lets you access the **Tree** view:

- Built-in **Views** are default entry points for browsing objects in your AD and Azure AD environment. **Personal views**, on the other hand, are filter or search queries that you can build and save to use later.
- The **Tree** view helps you browse AD and Azure AD objects via the hierarchical directory tree structure of the containers.

Web Interface Object list

When you select a container or view in the **Browse pane**, a list of objects appears. If you select a container (such as an Organizational Unit, or OU), the list includes the objects held in that container. If you select a view, the list includes the objects that match the view settings. The object list appears on a single page, allowing you to search the entire contents of the container or view easily.

In addition to browsing the object list, you can also:

- Use various built-in conditions or create custom conditions to filter the object list. You can also customize the list by sorting and filtering, and by adding or removing list columns.
- Select objects from the list and apply administration commands to the selected object(s). When you click the name of a container object, such as a domain or an OU, the list changes to display the objects held in that container, allowing you to browse through containers in the directory.

Web Interface Toolbar

Located above the list of objects, the **Toolbar** contains a number of controls allowing you to manage the current **Object list**:

- To save the current object list as a **Personal view**, add or remove list columns, or export the list to a text file, click **Menu** on the left side of the **Toolbar**.
- To filter the results of the **Object list**, enter your filtering conditions in the **Filter** field, then click the button next to the field.
- To configure filtering criteria based on object properties, click **Expand/Collapse** on the right side of the **Toolbar**. To have the list include only the objects that match your filtering criteria, click the button next to the **Filter** field.

Web Interface Command pane

Located to the right of the **Object list**, the **Command pane** provides administrative commands you can apply to the objects you select from the list, as well as commands you can apply to the current container.

- If no objects are selected in the **Object list**, the **Command pane** includes only the commands that apply to the current container. These commands are grouped under a heading that shows the name of the current container.
- If a single object is selected in the list, the **Command pane** also contains the set of commands that are applicable to the selected object, under a heading that shows the name of the object.
- If multiple objects are selected from the list, the **Command pane** contains a set of batch commands that apply to all of the objects, under a heading that shows the number of the selected objects.

Web Interface Summary pane

The **Summary pane** provides information about the selected object under the **Object list**. The information shown on the pane includes the commonly used properties of the object, and depends on the object type.

For example, user properties provide more detailed information about a user account, such as the login name, email address, description, job title, department, expiration date, and the date and time when the account was last changed.

TIP: If you do not see the **Summary pane**, click the area below the **Object list**.

Web Interface Personal views

Personal views provide a filter-based object list, with the objects either belonging to the same container, or to the same search query. When searching a container (such as an OU), you can filter the search using either via search conditions or filter conditions as you need, then save the resulting search or filter query as your **Personal view**.

The **Personal view** shows the list of objects that match your specified conditions, with the specified list sorting order and set of list columns. **Personal views** are stored on a per-user basis, so each user can have their own views.

Using Personal views

To locate directory objects, the Active Roles Web Interface lets you use search or filter queries. When creating a query, you specify a set of rules that determine the contents of the resulting **Object list**. You can, for instance, specify to list only user accounts from a specific OU. In addition, you can adjust the set of columns and the sort order in the list of search or filtering results.

Locating objects quickly and easily is a critical Web Interface feature, as you need to focus your attention only on the objects you actually need to manage. However, creating a search or filter query that displays the objects you are interested in for a particular task can be time-consuming.

Personal views provide a way for you to save that work. Once you created a query that shows just the objects you need, you can set a name for the query and save it for use later. That saved query is a **Personal view**. Each view saves the following settings that you specify:

- The container to search or filter.
- The search or filtering criteria.
- The set of columns and the sort order in the list of search or filtering results.

Creating a Personal view

Personal views are like search or filter queries that you named and saved. After creating a **Personal view**, you can reuse it without re-creating its underlying search or filter query. To reuse a personal view, click the name of the view on the **Views** tab in the **Browse pane**. The Web Interface then applies the search or filter query saved in the view, and displays the results in the list with the same set of columns and sort order with which you created the view.

To create a personal view

1. Configure and perform a search, or create a filtered list of objects.
2. On the left side of the **Toolbar**, click **Menu**, then click **Save current view**.
3. In the dialog that appears, specify a name for the **Personal view**, then click **Save**.

Locating directory objects in the Web Interface

The Active Roles Web Interface provides search and filtering tools to help you locate directory objects quickly and easily. By creating and applying a proper search or filter query, you can build shorter object lists, which makes it easier to select the objects needed to accomplish your administrative tasks.

You can also save search and filter queries as your **Personal views**, and use them again at a later time. Each view saves the following settings that you specify:

- The container to search or filter.
- The search or filtering criteria.
- The set of columns.
- The sort order in the list of search or filtering results.

Searching for directory objects in the Web Interface

To search for directory objects, use the **Search** page that allows you to select the container to search and specify criteria for the objects you want to find. The Web Interface runs searches both in the selected containers and their subcontainers.

The Web Interface opens the **Search** page when you do any of the following:

- Type in the **Search** field located in the upper right corner of the **Web Interface** window, then press **Enter** or click the magnifying glass icon in the **Search** field. In this case, the Web Interface will search all managed AD or Azure AD domains for objects whose naming properties match what you specified, and the **Search** page will list the search results accordingly. The naming properties include name, first name, last name, display name, and login name.
- Click **Search** on the **Navigation bar**. This will open the **Search** page, allowing you to configure and start a search.

To configure and start a search

1. On the **Toolbar** of the Web Interface, click **Search in**, then select the container that you want to search. You can select more than one container.
2. Specify the criteria for the objects that you want to find:
    - To search by naming properties, enter them in the **Search** field on the **Toolbar**. The Web Interface will then search for objects whose naming properties match your criteria. The naming properties include name, first name, last name, display name, and logon name.

- To search by other properties, expand the **Toolbar** by clicking the button on the right side of the **Toolbar**, click **Add criteria**, choose the properties by which you want to search, and click **Add**. Then, configure the criteria as appropriate. The Web Interface will search for objects that match the criteria you configured.

3. To start the search, press **Enter**.

The search results then appear on the **Search** page.

TIP: You can customize the list by adding or removing list columns and sorting the list by column data. To add or remove list columns, click **Menu** on the left side of the **Toolbar**, then click **Choose columns**. To sort the list by column data, click the column headings.

Example: Searching by object type

This example procedure shows how to use the **Search** option to list all groups that exist in the AD domains managed by Active Roles.

To list all groups in all AD environments managed by Active Roles

1. On the **Navigation bar** of the Web Interface, click **Search**.
2. Expand the **Toolbar** by clicking the button on the right side of the **Toolbar**, click **Add criteria**, select **Object type is User/InetOrgPerson/Computer/Group/Organizational Unit**, then click **Add**.
3. On the **Toolbar**, click **Group** in the list next to **The object type is**, then press **Enter**.

Filtering the contents of a container in the Web Interface

If a container, such as an OU in an AD, holds many objects, you can narrow down the displayed list of objects by filtering them.

To filter the objects held in a container

1. In the Active Roles Web Interface, navigate to the container whose contents you want to filter.

   To navigate to a container:

   - Search the container object, then click its name in the list of search results on the **Search** page.

- Alternatively, browse the container objects with the **Browse pane** and the **Object list**.

NOTE: The scope of filtering is always set to the current container, and does not include any subcontainers of that container. Filtering is essentially a search for objects stored in a given container only. If you want to search the current container and all of its subcontainers, click **Search under this container** in the **Command pane**, and configure a search instead.

2. Specify how you want to filter the objects of the container.
   - To filter objects by naming properties, specify your criteria in the **Filter** field on the **Toolbar**, then press **Enter**. Alternatively, click the button next to the **Filter** field. The list of objects will include only the objects whose naming properties match what you typed. The naming properties include name, first name, last name, display name, and login name.
   - To filter objects by other properties, expand the **Toolbar** by clicking the button on the right side of the **Toolbar**, click **Add criteria**, choose the properties by which you want to filter, and click **Add**. Then, configure the criteria as you need. The list of objects will include only the objects that match the criteria you configured.
3. To apply the filter, press **Enter** or click the button next to the **Filter** field on the **Toolbar**.

When the Active Roles Web Interface applies the configured filter, it lists a subset of all objects held in that container.

TIP: To view all objects again, remove the filter.

- If you did not specify any criteria, clear the **Filter** field on the **Toolbar**, and press **Enter**.
- If you specified any criteria, expand the **Toolbar**, click **Clear all**, and press **Enter**.

Example: Filtering by object type

This example procedure shows how to configure a filter that lists only user accounts in a specific OU, removing all other objects from the list.

To filter to user accounts in a specific OU

1. In the Active Roles Web Interface, navigate to the OU.
2. To expand the **Toolbar**, click the button on the right side of the Toolbar. Then, click **Add criteria**, select **Object type is User/InetOrgPerson/Computer/Group/Organizational Unit**, and click **Add**.
3. On the **Toolbar**, confirm that the field next to **The object type is** reads **User**, then either click the button next to the **Filter** field, or press **Enter**.

Active Roles Management Shell

Part of the Active Roles Management Tools, the Management Shell provides Windows PowerShell-based command-line tools (cmdlets), allowing you to run and automate administrative tasks in Active Roles.

These Management Shell cmdlets are shipped in two modules.

ActiveRolesManagementShell

The **ActiveRolesManagementShell** module provides cmdlets for the following administration operations:

- Managing users, groups, computers and other Active Directory (AD) objects via Active Roles.
- Managing digital certificates.
- Administering certain Active Roles objects.

The names of the cmdlets provided by this module start with the `QAD` or `QARS` prefixes, such as `New-QADUser`, `Add-QADCertificate`, or `New-QARSAccessTemplateLink`.

ActiveRolesConfiguration

The **ActiveRolesConfiguration** module (also known as the "Configuration Shell") provides cmdlets for configuring Active Roles Administration Service instances and Web Interface sites. The names of the cmdlets provided by this module start with the `AR` prefix, such as `New-ARDatabase`, `New-ARService`, or `New-ARWebSite`.

NOTE: Consider the following when planning to use the **ActiveRolesConfiguration** module:

- This module is available on 64-bit operating systems only.
- You can only install this module on computers where the Administration Service or Web Interface modules are also installed. Otherwise, the module will not provide all cmdlets.

For more information, see Active Roles Configuration Shell.

Getting started

You can start using the Management Shell component from the Windows Start menu or the Apps page, depending on the version of the operating system.

To start the Active Roles Management Shell

1. Log in to the computer where the Administration Service or the Management Shell is installed.

2. To start the Active Roles Management Shell, in the Windows Start menu or the Apps page, click **Active Roles 8.0.1 LTS Management Shell**.
3. To view the reference manual providing detailed information about the available cmdlets, in the Management Shell command-line interface, enter **`QuickRef`**, then press **Enter**.
4. To load the available modules and access their cmdlets, enter the **`Import-Module`** command, then press **Enter**.

Configuring and administering Active Roles

This section summarizes the major configuration, deployment, and maintenance features of Active Roles.

Active Roles Setup wizard

The Active Roles Setup wizard facilitates the evaluation, deployment, upgrade and configuration of Active Roles. The key highlights of the wizard include the following:

- **Unified setup process**: Active Roles is shipped with a single wizard for installing all core product components, including the Administration Service, the Web Interface, and the Console (also known as the MMC Interface).
- **Configuration Center**: After installation, Active Roles launches the Configuration Center, an application that you can use to perform the core configuration tasks after installation, or to finish upgrading Active Roles. As such, the Configuration Center lets you configure Administration Service instances and deploy Web Interface sites. For more information on the Configuration Center, see Active Roles Configuration Center.
- **Side-by-side deployment**: The Active Roles Setup allows you to deploy new Active Roles versions side-by-side on the same computers with Active Roles 6.9. This allows you to use the same hardware and infrastructure to run newer versions of Active Roles while also keeping Active Roles 6.9 deployed for your business needs.

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 domain. Different versions of Active Roles servers in the same AD domain will cause issues with dynamic groups, policies, workflows, or custom scripts, and can also cause 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 to be in a supported configuration.

For more information, see Knowledge Base Article 4307177.

NOTE: To avoid potential conflicts with Active Roles 6.9, newer versions of the product use a different name for the Windows service of the Administration Service and for the default Web Interface sites.

- **Separate component installation files**: Although the Active Roles Setup allows you to install every major product component at once, the installation `*.iso` delivers each component (such as the Administration Service, the Web Interface, the Add-on Manager, the SPML Provider, or the Management Shell) in separate `*.msi` files. This allows you to install the various Active Roles components individually without the need of running the Active Roles Setup.

Active Roles Configuration Center

The Active Roles Configuration Center is a configuration application that provides a unified configuration platform for the Active Roles Administration Service and the Web Interface component. This allows administrators to perform the core Active Roles configuration tasks from a single application, including the following:

- Performing the initial configuration of Active Roles, such as setting up the Administration Service instances and the default Web Interface sites.
- Importing the configuration database and the management history database from earlier Active Roles versions.
- Managing the core Administration Service resources, such as the Active Roles Admin account, service account, and database connections.
- Creating new Web Interface sites either based on the site configuration objects of the current Active Roles version, or by importing site configuration objects from earlier Active Roles versions.
- Managing core Web Interface site settings, such as site addresses on the web server, or the configuration object in the Administration Service.

- Configuring secure communication for the Active Roles Web Interface through forced SSL redirection.
- Integrating Active Roles with One Identity Starling. For more information, see *One Identity Starling Join and configuration through Active Roles* in the *Active Roles Administration Guide*.
- Managing user login settings for the Active Roles Console (also known as the MMC Interface).
- Configuring Federated Authentication, allowing you to access an application or website by authenticating against a certain set of rules, known as "claims".
- Configuring log management and Solution Intelligence.

For more information on these features, see the following subsections.

Getting Started

Active Roles Configuration Center is automatically installed and started by default if you select to install either the Administration Service or the Web Interface components to a computer. Later, you can start Configuration Center again either from the Windows Start menu, or from the Apps page of the operating system.

Configuration Center components

The Configuration Center provides a unified, single, simple, wizard-based user interface for all core Active Roles configuration tasks, making it a single point of access to all management wizards for all configuration tasks.

The Configuration Center consists of the following elements.

Initial configuration wizards

After installing Active Roles, the Configuration Center allows administrators to run the initial configuration wizards and create the new Active Roles instance, including the Administration Service and the Web Interface.

Hub pages and management wizards

Once the initial configuration is completed, the Configuration Center provides a consolidated view of the core Active Roles configuration settings, and offers tools for changing those settings.

The hub pages of the Configuration Center show the current settings specific to the Administration Service and the Web Interface, including the commands to start the management wizards for changing those settings. The available hub pages are the following:

- **Administration Service**: This page allows administrators to:
  - View or change the Active Roles Admin account, service account, and databases.
  - Import the configuration data and management history data either from an earlier Active Roles version or from the current Active Roles database.
  - View status information, such as whether the Administration Service is started and ready for use, stopped, or being restarted (along with the options to start, stop and restart the service).
- **Web Interface**: This page allows administrators to:
  - View, create, modify or delete Web Interface sites. The configurable site settings include the site address, and the configuration object that stores the site configuration data in the Administration Service.

    When creating or modifying a Web Interface site, administrators can either reuse an existing configuration object, or create a new one based on a template or by importing data from another configuration object or from an export file.
  - Export the configuration of any existing Web Interface site to a file.
  - Open each site in a web browser.

Configuration Shell

The `ActiveRolesConfiguration` module (also known as the Configuration Shell) of the Active Roles Management Shell allows administrators to access all Configuration Center features and functions from a Windows PowerShell command-line interface or with scripts, facilitating the unattended configuration of Active Roles components. The `ActiveRolesConfiguration` module provides cmdlets for key configuration tasks, such as:

- Creating the Active Roles database.
- Creating or modifying the Administration Service instances and the Web Interface sites.
- Performing data exchange between Active Roles databases and between site configuration objects.
- Querying the current state of the Administration Service.
- Starting, stopping or restarting the Administration Service.

Configuring a local or remote Active Roles instance

Configuration Center is installed as part of the Management Tools component if you install Active Roles on a 64-bit system. You can use the Management Tools package to perform configuration tasks on the local or remote computer that has the current version of the Administration Service or Web Interface installed.

Once installed, the Configuration Center looks for these components on the local computer, and if it does not find any of these components, it prompts you to connect to a remote computer. However, you can also connect to a remote computer by clicking the drop-down menu in the Configuration Center header.

NOTE: Consider the following when planning to use the Configuration Center on a remote computer:

- When connecting to a remote computer, Configuration Center prompts you for a user name and password. The account you use to log in must match the domain user account belonging to the Administrators group on the remote computer. In addition, whether you are going to perform configuration tasks on the local computer or on a remote computer, your login account must be a member of the Administrators group on the computer running Configuration Center.
- To perform configuration tasks on a remote computer, Configuration Center requires Windows PowerShell remoting to be enabled on that computer. PowerShell remoting is enabled by default on Microsoft Windows Server 2016 or newer operating systems; however, if it is turned off for any reason on the remote computer, you can enable it by running the **`Enable-PSRemoting`** command in Windows PowerShell. For more information, see Enable-PSRemoting in the *Microsoft PowerShell documentation*.

Running the Configuration Center

The Configuration Center is installed and, by default, automatically started after installing the Active Roles Administration Service or Web Interface component on a computer, allowing you to perform the initial configuration tasks for these components. If you close the Configuration Center, you can start it again later from the Windows Start menu or the Apps page of the operating system.

As the Configuration Center can manage Active Roles not only on the local computer but also on remote computers, you can run it both on client and server operating systems. However, you can only install the Configuration Center on a 64-bit operating system. Once the component is installed on a client operating system, you must start and connect it to the remote server where the Administration Service or Web Interface instances you want to configure are installed. Similarly to a server operating system, you can launch the Active Roles Configuration Center either from the Windows Start menu or from the Apps page.

NOTE: To run the Configuration Center on a client computer, you must be logged in with Administrator privileges.

If neither the Administration Service nor the Web Interface is installed on the local computer, the Configuration Center will prompt you to select a remote computer. In the **Select Server** dialog that appears, supply the fully qualified domain name of a server on which the Administration Service or the Web Interface instance is installed, then enter the name and password of a domain user account that has administrator rights on that server. You can connect to a remote server at any time by clicking the **Connect to another server** option in the header of the Active Roles Configuration Center.

Supported Configuration Center tasks

The Configuration Center lets administrators perform:

- Initial configuration tasks, such as creating the Administration Service instance and the default Web Interface sites. For more information, see Initial configuration tasks.
- Configuration management tasks, that is managing existing Administration Service and Web Interface instances. For more information, see Configuration management tasks.
- Managing user access to the Active Roles Console. For more information, see Delegating user access to the Active Roles Console.
- Managing the logging settings of Active Roles. For more information, see Configuring Active Roles logging settings.
- Configuring Solution Intelligence. For more information, see Configuring Solution Intelligence.

Initial configuration tasks

Once the Active Roles Setup wizard installs Active Roles, the Configuration Center starts automatically so that administrators can create an Administration Service instance and deploy the default Web Interface sites. The following sections describe these tasks in detail.

Configuring the Administration Service

The **Configure Administration Service** wizard creates the Administration Service instance, preparing it for use. The wizard needs the following data for configuration:

- The login name and password of the account in which the configured Administration Service instance will be running (service account). In case of a Group Managed Service account, you must specify the service account details.
- The name of the group or user account that will have full access to all Active Roles features and functions through the configured Administration Service instance. This group or account is known as the Active Roles Admin.
- The database in which the configured Administration Service instance will store the configuration data and management history data. When specifying the database, you can either create a new database, or use an existing database compatible with the current Active Roles version. You can use the same database for multiple Administration Service instances.
- The authentication mode that the configured Administration Service instance will use when connecting to the database:
    - When using **Windows authentication**, the Administration Service will use the credentials of the service account.

When using **SQL Server authentication**, the Administration Service will use the SQL login name and password you specify in the wizard.

To start the wizard, in the **Administration Service** tab, click **Configure**.

Configuring the Web Interface

The **Configure Web Interface** wizard creates the default Web Interface sites, getting the Web Interface component ready for use. The wizard prompts you to choose which Administration Service instance will be used by the Web Interface instance you are configuring. The Web Interface can:

- Use the Administration Service instance running on the same computer as the Web Interface.
- Use an Administration Service instance running on a different computer. In this case, you must supply the fully qualified domain name of the computer running the preferred instance of the Administration Service.
- Let the Web Interface choose any Administration Service instance that has the same configuration as the specified one. In this case, you must supply the fully qualified domain name of the computer running the Administration Service instance of the desired configuration.

  NOTE: If your environment uses Active Roles replication, you must specify the computer running the Administration Service instance whose database server acts as the Publisher of the Active Roles configuration database.

You can access the **Configure Web Interface** wizard from the **Configure** > **Web Interface** menu of the Configuration Center **Dashboard**.

After configuring the Web Interface, you can perform the following additional Web Interface configuration steps in the Configuration Center:

- **Forcing SSL redirection**: By default, Active Roles users can connect to the configured Web Interface sites via HTTP protocol that does not encrypt data during communication. To enable secure communication for the Web Interface on local and remote servers, One Identity recommends enabling the HTTPS protocol with the **Force SSL Redirection** option.
- **Federated authentication**: You can authenticate the Web Interface sites against a certain set of rules (known as "claims"), by using the federated authentication. The implementation in Active Roles uses Security Assertion Markup Language (SAML), through which you can sign in to an application via single sign-on, then authenticate to access the configured Web Interface sites. For more information, see *Working with federated authentication* in the *Active Roles Administration Guide*.

Configuring join to Starling

Active Roles supports integration with One Identity Starling via the Starling Join feature. Joining Active Roles to Starling enables access to the various Starling services, including Identity Analytics and Risk Intelligence, and Connect. For more information, see *One*

Identity Starling Join and configuration through Active Roles in the *Active Roles Administration Guide*.

Configuration management tasks

Once you completed the initial configuration of Active Roles in the Configuration Center as described in Initial configuration tasks, you can check the state of the Administration Service and Web Interface components anytime, and can also perform various management tasks on them. The following sections describe these tasks in detail.

Administration Service management tasks

After installing Active Roles, first you must create the Administration Service instance as described in Configuring the Administration Service. Then, you can use the Configuration Center to:

- View or change the core Administration Service settings, such as the Active Roles Admin account, Active Roles service account, and the Active Roles databases.

  For more information, see Viewing the core Administration Service settings and Modifying the core Administration Service settings.
- Import configuration data from another (current version or earlier version) Active Roles database to the current database of the Administration Service. For more information, see Importing configuration data.
- Import management history data from another (current version or earlier version) Active Roles database to the current database of the Administration Service. For more information, see Importing management history data.
- Check the state of the Administration Service. For more information, see Checking the state of the Administration Service.
- Start, stop or restart the Administration Service. For more information, see Starting, stopping or restarting the Administration Service.

Viewing the core Administration Service settings

On the **Administration Service** page of the Configuration Center, you can check:

- The login name of the Active Roles service account.
- The name of the group or user account that has the Active Roles Admin rights.
- The SQL Server instance that hosts the Active Roles database and the name of the Active Roles database.
- The database connection authentication mode (Windows authentication or SQL Server authentication).

Modifying the core Administration Service settings

On the **Administration Service** page of the Configuration Center, you can change:

- The service account. To do so, click **Service account** > **Change**. Then, in the wizard that appears, specify the login name and password of the domain user account, or if using a group Managed Service Account (gMSA), the service account details in which you want the Administration Service to run.
- The Active Roles Admin account. To do so, click **Active Roles Admin** > **Change**. Then, in the wizard that appears, specify the group or user account you want to have the Active Roles Admin rights.
- The Active Roles database. To do so, click **Active Roles database** > **Change**. Then, in the wizard that appears, specify the SQL Server instance and the database you want the Administration Service to use, and select the database connection authentication mode (Windows authentication or SQL Server login). You can also specify a separate database for storing management history data.

Importing configuration data

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.
- **sysadmin** fixed server role in the destination database.

If a limited SQL access account is used for performing the in-place upgrade, a manual action is required to pre-create the new Active Roles databases. For more information, see Knowledge Base Article 4303098 on the One Identity Support Portal.

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**.

The configuration operations available in the Configuration Center are fully scriptable using the Windows PowerShell command-line tools of the Active Roles Management Shell. For more information, see Active Roles Management Shell.

When upgrading the Administration Service, you must import configuration data from the earlier version of Active Roles to the new version of the product. To do so, in the Configuration Center, click **Administration Service** > **Import Configuration**, then follow the steps in the wizard that appears.

The wizard will prompt you to specify the Active Roles database from which you want to import the configuration data (known as the "source database"), then it will identify the current Administration Service database to which it will import the configuration data (known as the "destination database"). After that, you must choose the connection authentication mode (Windows authentication or SQL Server login) for each database. The wizard then performs 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.

Importing management history data

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.
- **sysadmin** fixed server role in the destination database.

If a limited SQL access account is used for performing the in-place upgrade, a manual action is required to pre-create the new Active Roles databases. For more information, see Knowledge Base Article 4303098 on the One Identity Support Portal.

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**.

Although importing management history data during an upgrade looks similar to importing configuration data, importing management history information is different because of two main reasons:

- Management history data typically has a much larger volume than configuration data. Because of this, importing configuration data takes much longer.
- Management history data has dependencies on configuration data (while configuration data has no dependencies on management history data). Because of this, during an Active Roles upgrade process, you must import the configuration data first, then (optionally) the management history data, if needed.

Because of these differences, the Active Roles Configuration Center provides a separate wizard for importing management history data, with the following feature set:

- The wizard does not replace the existing management history data in the destination database. Instead, it only retrieves and upgrades management history records from the source database, then adds the upgraded records to the destination database.
- The wizard allows you to specify the date range for the management history data you want to import. This way, you can import only records that occurred within a particular time frame instead of importing every management history record.
- Canceling the wizard while the management history data import operation is in progress does not result in losing the imported data. Because of this, you can stop the import operation at any time. The records imported by the time of you canceling the wizard are retained in the destination database. If you start the wizard again, the wizard will continue importing the records that have not yet been imported.

To start the wizard, in the Configuration Center, click **Administration Service** > **Import Management History**. The wizard will prompt you to specify the Active Roles database from which you want to import the management history data (known as the "source database"), then it will identify the current Administration Service database to which it will import the management history (known as the "destination database"). After that, you must choose the connection authentication mode (Windows authentication or SQL Server login) for each database. The wizard then performs the import operation.

During the import operation, the wizard retrieves and upgrades the management history records of the specified date and time range from the source database, and adds the upgraded records to the destination database.

Checking the state of the Administration Service

You can check the state of the Administration Service in the **Administration Service** page of the Active Roles Configuration Center. The page indicates the states of the service with the following status labels:

- **Ready for use**: Administration Service is running and is ready to process requests.
- **Getting ready**: Administration Service just started and is preparing to process client requests.
- **Stopping**: Administration Service is preparing to stop.
- **Stopped**: Administration Service is not running.
- **Unknown**: Configuration Center cannot check the state of Administration Service.

Starting, stopping or restarting the Administration Service

You can start, stop or restart the Administration Service in the **Administration Service** page of the Configuration Center by clicking the **Start**, **Stop** or **Restart** buttons.

Web Interface management tasks

After installing Active Roles, you can perform the initial configuration of the Web Interface in the Configuration Center, preparing the component for use. Then, you can use the Configuration Center to:

- Identify the Web Interface sites currently deployed on the web server running the Web Interface. For more information, see Identifying the Web Interface sites.
- Create, modify or delete Web Interface sites. For more information, see:
  - Creating a Web Interface site
  - Modifying a Web Interface site
  - Deleting a Web Interface site
- Export the configuration object of a Web Interface site to a file. For more information, see Exporting the configuration of a Web Interface site to a file.

Identifying the Web Interface sites

You can use the **Web Interface** page of the Configuration Center to identify the Web Interface sites 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 website holding the web application that runs the Web Interface site.
- **Web app alias**: The alias of the web application that runs the Web Interface site. Tha alias defines the virtual path of that application on the web server.
- **Configuration**: The object which holds the site configuration and customization data of the Web Interface site in the Active Roles Administration Service.

TIP: You can also open the configured Web Interface sites from the **Web Interface** page of the Configuration Center. To open any of the configured sites, click the site in the list, then click **Open in Browser**.

Creating a Web Interface site

You can create a new Web Interface site with the **Web Interface** > **Create** option of the Configuration Center. This opens the **Create Web Interface Site** wizard, allowing you to:

- Choose the IIS website configuration that will contain the web application which implements the Web Interface site.
- Specify the alias of the web application, defining the virtual path for the URL of the Web Interface site.

The wizard then lets you specify the object that will hold the configuration and customization data of the new Web Interface site in the Active Roles Administration Service. You can choose from the following options:

- **Create from a template**: If you select this option, Active Roles will create the new site from the configuration and customization settings of the template you select.
- **Use an existing configuration**: If you select this option, the new site will have the same configuration and customization as any existing Web Interface site that also uses the configuration object you select.

  TIP: Use this option if you want to create an additional instance of an existing Web Interface site on a different web server.
- **Import from an existing configuration**: If you select this option, the new Web Interface site will have the same configuration and customization as the site you select as a baseline. In this case, Active Roles imports the configuration data from the previous version of the configuration to the new Administration Service instance, then creates the new Web Interface configuration objects based on that earlier version.

  TIP: Use this option during upgrades if you want to create the new Web Interface sites based on the sites of the Active Roles version you upgraded from.
- **Import from a file**: If you select this option, the new Web Interface site will use the configuration and customization stored in the browsed export file.

  TIP: Use this option during upgrades if you want to create the new Web Interface sites from a previously exported configuration.

Modifying a Web Interface site

You can modify existing Web Interface sites with the **Web Interface** > **Modify** option of the Configuration Center. This opens the **Modify Web Interface Site** wizard, allowing you to:

- Modify the IIS website configuration that will contain the web application which implements the Web Interface site.
- Modify the alias of the web application, defining the virtual path for the URL of the Web Interface site.

The wizard then lets you specify the object that will hold the configuration and customization data of the modified Web Interface site in the Active Roles Administration Service. You can choose from the following options:

- **Keep the current configuration**: If you select this option, the wizard will keep the current configuration of the modified website.

  TIP: Use this option if you plan no further changes in the website configuration apart from changing the IIS website configuration or the site alias.
- **Create from a template**: If you select this option, Active Roles will change the configuration and customization settings of the modified Web Interface site to those of the template you select.
- **Use an existing configuration**: If you select this option, Active Roles will change the configuration and customization settings of the modified website to those of the site you select.

  TIP: Use this option if you want to align the configuration and customization of an existing Web Interface site with that of another existing website.
- **Import from an existing configuration**: If you select this option, Active Roles will change the configuration and customization of the modified Web Interface site to that of the configuration you select as baseline. In this case, Active Roles imports the configuration data from the previous version of the configuration to the new Administration Service instance, then creates the new Web Interface configuration objects based on that earlier version.

  TIP: Use this option during upgrades if you want to modify an existing Web Interface site based on another site of the Active Roles version you upgraded from.
- **Import from a file**: If you select this option, Active Roles will change the configuration and customization of the existing Web Interface site to that of the exported configuration you select.

  TIP: Use this option during upgrades if you want to align the configuration and customization of an existing Web Interface site with that of a previously exported configuration.

Deleting a Web Interface site

You can delete existing Web Interface sites with the **Web Interface** > **Delete** option of the Configuration Center. This opens the **Delete Web Interface Site** wizard, deleting the selected Web Interface site from the web server.

NOTE: The wizard does not delete the site configuration object from the Administration Service. This allows you to set up new Web Interface sites later even with the configuration of the deleted site.

Exporting the configuration of a Web Interface site to a file

You can export the configuration object of an existing Web Interface site with the **Web Interface** > **Export Configuration** option of the Configuration Center. This opens the **Export Web Interface Site Configuration** wizard, allowing you to save the configuration of the site from the Administration Service into an `*.xml` file with the specified name to the specified location.

TIP: Use this option to back up the configuration of existing Web Interface sites, then use them as a baseline for creating additional Web Interface sites in your organization.

Delegating user access to the Active Roles Console

By default, after installing Active Roles, every user can log in to the Active Roles Console (also known as the MMC Interface). To restrict user access to the Console, in the Configuration Center, use the **MMC Interface Access** > **Modify** menu, then select the **Restrict Console (MMC Interface) access for all users** option.

Doing so restricts all non-Active Roles Admin users from using the Active Roles Console.

> TIP: You can give Active Roles Console access later to selected users with the **User Interface Management - MMC Full control** Access Template (AT) of the Active Roles Console. This AT gives access permission to the **Server Configuration** > **User Interfaces** > **MMC Interface** object.
>
> For more information on how to use ATs, see *Applying Access Templates* in the *Active Roles Administration Guide*.

Configuring Active Roles logging settings

The Active Roles Configuration Center also allows you to manage the logging settings of the various Active Roles components. As part of this, you can:

- Enable or disable logging for each Active Roles component.
- Open the location of the various component log files.
- Open the component logs directly in the Active Roles Log Viewer utility.

To view, configure and manage Active Roles logs, in the Configuration Center, navigate to the **Logging** page. Once opened, the page lists the following information:

- **Component**: The name of the Active Roles component producing the log, such as the Administration Service or the Active Roles Console.
- **Logging**: Indicates whether logging is enabled or disabled for the component, and shows the logging level (**Basic** or **Verbose**). While **Basic** logging includes only errors, warnings and informational messages in the log files, **Verbose** logging also adds debugging and tracing messages.
- **Log location**: Indicates the full path of the log file.

The toolbar of the **Logging** page allows you to perform the following log management tasks:

- To enable or disable logging for a component, or change the logging level, select the component in the list, then click **Modify**.
- To open the folder that contains the log file(s) of a component, select the component in the list, then click **Browse with Explorer**.
- To open the Administration Service log in the Active Roles Log Viewer utility, select Administration Service in the list of components, then click **Open in Log Viewer**. For more information, see Active Roles Log Viewer.

Configuring Solution Intelligence

You can enable or disable **Solution Intelligence** in the Active Roles Configuration Center for your Web Interface sites. Solution Intelligence is an optional Active Roles feature used by One Identity to gather standard telemetry data about your Active Roles deployment, containing load, performance and usage metrics, exception reports, and other diagnostic information used to improve Active Roles.

Solution Intelligence is disabled by default.

Active Roles Configuration Shell

The **ActiveRolesConfiguration** module (also known as the "Configuration Shell") provides cmdlets for configuring Active Roles Administration Service instances and Web Interface sites. The names of the cmdlets provided by this module start with the `AR` prefix, such as `New-ARDatabase`, `New-ARService`, or `New-ARWebSite`.

NOTE: Consider the following when planning to use the **ActiveRolesConfiguration** module:

- This module is available on 64-bit operating systems only.
- You can only install this module on computers where the Administration Service or Web Interface modules are also installed. Otherwise, the module will not provide all cmdlets.

The following table lists the cmdlets of the Configuration Shell.

Table 1: Configuration Shell Cmdlets

Command	Description
Get-ARComponentStatus	Returns the installation and configuration status of the Active Roles components.
New-ARDatabase	Creates a new Active Roles database.
Import-ARDatabase	Transfers Active Roles configuration data or management history data from one database to another.
Backup-AREncryptionKey	Backs up the current encryption key of the configuration database in the local Administration Service instance into a file.
Restore-AREncryptionKey	Restores the configuration database encryption key from a backup file to the local Administration Service instance.
Reset-AREncryptionKey	Creates a new encryption key for the configuration database in the local Administration Service instance.
New-ARService	Creates the Active Roles Administration Service instance

Command	Description
	on the local computer.
Get-ARService	Gets the status of the Active Roles Administration Service instance from the local computer.
Set-ARService	Modifies the Active Roles Administration Service instance on the local computer.
Start-ARService	Starts the Active Roles Administration Service instance on the local computer.
Stop-ARService	Stops the Active Roles Administration Service instance on the local computer.
Restart-ARService	Stops and starts the Active Roles Administration Service instance on the local computer.
Remove-ARService	Deletes the Active Roles Administration Service instance from the local computer.
Test-ARServiceDatabaseSettings	Verifies whether the specified Active Roles database settings would cause Management History issues due to setting separate Configuration and Management History databases.
Get-ARServiceStatus	Gets the Active Roles Administration Service status information from the local computer.
Get-ARVersion	Gets the version of the local Active Roles installation.
New-ARWebSite	Creates a new Active Roles Web Interface site.
Get-ARWebSite	Gets the Active Roles Web Interface sites from the web server.
Set-ARWebSite	Modifies the specified Active Roles Web Interface site on the web server.
Remove-ARWebSite	Deletes the specified Active Roles Web Interface site from the web server.
Get-ARWebSiteConfig	Gets Web Interface site configuration objects from the Active Roles Administration Service.
Export-ARWebSiteConfig	Exports the specified Web Interface site configuration to a file.

Active Roles Log Viewer

The Active Roles Log Viewer tool allows you to browse and analyze:

- Diagnostic log files created by the Active Roles Administration Service.
- Event log files created by saving the Active Roles event logs in the Windows Event Viewer on the computer running the Administration Service.

The Log Viewer tool can help you to:

- Check the sequence or hierarchy of requests processed by the Administration Service.
- Identify error conditions that the Administration Service encountered during request processing.
- Find Knowledge Base (KB) Articles for specific log messages and errors.

You can open Active Roles diagnostic log files (`ds.log`) or saved event log files (`*.evtx`) with the Log Viewer tool, allowing you to check:

- The errors encountered by the Administration Service and recorded in the log file.
- Requests processed by the Administration Service and traced in the log file.
- All trace records found in the diagnostic log file.
- All events found in the event log file.

When you select an error from the list, you can also look for applicable One Identity KB Articles to learn more about the log entry or troubleshoot selected errors.

In addition, the Active Roles Log Viewer tool also allows you to:

- Search in the loaded log file for a particular text string, such as an error message.
- Filter the list by various conditions to narrow the listed items to those you are actually interested in.
- View detailed information about each list item, such as error details, request details or stack trace.

Getting started

To start using Active Roles Log Viewer, see the following resources:

- For more information on how to install Active Roles Log Viewer, see *Steps to install Diagnostic Tools* in the *Active Roles Quick Start Guide*.
- For more information on using Active Roles Log Viewer, see *Using the Log Viewer tool* in the *Active Roles Administration Guide*.

Voluntary threshold for managed object count

By default, Active Roles does not limit the number of managed objects you can manage. However, as the license fee is based on the managed object count, you may need to verify

that the object count stays under a certain threshold. To do so, you must specify a threshold value for the number of managed objects.

Once you configure this voluntary threshold, the scheduled task that counts the managed objects will raise an alert whenever it detects that the current number of managed objects exceeds the configured threshold value. Active Roles will indicate this alert in the **Product Usage Statistics** page of the Active Roles Console, and can also send a notification over email.

Getting started

For more information on how to configure the threshold, see *Voluntary thresholds for the managed object count* in the *Active Roles Administration Guide*.

Installation label

To identify your Active Roles installation in the Managed Object Statistics report, you can set a label for your deployment in the Active Roles Console.

This is useful, for example, if you have several Active Roles deployments installed in your organization (for example, separate pilot, non-production and production environments) and you want to easily distinguish them visually.

Once configured, the installation label appears in the title of the Managed Object Statistics report.

Getting started

For more information on how to configure an installation label for Active Roles, see *Installation label* in the *Active Roles Administration Guide*.

Safe mode

Active Roles provides a troubleshooting mode called "Safe mode" that starts Administration Service in a limited state.

When you enable Safe mode, Administration Service:

- Disregards all custom policies, workflows, scripts, scheduled tasks and other custom-made assets that may prevent Active Roles from starting and operating normally.
- Rejects connections from any users that do not have Active Roles Admin privileges.

While Safe mode is active, only Active Roles Admins can connect to Administration Service, so that they can troubleshoot problems by changing the existing Active Roles configuration or removing any customizations that could cause issues. Once troubleshooting is finished, Active Roles Admins can also turn off Safe mode and resume normal Active Roles operation.

Getting started

You can enable Safe mode from the Active Roles Management Shell.

To enable or disable Safe mode

1. On the computer running the Active Roles Administration Service, log in with a user account that has administrator rights on the computer.

   NOTE: You can enable or disable Safe mode only with a user account that has local administrator rights on the computer running Administration Service.

2. Start the Active Roles Management Shell from the Windows Start menu or the Apps page of the operating system.
3. To enable safe mode, enter the following commands in the Management Shell command-line interface:

   ```
   Set-ARService -SafeModeEnabled $true
   ```

   ```
   Restart-ARService
   ```

4. To enable safe mode, enter the following commands in the Management Shell command-line interface:

   ```
   Set-ARService -SafeModeEnabled $false
   ```

   ```
   Restart-ARService
   ```

5

FIPS compliance

Active Roles 8.0.1 LTS supports cryptography libraries and algorithms compliant with Federal Information Processing Standards (FIPS) 140-2. For more information on FIPS-compliant libraries and algorithms, see FIPS 140-2: Security Requirements for Cryptographic Modules.

NOTE: Consider the following when planning to use FIPS-compliant cryptography libraries or algorithms:

- Although Active Roles continues to support non-FIPS compliant cryptography libraries and algorithms, it will not work properly if it is configured to use non-FIPS compliant solutions in a FIPS-compliant environment.
- If you already use FIPS-compliant security algorithms in your environment (such as the TripleDES security algorithm, or the SHA256 hash algorithm), you must export your existing configuration, and import it in a new Active Roles installation.

LSA protection support

The Active Roles Synchronization Service Capture Agent supports Local Security Authority (LSA). For more information, see Configuring Additional LSA Protection in the *Microsoft Windows Server documentation*.

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