One Identity Active Roles 7.3

Feature Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Active Roles Feature Guide
Updated - May 2019
Version - 7.3

Contents

1

Introduction

This document provides an overview of the Active Roles (formerly known as ActiveRoles®) features.

Each feature is presented in a separate section containing the following elements:

- **Feature Name** The title of the section.
- **Description** An explanation of the feature.
- **How to Start** Instructions on how to find or start using the feature (if applicable).

Unless otherwise noted, the **How to Start** instructions assume that you are logged on as an Active Roles Admin. By default, an Active Roles Admin is any member of the Administrators local group on the computer running the Active Roles Administration Service. Additionally, you should verify that the Active Roles console is in Advanced view mode: on the **View** menu, click **Mode**, and then click **Advanced Mode**.

NOTE: For information on the Active Roles 7.3 features see the *Active Roles What's New Guide*.

Implementing Rules and Roles

This section provides an overview of features and enhancements relating to Active Roles' workflow capabilities, policies (administrative rules) and delegation model (administrative roles).

Synchronization Service

Identity information can be stored in various data systems, such as directories, databases, or even formatted text files. Management and synchronization of identity information among different data systems may require considerable time and effort. On top of that, performing data synchronization tasks manually is error-prone and can lead to duplication of information and incompatibility of data formats.

With Synchronization Service, you can automate 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, thereby reducing administrative workload and getting the new users up and running faster.

The use of scripting capabilities provides 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 administrators to concentrate on strategic issues, such as planning the directory, increasing enterprise security, and supporting business-critical applications.

Synchronization Service offers the following major features.

Bidirectional synchronization

Bidirectional synchronization allows you to synchronize all changes to identity information between your data systems. Using this type of synchronization, you can prevent potential

identity information conflicts between different data sources. Note that bidirectional synchronization is unavailable for some of the supported data systems.

Delta processing mode

Delta processing mode allows you to synchronize identities more quickly by processing only the data that has changed in the source and target connected systems since their last synchronization. Both the full mode and the delta mode provide you with the flexibility of choosing the appropriate method for your synchronization tasks. Note that delta processing mode is unavailable for some of the supported data systems.

Synchronization of group membership

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

Windows PowerShell scripting

Synchronization Service includes a Windows PowerShell based scripting Shell for data synchronization. The Shell is implemented as a Windows PowerShell module, allowing administrators to automate synchronization tasks by using PowerShell scripts.

Attribute synchronization rules

With Synchronization Service, you can create and configure synchronization rules to generate values of target object attributes. These rules support the following types of synchronization:

- **Direct synchronization** Assigns the value of a source object attribute to the target object attribute you specify.
- **Script-based synchronization** Allows you to use a Windows PowerShell script to generate the target object attribute value.
- **Rule-based synchronization** Allows you to create and use 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 Name (DN) for objects being created. These rules allow you to ensure that created objects are named in full compliance with the naming conventions existing in your organization.

Scheduling capabilities

You can schedule the execution of data synchronization tasks and automatically perform them on a regular basis to satisfy your company's policy and save your time and effort.

Extensibility

To access external data systems, Synchronization Service employs so-called *connectors*. A connector enables Synchronization Service to read and synchronize the identity data contained in a particular data system. Out of the box, Synchronization Service includes connectors that allow you to connect to the following data systems:

- Microsoft Active Directory Domain Services
- Microsoft Active Directory Lightweight Directory Services
- Microsoft Exchange Server
- Microsoft Skype for Business Server
- Microsoft Windows Azure Active Directory
- Microsoft Office 365
- Microsoft SQL Server
- Microsoft SharePoint
- Active Roles version 7.3, 7.2, 7.1, 7.0, and 6.9
- One Identity Manager version 6.1 or 6.0
- Data sources accessible through an OLE DB provider
- Delimited text files

How to start

For instructions on how to install, configure and user Synchronization Service, see the Synchronization Service Administration Guide document for Active Roles 7.3.

Exchange Resource Forest Management

Active Roles now includes a mailbox management solution—Exchange Resource Forest Management—to provision users with Exchange mailboxes in environments where mailbox server are deployed in a dedicated Active Directory forest while logon-enabled user accounts are defined in a different forest.

Exchange Resource Forest Management extends the mailbox management capabilities of Active Roles in the case of resource forest topology. This topology option assumes that you have:

- At least one Active Directory forest containing logon-enabled user accounts for your organization, referred to as an accounts forest. The accounts forest does not have Exchange Server installed, nor does it need to have the Active Directory schema extended with the Exchange Server attributes.
- An Active Directory forest with Exchange Server, referred to as the Exchange forest, to hold mailboxes for user accounts from the accounts forest.
- Trust relationships configured so that the Exchange forest trusts the accounts forest.

With Exchange Resource Forest Management, you can use Active Roles to:

- Create a mailbox for a user account from the accounts forest.

  You can create a mailbox when creating a user account in the accounts forest. It is also possible to create a mailbox for a user account that already exists in the accounts forest. As a result, Active Roles creates a disabled user account (shadow account) with a linked mailbox in the Exchange forest, and associates the shadow account and the mailbox with the user account (master account) held in the accounts forest.

- View or change mailbox properties, and perform Exchange tasks, on a user account from the accounts forest (master account) that has a linked mailbox in the Exchange forest.

  The pages for managing the master account include all Exchange properties and tasks that are normally available when the mailbox resides in the same forest as the managed user account. With Exchange Resource Forest Management, Active Roles synchronizes the Exchange properties displayed or changed on the pages for managing the master account with the properties of the linked mailbox.

- View or change the personal or organization-related properties of the master account while having them synchronized to the respective properties of the shadow account.

  When you use Active Roles to change the personal or organization-related properties of the master account, Exchange Resource Forest Management causes Active Roles to apply the changes to those properties of the shadow account as well. This function ensures correct information about the master account in the Exchange address lists.

- Deprovision a master account while having Active Roles deprovision the master account's mailbox in the Exchange forest.

When you deprovision a master account, Exchange Resource Forest Management causes Active Roles to apply the deprovisioning policies to both the master account and shadow account. As a result, Active Roles makes all the necessary changes to deprovision the mailbox. You can revert these changes by undeprovisioning the master account.

- Delegate Exchange mailbox management tasks by applying Access Templates to containers that hold master accounts.

  For example, you can apply the "Exchange - Recipients Full Control" Access Template to a container in the accounts forest, which enables the delegated administrator to create, view or change linked mailboxes in the Exchange forest by managing master accounts held in that container.

- Enable a master account to update membership list of a distribution group held in the Exchange forest.

  When you make a shadow account the manager or a secondary owner of a distribution group and allow the manager or secondary owners to update membership list, Exchange Resource Forest Management ensures that the corresponding master account has sufficient rights to add or remove members from that group using Exchange clients such as Microsoft Outlook or Outlook Web App.

Exchange Resource Forest Management also enables Active Roles to provide all these administrative capabilities for linked mailboxes created by Active Roles with an earlier version of Exchange Resource Forest Management or without Exchange Resource Forest Management, or created by tools other than Active Roles. Exchange Resource Forest Management schedules Active Roles to search the managed domains for linked mailboxes whose master account:

- Is in the scope of the Exchange Resource Forest Management policy for mailbox management
- Does not have a reference to the shadow account expected by Exchange Resource Forest Management

For each master account that meets these conditions, Active Roles updates the master account with a reference to the shadow account, thereby extending the capabilities of Exchange Resource Forest Management to that master account and its linked mailbox. As a result, the linked mailbox falls under the control of Exchange Resource Forest Management.

How to start

For instructions on how to install, configure and user Exchange Resource Forest Management, see the Exchange Resource Forest Management Administration Guide document for Active Roles 7.3.

Skype for Business Server User Management

Active Roles now includes a user management solution—Skype for Business Server User Management—to provision Skype for Business Server user accounts in Active Directory environments with a single forest or multiple forests.

The Skype for Business Server User Management solution enables Active Roles to administer Skype for Business Server user accounts. This solution provides built-in policies that synchronize user account information between Active Roles and Skype for Business Server, allowing Skype for Business Server user management tasks to be performed using the Active Roles Web Interface.

With Skype for Business Server User Management, you can use Active Roles to perform the following tasks:

- Add and enable new Skype for Business Server 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

Skype for Business Server User Management adds the following elements to Active Roles:

- Built-in Policy Object containing a policy that enables Active Roles to perform user management tasks on Skype for Business Server.
- Built-in Policy Object containing a supplementary policy that enables Active Roles to administer Skype for Business Server users in environments that involve multiple Active Directory forests.
- Commands and pages for managing Skype for Business Server users in the Active Roles Web Interface.
- Access Templates 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 Skype for Business Server user creation and administration:

- Rule for generating the SIP user name. 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.
- Rule for selecting a SIP domain. 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.
- Rule for selecting a Telephony option. When configuring Telephony for a Skype for Business Server user, Active Roles can restrict the list of selectable Telephony options and suggest which option to select by default.

- Rule for selecting a Skype for Business Server pool. 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 selection of 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 Access Templates 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

Supported Active Directory topologies

Skype for Business Server User Management supports the same Active Directory Domain Services (AD DS) topologies as Microsoft Lync 2013. The following topologies are supported:

- Single forest with a single tree or multiple trees
- Multiple forests in a resource forest topology
- Multiple forests in a central forest topology

Single forest

The single forest topology assumes that the logon-enabled user accounts managed by Active Roles are defined in the Active Directory forest in which Skype for Business Server is deployed. To perform Skype for Business Server user management tasks on a given user account, Active Roles makes changes to the attributes of that use account, and then, based on the attribute changes, the Skype for Business Server User Management policy requests the Skype for Business Server remote shell to update the user account accordingly. For example, when creating a new Skype for Business Server user, Active Roles sets a virtual attribute on that user's account directing the policy to invoke the remote shell command for enabling the new user for Skype for Business Server. When making changes to an existing Skype for Business Server user, Active Roles populates the attributes of the user's account with the desired changes, causing the policy to apply those changes via the remote shell.

Multiple forests - Resource forest

The resource forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server but does not host any logon-enabled user accounts. Outside the Skype for Business Server forest, user forests host logon-enabled user accounts but no servers running Skype for Business Server. When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a disabled user account in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the disabled user account in the Skype for Business Server forest (shadow account), and enables the shadow account for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the shadow account are synchronized with the attributes of the master account, so that Skype for Business Server user properties can be administered on the master account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the master account to the shadow account, and translates them to remote shell commands on Skype for Business Server, similarly to the Single forest case.

Multiple forests - Central forest

The central forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server and may also host logon-enabled accounts. Outside the Skype for Business Server forest, user forests host logon-enabled user accounts but no servers running Skype for Business Server.

With the Skype for Business Server User Management policy applied to logon-enabled user accounts in the Skype for Business Server forest, Active Roles can enable and administer those user accounts for Skype for Business Server in the same way as in the Single forest case.

When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a contact in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the contact in the Skype for Business Server forest (shadow account), and enables that contact for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the contact are synchronized with the attributes of the user account, so that Skype for Business Server user properties can be administered on the user account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the user account to the contact, and translates them to remote shell commands on Skype for Business Server, similarly to the Single forest case.

How to start

For instructions on how to install, configure and user Skype for Business Server User Management, see the Skype for Business Server User Management Administration Guide document for Active Roles 7.3.

New workflow activity: Save Object Properties

Save Object Properties activity is intended to save properties of a particular object at workflow execution time. The properties are saved in the workflow data context, and can be retrieved by other activities before or after the object has changed. This capability is instrumental in situations that require knowing not only the changed object state or properties but also the previous or old values of certain properties. Old values may be required to determine the previous state of an object in order to make some decision or perform a certain action based on those values. For example, to notify of object deletions, you can create a workflow that starts when deletion of an object is requested, saves the object's name, and then, after the object is deleted, sends a notification message that includes the saved name of the deleted object.

This activity has the following configuration options:

- **Activity target** This option lets you specify the object whose properties you want the activity to save. You can choose to specify:
  - **Workflow target object** In a change workflow, the target object of the request that started the workflow. For example, in a workflow that starts upon a deletion request, this choice causes the activity to save the properties of the object whose deletion is requested.
  - **Fixed object in directory** A particular object you select from Active Directory.
  - **Object identified by workflow parameter** The object specified by the value of a certain parameter of the workflow. You can choose the desired parameter from the workflow definition.
  - **Object from workflow data context** The object will be selected by the activity on the basis of the data found in the workflow environment at the time of executing the workflow. You can specify which object you want the activity to select at workflow execution time.
  - **Object identified by DN-value rule expression** The object whose Distinguished Name (DN) is specified by 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 environment at the time of executing the workflow. You can create the desired rule expression when you configure the activity.
- **Target properties** This option lets you specify the object properties you want the activity to save. The workflow designer proposes the default list of properties, and allows you to change the list as needed. By default, the activity saves all single-value non-constructed attributes found in the directory schema for the target object, including custom virtual attributes added to the directory schema by Active Roles.
- **Notification** You can configure the activity to subscribe recipients to the notifications of the following events:

- **Activity completed successfully** When configured to notify of this event, the activity causes Active Roles to send a notification e-mail if no significant errors occurred during execution of this activity.
- **Activity encountered an error** When configured to notify of this event, the activity causes Active Roles to send a notification e-mail if any significant errors occurred during execution of this activity.

The notification settings specify the event to notify of, and notification recipients. When executed by the workflow, the activity prepares a notification message appropriate to the specified event. Active Roles retains the message prepared by the activity, and sends the message to the specified recipients upon occurrence of that event.

- **Error handling** You can choose whether to suppress errors encountered by the activity. The following option is available: **Continue workflow even if this activity encounters an error**. If this option is not selected (default setting), then an error condition encountered by the activity causes Active Roles to terminate the workflow. If you select this option, the workflow continues regardless of whether or not the encounters an error condition.

Retrieving saved properties

In a workflow that includes an activity of the Save Object Properties type, you can configure other activities to retrieve object properties saved by that activity:

- By using the following expression in a Script activity:
  `$workflow.SavedObjectProperties("activityName").get("attributeName")`

  In this expression, `activityName` stands for the name of the Save Object Properties activity and `attributeName` is the LDAP display name of the attribute representing the property you want the script to retrieve. You should specify an attribute listed in the **Target properties** setting of the "Save Object Properties" activity; otherwise, this expression returns no property value at workflow execution time.
- By adding the **Workflow - Saved Object Properties** token to the notification message template.

  To add the token:

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

     You should select a property listed in the **Target properties** setting of the Save Object Properties activity; otherwise, the token you have configured returns no property value at workflow execution time.
- By choosing the **Property of object from workflow data context** configuration option, available in If-Else branch conditions, Search filter, "Create" activity,

"Update" activity, and Add Report Section activity.

If you choose this option, then you need to perform the following configuration steps:

1. In the **Object Property** dialog box, click the link in the **Target object** field, and then click **More choices**.
2. In the dialog box that appears, click **Saved Object Properties** in the left pane, select the name of the Save Object Properties activity from the **Activity** list, and then click **OK**.
3. In the **Object Property** dialog box, click the link in the **Target property** field, and select the property you want.

   You should select a property listed in the **Target properties** setting of the Save Object Properties activity; otherwise, the entry you have configured returns no property value at workflow execution time.

How to start

For configuration instructions, see the "Configuring a Save Object Properties activity" section in the Active Roles 7.3 Administration Guide.

New workflow activity: Modify Requested Changes

Modify Requested Change activity is intended to update the change request that started the workflow, allowing you to add or remove changes to the properties of the workflow target object at workflow execution time. For example, in a workflow that starts when creation of an object is requested, you can use this activity to modify the properties that are going to be assigned to the new object, or change the container in which to create the object. In a workflow that starts upon a request to change an object, you can use this activity to modify the requested changes to the properties of that object.

This activity has the following configuration options:

- **Target changes** You can define the property changes to add or remove from the change request. When you configure this activity, you can choose the properties you want the activity to change and, for each property, choose to remove the property from the request, clear the property value in the request, or specify the new value to be assigned to that property. For a multi-value property, you can choose to add or remove a value from that property. The following options are available:
- **Text string** Use the given string of characters as the value of the property. You can type the desired string.
- **Property of workflow target object** Use the value of a certain property of the target object of the request that started the workflow. You can select the desired property from a list of object properties.

- **Property of workflow initiator** Use the value of a certain property of the user whose request started the workflow. You can select the desired property from a list of object properties.
- **Changed value of workflow target object property** Use the value that is requested to be assigned to a certain property of the workflow target object. You can select the desired property from a list of object properties.
- **Workflow parameter value** Use the value of a certain parameter of the workflow. You can choose the desired parameter from a list of the workflow parameters.
- **Property of object from workflow data context** Use the value of a certain property of the object that will be 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 at workflow run time.
- **Value generated by rule expression** Use 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 run-time environment. You can create the desired rule expression when you configure the activity.
- **Notification** You can configure the activity to subscribe recipients to the notifications of the following events:
    - **Activity completed successfully** When configured to notify of this event, the activity causes Active Roles to send a notification e-mail if no significant errors occurred during execution of this activity.
    - **Activity encountered an error** When configured to notify of this event, the activity causes Active Roles to send a notification e-mail if any significant errors occurred during execution of this activity.

  The notification settings specify the event to notify of, and notification recipients. When executed by the workflow, the activity prepares a notification message appropriate to the specified event. Active Roles retains the message prepared by the activity, and sends the message to the specified recipients upon occurrence of that event. The notification settings are similar to the notification settings of a Notification activity.
- **Error handling** You can choose whether to suppress errors encountered by the activity. The following option is available: **Continue workflow even if this activity encounters an error**. If this option is not selected (default setting), then an error condition encountered by the activity causes Active Roles to terminate the workflow. If you select this option, the workflow continues regardless of whether or not the encounters an error condition.
- **Additional settings** You can configure the activity to:
    - Change the container where to create new objects while ensuring that the policies and workflows are applied from the container where the object will actually be created rather than from the container that was originally specified in the object creation request.
    - Add or remove Active Roles controls from the request.

Controls are certain pieces of data that can be used to provide additional information to Active Roles on how to process the request. If no controls are added to a request, then Active Roles determines how to process the request based solely on the type of the request. You can 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 information about Active Roles controls, see Active Roles SDK.

NOTE: The Modify Requested Changes activity type is unavailable in case of an automation workflow. You can add activities of this type to a change workflow only.

How to start

For configuration instructions, see the "Configuring a Modify Requested Changes activity" section in the Active Roles 7.3 Administration Guide.

New workflow feature: Initialization script

When executing a workflow instance, Active Roles uses a single PowerShell operating environment, referred to as a runspace, for all script activities held in that workflow. The workflow run-time engine creates a runspace once the workflow instance has been started, and maintains the runspace during the execution of the workflow instance.

When you configure a workflow, you can specify PowerShell commands you want the workflow run-time engine to execute immediately after the runspace creation. These commands constitute the initialization script that the workflow engine runs prior to performing script activities.

With an initialization script, you can define runspace configuration data separately from the logic of the script activities and use it to initialize the environment for executing 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 run time. 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 script 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 run time. 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 that is defined in the initialization script, the activity script must use the `$global:` qualifier, such as `$global:rGuid`.

When execution of the workflow instance is suspended (for example, waiting for approval), and then resumed (for example, after receiving an approval decision), the runspace is reinitialized so the global variables may change. If you need to preserve the value of a global variable, add the `[Persist()]` attribute to the variable's name in the initialization script, such as `[Persist()]$rGuid = [Guid]::NewGuid()`. The global variables defined in this way are saved to a persistent storage upon suspending the workflow instance and 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 signified by that 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.

How to start

1. In the Active Roles console tree, expand **Configuration | Policies | Workflow**, and select the workflow you want to configure.

   This opens the Workflow Designer window in the details pane, representing the workflow definition as a process diagram.

2. In the details pane, click the **Workflow options and start conditions** button to expand the area above the process diagram, and then click the **Configure** button.
3. Click the **Initialization script** tab in the dialog box that opens.

The **Initialization script** tab displays the current script. You can add or modify the script by typing in the edit box on that tab.

Search for user accounts that are about to expire

In an Active Roles workflow, a Search activity allows you to perform searches against directory data to find objects, such as users or groups, that match the criteria you specify based on object properties and pass those objects to other activities so that the workflow can perform the appropriate actions on them. Search options have been extended to enable the activity to search for user account that will expire within a certain number of days.

How to start

When configuring a Search activity to search for users, click the option **Retrieve only expiring user accounts** to restrict your search to user accounts that will expire within a certain number of days. In the dialog box that opens, specify the desired number of days.

Plain-text notification messages

In an Active Roles workflow, notification messages are based on a message template that determines the format and contents of an e-mail notification message, including the message subject and body. Notification messages are created, and normally sent, in HTML format. You can now configure the Notification or Approval activity to format and send notification messages as plain text. This option may be helpful in integration solutions that use mail flow for data exchange between Active Roles and other solution components.

How to start

When configuring notification message settings for a Notification activity or an Approval activity, select the **Format notification message as plain text** check box on the **Notification Message** page.

3

Using Active Roles

This section summarizes the features and enhancements that improve the user experience of those who use Active Roles to perform day-to-day administrative tasks.

Web Interface redesigned

The Active Roles Web Interface is a highly customizable Web application that provides administrative coverage for all aspects of Active Directory data management. In the new version, the Web Interface has been redesigned for greater clarity and ease of use, to ensure consistent look and feel, and to improve user experience by adding new navigation options, optimizing search pages, and enhancing the point-and-click interface for creating and reusing search conditions. Also, steps have been taken to decrease response time and improve performance of the Web Interface.

The brand-new user experience simplifies and streamlines the management tasks in the Web Interface. Key highlights include:

- **Single-page lists** You no longer need to page through search results. All results are now listed on a single page. The single-page list starts displaying search results much faster, and makes it easier to sort, filter, locate and select the objects you want to find.
- **Enhanced search tools** Unified toolbar for configuring search conditions or filter conditions 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** Pages for creating, viewing or changing objects are now displayed on top of the list of objects, which allows you not to lose the entire list while selecting and managing individual objects.
- **Views** You can create, save and reuse your personal views of containers. Each view is essentially a search query for objects held in a particular container that returns the list of objects matching the specified search conditions, with the specified set of list columns and list sorting order.

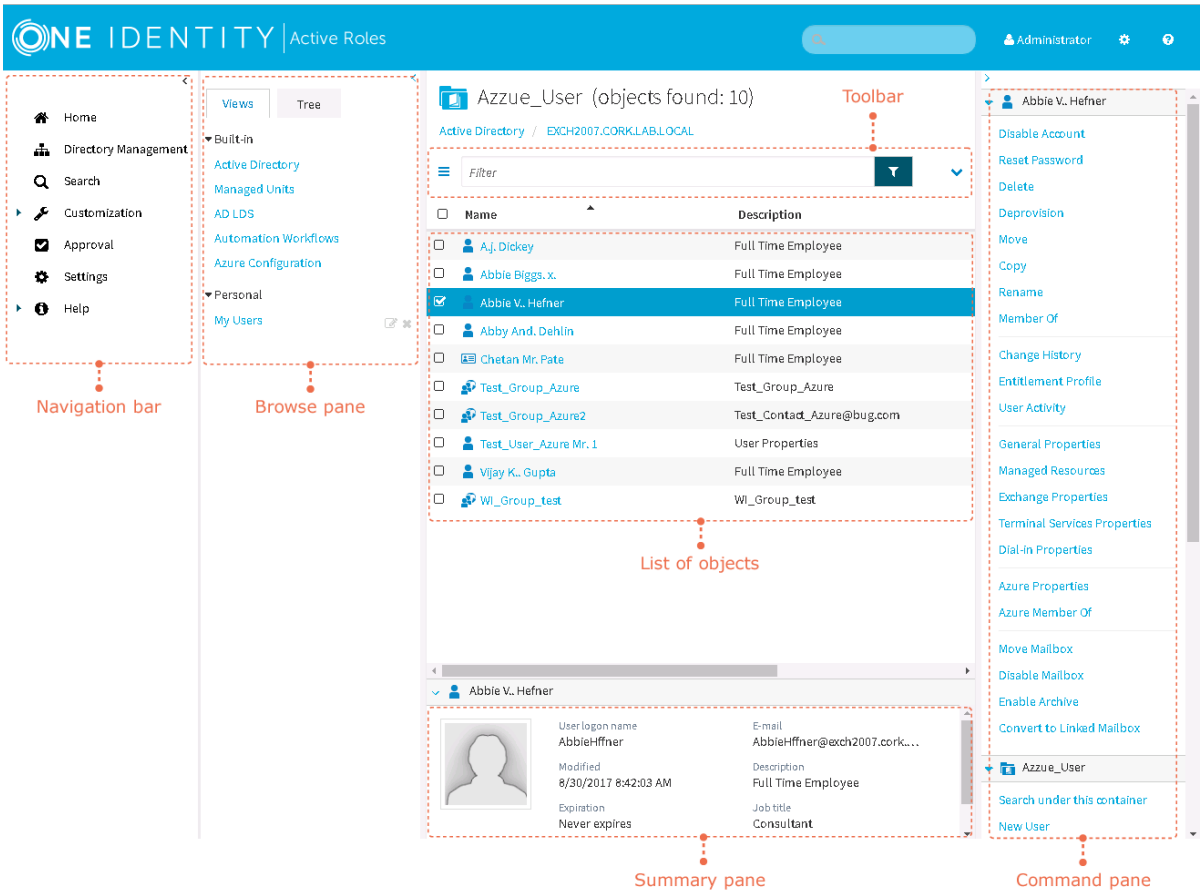
The new Web Interface retains and improves upon all the enterprise-class features of its predecessor, including individually customizable Web Interface sites, user permission-

based view of the Web Interface pages, and support for self-administration. It combines an attractive design with superior flexibility and many advanced features. The result is a solution that can be tailored for any category of administrative personnel, whether day-to-day administrators, business data owners, help desk operators, or even regular end-users.

The Web Interface is now easier to navigate. It features simplified layout and large UI elements. Most of UI areas can be resized, collapsed or expanded. This allows you to adapt your workspace on UI to your needs.

The main UI elements include the Header area at the top of the page; the Navigation bar and the Browse pane (Views/Tree) on the left side; the list of objects next to the Browse pane; the Command pane on the right side; and the Summary pane under the list of objects, as shown in the figure that follows.

Figure 1: UI Elements



Navigation bar

Located on the left side of the page, the Navigation bar provides the first level of navigation for most of the tasks you can perform in the Web Interface. The Navigation bar is organized by Web Interface areas, and includes the following items:

- **Home** Go to the Web Interface home page.
- **Directory Management** Browse for, and administer, directory objects in your organization.
- **Search** Search for, and administer, directory objects in your organization.
- **Customization** Customize Web Interface pages. Available to Active Roles Admin only.
- **Approval** Perform the tasks relating to approval of administrative operations.
- **Settings** View or change your personal settings that control the display of the Web Interface.

Browse pane

Located next to the Navigation bar, the Browse pane lists the built-in views and personal views, and allows you to access the tree view:

- Built-in views provide entry points to browsing for objects in the directory. Personal views are filter or search queries you build and save to use them again at a later time.
- The tree view helps you browse for directory objects by using the directory tree to navigate through the hierarchical structure of containers.

List of objects

When you select a container or view in the Browse pane, you'll see a list of objects. If you select a container, 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 list of objects is no longer divided into multiple pages. Instead, the Web Interface now loads all objects on a single page. This allows you to see the entire contents of an OU or all results of a search operation at a time.

You can use various built-in conditions or create custom conditions to filter the list of objects. It is also possible to customize the list by sorting and filtering, and by adding or removing list columns.

You can select objects from the list and apply commands to the selected object or objects. When you click the name of a container object, such as a domain or an organizational unit, the list changes to display the objects held in that container, thereby enabling you to browse through containers in the directory.

Toolbar

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

- Click the Menu button on the left side of the Toolbar to save the current list as a personal view, add or remove list columns, or export the list to a text file.
- Type in the Filter field and then click the button next to that field to have the list include only those objects whose naming properties match what you typed.
- Click the Expand/Collapse button on the right side of the Toolbar to configure filtering criteria based on object properties. To have the list include only the objects that match your filtering criteria, click the button next to the Filter field.

Command pane

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

- If no objects are selected in the list, the menu 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 commands that apply to the selected object are added in the top of the menu, under a heading that shows the name of the selected object.
- If multiple objects are selected from the list, the commands that apply to all of the selected objects are added in the top of the menu, under a heading that shows the number of the selected objects.

Summary pane

When you select an object from the list, information about that object is displayed in the Summary pane under the list of objects. The information includes some commonly used properties of the object, and depends upon the object type. For example, user properties provide more detailed information about a user account, such as the logon name, e-mail address, description, job title, department, expiration date, and the date and time that the account was last changed. If you don’t see the Summary pane, click in the area beneath the list of objects.

Personal views

Personal views is a new feature of the Web Interface. Each view displays a filter-based list of objects held in a given OU or container, or a list of search results. You can search a container or filter the contents of a container using search conditions or filter conditions as needed, and then save the resulting search or filter query as your personal view. The view displays the list of objects that match the specified conditions, with the specified list sorting order and set of list columns. Personal views are stored on a per-user basis, so each end-user can have his own views.

Locating directory objects in the Web Interface

The Web Interface provides search and filtering tools to help you locate directory objects quickly and easily. By creating and applying an appropriate search or filter query, you can build shorter lists of objects, 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 and the sort order in the list of search or filtering results.

Searching for directory objects

To search for directory objects, you can 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 searches in the container you select and in all of its 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, and then press Enter or click the magnifying glass icon in the Search field. In this case, the Web Interface searches all managed Active Directory domains for objects whose naming properties match what you typed and the **Search** page lists the search results. The naming properties include name, first name, last name, display name, and logon name.
- Click **Search** on the Navigation bar. The **Search** page opens, allowing you to configure and start a search.

To configure and start a search

1. Click the **Search in** box on the Toolbar, and then select the container that you want to search. You can select more than one container.

   The Web Interface will search in the selected container and all of its subcontainers.

2. Specify criteria for the objects that you want to find:

- To search by naming properties, type in the Search field on the Toolbar. The Web Interface will search for objects whose naming properties match what you typed. The naming properties include name, first name, last name, display name, and logon name.
- To search by other properties, click the button on the right side of the Toolbar to expand the Toolbar, click **Add criteria**, choose the properties by which you want to search, click **Add**, and then configure the criteria as appropriate. The Web Interface will search for objects that match the criteria that you configured.

3. Press Enter to start the search.

   The search results are listed on the **Search** page. 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 the Menu button on the left side of the Toolbar and then click **Choose columns**. To sort the list by column data, click column headings.

Example: Searching by object type

The following steps demonstrate how you can use the search function to list all groups that exist in the Active Directory domains managed by Active Roles:

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

Filtering the contents of a container

If a container, such as an organizational unit in your Active Directory, holds large number of objects, you can narrow down the displayed list of objects by filtering the objects held in that specific container.

To filter the objects held in a container

1. Navigate to the container in the Web Interface.

   To navigate to a container, you can search for the container object (see Searching for directory objects) and then click its name in the list of search results on the **Search** page. Alternatively, you can browse for the container objects by using the Browse pane and the List of objects.

IMPORTANT: 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 held 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 then configure and perform a search as described in Searching for directory objects earlier in this document.

2. Specify how you want to filter the objects held in the container:

- To filter objects by naming properties, type in the Filter field on the Toolbar and then press Enter or 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 logon name.
- To filter objects by other properties, click the button on the right side of the Toolbar to expand the Toolbar, click **Add criteria**, choose the properties by which you want to filter, click **Add**, and then configure the criteria as appropriate. 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 a filter is applied to a container, the Web Interface lists a subset of all objects held in that container. You can remove the filter to view all objects: If you did not add criteria, clear the Filter field on the Toolbar and then press Enter; otherwise, expand the Toolbar, click **Clear all**, and then press Enter.

Example: Filtering by object type

The following steps demonstrate how you can configure a filter that lists only user accounts held in a particular organizational unit, removing objects of any other type from the list:

1. Navigate to the organizational unit in the Web Interface.
2. Click the button on the right side of the Toolbar to expand the Toolbar, click **Add criteria**, select the check box next to **Object type is User/InetOrgPerson/Computer/Group/Organizational Unit**, and then click the **Add** button.
3. On the Toolbar, confirm that the field next to **The object type is** reads **User** and then click the button next to the Filter field, or press Enter.

Using personal views

In the Web Interface, you can use search or filter queries to locate directory objects. To create a query, you specify a set of rules that determine the contents of the resulting list of objects. You can, for instance, specify that only user accounts held in a particular organizational unit should be listed. In addition, you can adjust the set of columns and the sort order in the list of search or filtering results.

The ability to locate the objects you target is crucial as you need to focus your attention on only those objects that apply to the task you are performing. 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 have created a query that displays just the objects you need, you can provide the query with a name and save it to 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 have named and saved. After creating a personal view, you will be able to reuse it without re-creating its underlying search or filter query. To reuse a personal view, click the name of that view on the **Views** tab in the Browse pane. The Web Interface 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 as when you created the view.

To create a personal view

1. Do one of the following:
   - Configure and perform a search. For instructions, see Searching for directory objects.
   - Create a filtered list of objects. For instructions, see Filtering the contents of a container.
2. Click the Menu button on the left side of the Toolbar, and then click **Save current view**.
3. In the dialog box that appears, type a name for the personal view, and then click **Save**.

How to start

To connect to the Web Interface, you need to know the name of the Web server running the Web Interface and the name of the Web Interface site you want to access. The default site names are as follows:

- **ARWebAdmin** Site for administrators; supports a broad range of administrative tasks
- **ARWebHelpDesk** Site for Help Desk; supports the most common administrative tasks
- **ARWebSelfService** Site for self-administration; enables end users to manage their personal accounts

To connect to the Web Interface, type the address of the Web Interface site in the address box of your Web browser, and then press Enter.

For example, to connect to the default site for administrators, you might type **http://server/ARWebAdmin** where **server** stands for the name of the Web server running the Web Interface.

Management Shell integrated into Active Roles

Management Shell, which provides Windows PowerShell based command-line tools (cmdlets) for executing and automating administrative tasks in Active Roles, is now a part of the Management Tools component included in the Active Roles Setup. The Management Shell cmdlets are packaged in two modules:

- The **ActiveRolesManagementShell** module provides cmdlets for managing users, group, computers and other objects in Active Directory via Active Roles; managing digital certificates; and administering certain Active Roles objects. The cmdlets provided by this module have their noun perfixed with QAD or QARS, such as `New-QADUser`, `Add-QADCertificate`, or `New-QARSAccessTemplateLink`.
- The **ActiveRolesConfiguration** module provides cmdlets for configuring Active Roles Administration Service instances and Web Interface sites. This module is available on 64-bit (x64) systems only. It requires the Active Roles Administration Service or Web Interface to be installed; otherwise, the module does not provide all cmdlets. The cmdlets provided by this module have their noun prefixed with AR, such as `New-ARDatabase`, `New-ARService`, or `New-ARWebSite`.

You can use the `Import-Module` command to load these modules and gain access to all cmdlets provided by Active Roles Management Shell.

How to start

1. Log on to the computer on which the Administration Service or Web Interface is installed.
2. Open Active Roles Management Shell on that computer. To open Management Shell, click **Active Roles 7.3 Management Shell** on the **Apps** page or **Start** menu depending upon the version of your Windows operating system.
3. Enter the **QuickRef** command at the Management Shell command prompt to view the Reference Manual that provides detailed information about all commands available in Active Roles Management Shell.

4

Administering Active Roles

This section summarizes the features and enhancements that improve the user experience of those who deploy and administer Active Roles, implementing and maintaining the Active Roles-based administrative structure.

Brand-new installation and upgrade experiences

With the brand-new installation and upgrade experiences, Active Roles has become much easier to evaluate, deploy, upgrade and configure. Key highlights include:

- **Unified Setup wizard** Active Roles Setup now provides a single wizard for installing all components, including the Administration Service, Web Interface and Console (MMC Interface). You no longer need to install components using individual installer packages.
- **Configuration Center** Active Roles now includes Configuration Center—a solution for configuring Administration Service instances and Web Interface sites that allows you to perform the core configuration tasks from a single location. For further details, see Configuration Center later in this document.
- **Side-by-side deployment** You can deploy the new Active Roles version side-by-side with your earlier Active Roles version on the same computers, and perform an upgrade without interrupting operations or affecting the configuration of your earlier Active Roles version.

Separation of installation and configuration

Active Roles now provides a single installation file SETUP.EXE instead of numerous installation MSI files. With this single installation file, you can install the core Active Roles components, including Administrative Service, Web Interface and Management Shell.

Some solutions still have separate MSI files, such as Add-on Manager or SPML Provider. You can get them from the Active Roles distribution media.

Side-by-side installation

Active Roles can now coexist with an earlier version of Active Roles on the same computer, so you can run the new version of Active Roles side-by-side with the earlier Active Roles version. In this way, you can use the same hardware during upgrade of Active Roles from an earlier version while keeping the earlier version available for business needs.

Note that the name of the Windows service running the Administrative Service and the names of the default Web Interface sites have changed, to avoid conflicts with the names used in the earlier Active Roles version.

Configuration Center

Active Roles 7.3 introduces a new configuration management solution that unifies management of core configuration for the Active Roles Administration Service and Web Interface. Configuration Center provides a single solution for configuring Administration Service instances and Web Interface sites, allowing administrators to perform the core configuration tasks from a single location. Highlights include:

- Initial configuration tasks such as creation of Administration Service instances and default Web Interface sites
- Import of configuration and management history from earlier Active Roles versions
- Management of core Administration Service settings such as the Active Roles Admin account, service account, and database connection
- Creation of Web Interface sites based on site configuration objects of the current Active Roles version or by importing site configuration objects of earlier Active Roles versions
- Management of core Web Interface site settings such as the site's address on the Web server and configuration object on the Administration Service
- Active Roles version 7.3 supports integration with One Identity Starling services. The Starling Join feature in Active Roles now enables you to connect to One Identity Starling, the Software as a Service (SaaS) solution of One Identity. For more information on Starling Join configuration, see **One Identity Starling Join and Configuration through Active Roles** in the *Active Roles Administration Guide*.

The Configuration Center operations are fully scriptable using Windows PowerShell command-line tools provided by the Active Roles Management Shell.

Benefits of using Configuration Center

While managing core configuration of Active Roles components is not new, Configuration Center unifies the functionality of multiple earlier tools in a single, simple, wizard-based

user interface. Configuration Center provides a single point of access to management wizards for all configuration tasks.

With earlier Active Roles versions, administrators were required to use several tools for core configuration tasks: the Setup program to perform initial configuration, and to import configuration data during upgrade; the Management History Migration tool to import management history data; and the Web Interface Sites Configuration tool to create and manage Web Interface sites on the Web server. Configuration Center integrates the functionality exposed in those tools into a single, unified console, and adds a number of new capabilities, making Active Roles much easier to deploy and upgrade.

Configuration Center is composed of the following elements:

- **Initial configuration wizards** After completing Active Roles Setup, the administrator uses the initial configuration wizards to create a new Active Roles instance, including the Administration Service and Web Interface. The wizards allow the administrator to specify, in a logical manner, the configuration settings that were previously exposed in the Setup program.

  In earlier Active Roles versions, Administration Service Setup prompted for various configuration settings, and created a new, fully configured Administration Service instance; Web Interface Setup created the default Web Interface sites, which required the Administration Service to be up and running. Overall, this setup practice complicated and slowed Active Roles setup, as the completion of Active Roles installation would be delayed until the administrator responded to the prompts and the Setup program finished all the core configuration tasks. Configuration Center allows the administrator to postpone these tasks, and perform them at a convenient time after completing Active Roles Setup. By separating the configuration tasks from the Setup program, Configuration Center simplifies Active Roles installation and streamlines deployment of Active Roles components in an enterprise.

- **Hub pages and management wizards** Once initial configuration has been completed, Configuration Center provides a consolidated view of the core Active Roles configuration settings, and offers tools for changing those settings. Hub pages in the Configuration Center main window display the current settings specific to the Administration Service and Web Interface, and include commands to start management wizards for changing those settings.

  - From the **Administration Service** page, the administrator can view or change the service account, admin account, and database; import configuration data or management history data from an Active Roles database of an earlier version or the current version; view status information, such as whether the Administration Service is started and ready for use; start, stop or restart the Administration Service.

    Earlier Active Roles versions allowed you to import configuration data only one time, when using the Setup program for in-place upgrade of the Administration Service. In many cases, this limitation complicated the process of deploying a new Active Roles version that would inherit the configuration of an existing, earlier Active Roles version. By allowing configuration data to be imported at any convenient time, Configuration Center makes Active Roles much easier to upgrade. You can now install the new Administration Service version side-by-

side with an earlier version and then import configuration data to the new version as needed.

- From the **Web Interface** page, the administrator can view, create, modify or delete Web Interface sites; export configuration of any existing Web Interface site to a file; open each site in a Web browser. The site parameters available for setting, viewing and changing include the site's address (URL, which is based on the Web site and alias of the Web application that implements the Web Interface site on the Web server) and the configuration object that stores the site's configuration data on the Administration Service. When creating or modifying a Web Interface site, the administrator can reuse an existing configuration object, or create a new configuration object based on a template or by importing data from another configuration object or from an export file.

  Earlier Active Roles versions exposed this functionality in a separate tool for configuring Web Interface sites on the Web server. Configuration Center replaces that tool, to make configuration management more efficient by providing a unified experience for administrators to perform various types of configuration tasks.

Wizards that start from hub pages help the administrator manage configuration settings. Management wizards streamline the core configuration tasks by reducing time it took in earlier versions to change the service account, admin account and database; import configuration and management history; and configure Web Interface sites on the Web server.

- **Configuration Shell** A new Windows PowerShell module in Active Roles Management Shell enables access to all Configuration Center features and functions from a command line or from a script, allowing for unattended configuration of Active Roles components. The `ActiveRolesConfiguration` module provides command-line tools (cmdlets) for the key set of configuration tasks, such as creation of the Active Roles database, creation or modification of Administration Service instances and Web Interface sites, data exchange between Active Roles databases and between site configuration objects, querying the current state of the Administration Service, and starting, stopping or restarting the Administration Service. The cmdlets provided by the `ActiveRolesConfiguration` module have their noun prefixed with AR, such as `New-ARDatabase`, `Set-ARService`, or `Set-ARWebSite`.

Configuring a local or remote Active Roles instance

Configuration Center is installed as part of the Management Tools component when you install Active Roles on a 64-bit (x64) system. You can use this tool to perform configuration tasks on the local or remote computer that has the current version of the Administration Service or Web Interface installed. Configuration Center looks for these components on the local computer and, if no components has been found, prompts you to connect to a remote computer. Another way to connect to a remote computer is by using the menu on the heading bar at the top of the Configuration Center main window.

When connecting to a remote computer, Configuration Center prompts you for a user name and password. This must be the name and password of a domain user account that belongs 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 logon 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. Run the `Enable-PSRemoting` command in the PowerShell console to enable remoting (see the Enable-PSRemoting help topic at http://go.microsoft.com/fwlink/?LinkID=144300 for further details). On Windows Server 2012 or later, remoting is enabled by default.

Running Configuration Center

Configuration Center is installed and, by default, automatically started after you install the Administration Service or Web Interface, allowing you to perform initial configuration tasks on the computer on which you have installed those components. If you close Configuration Manager and want to start it again, you can start Configuration Manager from the following locations:

- On Windows Server 2008 R2, select **Start | All Programs | Active Roles 7.3 | Active Roles 7.3 Configuration Center**.
- On Windows Server 2012 or later, click the **Active Roles 7.3 Configuration Center** tile on the **Apps** page.

As Configuration Center can manage Active Roles not only on the local computer but also on remote computers, it is possible to use it on a client operating system as well as on server operating systems. You can install Configuration Center by installing Active Roles Management Tools on a 64-bit (x64) server or client operating system, and then connect it to a remote computer on which the Administration Service or Web Interface is installed. To start Configuration Center on a client operating system:

- On Windows 7, select **Start | All Programs | Active Roles 7.3 Active Roles | Active Roles 7.3 Configuration Center**.
- On Windows 8 or later, click the **Active Roles 7.3 Configuration Center** tile on the **Apps** page.

To run Configuration Center on a given computer, you must be logged on with a user account that has administrator rights on that computer.

If neither the Administration Service nor the Web Interface is installed on the local computer, then Configuration Center prompts you to select a remote computer. In the **Select Server** dialog box that appears, supply the fully qualified domain name of a server, on which the Administration Service or the Web Interface (or both) is installed, and type the logon 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 selecting the **Connect to another server** command from the menu on the heading bar at the top of the Configuration Center main window, which also displays the **Select Server** dialog box.

Tasks you can perform in Configuration Center

Configuration Center enables you to perform:

- Initial configuration tasks, creating the Administration Service instance and the default Web Interface sites
- Configuration management tasks, letting you manage the existing instance of the Administration Service or Web Interface

Initial configuration tasks

Unlike Setup programs of earlier Active Roles versions, the current Setup program only installs and registers the Active Roles files, without performing any configuration. Upon completion of Active Roles Setup, Configuration Center is used to create an instance of the Administration Service and deploy the default Web Interface sites. Here you can find an overview of these initial configuration tasks.

Configure the Administration Service

The Configure Administration Service wizard creates the Administration Service instance, getting the Administration Service ready for use. The wizard prompts you to supply the following settings:

- The logon name and password of the account in which this Administration Service instance will be running (service account)
- The name of the group or user account that will have full access to all Active Roles features and functions through this Administration Service instance (Active Roles Admin)
- The database in which this Administration Service instance will store the configuration data and management history data

  You have the option to create a new database, or use an existing database of the current Active Roles version. It is possible to have multiple Administration Service instances use the same database.

- The authentication mode that this Administration Service instance will use when connecting to the database

  With the Windows authentication option, the Administration Service will use the credentials of the service account; with the SQL Server authentication option, the Administration Service will use the SQL login name and password you supply in the wizard.

To start the wizard, click **Configure** in the **Administration Service** area on the **Dashboard** page in the Configuration Center main window.

Configure the Web Interface

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

- Use the Administration Service instance running on the same computer as the Web Interface
- Use the Administration Service instance running on a different computer

  This option requires you to supply the fully qualified domain name of the computer running the desired instance of the Administration Service.
- Let the Web Interface choose any Administration Service instance that has the same configuration as the given one

  This option requires you to supply the fully qualified domain name of the computer running the Administration Service instance of the desired configuration. If your environment employs Active Roles replication, this must be the computer running the Administration Service instance whose database server acts as the Publisher for the Active Roles configuration database.

To start the wizard, click **Configure** in the **Web Interface** area on the **Dashboard** page in the Configuration Center main window.

Administration Service management tasks

After installing Active Roles, you perform the initial configuration task to create the Administration Service instance, getting it ready for use. Then, you can use Configuration Center to:

- View or change the core Administration Service settings such as the service account, the admin account, and the database
- Import configuration data from an Active Roles database of the current version or an earlier version to the current database of the Administration Service
- Import management history data from an Active Roles database of the current version or an earlier version to the current database of the Administration Service
- View the state of the Administration Service
- Start, stop or restart the Administration Service

View the core Administration Service settings

On the **Administration Service** page in the Configuration Center main window, you can view:

- The logon name of the 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 login)

Change the core Administration Service settings

From the **Administration Service** page in the Configuration Center main window, you can change:

- The service account—Click **Change** in the **Service account** area. In the wizard that appears, supply the logon name and password of the domain user account in which you want the Administration Service to run.
- The Active Roles Admin account—Click **Change** in the **Active Roles Admin** area. In the wizard that appears, specify the group or user account you want to have the Active Roles Admin rights.
- The Active Roles database—Click **Change** in the **Active Roles database** area. In the wizard that appears, specify the SQL Server instance and the database you want the Administration Service to use, and choose the database connection authentication mode (Windows authentication or SQL Server login). You have the option to specify a separate database for storing management history data.

Import configuration data

The task of importing configuration data arises when you upgrade the Administration Service. In this case, you need to transfer the Active Roles configuration data from the database used by your Administration Service of the earlier version to the database used by your Administration Service of the new version. To perform this task, click **Import Configuration** on the **Administration Service** page in the Configuration Center main window, and follow the steps in the Import Configuration wizard that appears.

The Import Configuration wizard prompts you to specify the Active Roles database from which you want to import the configuration data (source database) and identifies the database of the current Administration Service to which the configuration data will be imported (destination database), letting you choose the connection authentication mode (Windows authentication or SQL Server login) for each database. Then, the wizard 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.

Import management history data

Although this task looks similar to the task of importing configuration data, there are important differences:

- Due to a much larger volume of management history data compared to configuration data, importing management history data takes much longer than importing configuration data.
- As management history data has dependencies on configuration data (but not vice versa), configuration data must be imported first, and then management history data can be imported as needed.

Because of these considerations, Configuration Center provides a different wizard for importing management history. The distinctive features of the Import Management History wizard are as follows:

- The wizard does not replace the existing data in the destination database. It only retrieves and upgrades management history records from the source database, and then adds the upgraded records to the destination database.
- The wizard allows you to specify the date range for the management history records you want to import, so you can import only records that occurred within a particular time frame instead of importing all records at a time.
- Canceling the wizard while the import operation is in progress does not cause you to lose the import results, so you can stop the import operation at any time. The records imported by the time that you cancel the wizard are retained in the destination database. If you start the wizard again, the wizard imports only records that were not imported earlier.

To start the Management History Import wizard, click **Import Management History** on the **Administration Service** page in the Configuration Center main window. The wizard prompts you to specify the Active Roles database from which you want to import the management history data (source database) and identifies the database of the current Administration Service to which the management history data will be imported (destination database), letting you choose the connection authentication mode (Windows authentication or SQL Server login) for each database. Then, the wizard lets you choose whether you want to import all management history records or only records within a certain date range, and performs the import operation. During the import operation, the wizard retrieves and upgrades management history records from the source database, and adds the upgraded records to the destination database.

View the state of the Administration Service

On the **Administration Service** page in the Configuration Center main window, you can view the state of the Administration Service, such as:

- **Ready for use** Administration Service is running and ready to process client requests
- **Getting ready** Administration Service has just started and is preparing to process client requests
- **Stopping** Administration Service is preparing to stop
- **Stopped** Administration Service is stopped
- **Unknown** Unable to retrieve the state information

Start, stop or restart the Administration Service

You can start, stop or restart the Administration Service by clicking the **Start**, **Stop** or **Restart** button at the top of the **Administration Service** page in the Configuration Center main window. If the function of a given button is not applicable to the current state of the Administration Service, the button is unavailable.

Web Interface management tasks

After installing Active Roles, you perform the initial configuration task to create the default Web Interface sites, getting the Web Interface ready for use. Then, you can use Configuration Center to:

- Identify the Web Interface sites that are currently deployed on the Web server running the Web Interface
- Create, modify or delete Web Interface sites
- Export a Web Interface site's configuration object to a file

Here you can find an overview of these tasks.

Identify Web Interface sites

The **Web Interface** page in the Configuration Center main window lists all Web Interface sites that are deployed on the Web server running the Web Interface. For each Web Interface site, the list provides the following information:

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

From the **Web Interface** page, you can open Web Interface sites in your Web browser: Click an entry in the list of Web Interface sites and then click **Open in Browser** on toolbar.

Create a Web Interface site

You can create a Web Interface site by clicking **Create** on the **Web Interface** page in the Configuration Center main window. The Create Web Interface Site wizard appears, prompting you to:

- Choose the Web site to contain the Web application that implements the new Web Interface site

- Supply the desired alias for that Web application. The alias defines the virtual path that becomes part of the Web Interface site's address (URL).

Then, the wizard lets you specify the object to hold the configuration and customization data of the new Web Interface site on the Active Roles Administration Service. You can choose from the following options:

- Create the object from a template

  The new site will have the default configuration and customization based on the template you select.

- Use an existing object

  The new site will have the same configuration and customization as any existing Web Interface site that also uses the object you select. This option is intended for the scenario where you create an additional instance of one of your existing Web Interface sites on a different Web server.

- Create the object by importing data from another object

  The new site will inherit the configuration and customization of the site that used the object you select for data import. This option is mainly intended for the upgrade scenario where you create Web Interface sites of the new Active Roles version that have the same configuration and customization as your Web Interface sites of an earlier Active Roles version. In this scenario, you import the configuration data of the earlier version to the Administration Service of the new version (which also imports the site configuration objects of the earlier version), and then create configuration objects for Web Interface sites of the new version by importing data from site configuration objects of the earlier version.

- Create the object by importing data from an export file

  Active Roles

Modify a Web Interface site

From the **Web Interface** page in the Configuration Center main window, you can make changes to existing Web Interface sites: Click an entry in the list of sites and then click **Modify** on the toolbar. The Modify Web Interface Site wizard starts, allowing you to:

- Choose the Web site to contain the Web application that implements the Web Interface site
- Supply the desired alias for that Web application. The alias defines the virtual path that becomes part of the Web Interface site's address (URL).

Then, the wizard lets you specify the object to hold the site's configuration and customization data on the Active Roles Administration Service. You can choose from the following options:

- Keep on using the current object (default option)

  The site's configuration will remain intact. The wizard displays the name and version of the current configuration object.

- Create the object from a template

  The site will have the default configuration and customization based on the template you select.

- Use an existing object

  The site will have the same configuration and customization as any existing Web Interface site that also uses the object you select. You could use this option to deploy an additional instance of one of your existing Web Interface sites on a different Web server.

- Create the object by importing data from another object

  The site will inherit the configuration and customization of the site that used the object you select for data import. You could use this option to deploy a Web Interface site of the new Active Roles version with the same configuration and customization as one of your Web Interface sites of an earlier Active Roles version. In this case, you import the configuration data of the earlier version to the Administration Service of the current version (which also imports the site configuration objects of the earlier version), and then create the site configuration object by importing data from the appropriate site configuration object of the earlier version.

- Create the object by importing data from an export file

  The site will inherit the configuration and customization of the site whose configuration data was saved to the export file you specify. You can choose an export file of any supported Active Roles version.

Delete a Web Interface site

On the **Web Interface** page in the Configuration Center main window, you can delete Web Interface sites: Click an entry in the list of sites and then click **Delete** on the toolbar. This operation only deletes the Web Interface site from the Web server, without deleting the site's configuration object from the Administration Service.

When you delete a site, the site's configuration object remains intact on the Administration Service. You can set up a Web Interface site with the same configuration as the site you have deleted, by choosing the option to use that object on the **Configuration** step in the wizard for creating or modifying Web Interface sites.

Export a Web Interface site's configuration object to a file

From the **Web Interface** page in the Configuration Center main window, you can export site configuration objects: Click an entry in the list of sites and then click **Export Configuration** on the toolbar. A wizard starts, prompting you to specify the export file. The wizard then retrieves the site's configuration object from the Administration Service, and saves the data from that object to the export file.

The export file could be considered a backup of the site's configuration. You can set up a Web Interface site with the configuration restored from an export file, by importing that file on the **Configuration** step in the wizard for creating or modifying Web Interface sites.

Logging management tasks

You can use Configuration Center to enable or disable, and view diagnostic logs for the Active Roles components that are installed on the computer running Configuration Center. On the **Logging** page, Configuration Center lists the following information:

- **Component** Name of the component, such as Administration Service, Web Interface or Console (MMC Interface)
- **Logging** Indicates whether logging is enabled or disabled for the given component, and the logging level, such as Basic or Verbose
- **Log location** Depending upon the component, identifies either the folder containing the log files or the log file for that component

The toolbar on the **Logging** page allows you to perform the following tasks:

- To enable or disable logging for a given component, select the component in the list, and then click **Modify** on the toolbar.
- To open the folder that contains the log file or files for a given component, select the component in the list, and then click **Browse with Explorer** on the toolbar.
- To examine the Administration Service log file in Log Viewer, select Administration Service in the list of components and then click **Open in Log Viewer** on the toolbar. For information about Log Viewer, see Active Roles Log Viewer later in this document.

How to start

Configuration Center is installed and, by default, automatically started after you install the Administration Service or Web Interface, allowing you to perform initial configuration tasks on the computer on which you have installed those components. If you close Configuration Center and want to start it again, you can start Configuration Center from the following locations:

- On Windows Server 2008 R2, select **Start | All Programs | Active Roles Active Roles 7.3 | Active Roles 7.3 Configuration Center**.
- On Windows Server 2012 or later, click the **Active Roles 7.3 Configuration Center** tile on the **Apps** page.

Configuration Shell

Active Roles Management Shell has been extended with a new module, **ActiveRolesConfiguration**, that provides command-line tools (cmdlets) for configuring Active Roles Administration Service instances and Web Interface sites. This module is available on 64-bit (x64) systems only. It requires the Active Roles Administration Service or Web Interface to be installed; otherwise, the module does not provide all cmdlets. The following table lists and briefly describes the cmdlets provided by this module.

Table 1: Configuration Shell Cmdlets

Command	Description
Get-ARComponentStatus	Returns installation and configuration status of 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	Creates a file that stores a copy of the current encryption key used in the configuration database of the local Administration Service instance.
Restore-AREncryptionKey	Restores the encryption key from a backup file to the configuration database of the local Administration Service instance.
Reset-AREncryptionKey	Creates a new encryption key for the configuration database of the local Administration Service instance.
New-ARService	Creates the instance of the Active Roles Administration Service on the local computer.
Get-ARService	Retrieves 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 stopped Active Roles Administration Service on the local computer.
Stop-ARService	Stops the Active Roles Administration Service running on the local computer.
Restart-ARService	Stops and then starts the Active Roles Administration Service on the local computer.
Remove-ARService	Deletes the Active Roles Administration Service from the local computer.
Test-ARServiceDatabaseSettings	Verifies whether the given Active Roles database settings would cause Management History issues due to separate Configuration and Management History databases.
Get-ARServiceStatus	Retrieves the Active Roles Administration Service status information from the local computer.
Get-ARVersion	Retrieves the version number of the local Active Roles installation.

Command	Description
New-ARWebSite	Creates a new Active Roles Web Interface site.
Get-ARWebSite	Retrieves 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	Retrieves Web Interface site configuration objects from the Active Roles Administration Service.
Export-ARWebSiteConfig	Exports a Web Interface site configuration to a file.

How to start

1. Log on to the computer on which the Administration Service or Web Interface is installed.
2. Open Active Roles Management Shell on that computer.

   To open Management Shell, click **Active Roles 7.3 Management Shell** on the **Apps** page or **Start** menu depending upon the version of your Windows operating system.
3. Enter the **QuickRef** command at the Management Shell command prompt to view the Reference Manual that provides detailed information about all commands available in Active Roles Management Shell.

Active Roles Log Viewer

The Log Viewer tool enables you to browse and analyze diagnostic log files created by the Active Roles Administration Service as well as event log files created by saving the Active Roles event log in Event Viewer on the computer running the Administration Service. Log Viewer can help you drill down through the sequence or hierarchy of requests processed by the Administration Service, identify error conditions that the Administration Service encountered during request processing, and find Knowledge Articles that apply to a given error condition.

With Log Viewer, you can open an Active Roles diagnostic log file (ds.log) or saved event log file (.evtx), and view a list of:

- 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 in the list, you can choose a command to look for solution in Knowledge Base. The command performs a search in One Identity Software Knowledge Base to list the Knowledge Articles that can provide helpful information on how to troubleshoot the error you selected.

Log Viewer also enables you to:

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

How to start

To start Log Viewer, click **Start Log Viewer** in the Configuration Center main window.

Once you have started Log Viewer, open your Active Roles diagnostic log file or saved event log file: Click **Open** on the Log Viewer toolbar, and supply the path and name of the log file.

By default, Log Viewer displays a list of errors encountered by the Administration Service and recorded in the log file. You can use Log Viewer to look for information on how to troubleshoot a given error: Right-click the error in the list and then click **Look for solution in Knowledge Base**. Log Viewer performs a search in One Identity Software Knowledge Base to list the Knowledge Articles that apply to the error you selected.

Other tasks you can perform:

- To view a list of requests processed by the Administration Service and traced in the log file, click **Requests** in the **View** area on the Log Viewer toolbar.
- To view all trace records found in the diagnostic log file or all events found in the event log file, click **Raw log records** in the **View** area on the Log Viewer toolbar.
- To search the list for a particular text string, such as an error message, type the text string in the **Search** box on the Log Viewer toolbar and press Enter.
- To narrow the set of list items to those you are interested in, click **Filter** on the Log Viewer toolbar and specify the desired filter conditions.
- To view detailed information about an error, request, trace record or event, right-click the corresponding list item, and click **Details**.
- To view all trace records that apply to a given request, right-click the corresponding item in the **Requests** list and click **Stack trace**. This task is unavailable in case of an event log file.
- To view the request that caused a given error, right-click the error in the **Errors** list and click **Related request**. This task is unavailable in case of an event log file.
- To view all trace records that apply to the request that caused a given error, right-click the error in the **Errors** list and click **Stack trace for related request**. This task is unavailable in case of an event log file.

Voluntary thresholds for the managed object count

By default, Active Roles does not limit the number of managed objects. However, as Active Roles' license fee is based on the managed object count, you may need to verify if the object count is under a certain threshold. You can perform this task by specifying a threshold value for the number of managed objects. The scheduled task that counts managed objects then raises an alert each time it detects that the current number of managed objects exceeds the threshold value. The alert makes the **Product Usage Statistics** section red on the root page in the Active Roles console, and can send a notification over e-mail.

How to start

1. Log on as Active Roles Admin, open the Active Roles console, and select the root node in the console tree.
2. In the details pane, expand the **Product Usage Statistics** area, and then click **Change** next to the **Threshold value** field.

For further details, see the "Voluntary thresholds for the managed object count" section in the Active Roles Administration Guide.

Installation label

The Active Roles console allows you to set a text label that helps you identify your Active Roles installation in the Managed Object Statistics report—a report that lists the managed object counts. You can use the installation label to distinguish, for example, between production and non-production or pilot installations. The label text is displayed in the title of the Managed Object Statistics report.

How to start

1. Log on as Active Roles Admin, open the Active Roles console, and select the root node in the console tree.
2. In the details pane, expand the **Product Usage Statistics** area, and then click **Change** next to the **Installation label** field.

Safe mode

Active Roles provides a troubleshooting option, referred to as *safe mode*, that starts the Administration Service in a limited state. When safe mode is enabled, the Administration Service disregards all custom policies, workflows, scripts, scheduled tasks and other

customizations that may block it from starting and operating normally, and rejects connections from any user other than Active Roles Admin. Active Roles Admin can connect to the Administration Service and make changes in order to fix or remove customizations that cause issues, and then disable safe mode.

How to start

1. Log on to the computer running the Administration Service with a user account that has administrator rights on that computer. Local administrator rights are required to enable or disable safe mode.
2. Open Active Roles Management Shell on the computer running the Administration Service: Click **Active Roles 7.3 Management Shell** on the **Apps** page or **Start** menu depending upon the version of your Windows operating system.
3. To enable safe mode, enter the following commands at the Management Shell command prompt:

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

4. To disable safe mode, enter the following commands at the Management Shell command prompt:

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

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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