Active Roles 8.1.3

Web Interface User Guide

Legend

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

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

Active Roles Web Interface User Guide
Updated - 12 November 2024, 14:45

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

Contents

1

Getting Started

Active Roles offers a convenient, easy-to-use, customizable Web Interface that enables authorized users to perform day-to-day administrative tasks, including user management tasks such as modifying personal data or adding users to groups. Via the Web Interface, an intranet user can connect to Active Roles using a web browser. A user sees only the commands, directory objects, and object properties to which the user's role provides administrative access.

By default, the Web Interface includes three different sites: the Administration Site, the Helpdesk Site, and the Self-Service Site. The Administration Site supports a rich variety of administrative tasks, while the Helpdesk Site supports a simplified set of tasks, mostly aimed for resolving support tickets. Finally, the Self-Service Site is intented for users to manage their own personal accounts.

The Web Interface also allows setting the user interface language according to your preferences. The language setting has effect on all menus, commands, and forms that come with the Web Interface, as well as the tooltips. As such, users can work with the Web Interface in their own language.

The Web Interface delivers a reliable, comprehensive solution for users who have administrative access to Active Roles to modify commands that the Web Interface provides for without writing a single line of code, and enables such users to add and remove commands on menus, and modify command pages by adding and removing fields that display property values. For information on how to customize the Web Interface, refer to the *Active Roles Web Interface Configuration Guide*.

This document is for personnel who are responsible for performing day-to-day administrative tasks. As such, the document provides a brief overview of the Web Interface, and includes step-by-step instructions on how to perform administrative tasks.

The following topics describe the procedures for connecting to the Web Interface. First, configure your web browser to display the Web Interface pages properly. Then, connect to the Web Interface. Finally, you may specify personal settings for the Web Interface.

- Configuring the web browser
- Connecting to the Web Interface
- Changing personal settings in the Web Interface
- Logging out of the Web Interface

Configuring the web browser

Active Roles supports several web browsers for accessing the Active Roles Web Interface. To access a Web Interface site, the browser must have JavaScript and cookies enabled.

- JavaScript is a programming language for making web pages interactive.
- Cookies are small files stored on your computer that contain information about the Web Interface.

For more information on how to enable JavaScript and cookies in your browser, see the applicable topic:

- Configuring Google Chrome
- Configuring Mozilla Firefox

Configuring Google Chrome

To access the Active Roles Web Interface with Google Chrome, make sure that the browser has JavaScript and cookies enabled. For more information, see Activate JavaScript in your browser in the *Google Support Portal*.

Configuring Mozilla Firefox

To access the Active Roles Web Interface, Mozilla Firefox must have cookies enabled. For more information on how to turn on cookies, see Check Cookie Settings in the *Mozilla Support Portal*.

NOTE: JavaScript is enabled in Mozilla Firefox by default. Also, starting from Firefox 23, you cannot disable or re-enable it via the **Options** menu of the browser.

Connecting to the Web Interface

To connect to the Web Interface, you must 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**: The Administration Site for administrators, supporting a wide range of organization-level and Active Roles administration tasks.
- **ARWebHelpDesk**: The Helpdesk Site, supporting the most common resource administration tasks.

- **ARWebSelfService**: The Self-Service Site, allowing users to manage their own accounts.

To connect to the Web Interface

1. Open the web browser of your choice.
2. In the address bar of your browser, enter the address of the Web Interface site you want to connect, then press **Enter**.

   For example, to connect to the default site for administrators, enter `<server>/ARWebAdmin` where `<server>` is the name of the web server running the Web Interface.

   > TIP: If you want to open a Web Interface site on the computer where the Active Roles Web Interface component is deployed, you can also specify `localhost` in the address instead of the server name, such as: `localhost/ARWebAdmin`.

Changing personal settings in the Web Interface

When using the Web Interface, you can configure various personal settings, like the user interface language, or the amount of directory objects to list per page.

To change personal settings in the Web Interface

1. In your browser, open the Active Roles Web Interface.
2. In the header, click **Active Roles 8.1.3** > **Settings**.
3. Configure the following settings as you need:
   - **User interface language**: Specifies the language of the Web Interface. This setting affects all menus, commands, and forms of the Web Interface, as well as tooltips and help text.

     > NOTE: By default, the Web Interface contains only English localization. Installing the Active Roles Language Pack adds support for the following languages:
     >
     > - Chinese (Simplified and Traditional)
     > - French
     > - German
     > - Portuguese (Brazilian and European)
     > - Spanish
     >
     > For more information, see *Active Roles Language Pack* in the *Active Roles Administration Guide*.

- **Maximum number of objects to display in search results**: Specifies the maximum number of objects to display in single-page lists, such as lists of search results or lists that show contents of containers. The supported value range is 1–20000, and the default value is 1000.

  TIP: Use this setting carefully, as displaying a large number of objects may negatively impact browser performance. Instead of displaying all objects, One Identity recommends using the available search and filtering options to find the objects you need.

- **Number of items to display per page in paged lists**: Specifies the maximum number of list items displayed on a single page in multi-page lists. This setting affects only lists (such as approval task lists) that are divided into pages. The supported value range is 1–10000, and the default value is 20.

  TIP: Use this setting carefully, as specifying a small value may result in many pages to list through, while specifying a large value can negatively impact browser performance.

- **Number of page links to display for paged lists**: Specifies the maximum number of page number links displayed for multi-page lists. This setting affects only lists (such as approval task lists) that are divided into pages. The supported value range is 1–1000, and the default value is 5.
- **Time (in minutes) for which the notification is visible**: Specifies the number of minutes for which Web Interface notifications will be visible on the user interface. The supported value range is 0–43200, and the default value is 0. Keeping the default value of 0 results in notifications never disappearing.
- **Maximum number of notifications to be stored in Active Roles**: Specifies the maximum number of notifications to be stored in the Active Roles database. The supported value range is 5–1000, and the default value is 1000.
- **Show objects owned by inheritance or secondary ownership**: When selected, the **My Managed Resources** page of the Web Interface will also list objects of which the user is not the primary owner (manager), but the secondary or inherited owner.

4. To apply your changes, click **Save**.

   TIP: Active Roles saves the personal settings on a per-user basis in the Web Interface site configuration. Once saved, the personal settings take effect regardless of which computer you use to access Web Interface. As such, you can configure different personal settings for different Web Interface sites.

Logging out of the Web Interface

Logging out of the Web Interface can save Web Interface users from harmful security breaches. Therefore, make sure to always log out of the Web Interface when you finished working with the Web Interface.

NOTE: Failure to log out after finishing work in the Web Interface may pose a security risk (for example, when accessing the Web Interface from a public computer). Therefore, the Web Interface can automatically stop your session in case of user inactivity.

Active Roles administrators can specify the duration of this inactivity timeout, ensuring that the session is not stopped unexpectedly. The Active Roles Web Interface warns you with a pop-up message if you approach the configured idle timeout limit. The session is then stopped after an additional grace period if you take no action.

To log out of the Web Interface

1. In the Web Interface title bar, click your user name.
2. Click **Log out**.

   Active Roles then closes the current Web Interface session and deletes all session-related data from the computer you used to access the Web Interface.

2

Web Interface Basics

The following sections provide an overview on the components and usage of the Active Roles Web Interface.

- Administrative tasks overview
- User interface overview
- Managing the list of objects
- Locating directory objects
- Using personal views

Administrative tasks overview

The Web Interface home page displays categories of administrative tasks supported by the Web Interface. The same categories are displayed along the vertical strip on the left side of the Web Interface, referred to as Navigation bar. You can perform the following tasks from the Navigation bar:

- Directory Management Browse for, and manage, directory objects, such as users and groups. You can navigate through containers in the directory; view, filter and select objects held in the container; and apply commands to the selected object or container.
- Search Search for, and manage, directory objects. You can select containers in the directory, and specify search criteria. The Web Interface searches in the selected containers and all of their subcontainers, and lists the objects that match your search criteria, allowing you to apply commands to objects in the list.
- Approval Perform the tasks related to approval of administrative operations. The scope of your responsibilities depends upon your role in the approval workflow processes.
- Settings Set up your personal settings that control the display of the Web Interface pages.
- Customization: Add, remove, or modify user interface elements, such as menu items (commands) and pages (forms), intended to manage directory objects.

NOTE: Customizing the Web Interface requires Active Roles Admin privileges. For more information, see the *Active Roles Web Interface Configuration Guide*.

NOTE: Consider the following additional features when using the Web Interface:

- For more information on extending the Active Roles provisioning and account administration capabilities to your cloud applications, check the **Active Roles 8.1.3** > **What's New** page.
- To provide product feedback on the Web Interface Administration Site, use the **Feedback** button.
    - To enable the **Feedback** button on the Web Interface Helpdesk Site, navigate to **Customization** > **Global Settings**, and select **Enable user feedback link**.
    - The **Feedback** button is not available on the Web Interface Self-Service Site.

Directory Management

Directory Management allows you to browse for, and administer, directory objects in your organization. Your Active Roles permissions determine which tasks you can perform.

Directory Management provides the following views:

- **Active Directory**: Lists Active Directory domains managed by Active Roles, allowing you to navigate through containers in those domains. You can view, filter and select objects held in the container, and apply commands to the selected object or container.
- **Managed Units** Lists Managed Units defined in Active Roles, allowing you to view objects, and navigate through containers, held in Managed Units. You can filter and select objects, and apply commands to the selected object or container.

For information on how to administer Active Directory objects, see Managing Active Directory objects.

Search

Search provides a flexible, query-based mechanism that helps locate directory objects quickly and without browsing through the directory tree. You can select containers in the directory, and build a query by specifying search criteria. The Web Interface searches in the selected containers and all of their subcontainers, and lists the objects that match your search criteria. When the objects you target are returned as the results of a search query, you can then perform the necessary administrative tasks.

You can also save the queries that you build and use them again at a later time. The Web Interface saves queries as your personal views, with each view consisting of the containers and search criteria that you select, as well as the customized sorting and column information that you specify.

For instructions on how to perform a search, see Searching for directory objects.

Approval

Approval provides you with the tools for performing tasks related to approval workflow. You can use these tools to complete approval tasks assigned to you as an Approver, and to monitor the status of the operations that you initiated, if those require approval.

For details on how to perform approval tasks, see Using Approval workflows.

Settings

By using **Settings**, you can specify:

- The language of the Web Interface pages.
- The maximum number of objects displayed in single-page lists.
- The maximum number of list items displayed on a single page in multi-page lists.
- The maximum number of links to pages displayed for multi-page lists.
- Maximum time in minutes, for which the notification is to be visible.
- Maximum number of notifications to be stored in Active Roles.

You can also enable **Show objects owned by inheritance or secondary ownership**. Selecting this check box allows Self-Administration Web Interface users to view objects in **My Managed Resources** even if the user is not assigned to the objects as the primary owner (manager), but as a secondary or inherited owner.

Settings are saved on a per-user basis in the configuration of the Web Interface site. For more information on changing these settings, see Changing personal settings in the Web Interface.

Customization

Customization allows you to tailor the Web Interface to suit the specific needs of your organization. The **Customization** menu appears only if you are logged in as an Active Roles Admin. The default Active Roles Admin account is created during the configuration of the Active Roles Administration Service.

Customization includes the following tasks:

- **Directory Objects**: Modify menus, commands, and forms for administering directory objects. View or change global settings, such as the logo image and color scheme.
- **Restore Default**: Restore the original (default) menus, commands, and forms, discarding all previous customizations.
- **Reload**: Reload the menus, commands, and forms that you have customized.

The customization settings determine the configuration of the Web Interface site for all users.

For more information about customizing the Web Interface, see *Customizing the Web Interface* in the *Active Roles Web Interface Configuration Guide*.
>

User interface overview

The section describes the user interface elements that are common across the Web Interface.

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 the currently opened Web Interface site.

  NOTE: The **Customization** menu is available for Active Roles administrators only.
- **Approval**: Perform tasks related to the approval of administrative operations.
- **Settings**: View or change your personal settings that control the display of the Web Interface.
- **Help**: Open useful resources about the usage of the Web Interface.

For more information about the usage of the Navigation Bar, see Administrative tasks overview.

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. To see built-in views and personal views, click the **Views** tab at the top of the Browse Pane.
- The tree view helps you browse for directory objects by using the directory tree to

navigate through the hierarchical structure of containers. To see the tree view, click the **Tree** tab at the top of the Browse Pane.

List of objects

When you select a container or view in the Browse pane, you will 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. 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

The Toolbar contains a number of controls allowing you to manage the current list of objects:

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

Current container

The area above the Toolbar displays the name of the current container, the container that holds the objects shown in the list, and identifies the hierarchical path to the current container in the directory. To view a list of objects held in the container, click its name in the path.

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 do not see the Summary pane, click in the area beneath the list of objects.

Notification and Feedback

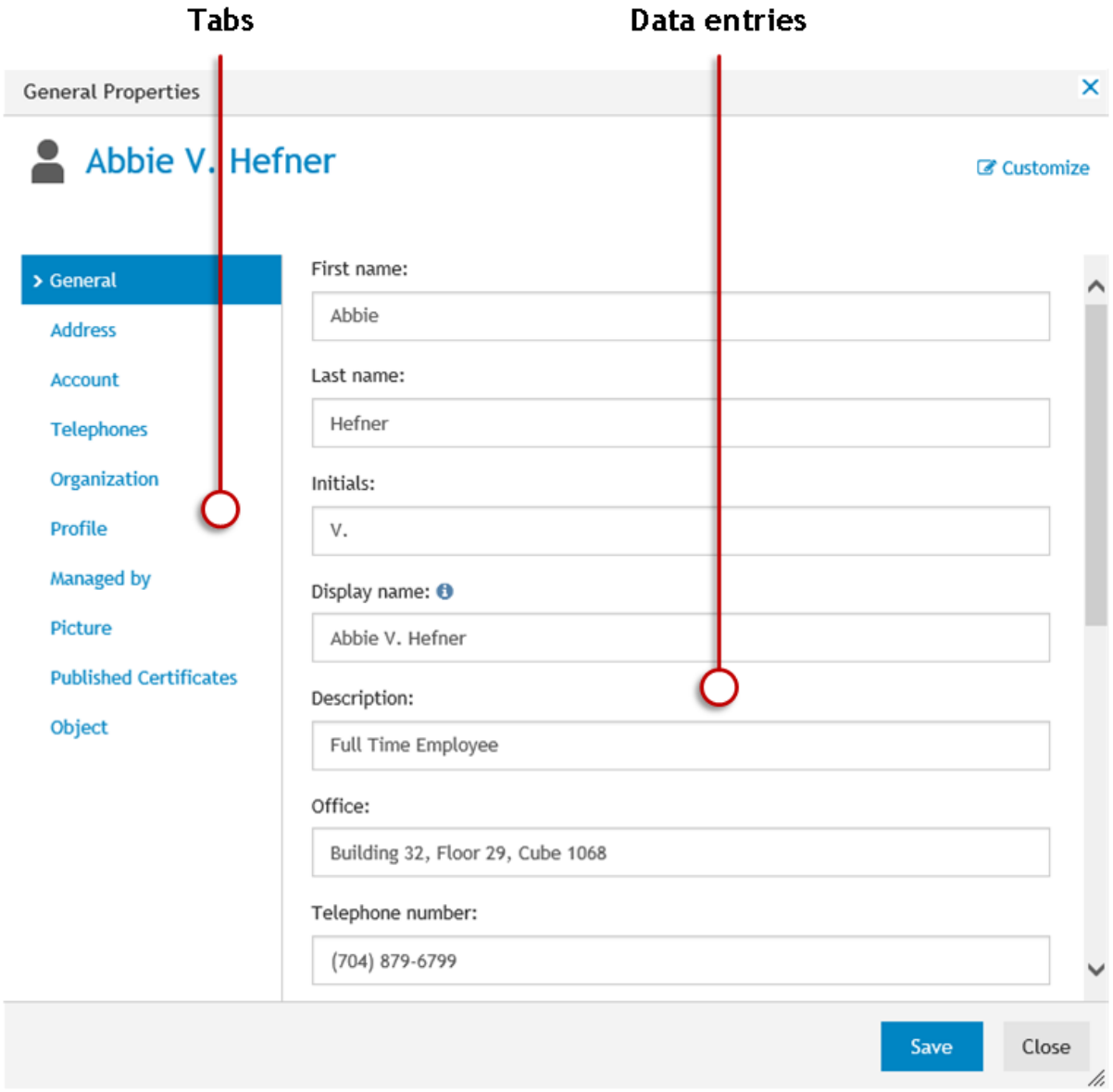
The upper right corner of the Web Interface contains the **Feedback** button, the **Active Roles 8.1.3** menu, the **Notification** icon, and your user name with the following features:

- **Feedback**: Allows you to provide product feedback for One Identity.
- **Active Roles 8.1.3**: Provides technical and legal information about the current release, and also provides a shortcut to the **Settings** menu.
- **Notification** icon: Lists the latest Startling Connect release highlights.
- User name: Allows you to log out of the Web Interface.

Object property pages

Property pages are used in the Web Interface to modify directory objects. The following figure gives an example of the property page that appears when you select a user account from the list of objects and click **General Properties** in the Command pane.

Figure 1: Object Property page



The property page consists of several tabs. Each tab provides a number of data entries allowing you to view or change certain properties of the directory object. Click a tab to access the data entries on that tab. To apply the changes you have made in the data entries, click the **Save** button.

An Active Roles Admin can use the **Customize** link in the upper right corner of the page to add or remove data entries or entire tabs from the property page. The **Customize** link is not displayed unless you are logged on as a member of the Active Roles Admin account, which specified in the configuration settings of the Active Roles Administration Service.

Managing the list of objects

The list of objects in the Web Interface has a number of features that help you locate the objects you target. Thus, you can sort objects in a list and apply a filter to a list. You can also add or remove list columns.

Sorting and filtering the list of objects

The Web Interface allows you to set a sort order and apply a filter in the list of objects.

To sort the list of objects by name

- Click the **Name** column heading once or twice to sort the list by object name in ascending or descending order. An arrow in the column heading indicates the sort order.

You can also sort the list by other columns. Click a column heading to change the sort order. For more information on how to add or remove columns, see Adding or removing columns from the list of objects.

To filter the list of objects

- To filter the list by naming properties, enter the filtering conditions in the **Filter** field on the Toolbar, then press **Enter** or click the button next to the **Filter** field. As a result, the list includes 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 the list by other properties, expand the Toolbar by clicking the button on the right side of the Toolbar. Then, click **Add criteria**, choose the properties by which you want to filter, click **Add**, then configure the criteria as appropriate. When finished, press **Enter** or click the button next to the **Filter** field on the Toolbar. As a result, the list includes only the objects that match the criteria you configured.

After you have applied a filter, the list includes only the objects that match the filter. For example, you can type a few characters in the **Filter** field on the Toolbar, then press **Enter** to view only the objects whose name starts with the characters you typed.

To remove the filter and restore the original list of objects

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

Adding or removing columns from the list of objects

You can customize the list of objects by adding or removing list columns. Each column is intended to display a certain property of objects in the list, and can be used to set a sort order.

To add or remove list columns

1. On the left side of the **Toolbar**, click **Menu** > **Choose columns**.
2. To add a column for a certain property, click the name of the property in the **Hidden columns** list, then click the right arrow button to move the property to the **Displayed columns** list.
3. To remove a column for a certain property, click the name of the property in the **Displayed columns** list, then click the left arrow button to move the property to the **Hidden columns** list.

TIP: You can reorder list columns by moving list items up and down in the **Displayed columns** list. To do so, click the name of the property in the list, then click the applicable arrow button next to the list.

Locating directory objects

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, 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, 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**, 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** (see also Adding or removing columns from the list of objects). To sort the list by column data, click column headings.

Searching by object type

You can list objects by type in the Active Roles Web Interface. This is useful, for example, to look for specific object types or to narrow the conditions of a search. The following example shows how to use this feature by listing all groups in an Active Directory domain managed with Active Roles.

To list all groups that exist in your Active Directory domain

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

Filtering the contents of a container

If a container, such as an Organizational Unit in your Active Directory, holds a 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), then click its name in the list of search results on the **Search** page.
    - 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, then configure and perform a search as described in Searching for directory objects.
2. Specify how you want to filter the objects held in the container:
    - To filter objects by naming properties, enter them in the **Filter** field on the Toolbar, 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 entered. The naming properties include name, first name, last name, display name, and login name.
    - To filter objects by other properties, expand the Toolbar with the button on the right side of the Toolbar, and click **Add criteria**. Then, choose the properties by which you want to filter, click **Add**, and 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. Once you no longer need it, you can remove the filter to view all objects again:

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

Filtering by object type

To improve searching for specific objects, you can filter by object type in the Active Roles Web Interface. The following example procedure shows to configure such a filter.

To configure a filter that lists only user accounts held in a particular Organizational Unit or remove objects of any other type from the list

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

Performing Batch operations

The Active Roles Web Interface supports selecting multiple objects (such as users, groups and computers), and performing specific commands on the selected objects. This allows you to perform a batch operation on all the selected objects at a time instead of running the command on each object separately. The Web Interface supports the following batch operations:

- **Delete**: Allows you to delete multiple objects at a time.
- **Deprovision**: Allows you to deprovision multiple users or groups at a time.
- **Move**: Allows you to move a batch of objects to a different Organizational Unit or container.
- **Add to groups**: Allows you to add a batch of objects to one or more groups of your choice.
- **Update object attributes**: Allows you to perform bulk attributes operations for multiple users at a time.
- **Reset Password**: Allows you to reset the password for multiple users at a time.

Batch operations are available in the list of objects on the following Web Interface pages:

- **Search**: This page lists the search results when you perform a search.
- **View Contents**: This page displays the objects held in a given Organizational Unit, Managed Unit, or container.

To perform a batch operation, select the check box next to the name of each of the desired objects in the list, then click a command in the top area of the **Command pane**. This runs the command on each object within your selection.

NOTE: Active Roles administrators can customize Web Interface by adding and removing commands, and modifying pages associated with commands. For more information, see *Customizing the Web Interface* in the *Active Roles Web Interface Configuration Guide*.

Performing bulk operation

Active Roles Web Interface enables you to perform bulk attributes operation for multiple users at a time.

To perform bulk attribute operation

1. On the **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click the required container.
3. From the list of objects displayed for the selected container, select the required users for which you need to perform bulk attributes operation.

   The batch operations that can be performed on users are displayed in the **Command** pane.
4. In the **Command** pane, click **Update object attributes**.

   The **Update object attributes** window is displayed, which lists the user attributes that can be selected for bulk operation.
5. From the **Attribute List** tab, select the required attribute on which you want to perform the bulk operation, and click the **+** symbol.
6. On the **Update object attributes** dialog box that is displayed, in the **New Value** field, enter a value for the attribute, and click **OK**.

   The selected attribute with the updated value is displayed in the **Select attribute** table.
7. Repeat step 5 and step 6 to select and update more attributes, and then click **Next**.

   The **Preview tab** > **Operation Summary** section displays the summary of the selected attributes with the new values to be updated after the bulk operation is performed. To export the details, click **Export as CSV**.
8. Click **Finish**, to complete the bulk operation on the selected attributes for the multiple users.

NOTE:

- The bulk operation does not complete and an error is displayed if no attributes are selected or if no changes are made to the values of the attributes selected for the bulk operation.
- The bulk operation cannot be performed beyond 1500 users. However, you can configure the limit to increase the number of users. For more information on configuring the limit, see Not able to query or update groups with more than 1500 members.

Performing bulk users password reset operation

Active Roles Web Interface enables you to reset the password for multiple users at a time.

To perform bulk users password reset operation

1. On the **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click the required container.
3. From the list of objects displayed for the selected container, select the required users for which you need to perform password reset operation.

   The batch operations that can be performed on users are displayed in the **Command** pane.
4. In the **Command pane**, click **Reset Password**.

   The **Reset Password** window is displayed.
5. On the **General** tab dialog box, click **Generate** to generate a new password for the selected users.
6. Under **Account** options, select the check box corresponding to the required rule to be applied for change of password, and then click **Save**.

The password reset gets completed and the changes can be viewed on the selected user's **Change History** tab.

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 must 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 can 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, then click **Save current view**.
3. In the dialog box that appears, type a name for the personal view, then click **Save**.

Changing a personal view

The personal views that you created are listed on the **Views** tab in the Browse pane. When you select a view in the Browse pane, 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. At this point, you can make changes to the search or filter criteria, set of columns and sort order, and then save the changed settings to the selected personal view or create a new personal view based on the changed settings.

To save the changed settings to the selected personal view

1. Select a personal view in the Browse pane.
2. Make changes to the search or filter criteria, list columns or sort order.
3. Click the Menu button on the left side of the Toolbar, then click **Save current view**.
4. In the dialog box that appears, keep the current name of the view. Click **Save**.

To create a new personal view based on the changed settings

1. Select a personal view in the Browse pane.
2. Make changes to the search or filter criteria, list columns or sort order.
3. Click the Menu button on the left side of the Toolbar, then click **Save current view**.
4. In the dialog that appears, type a name for the new personal view, then click **Save**.

You can also rename or delete personal views.

To rename a personal view

- On the **Views** tab in the Browse pane, click **Edit** next to the name of the view, type a new name, then press **Enter** or click **Edit** again.

To delete a personal view

- On the **Views** tab in the Browse pane, click **Delete** next to the name of the view.

Performing Management Tasks

The Active Roles Web Interface provides the following management tasks for administrators and helpdesk personnel.

- Managing your personal account
- Managing Active Directory objects
- Running an automation workflow
- Managing temporal group memberships
- Managing AD LDS data
- Managing computer resources
- Restoring deleted objects

Managing your personal account

You can view or modify your own user information (such as phone number or email address) with the **User Profile Editor** of the Active Roles Self-Service Site. The available options of the **User Profile Editor** are customized by the Active Roles administrator of your organization, who can add new elements to the pages, modify or remove existing elements, and regroup related elements on different tabbed pages.

To view or modify your user account

1. In your web browser, open the Self-Service Site of the Web Interface.

   By default, the address is `http://<server>/ARWebSelfService` where `<server>` is the name of the machine running the Web Interface component.
2. On the home page of the Self-Service Site, click **User Profile Editor**.
3. Use the available options to view or modify your account as needed.

   NOTE: The number and type of fields you can edit depend on your organizational policies, and are configured accordingly by Active Roles administrators. The **User Profile Editor** also shows the fields that you cannot edit: those fields are indicated

as read-only.

4. To apply your changes, click **Save**.

Managing Active Directory objects

The **Directory Management** section of the Web Interface allows you to browse for, and administer, directory objects in your organization. You can navigate through containers in the directory; view, filter and select objects held in the container; and apply commands to the selected object or container.

Whether you can perform a certain management task depends upon permissions granted to your user account, and the Web Interface customization settings.

NOTE: If your environment has a large number of Microsoft Exchange mailboxes (or a complex Microsoft Exchange deployment), Active Roles may retrieve the properties of users with Exchange mailboxes slower than for users without Exchange mailboxes.

To solve this problem, enable a performance fix by creating a new registry key as described in Knowledge Base Article 4336544:

1. On the machine(s) running the Administration Service and the Web Interface, launch the Windows Registry Editor.
2. In the Registry Editor, navigate to the following registry path:

   `HKEY_LOCAL_ MACHINE\SOFTWARE\One Identity\Active Roles\Configuration`
3. Create a new **DWORD (32-bit) Value** named `PerformanceFlag`.
4. Double-click the new **PerformanceFlag** DWORD, and set its **Value data** to `1`.
5. To apply the fix, restart the Active Roles Administration Service and IIS. If the fix is enabled successfully, the following Active Roles event log with Event ID 2508 will appear in the Event Viewer:

   ```
   Performance flag value set to 1.
   ```
6. (Optional) To deactivate the fix later, set the **Value data** of the **PerformanceFlag** DWORD to 0.

The **PerformanceFlag** registry key accepts only a value of `1` (to activate the fix) or `0` (to deactivate it).

To perform a management task

1. On the Navigation bar, click **Directory Management**.
2. On the **Views** tab in the Browse pane, click one of the following:
   - To manage objects in Active Directory containers, such as domains or Organizational Units, click **Active Directory**. This displays a list of Active Directory domains.

- To manage directory objects in a certain Managed Unit, click **Managed Units**. This displays a list of Managed Units.

3. In the list of objects, do one of the following:
   - To navigate to a container, such as an Organizational Unit, click the name of that container.
   - To perform a command that applies to the current container, click that command in the Command pane under the name of the current container.
   - To perform a command on a particular object held in the current container, select the check box next to the name of that object, then click the command in the top area of the Command pane, under the name of the object.
   - To perform a command on two or more objects at a time, select the check box next to the name of each object, then click the command in the top area of the Command pane.

   NOTE: In the list of objects, clicking the name of a leaf object such as a user or group, will display a page where you can view or modify object properties. Clicking a container object such as a domain or an organizational unit will display a list of objects held in that container.

When you perform a management tasks, the Web Interface supplements and restricts your input based on policies and permissions defined in Active Roles. The Web Interface displays the data generated by policies, and prevents the input of data that would cause policy violations. The following rules apply:

- If a policy requires that a value be specified for a particular property, the name of the field for that property is marked with an asterisk (*).
- If a policy imposes any restrictions on a property, an information icon is displayed next to the name of the field for that property. Click the icon to view policy information, which you can use to enter an acceptable value.
- When you specify a property value that violates a policy, and click **Save**, the Web Interface displays an error message. Review the error message and correct your input.
- Pages for object creation must include the entries for all required properties. Otherwise, the Web Interface fails to create the object. For information on how to configure forms, see *Configuring forms* in the *Active Roles Web Interface Configuration Guide*.
- Object property pages display the values of the properties for which you have the Read permission. You can modify only those properties for which you have the Write permission. The properties for which you only have the Read permission are displayed as read-only.
- The Command pane includes only the commands that you are permitted to use.
- The list of objects includes only the objects that you are permitted to view.

Batch operations

In the Web Interface, you can select multiple objects (such as users, groups and computers), then apply a certain command to your selection of objects. This allows you to perform a batch operation on all the selected objects at a time instead of running the command on each object separately. The Web Interface supports the following batch operations:

- **Delete** Allows you to delete multiple objects at a time.
- **Deprovision** Allows you to deprovision multiple users or groups at a time.
- **Move** Allows you to move a batch of objects to a different Organizational Unit or container.
- **Add to groups** Allows you to add a batch of objects to one or more groups of your choice.
- **Update object attributes** Allows you to perform bulk attributes operations on multiple users at a time.
- **Reset Password** Allows you to reset the password for multiple users at a time.

Batch operations are available in the list of objects on the following Web Interface pages:

- **Search** This page lists the search results when you perform a search.
- **View Contents** This page displays the objects held in a given Organizational Unit, Managed Unit, or container.

To perform a batch operation, select the check box next to the name of each of the desired objects in the list, then click one of the available commands in the Command pane. This runs the command on each object within your selection.

NOTE: Active Roles administrators can customize Web Interface by adding and removing commands, and modifying pages associated with commands. For more information, see *Customizing the Web Interface* in the *Active Roles Web Interface Configuration Guide Guide*.

Enabling a user account

You can enable a disabled user account with the Web Interface.

To enable a disabled user account

1. Locate the user account you want to enable. For instructions on how to locate objects in the Web Interface, see Locating directory objects.
2. In the list of objects, select the user account you want to enable.
3. In the Command pane, click **Enable Account**.

NOTE: If the user account is not disabled, the Command pane includes the **Disable Account** command instead of the **Enable Account** command.

Adding a user to a group

You can add user accounts to a group with the Web Interface.

To add a user account to a group

1. In the Web Interface, locate and select the user account. For more information on locating objects in the Web Interface, see Locating directory objects.
2. In the Command pane, click **Member Of**.
3. On the **Member Of** page that appears, click **Add**.
4. On the **Select Object** page that appears, perform a search to locate the group. For more information on how to search in the Web Interface, see Searching for directory objects.
5. In the list of search results on the **Select Object** page, select the group to which you want to add the selected user account, then click **Add**.

Running an automation workflow

Workflow refers to a sequence of actions that leads to the completion of a certain task. Active Roles allows administrators to configure various workflows that can be started on a scheduled basis or on user demand. This workflow type is called *automation workflow*. For more information, see *Automation workflow* in the *Active Roles Administration Guide*.

If an automation workflow is configured so that running it on demand is allowed, then such a workflow can be run from the Web Interface.

To run an automation workflow from the Web Interface

1. On the Navigation bar, click **Directory Management**.
2. On the **Tree** tab in the Browse pane, expand the **Workflow** branch and click the container that holds the desired workflow.
3. In the list of objects, select the desired workflow.
4. In the Command pane, click **Run**.
5. If prompted, review or change the values of the workflow parameters.
6. Click **OK** in the confirmation message box.

The Web Interface prompts you for parameter values if the workflow has any parameters that need to be supplied by the user running the workflow on demand. If the workflow has no parameters that require user input, then the Web Interface starts the workflow without prompting you for parameter values.

Once you have started an automation workflow, the Web Interface opens a run history report allowing you to examine the progress of the workflow run. The report displays the workflow run status along with information about the activities performed during the run. For a workflow that is in progress, you can cancel its run by clicking **Terminate**.

After the workflow is completed, the report retains history information about the workflow run. For each completed run of the workflow, the report allows you to identify when and by whom the workflow was started, when the workflow was completed, and what parameter values were used.

The report also lists the workflow activities that were initiated during the workflow run. For each activity, you can determine whether the activity was completed successfully or returned an error. In case of error, the report provides an error description. For activities requesting changes to directory data (for example, activities that create new objects or modify existing objects), you can examine the requested changes in detail by clicking the Operation ID number in the run history report.

To view run history of an automation workflow in the Web Interface

1. On the Navigation bar, click **Directory Management**.
2. On the **Tree** tab in the Browse pane, expand the **Workflow** branch and click the container that holds the desired workflow.
3. In the list of objects, select the desired workflow.

In the Command pane, click **Run History**.

Managing temporal group memberships

By using temporal group memberships, you can manage group memberships of objects such as user or computer accounts that need to be members of particular groups for only a certain time period. This feature gives you flexibility in deciding and tracking what objects need group memberships and for how long.

This section guides you through the tasks of managing temporal group memberships in the Web Interface. If you are authorized to view and modify group membership lists, then you can add, view and remove temporal group members as well as view and modify temporal membership settings on group members.

Adding temporal members

A temporal member of a group is an object, such as a user, computer or group, scheduled to be added or removed from the group. You can add and configure temporal members using the Web Interface.

To add temporal members to a group

1. In the Web Interface, select the group, and then choose the **Members** command.
2. On the **Members** page, click **Add**.
3. In the **Select Object** dialog, find and select the objects that you want to make temporal members of the group, then click **Temporary Access**.
4. In the **Temporal Membership Settings** dialog, select the appropriate options, then click **OK**:
    - To have the temporal members added to the group on a certain date in the future, select **On this date** under **Add to the group**, and choose the date and time you want.
    - To have the temporal members added to the group at once, select **Now** under **Add to the group**.
    - To have the temporal members removed from the group on a certain date, select **On this date** under **Remove from the group**, and choose the date and time you want.

- To retain the temporal members in the group for indefinite time, select **Never** under **Remove from the group**.

NOTE: You can make an object a temporal member of particular groups by managing the object rather than the groups. Select the object, and then choose the **Member Of** command. On the **Member Of** page, click **Add**. In the **Select Object** dialog box, find and select the groups, and specify the temporal membership settings as appropriate for your situation.

Viewing temporal members

In the list of group members displayed by the Web Interface, you can distinguish between regular and temporal group members. It is also possible to hide or display so-called pending members, the temporal members that are scheduled to be added to the group in the future but are not actual members of the group so far.

To view temporal members of a group

1. In the Web Interface, select the group, and then choose the **Members** command.
2. Review the list on the **Members** page:
   - An icon of a small clock overlays the icon for the temporal members.
   - If the **Show pending members** check box is selected, the list also includes the temporal members that are not yet added to the group.

The list of group memberships for a particular object makes it possible to distinguish between the groups in which the object is a regular member and the groups in which the object is a temporal member. It is also possible to hide or display so-called pending group memberships, the groups to which the object is scheduled to be added in the future.

To view groups in which an object is a temporal member

1. In the Web Interface, select the object, then choose the **Member Of** command.
2. Review the list on the **Member Of** page:
   - An icon of a small clock overlays the icon for the groups in which the object is a temporal member.
   - If the **Show pending group memberships** check box is selected, the list also includes the groups to which the object is scheduled to be added in the future.

Rescheduling temporal group memberships

The temporal membership settings on a group member include the **start time** and **end time** settings.

The start time setting specifies when the object is to be actually added to the group. This can be specific date and time or an indication that the object should be added to the group right away.

The end time setting specifies when the object is to be removed from the group. This can be specific date and time or an indication that the object should not be removed from the group.

You can view or modify both the start time and end time settings using the Web Interface.

To view or modify the start or end time setting for a member of a group

1. In the Web Interface, select the group, then choose the **Members** command.
2. In the list on the **Members** page, select the member, then click the **Temporary Access** button.
3. To view or modify the start or end time settings, use the **Temporal Membership Settings** dialog.

The **Temporal Membership Settings** dialog box provides the following options:

- **Add to the group** > **Now**: Adds the object to the group immediately.
- **Add to the group** > **On this date**: Adds the object to the group on the specified date and time.
- **Remove from the group** > **Never**: Specifies that the object will not be removed from the group automatically.
- **Remove from the group** > **On this date**: Removes the object from the group on the specified date and time.

Regular members have the **Add to group** and **Remove from group** options set to **Already added** and **Never**, respectively. To convert a regular member to a temporal member, set a specific date with these options for the member.

NOTE: Consider the following when configuring temporal group memberships:

- You can view or modify the start time and end time settings by managing an object rather than the groups in which that object has memberships. To do so, select the object, then choose the **Member Of** command. On the **Member Of** page, select the group for which you want to manage the object's start or end time setting and click **Temporary Access**.
- On the **Members** or **Member Of** page, you can change the start or end time setting for multiple members or groups at a time. On the page, select multiple list items, click **Temporary Access**, then, in the **Temporal Membership Settings** dialog, make the changes you want.

Removing temporal members

You can remove temporal group members in the same way as regular group members. Removing a temporal member of a group deletes the temporal membership settings for that object with respect to that group. As a result, the object will not be added to the group.

If the object already belongs to the group at the time of removal, then it is removed from the group.

To remove a temporal member of a group

1. In the Web Interface, select the group, then click **Members**.
2. On the **Members** page, select the member, and click **Remove**.

NOTE: You can remove an object that is a temporal member of a group by managing the object rather than the group. Select the object, then choose the **Member Of** command. On the **Member Of** page, select the group from the list and click **Remove**.

Managing Azure AD, Microsoft 365, and Exchange Online objects

Active Roles facilitates the administration and provisioning of Active Directory (AD), Exchange, and Azure AD resources in on-premises, cloud-only and hybrid environments as well. You can manage all these resources through the Active Roles Web Interface.

Managing cloud-only Azure contacts

Active Roles provides the facility to perform administrative tasks such as create, read, update, and delete Azure contact on cloud through web interface. You can also perform other operations such as viewing and modifying the Azure cloud-only contact, view change history, and other operations related to Azure cloud-only contacts.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

Create a new Microsoft 365 contact

You can use the Active Roles Web Interface to create and enable a new Microsoft 365 contact.

To create a new Microsoft 365 contact

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the domain in which you want to create a new contact.

4. In the list, click the required **Container** or the **Organizational Unit**.
5. In the **Command** pane, click **New Contact**.
6. In the **New Contact <OU-name>-General** wizard, enter the contact details such as **First Name**, **Last Name**, **Initials**, and **Display name**.
7. Click **Next**.
8. In the **Create Azure Account Properties** wizard, select **Create Azure Contact**.
9. From the **Tenant**, select the **Tenant name**.
10. In the **External e-mail address** field, enter the email address for the contact, and click **Finish**.

    The Microsoft 365 account details for the new contact are generated automatically and populated in the respective fields.

NOTE: In Federated or Synchronized environments, Microsoft 365 contact creation is not supported. The contact is created in Active Roles and is synchronized eventually to Microsoft 365 using Microsoft Native tools, such as AAD Connect. To manage the Microsoft 365 contact through Active Roles, you must perform periodic back-synchronization to on-premise AD.

View or modify the Microsoft 365 contact properties

For an existing Microsoft 365 contact, you can use the Active Roles Web Interface to modify the Microsoft 365 contact properties.

To view or modify the Microsoft 365 contact properties

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then select the check box corresponding to the specific contact for which you want to view or update the Manager information.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** dialog for the contact is displayed.
5. To view or modify properties of the Microsoft 365 contact, use the tabs in the **Azure Properties** dialog.
6. After setting all the required properties, click **Save**.

View the change history of an Microsoft 365 contact

You can use the Active Roles Web Interface to view the change history of an Microsoft 365 contact.

To view the change history of an Microsoft 365 contact

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then the specific contact.
4. In the **Command** pane, click **Change History**.

   Change History displays the information on changes that were made to the contact through Active Roles.

Delete an Microsoft 365 contact

You can use the Active Roles Web Interface to delete a contact for logon to Azure.

To delete an Microsoft 365 contact

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then the specific contact that you want to delete.
4. In the **Command** pane, click **Delete**.

   The contact is deleted.

Managing Hybrid AD users

The Active Roles Web Interface allows you to perform administrative tasks, for example, create, read, update, deprovision, undo-deprovison, and delete Azure AD users in Hybrid environment. You can also perform other operations, for example, add and remove Azure AD users to groups and assign Office 365 licenses to users. Some of the user operations can be performed using the Management Shell in addition to the Web Interface. The following section guides you through the Active Roles Web Interface and Management Shell to manage Azure AD users.

Creating a new Azure AD user with the Web Interface

You can use the Active Roles Web Interface to create and enable a new Azure AD user. You can also assign Microsoft 365 licenses to the new user.

To create a new Azure AD user with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the domain in which you want to create a new user.
4. In the list of objects, click the required **Container** or the **Organizational Unit**.
5. In the **Command** pane, click **New User**.
6. In the **New User** in **<OU name>** > **General** wizard, enter the user details, for example, **First Name**, **Last Name**, **Initials**, and **User logon name.**
7. Click **Next**.
8. In the **Account** properties wizard, to generate a password for the Account, click **Generate** , select the required Account options and then click **Next**.

   Alternatively, you can set the password manually and re-enter in the **Confirm Password** field to confirm the entered password.
9. In the **Create Azure Account** wizard, select the option **Create Azure Account**.

   The Azure AD account details for the new user are generated automatically and populated in the respective fields.

   NOTE: The **Temporary Password** field is populated with the default password set for the Active Roles user. You can reset the password for the Azure AD account if required.
10. Select the **Tenant name** from the **Tenant list** drop down. From the **User Principal Name** drop-down list, select the AD domain to which you want to associate the Azure AD user.
11. In **Usage Location**, select the geographical location where Active Roles will be used.

    NOTE: Local rules and regulations for using products and services associated with the configured user can vary by user location. As a result, the **Usage Location** field is mandatory: if you do not select a country, Active Roles cannot assign Microsoft licenses to the hybrid Azure user.
12. Click **Next**.

    The **Licenses** wizard displays the Microsoft 365 licenses, for example the Microsoft 365 Business Essentials and Business Premium licenses, and the number of licenses that are available to assign to the user.

13. Select the check boxes corresponding to the license that needs to be assigned to the user, and click **Next**.

    The **O365 Roles** wizard displays the Microsoft 365 roles, for example, the **Helpdesk Administrator**, **Directory Readers**, and more.

14. Select the Microsoft 365 roles that you want to assign to the user, and click **Finish**.

You can view the assigned licenses on the user's **Azure Properties** > **Licenses** wizard.

You can view the assigned Microsoft 365 roles on the user's **Azure Properties** > **O365 Roles** wizard.

The results can also be viewed on the Azure portal's **Licenses** and **Directory role** tabs.

Viewing or updating the Azure AD user properties with the Web Interface

For an existing Azure AD user, you can use the Active Roles Web Interface to view or update the properties.

To view or modify the Azure AD user properties with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Tree** tab in the **Browse** pane, click **Active Directory** > **<Domain>** > **<Organizational Unit>**.

   The list of existing AD users are displayed.

3. Select the specific Azure AD user for which you want to view or modify the Azure properties.
4. In the **Command** pane, click **Azure Properties**.

   The **Azure Properties** wizard for the Azure AD user is displayed.

5. Use the fields in the **Azure Properties** wizard to view or modify the properties of the Azure AD user.
6. After setting all the required properties, click **Save**.

   You can view the modified settings on the Azure Portal.

Viewing or modifying the manager of a hybrid Azure user

You can use the **Managed by** setting of the Active Roles Web Interface to modify the assigned manager of a hybrid Azure user. This is typically required in case of organizational changes, for example during a change of management, or when the user is assigned to another team or department within your organization.

To view or modify the Managed by setting of a hybrid Azure user

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Active Directory**.

   The list of Active Directory (AD) domains configured in your organization appears.
2. Click the specific domain, container or Organizational Unit (OU) where the hybrid Azure user is managed.
3. To view the management properties of the user, select the user, then click **General properties** > **Managed by**.
4. To modify the management properties of the user, in the **Managed by** tab, click **Change**. Then, use the **Select Objects** dialog to locate and select the manager to assign to the user. To apply your selection, click **OK**.

   The new manager then appears in the **Manager** field.
5. To apply your changes, click **Save**.

   The **Azure Properties** > **Manager ID** field will then display the new manager information.

TIP: To verify the changes in Microsoft Azure, check the **Work Info** > **Manager ID** value of the Azure Portal.

Disabling an Azure AD user

You can use the Active Roles Web Interface to disable a user for logon to Azure. This allows you to disable a previously enabled user in Azure AD while retaining all the Azure settings that were configured for the user. The Azure AD user settings are retained for a disabled account. Hence you can re-enable a disabled user again without having to reconfigure the user.

To disable a previously enabled user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user that you want to disable.
4. In the **Command** pane, click **Disable**.

   The account is disabled and marked with a disabled icon.

If you want to enable a previously disabled Azure AD user, see Enabling an Azure AD user.

Enabling an Azure AD user

Active Roles Web Interface allows you to enable a previously disabled user in Azure AD while retaining all the Azure settings that were configured for the user. The Azure AD user settings are retained for a disabled account. Hence you can re-enable a disabled user again without having to reconfigure the user.

To enable a previously disabled user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user that you want to disable.
4. To enable a disabled account, select the disabled account and in the **Command** pane click **Enable**.

   NOTE: The **Enable** command only appears for a disabled account.

   The account is enabled again.

If you want to disable a previously enabled Azure AD user, see Disabling an Azure AD user.

Deprovisioning of an Azure AD user

Active Roles provides the ability to deprovision rather than delete or only disable users. Deprovisioning a user refers to a set of actions that are performed by Active Roles in order to prevent the user from logging on to the network and accessing network resources such as the user's mailbox or home folder.

The **Deprovision** command on a user updates the account as prescribed by the deprovisioning policies. Active Roles comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the administrator to configure and apply additional policies.

To deprovision a user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Select the user, and in the **Command** pane, click **Deprovision**.

   A message is displayed prompting you to confirm the account deprovision.
4. Click **Yes**, to continue.

   Wait while Active Roles updates the user.

After the task is completed, a message is displayed that the account is deprovisioned successfully from Active Roles.

If you want to undo the deprovisioning of an Azure AD user, see Undo deprovisioning of an Azure AD user.

Undo deprovisioning of an Azure AD user

To undo deprovision of a user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Select the user, and in the **Command** pane, click **Undo Deprovisioning**.

   The **Password Options** dialog is displayed.
4. Select the option to **Leave the Password** unchanged or **Reset** the password, and click **OK**.

If you want to deprovision an Azure AD user, see Deprovisioning of an Azure AD user.

Adding an Azure AD user to a group

You can use the Active Roles Web Interface to add an existing Azure AD user to a group.

To add an Azure AD user to a group

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user that you want to add to a group.
4. Select the user and in the **Command** pane click **Member Of**.

   The existing Group information for the user is displayed.
5. To add the user to another group, in the **<User> (objects found)** wizard, click **Add**.
6. In the **Select Object** wizard, search and select the group to which you want to add the user.
7. In details pane, right-click the user, and then click **Add to a Group**.

   The **<User> (objects found)** wizard displays all the groups to which the account has been added as a member.

If you want to remove an existing Azure AD user from a group, see Removing an Azure AD user from a group.

Removing an Azure AD user from a group

You can use the Active Roles Web Interface to remove an existing Azure AD user from a group.

To remove an Azure AD user from a group

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user that you want to remove from a group.
4. Select the user and in the **Command** pane click **Member Of**.

   The existing Group information for the user is displayed.
5. In the **<User> (objects found)** wizard, select the group from which you want to remove the user and click **Remove**.

   A message prompts you to confirm the action.
6. Click **Yes** to continue.

   The group information is removed from the **<User> (objects found)** wizard.

If you want to add an existing Azure AD user to a group, see Adding an Azure AD user to a group.

View the change history and user activity for an Azure AD user

You can use the Active Roles Web Interface to view the change history and user activity of an Azure AD user.

To view the change history and user activity of an Azure AD user

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user.
4. In the **Command** pane, click **Change History** or **User Activity**.

- **Change History** displays the information on changes that were made to the user through Active Roles.
- **User Activity** displays information on management actions that were performed by a given user.

Deleting an Azure AD user with the Web Interface

You can use the Active Roles Web Interface to delete a user for logon to Azure.

Prerequisites

Only **Global Admins** can delete Azure users with any roles assigned to them.

CAUTION: Hazard of data loss!

Deleting a user is a destructive operation that cannot be undone. A new user with the same name as a deleted user does not automatically get the same permissions and memberships as the deleted account. Because of this, One Identity recommends to disable rather than delete accounts.

To delete an Azure AD user with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then the specific user that you want to delete.
4. In the **Command** pane, click **Delete**.

   The account is deleted.

NOTE: In a hybrid environment, the user must be deleted in the on-premises AD first and then the changes must be synchronized with Azure AD. In case, the user is deleted in Azure AD first, the Active Roles Web Interface still displays the Azure properties link for the deleted user but with no information. Further modification of the Azure properties for the deleted user will not be valid.

Creating a new hybrid Azure user with the Active Roles Web Interface

You can use the Active Roles Web Interface to create new hybrid Azure users in your organization.

Prerequisites

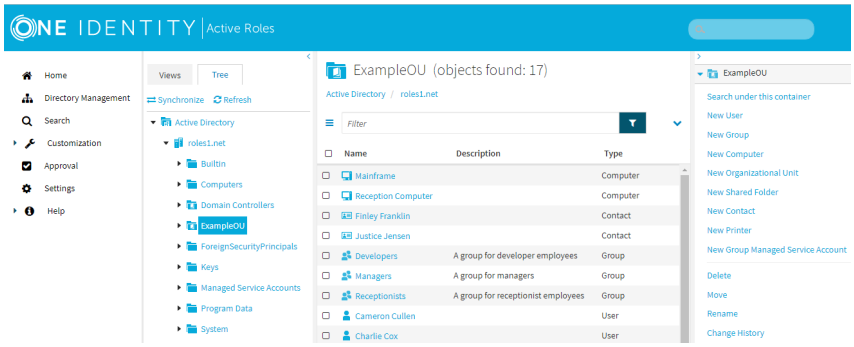
To create new hybrid Azure users, your organization must meet the following requirements:

- To enable remote mailboxes, the Exchange management tools of an on-premises Microsoft Exchange installation must be available. For more information on the Microsoft Exchange Server versions supported by Active Roles, see *System requirements* in the *Active Roles Release Notes*.
- The Active Roles service account must be a part of the **Recipient Management** management role group to run Exchange hybrid commands.

To create a new hybrid user

1. In the Active Roles Web Interface, under **Directory Management** > **Tree** > **Active Directory**, navigate to the OU where you want to create the new hybrid Azure user.

Figure 2: Active Roles Web Interface – Navigating to the OU of the Hybrid Azure user



2. In the list of actions available for the selected OU, click **New User**.
3. In the **General** step, specify the following information as required by your organization:
    - **First name**: The first name of the user.
    - **Last name**: The last name of the user.
    - (Optional) **Initials**: The initials of the user.
    - **Name**: The fully-qualified user name of the user. By default, Active Roles automatically fills this property based on the specified **First name**, **Last name**, and **Initials**.
    - **Display name**: The name of the user as it will appear in Active Directory. By default, Active Roles automatically fills this property based on the specified **Name**.
    - **User logon name**: The user name used to log in to the domain. The **User logon name** also contains a user principal name (UPN) suffix. To configure the appropriate UPN suffix, use the drop-down button and select the appropriate

domain for the user.

NOTE: The list contains:

- The full DNS name of the current domain.
- The full DNS name of the root domain of the current forest.
- Any alternative UPN suffixes created via the Active Directory Domains and Trusts console.

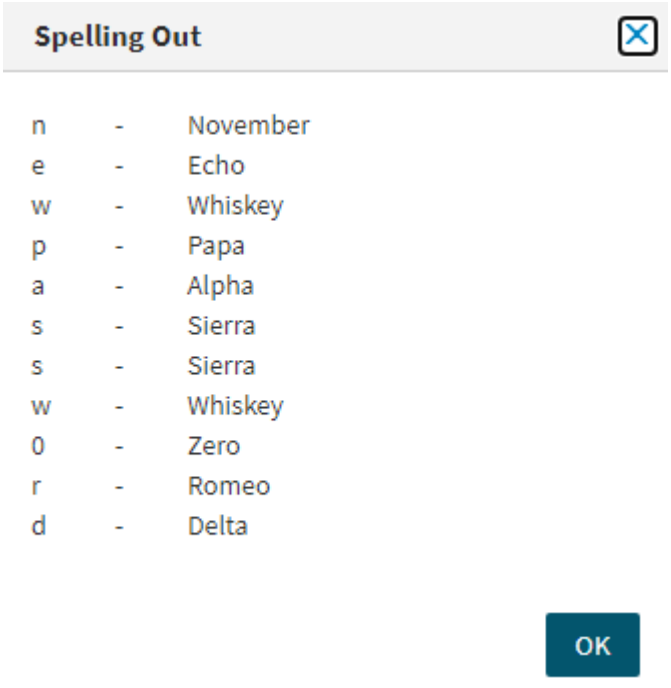
- (Optional) **User logon name (pre-Windows 2000)**: The user name used to log in to the domain, following the pre-Windows 2000 logon name format: `<domain-name>\<user-name>`. By default, Active Roles automatically fills this property based on the specified **User logon name**.

4. In the **Account** step, specify the security settings of the user:

   - **Password** and **Confirm password**: The initial password of the user and the corresponding password confirmation field. You can specify the password either manually, or **Generate** one with Active Roles that follows the password policy requirements of your organization.

     To clear the specified password, click **Clear**. To spell out each character of the password for clarification, click **Spell out**.

     Figure 3: Active Roles Web Interface – Spelling out the characters of the generated or specified password

   - **Account options**: Use these options to specify additional security settings for the user (for example, to have them change the configured password during their next login attempt, or have the configured password expire after some

time). If you want to enable the created user account later for increased security (for example, because the new user joins later to your organization), select **Account is disabled**.

5. In the **Create Mailbox** step, configure whether you want to set up an on-premises Exchange mailbox for the hybrid user, or an Exchange Online mailbox in the cloud:
   - To create a new on-premises Exchange mailbox for the user, keep **Create Exchange Mailbox** selected.
   - To create a new Exchange Online cloud mailbox for the user, deselect **Create Exchange Mailbox**.
6. In the **Create Azure Account** step, to generate the Azure AD account of the hybrid user, select **Create Azure Account**. This automatically populates all respective fields of the configured hybrid user.

   NOTE: Active Roles sets the **Temporary Password** to the default password of the Active Roles user. You can reset this password for the Azure AD account, if required by the security policies of your organization.
7. From the **Tenant** drop-down list, select the Azure tenant where you want to store the new hybrid Azure user.
8. From the **User Principal Name** drop-down list, select the Active Directory (AD) domain with which you want to associate the new hybrid Azure user.
9. In the **Usage Location** field, enter the two-letter county code of the location where the user is expected to log in from.

   NOTE: Local rules and regulations for using products and services associated with the configured user may vary by user location. As a result, the **Usage Location** field is required, as Active Roles cannot assign Microsoft licenses to the hybrid Azure user if no country code is set here.
10. In the **Licenses** step, select **Exchange Online (Plan 2)**, and click **Finish**.

    TIP: You can check the licenses assigned to the new user later by selecting the user, then navigating to **Azure properties** > **Licenses**.

Converting an on-premises user with an Exchange mailbox to a hybrid Azure user

To convert an existing on-premises user with an Exchange mailbox to a hybrid user with an Exchange Online mailbox, follow the procedure described in Move mailboxes between on-premises and Exchange Online organizations in hybrid deployments in the *Microsoft 365 documentation*. Describing the procedure in detail is not in the scope of the *Active Roles Administration Guide*.

NOTE: After the on-premises user mailboxes have been migrated to the Azure cloud, you can enable cloud management in Active Roles by configuring and running the Azure BackSync feature of Active Roles Synchronization Service.

For more information on how to set up Azure BackSync, see *Configuring Azure BackSync* in the *Active Roles Synchronization Service Administration Guide*.

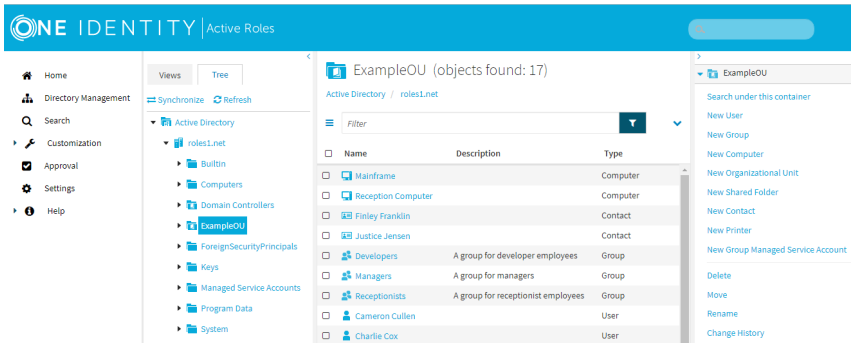
Licensing a hybrid Azure user for an Exchange Online mailbox

To license a hybrid Azure user for an Exchange Online mailbox, use the **Azure Properties** action of the Active Roles Web Interface.

To license a hybrid user for an Exchange Online mailbox

1. In the Active Roles Web Interface, under **Directory Management** > **Tree** > **Active Directory**, navigate to the OU where you want to license the on-premises user.

   Figure 4: Active Roles Web Interface – Navigating to the OU of the on-premises user

2. Select the user that you want to license, then in the list of actions, click **Azure Properties**.
3. In the **Licenses** step, select **Exchange Online (Plan 2)**, and click **Finish**.

Viewing or modifying the Exchange Online properties of a hybrid Azure user

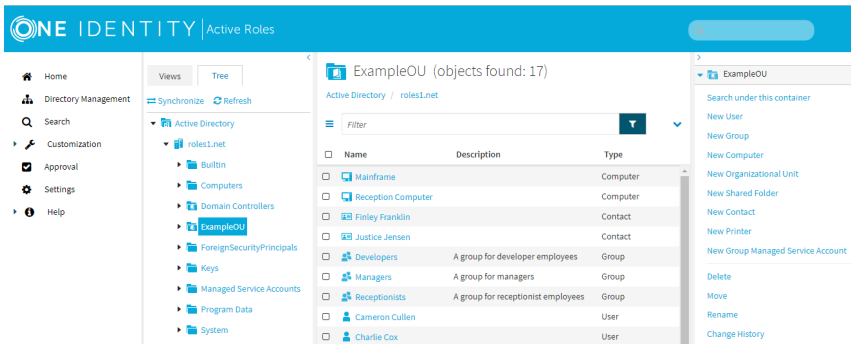
You can view or modify the Exchange Online properties of a hybrid Azure user via the **Exchange Online Properties** action of the Active Roles Web Interface. This is typically required during organizational changes or when the personal information of the user is updated.

NOTE: If the hybrid user is in a Synchronized Identity domain or Federated domain, you can edit most of their Exchange Online attributes with the **Exchange Online Properties** action of the Active Roles Web Interface. However, you cannot edit the **Email address** attribute, as that attribute is synchronized only through native Microsoft tools.

To view or change the Exchange Online properties of hybrid Azure user

1. In the Active Roles Web Interface, under **Directory Management** > **Tree** > **Active Directory**, navigate to the OU of the hybrid user whose Exchange Online properties you want to view or modify.

Figure 5: Active Roles Web Interface – Navigating to the OU of the hybrid user



2. Select the user whose Exchange Online properties you want to check, then in the list of actions, click **Exchange Online Properties**.
3. In the available **Exchange Online Properties** tabs, configure the Exchange Online mailbox settings as you need.

Table 1: Available Exchange Online properties

Page	Description
Mail Flow Settings	View and configure rules for the emails that the mailbox sends or receives via the Exchange Online service.
Delegation	Configure the email account as a shared mailbox.
General	View and configure the email addresses associated with the mailbox.
Mailbox Features	View and configure various Exchange Online mailbox features, for example mobile access, additional mailbox protocols, or archival settings.
Mailbox Settings	View and configure Messaging Records Management (MRM) settings for the mailbox.

4. To apply your changes, click **OK**, then **Finish**.

Configuring the mail flow settings of an Exchange Online mailbox

You can set up rules for the emails that Exchange Online mailboxes send or receive in the organization with the **Exchange Online Properties** > **Mail Flow Settings** tab of the Active Roles Web Interface. Active Roles supports setting up two types of such rules:

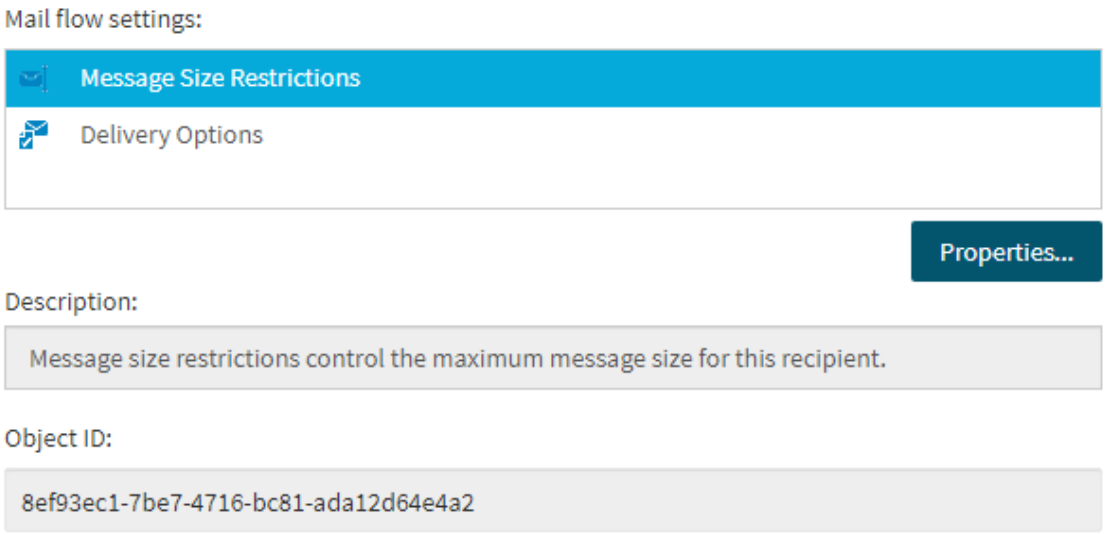
- Message size settings, specifying the size of the emails that the guest user can send or receive.
- Email delivery and forwarding settings, allowing the guest user to send emails on behalf of a specified group, or have their received emails automatically forwarded to an additional specified address.

Such mail flow settings are typically configured if the organization enforces specific email messaging policies for users and guest users.

To configure the mail flow settings for an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the mail flow settings, click the **Mail Flow Settings** tab.

Figure 6: Exchange Online Properties > Mail Flow Settings — Configuring the message size and forwarding settings of an Exchange Online mailbox



5. Select **Message Size Restrictions**, and click **Properties...**.

6. Configure the size of the emails (in KB) that are sent or received by the mailbox. By default, both the **Sending message size** and the **Receiving message size** settings use the default limit of the Azure tenant.
7. To apply your changes and close the **Message Size Restrictions** dialog, click **Save**.
8. Select **Delivery Options**, and click **Properties** to configure the following email delivery and forwarding settings.
    - **Send on Behalf**: When configured, the mailbox can send emails on behalf of the specified mailbox or group.
    - **Forwarding Address**: When configured, the emails received by the mailbox are always forwarded to the specified email address.
9. To apply any changes you made in the **Delivery Options** dialog, click **Save**.
10. To close the **Exchange Online Properties** window, click **Close**.

Configuring the delegation settings of an Exchange Online mailbox

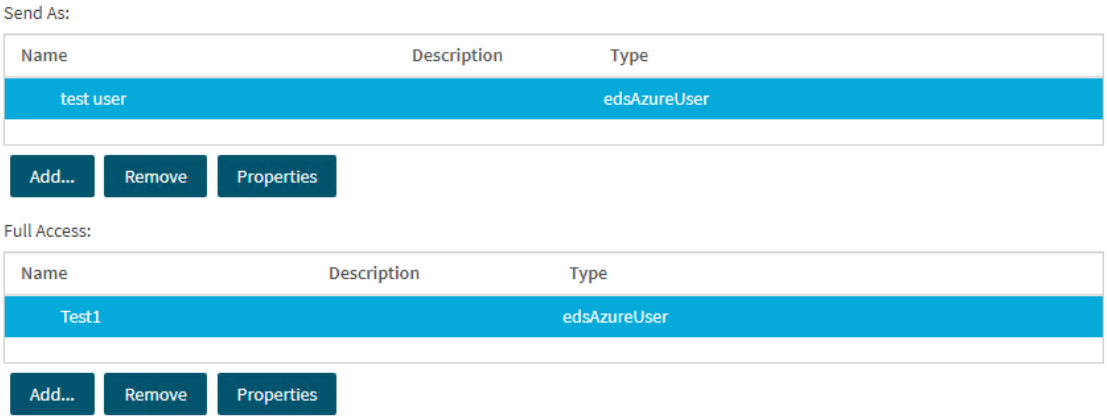
You can set up an Exchange Online mailbox as a shared mailbox in the **Exchange Online Properties** > **Delegation** tab of the Active Roles Web Interface. This is typically performed if the configured email account is used as a group account, such a common support or information email address.

The Active Roles Web Interface supports granting *Send as* and *Full access* permissions to the specified users and guest users. For more information on shared mailboxes and these permissions, see Shared mailboxes in Exchange Online in the *Microsoft Exchange documentation*.

To configure the email delegation settings of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the delegation settings, click the **Delegation** tab.

Figure 7: Exchange Online Properties > Delegation — Accessing the email account delegation settings of an Exchange Online mailbox



5. To delegate *Send as* permission to a user (or users), click **Add...** under the **Send As** list.
6. Select the user(s) you want to grant *Send as* rights for the email address, then click **OK**.
7. To delegate *Full Access* permission to a user (or users) click **Add...** under the **Full Access** list.
8. Select the user(s) you wish to grant *Full access* rights for the email address, then click **OK**.
9. To remove a delegated user either from the **Send As** or **Full Access** list, click **Remove** and select the user(s) you want to revoke the permission from.
10. To apply your changes, click **Save**, then **Close**.

Configuring the general email address settings of an Exchange Online mailbox

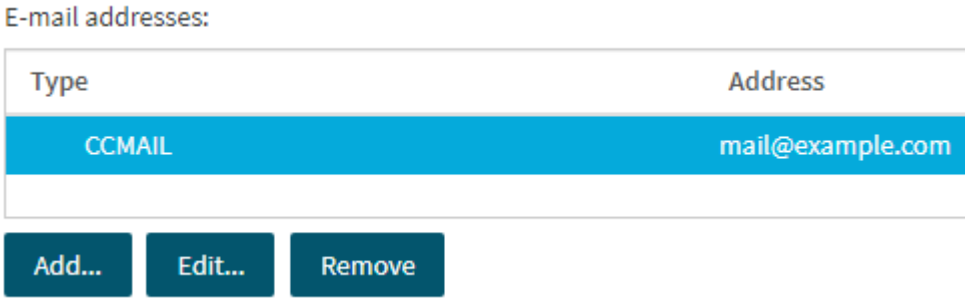
You can add, edit or remove email addresses to or from an Exchange Online mailbox in the **Exchange Online Properties** > **General** tab of the Active Roles Web Interface. Adding, editing, or removing email addresses is typically required in case of organizational changes (for example, the mailbox user is assigned to a new project, or the contract of a guest user ends within the organization).

To add a new email address to an Exchange Online mailbox

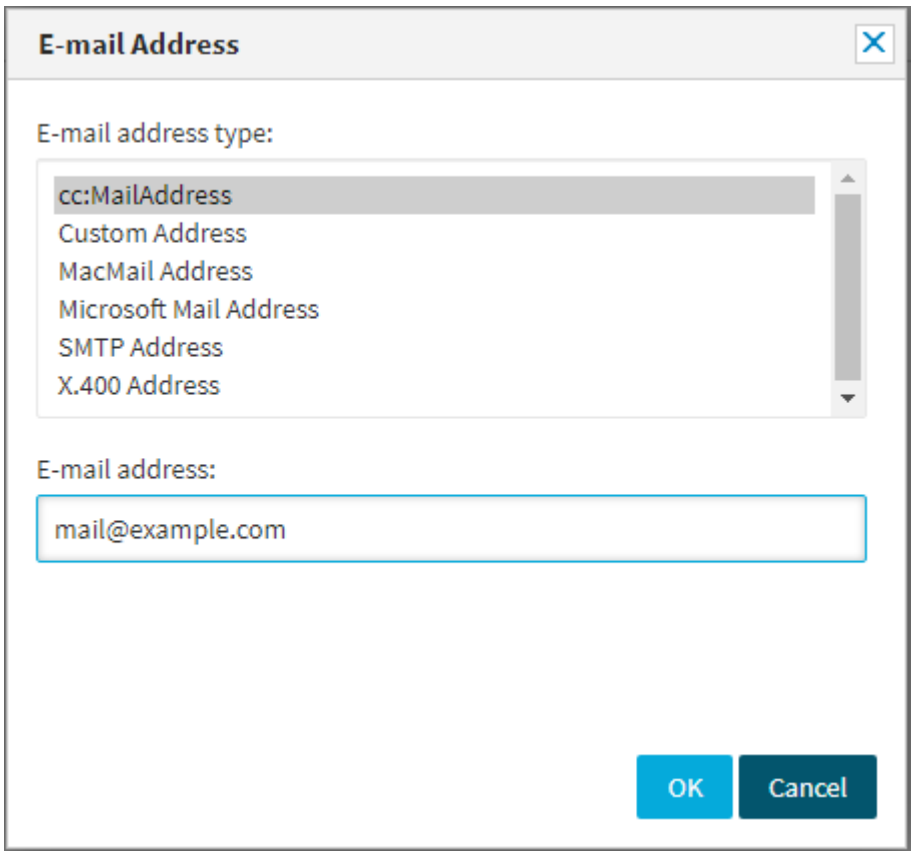
1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.

3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.

Figure 8: Exchange Online Properties > General — Accessing the email account settings of an Exchange Online mailbox



5. Click **Add...**. The **E-mail Address** dialog then opens.



6. From the **E-mail address type** list, select the email account type applicable to your organization.
7. In the **E-mail address** text box, specify the address of the new account.

8. To apply your changes and create the new email account, click **OK**.
9. To close the **Exchange Online Properties** window, click **Close**.

To edit an existing email address of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.
5. To open the settings of an email address, select the email address, then click **Edit...**.
6. In the **E-mail address** text box, modify the current email address.

   NOTE: You cannot modify the **E-mail address type** of an existing email account. You can only change the name of the existing address.
7. To apply your changes, click **OK**.
8. To close the **Exchange Online Properties** window, click **Close**.

To remove an existing email address of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.
5. In the **E-mail addresses** list, select the address you want to remove.
6. Click **Remove** and confirm the deletion of the email address.
7. To close the **Exchange Online Properties** window, click **Close**.

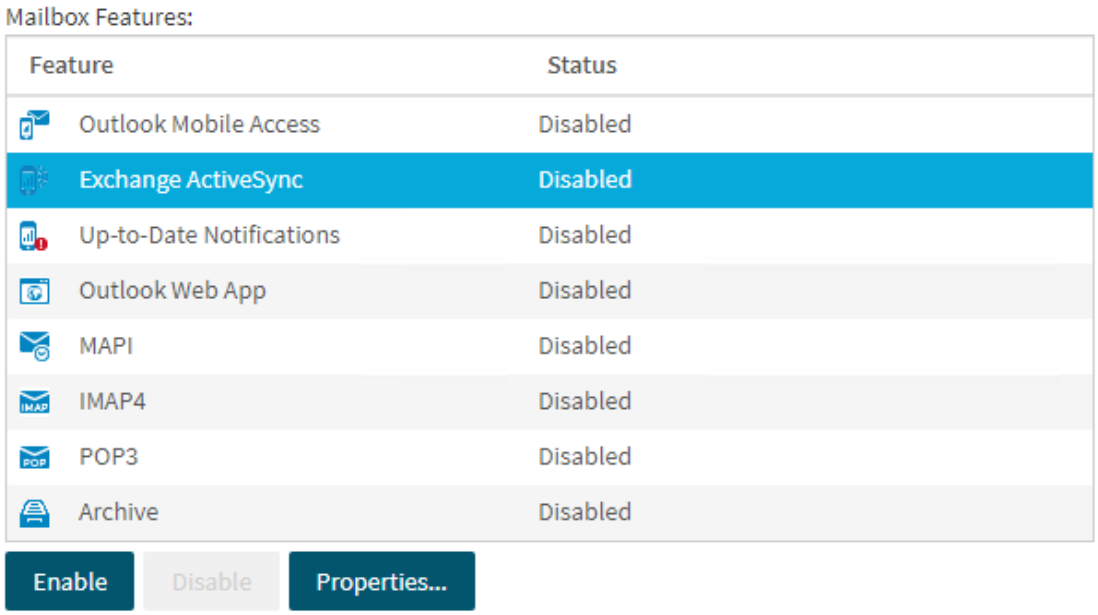
Configuring the mailbox features of an Exchange Online mailbox

You can enable or disable various Exchange Online mailbox features for an Exchange Online mailbox (such as Outlook Mobile Access or support for messaging protocols like IMAP4 or POP3) in the **Exchange Online Properties** > **Mailbox Features** tab of the Active Roles Web Interface. This is typically required if the organization supports specific applications and protocols for its Exchange mailboxes.

To enable or disable Exchange Online mailbox features for an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the mailbox feature settings, click the **Mailbox Features** tab.

Figure 9: Exchange Online Properties > Mailbox Features — Configuring mailbox features for an Exchange Online mailbox



5. Select the Exchange Online mailbox feature that you want to enable or disable:
   - **Outlook Mobile Access**: Enables or disables the Outlook Mobile Access (OMA) mobile browsing service for the mailbox. Enabling this settings allows the mailbox user use OMA on their mobile device to access their account.
   - **Exchange ActiveSync**: Enables or disables the Exchange ActiveSync synchronization protocol for the mailbox. Enabling this setting allows the mailbox user synchronize their configured mobile device with their mailbox.
   - **Up-to-Date Notifications**: Enables or disables the Up-to-date (UTD) feature notifications for the mailbox.
   - **Outlook Web App**: Enables or disables access to the browser-based Outlook Web App for the mailbox user.

- **MAPI**, **IMAP4**, **POP3**: Enables or disables support for the MAPI, IMAP4 or POP3 protocols for the mailbox user. If MAPI is enabled, the mailbox user can access their mailbox through the Outlook desktop app (or other MAPI clients). If IMAP4 or POP3 is enabled, they are also able to access their mailbox with any IMAP4 or POP3 email client.
- **Archive**: Enables or disables the archive mailbox feature for the mailbox.

6. Click **Enable** to enable the selected mailbox feature, or **Disable** to disable it.
7. Once you are done with the configuration, click **Close**.
8. To close the **Exchange Online Properties** window, click **Close**.

Configuring the mailbox settings of an Exchange Online mailbox

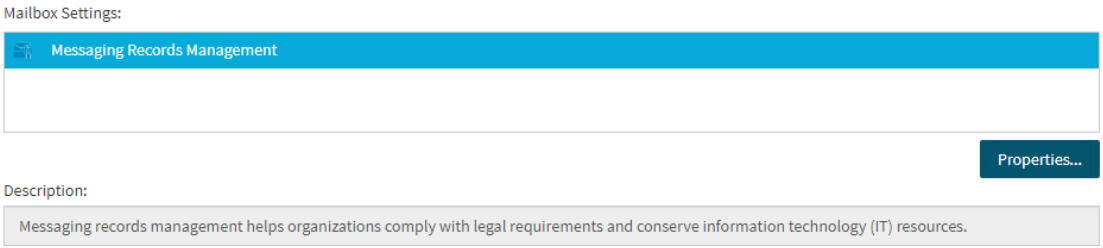
You can configure settings related to Messaging Records Management (MRM) for an Exchange Online mailbox in the **Exchange Online Properties** > **Mailbox Settings** tab of the Active Roles Web Interface. MRM settings are typically configured to meet mailbox archiving policies in effect within the organization.

For more information about MRM in Exchange Online, see Messaging records management in the *Microsoft Exchange Online documentation*.

To configure Messaging Records Management settings for an Exchange Online mailbox

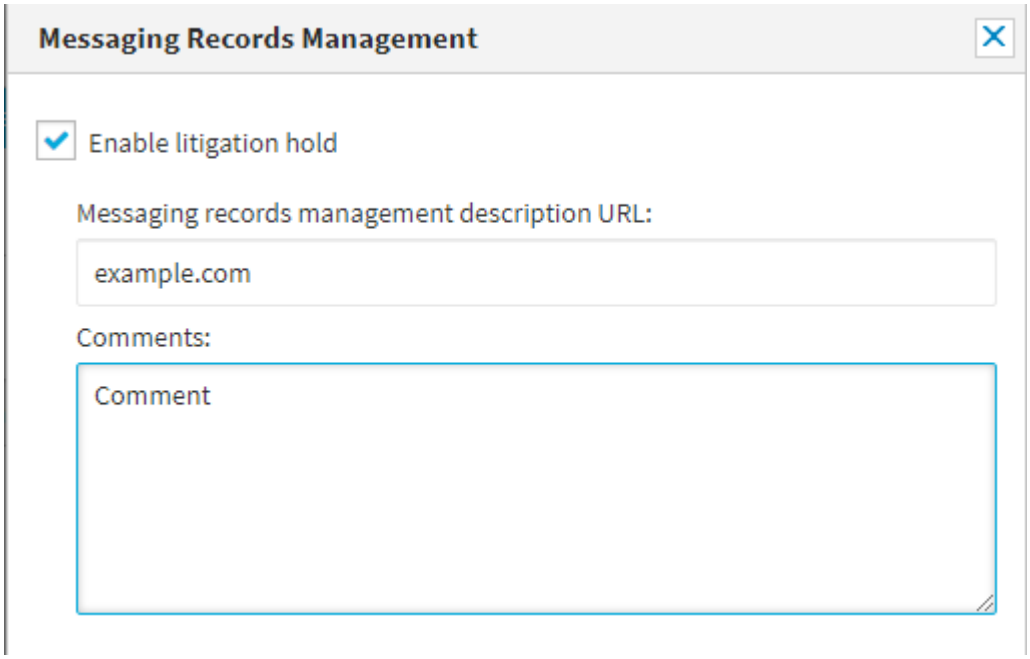
1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the MRM settings, click the **Mailbox Settings** tab.

Figure 10: Exchange Online Properties > Mailbox Settings — Accessing the MRM settings of an Exchange Online mailbox



5. Under **Mailbox Settings**, make sure that **Messaging Records Management** is selected, then click **Properties**. The **Messaging Records Management** dialog

opens.



6. To enable placing the entire contents of the user mailbox on hold, enable the **Enable litigation hold** check box. For more information on the Litigation Hold feature of Exchange Online, see the In-Place Hold and Litigation Hold page of the official Microsoft documentation.
7. (Optional) If your organization has an internal resource on the litigation hold practices, specify its URL in the **Messaging records management description URL** text box.
8. (Optional) If you want to display a customized message in Outlook for the mailbox user on the litigation hold, write the message in the **Comments** text box.
9. Click **Save** to apply your changes and close the **Messaging Records Management** dialog.
10. To close the **Exchange Online Properties** window, click **Close**.

Creating a new Azure AD user with Management Shell

You can use the Active Roles Management Shell to create a new user.

To create a new Azure AD user with the Management Shell interface

1. On the Management Shell interface, run the **New-QADUser** cmdlet.
2. To create and enable a new Azure AD user, run this cmdlet with the additional `AzureUserAccountEnabled`, `AzureOffice365Enabled`, and `AzureAssociateTenantId`

Boolean parameters.

3. To retrieve and update Azure properties, the **edsvaAzureObjectID** attribute with correct value is required.

For more information on creating a new Azure AD user using the Management Shell interface, see the *Active Roles Management Shell Help*.

Example: Creating a new Azure AD user

```
C:\PS> New-QADUser -name 'user64' -ParentContainer 'CN=Users,DC=SS64,DC=com'
-UserPassword 'Pass123w0rd' -AzureUserAccountEnabled $true -
AzureOffice365Enabled $true -AzureUserPrincipalName 'user64@Azuredomain'-
AzureAssociatedTenantId 'f918cb6c-275a-4815-8863-d7cbb90598b2'
```

Example: Adding additional attribute using -attr @{}

```
C:\PS> New-QADUser -name 'user64' -ParentContainer 'CN=Users,DC=SS64,DC=com'
-UserPassword 'Pass123w0rd' -AzureUserAccountEnabled $true -
AzureOffice365Enabled $true -AzureUserPrincipalName 'user64@Azuredomain' -
AzureAssociatedTenantId 'f918cb6c-275a-4815-8863-d7cbb90598b2' -attr @
{edsaAzureUserGivenName='user64';edsaAzureUserUsageLocation='IN'}
```

Updating the Azure AD user properties with the Management Shell

You can use the Active Roles Management Shell to modify attributes of an Azure AD user in Active Directory.

To update the Azure AD user properties with the Management Shell

- On the Management Shell interface, run the **Set-QADUser** cmdlet.

For more information on modifying an Azure AD user using the Management Shell interface, see the *Active Roles Management Shell Help*.

NOTE: The **Set-QADUser** cmdlet does not work for Azure attributes in Synchronized Identity and Federated environment.

Viewing the Azure AD user properties with the Management Shell

You can use the Active Roles Management Shell to retrieve all Azure AD users in a domain or container that match the specified conditions.

To view the Azure AD user properties with the Management Shell

- On the Management Shell interface, run the **Get-QADUser** cmdlet.

For more information on viewing the Azure AD users using the Management Shell interface, see the *Active Roles Management Shell Help*.

Delete an Azure AD user with the Management Shell

You can use the Active Roles Management Shell to delete a user from Azure.

To delete an Azure AD user with the Management Shell

- On the Management Shell interface, run the **remove-QADObject** cmdlet.

For more information on deleting a user from Azure using the Management Shell interface, see the *Active Roles Management Shell Help*.

NOTE: In Synchronized or Federated environment, **remove-QADObject** removes the user from AD and then gets synchronized to the Azure portal.

Assigning Microsoft 365 licenses to new hybrid users

You can use the Active Roles Web Interface to assign Microsoft 365 licenses to new hybrid users.

To assign a Microsoft 365 license (or licenses) to new hybrid users

1. On the Active Roles Web Interface, create a new Azure AD user.

   For more information on creating a new Azure AD user, see Creating a new cloud-only Azure user.

2. In **Create Azure Account** > **Usage Location**, select the location where Active Roles will be used.

   NOTE: Local rules and regulations for using products and services associated with the configured user can vary by user location. As a result, the **Usage Location** field is mandatory: if you do not select a country, Active Roles cannot assign

Microsoft licenses to the hybrid Azure user.

3. Click **Next**.

   The **Licenses** wizard displays the Microsoft 365 licenses, for example, the Microsoft 365 Business Essentials and Business Premium licenses, and the number of licenses that are available to assign to the user.

4. Select the check boxes next to the licenses that you want to assign to the user, and click **Finish**.

   To check the assigned licenses, select the user, then navigate to **Azure Properties** > **Licenses**.

Assigning Microsoft 365 licenses to existing hybrid users

You can use the Active Roles Web Interface to assign Microsoft 365 licenses to existing hybrid users.

To assign Microsoft 365 license to existing hybrid users

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.

3. Click the specific domain, container or the Organizational Unit, and then select the specific user for which you want to view or update the properties.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** dialog for the user is displayed.

5. In the **Azure Properties** dialog, click **Settings.**
6. If the usage location is not entered in the **Usage Location** field, select the location where the product will be used, and click **Save**.

   NOTE: Local rules and regulations for using products and services associated with the configured user can vary by user location. As a result, the **Usage Location** field is mandatory: if you do not select a country, Active Roles cannot assign Microsoft licenses to the hybrid Azure user.

   Alternatively, to assign the Microsoft 365 license to the user if the product usage location has been entered for the user earlier, navigate to the **Licenses** wizard.

7. Re-open the **Azure Properties** dialog for the user, and click **Licenses**.

   The **Licenses** wizard displays the Microsoft 365 licenses, for example Microsoft 365 Business Essentials and Business Premium licenses, that are available for assigning to the user.

8. Select the license that you want to assign to the user.

9. To view the products included in the license, click the drop-down arrow corresponding to the selected license.

   By default, all the products are enabled for the user.
10. Clear the check boxes next to the products in the license that you want to disable for the user.
11. Click **Save**.

Modifying or removing Microsoft 365 licenses assigned to hybrid users

You can use Active Roles Web Interface to modify or remove Microsoft 365 licenses assigned to hybrid users.

To modify or remove the Microsoft 365 license assigned to existing hybrid users

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, container or the Organizational Unit, and then select the specific user for which you want to view or update the properties.
4. In the **Command** pane, click **Azure Properties**.
5. In the **Azure Properties** dialog, click **Licenses**.

   The **Licenses** wizard displays the Microsoft 365 licenses, for example, Microsoft 365 Business Essentials and Business Premium licenses, that are available and assigned to the user.
6. Click the drop-down arrow next to the available licenses.

   The products that are included and assigned to the user in the license are displayed.
7. Select or clear the check box next to the product included in the license that you want to enable or remove for the user.
8. Click **Save**.

NOTE: Consider the following when modifying or removing Microsoft 365 licenses assigned to hybrid users:

- When you deprovision or delete a user, all the licenses that were assigned to the user are removed. You can assign these licenses to other hybrid users.
- When you undo deprovision a hybrid user, the license assignment gets restored to this user when the undo deprovision operation is completed successfully.
- For information on Azure AD user deprovisioning policy for Microsoft 365 licenses management see *Office 365 Licenses Retention* in the *Active Roles Administration Guide*.

Updating Microsoft 365 licenses display names

To update the names of the licenses displayed on Azure properties > Licenses page of a hybrid user

1. On the system running the Active Roles Service, navigate to `...\One Identity\Active Roles\8.1.3\Service\AzureLicenses.xml`.
2. Open the `AzureLicenses.xml` file and edit the required SKU with the new license display name.

   NOTE: If the `AzureLicenses.xml` file with Azure licenses is not available or it is not well formed, then the default SKUs as derived from Azure Graph APIs are displayed on the **Azure Properties** > **Licenses** page for the Azure AD user.

   The updated license display names can be viewed on the user's **Azure Properties** > **Licenses** page.

Microsoft 365 roles management for hybrid environment users

Active Roles allows you to perform the following Microsoft 365 roles management tasks for hybrid users:

- Assign Microsoft 365 roles to existing hybrid users
- Modify or remove Microsoft 365 roles assigned to hybrid users
- Microsoft 365 user roles management

IMPORTANT: The Active Roles Web Interface only displays Azure roles that have been enabled. To list the Microsoft 365 Roles on the Web Interface, run the following commands.

- To get the guest inviter directory role template, run `$roleTemplate = Get-AzureADDirectoryRoleTemplate | ? { $_.DisplayName -eq "Guest Inviter" }`.
- To enable an instance of the DirectoryRole template, run `Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId`.

For more information on allowing the Azure roles to be listed on the Web Interface, see *Enabling Azure Roles* in the *Active Roles Administration Guide*.

Assigning Microsoft 365 roles to existing hybrid users

To assign Microsoft 365 roles to existing hybrid users

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

The list of Active Directory domains is displayed.

3. Click the specific domain, Container or the Organizational Unit, and then select the specific user for which you want to view or update the properties.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** of the user are displayed.
5. Click **O365 Roles** tab.

   The **O365 Roles** wizard displays the Microsoft 365 roles, for example, the **Helpdesk Administrator**, **Directory Readers**, and more.
6. Select the Microsoft 365 roles that you want to assign to the user, and click **Finish**.

To check the Microsoft 365 roles assigned to the user, select the user, then navigate to **Azure Properties** > **O365 wizard**.

Modifying Microsoft 365 roles assigned to hybrid users

To modify the Microsoft 365 roles assigned to existing hybrid users

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then select the specific user for which you want to view or update the properties.
4. In the **Command** pane, click **Azure properties**.
5. In the **Azure Properties** dialog, click **O365 Roles** tab.
6. Click the specific domain, Container or the Organizational Unit, and then select the specific user for which you want to view or update the properties.

NOTE: When a user is deprovisioned, all the roles that were assigned to the user are retained.

Managing Hybrid AD groups

Active Roles provides the facility to perform administrative tasks, for example, create, read, update, and delete groups in Azure Active Directory (Azure AD) through the Web Interface. You can also perform other operations, for example, add and remove members to Azure AD groups. Some of the group operations can be performed using the Management Shell in addition to the Web Interface. The following section guides you through the Active Roles Web Interface and Management Shell to manage Azure AD groups.

Configuring Hybrid AD groups with the Web Interface

Active Roles allows you to perform the management tasks on Hybrid AD groups using the Web Interface.

Creating an Azure AD group with the Web Interface

To create and enable a new Azure AD group, you can use the Active Roles Web Interface.

To create a new Azure AD group with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the domain in which you want to create a new group.
4. In the list, click the required **Container** or the **Organizational Unit**.
5. In the **Command** pane, click **New Group**.
6. In the **General Properties** > **New Group** > **<OU name>** wizard, enter the group details such as group name, pre-Windows 2000 group name, description, group scope, and group type.

   Group scope provides the option to create a **Global** or **Universal** group, and **Group type** enables you to create a **Security** or **Distribution** group.
7. Click **Next**.
8. In the **Create Azure Group** wizard, select **Create Azure Group**.

   Select the **Tenant name** from the **Tenant list** drop down. The Azure AD details for the new group are generated automatically and populated in the respective fields.

   NOTE: To set values for additional properties in the **General Properties** wizard, select the check-box corresponding to **Open properties for this object when I click Finish**.
9. Click **Finish**.

NOTE: In Federated or Synchronized environments, Azure AD group creation is not supported. The group is created in Active Roles and it is synchronized eventually to Azure using Microsoft Native tools, such as AAD Connect. To manage the Azure AD group through Active Roles, you must perform periodic back-synchronization to on-premise AD.

Viewing or modifying Azure AD group properties with the Web Interface

To view or modify the properties of an existing Azure AD group, you can use the Active Roles Web Interface.

To view or modify the Azure AD group properties with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then the specific group for which you want to view or update the Azure AD group properties.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** wizard for the group account is displayed.
5. To view or modify properties of the Azure AD group, use the tabs in the **Azure Properties** wizard.
6. After setting all the required properties, click **Save**.

Adding or removing members from an Azure AD group with Web Interface

To add or remove members from an Azure AD group, you can use the Active Roles Web Interface.

To add a member to an Azure AD group with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then the specific group to which you want to add members.
4. Select the Azure AD group and in the **Command** pane click **Members**.

   The existing member information for the group is displayed.
5. To add a user to the group, in the **<Group> (objects found)** wizard, click **Add**.
6. In the **Select Object** wizard, search and select the members that you want to add to the group.

   NOTE: To specify the date and time when the selected members should be added or removed from the group, click **Temporal Membership Settings**.
7. Click **OK**.

   The **<Group> (objects found)** wizard displays all the members that are added to the group.

To remove a member from an Azure AD group with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

The list of Active Directory domains is displayed.

3. Click the specific domain, Container or the Organizational Unit, and then the specific group to which you want to add members.
4. Select the Azure AD group and in the **Command** pane click **Members**.

   The existing member information for the group is displayed.
5. In the **<Group> (objects found)** wizard, select the member that you want to remove and click **Remove**.

   A message prompts you to confirm the action.
6. Click **Yes** to continue.

   The member information is removed from the **<Group> (objects found)** wizard.

Viewing the change history for an Azure AD group with the Web Interface

To view the Change History for an Azure AD group, you can use the Active Roles Web Interface.

To view the change history of an Azure AD group with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. Click the specific domain, Container or the Organizational Unit, and then the specific user.
4. In the **Command** pane, click **Change History**.

   The information on changes that were made to the group properties through Active Roles is displayed.

Deleting an Azure AD group with the Web Interface

To delete an Azure AD group, you can use the Active Roles Web Interface.

CAUTION: Hazard of data loss!

Deleting a user is a destructive operation that cannot be undone. A new user with the same name as a deleted user does not automatically get the same permissions and memberships as the deleted account. Because of this, One Identity recommends to disable rather than delete accounts.

To delete an Azure AD group with the Web Interface

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

The list of Active Directory domains is displayed.

3. Click the specific domain, Container or the Organizational Unit, and then the specific Azure AD group to be deleted.
4. In the **Command** pane, click **Delete**.

   A message prompts you to confirm the action.
5. Click **Yes** to continue.

   The Azure AD Group is deleted.

Configuring Hybrid AD groups with the Management Shell interface

Active Roles allows you to perform the management tasks on Hybrid AD groups using the Management Shell interface.

Creating a new Azure AD group with the Management Shell

To create a new user, you can use the Active Roles Management Shell.

To create a new Azure AD group with the Management Shell interface

1. On the Management Shell interface, run the **new-qadGroup** cmdlet.
2. To create and enable a new Azure AD group, use this cmdlet with the additional `AzureOffice365Enabled` and `AzureAssociateTenantId` Boolean parameters.

For more information on creating a newAzure AD group using the Management Shell interface, see the *Active Roles Management Shell Help*.

Updating the Azure AD group properties with the Management Shell

To modify attributes of an Azure AD user in Active Directory, you can use the Active Roles Management Shell.

To update the Azure AD group properties with the Management Shell

- On the Management Shell interface, run the **Set-QADGroup** cmdlet.

For more information on modifying an Azure AD user using the Management Shell interface, see the *Active Roles Management Shell Help*.

Adding or removing members from an Azure AD group with the Management Shell

To add or remove a member from an Azure AD group, you can use the Active Roles Management Shell.

To add a member to an Azure AD group with the Management Shell

- On the Management Shell interface, run the **Add-QADGroupMember** cmdlet.

To remove a member from an Azure AD group with the Management Shell

- On the Management Shell interface, run the **Remove-QADGroupMember** cmdlet.

For more information on adding or removing a member from an Azure AD group using the Management Shell interface, see the *Active Roles Management Shell Help*.

Deleting an Azure AD group with the Management Shell

To delete an Azure AD group, you can use the Active Roles Management Shell.

To delete an Azure AD group with the Management Shell interface

- On the Management Shell interface, run the **remove-QADObject** cmdlet.

For more information on deleting a group from Azure AD using the Management Shell interface, see the *Active Roles Management Shell Help*.

Managing Microsoft 365 Groups

Active Roles supports CRUD (create, read, update and delete) operations for Microsoft 365 (M365) groups and also lets you specify owners and add/remove members to or from existing M365 groups in your organization.

M365 groups facilitate teamwork within an organization by providing the same set of permissions to users and guest users, allowing you to provide access efficiently to various shared resources (such as a common Microsoft Outlook inbox and calendar, a shared OneNote notebook, or other Microsoft 365 resources). For more information on M365 groups, see Overview of Microsoft 365 Groups for administrators in the *Microsoft 365 documentation*.

You can administer M365 groups either via the Active Roles Web Interface or through the Active Roles Management Shell.

- For more information on managing M365 groups with the Active Roles Web Interface, see Configuring M365 Groups with the Web Interface.
- For more information on managing M365 groups with the Active Roles Management Shell, see Microsoft 365 Group management tasks using Management Shell interface.

Configuring M365 Groups with the Web Interface

You can use the Active Roles Web Interface to:

- Create, view, modify or delete M365 groups in your organization.
- Assign or remove owners and members to or from existing M365 groups.
- View the change history of existing M365 groups.

NOTE: You cannot use the Active Roles Web Interface to synchronize existing M365 groups. To synchronize M365 groups, configure an M365 synchronization schedule task with the Active Roles Console (also known as the MMC Interface). For more information, see Scheduling an Azure object synchronization task.

Creating an M365 Group with the Web Interface

To create and enable new Microsoft 365 (M365) groups, you can use the Active Roles Web Interface.

For more information on M365 groups, see Overview of Microsoft 365 Groups for administrators in the *Microsoft 365 documentation*.

To create a new M365 group

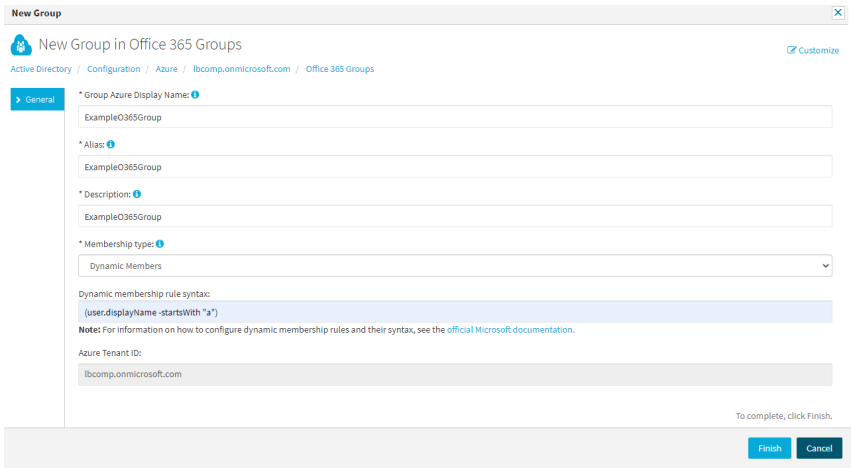
1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.

2. In the right-side pane, click **New Group**.

   The **New Group in Microsoft 365 Groups** window appears.



3. Specify the **Group Azure Display Name** of the configured group.

   TIP: You can configure multiple groups with the same **Group Azure Display Name** in the same Azure tenant.

4. Specify the Exchange Online **Alias** of the M365 group. This value is used for naming the SharePoint site URL of the M365 group, and will also name the primary email address of the shared mailbox associated with the M365 group.

   NOTE: The **Alias** of the M365 group must be unique within the Azure tenant.

5. Provide a short **Description** for the group.

6. Configure the **Membership type** of the group:

   - **Assigned**: When selected, you can add or remove members to or from the group manually later. For more information, see Adding or removing members from an M365 Group with the Web Interface.
   - **Dynamic Members**: When selected, Active Roles sets up the group as a dynamic membership group, and will automatically update group membership based on the configured **Dynamic membership rule syntax**.

   TIP: Consider the following when configuring the **Membership type**:

   - Select **Dynamic Members** to quickly configure a group based on a certain membership logic. For example, if you need to set up a group for employees from the same geographical location, business unit, or functional area, One Identity recommends configuring the group with **Dynamic Members**.
   - If you select **Dynamic Members**, you will not be able to manually add or remove members to or from the M365 group, unless you change its **Membership type** to **Assigned** later. However, you can still manually configure the owner(s) for a dynamic M365 group, as described in Adding or removing owners from an M365 Group with the Web Interface.
   - You can always change the **Membership type** later by navigating to the **Azure Properties** > **General** page of the selected M365 group on the Active Roles Web Interface:
   - Changing the **Membership type** from **Dynamic Members** to **Assigned** later will keep the last set of members that were dynamically assigned to the group.

7. If you set the **Membership type** to **Dynamic Members**, specify the **Dynamic membership rule syntax**. Active Roles will send the logic configured in this field to Azure to automatically assign or remove members to or from the group later.

   NOTE: Consider the following when using the **Dynamic membership rule syntax** setting:

   - This setting is enabled only if **Membership type** is set to **Dynamic Members**. However, in that case, it is mandatory and cannot be empty.
   - The specified dynamic membership rule must meet all rule syntax requirements, otherwise the window will return an error. For more information on the available membership rule properties, operators and

values, see Dynamic membership rules for groups in Azure AD in the *Microsoft 365 documentation*.

- Whenever you modify the dynamic membership rule of a dynamic M365 group, it can take several minutes for Azure to update the list of group members in the **Dynamic Members** window.

8. To complete the configuration of the new M365 group, click **Finish**.

   The new M365 group will appear under the **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups** node.

Modifying an M365 Group with the Web Interface

You can use the Active Roles Web Interface to modify the Azure properties of existing Microsoft 365 (M365) groups in your Azure tenant. This is typically useful if you must:

- Modify the display name of the M365 group, for example because of an organizational change.
- Change the configured membership type (manually assigned or dynamic) of the M365 group.

NOTE: You cannot change the Exchange Online alias of an existing M365 group.

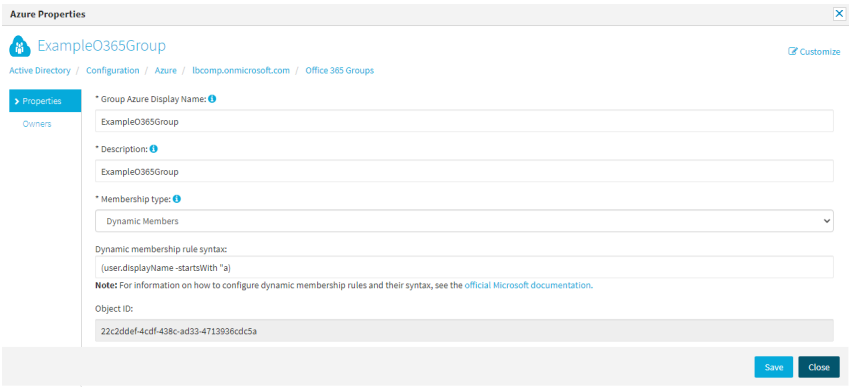
To modify the Azure properties of an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.

2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. In the left-side pane of the **Azure Properties** window, click **Properties**.



5. (Optional) Specify the **Group Azure Display Name** of the configured group.

TIP: You can configure multiple groups with the same **Group Azure Display Name** in the same Azure tenant.

6. (Optional) Provide a short **Description** for the group.
7. (Optional) Configure the **Membership type** of the group:
   - **Assigned**: When selected, you can add or remove members to or from the group manually later. For more information, see Adding or removing members from an M365 Group with the Web Interface.
   - **Dynamic Members**: When selected, Active Roles sets up the group as a dynamic membership group, and will automatically update group membership based on the configured **Dynamic membership rule syntax**.

   TIP: Consider the following when configuring the **Membership type**:
   - Select **Dynamic Members** to quickly configure a group based on a certain membership logic. For example, if you need to set up a group for employees from the same geographical location, business unit, or functional area, One Identity recommends configuring the group with **Dynamic Members**.
   - If you select **Dynamic Members**, you will not be able to manually add or remove members to or from the M365 group, unless you change its **Membership type** to **Assigned** later. However, you can still manually configure the owner(s) for a dynamic M365 group, as described in Adding or removing owners from an M365 Group with the Web Interface.
   - Changing the **Membership type** from **Dynamic Members** to **Assigned** later will keep the last set of members that were dynamically assigned to the group.
8. (Optional) If you set the **Membership type** to **Dynamic Members**, specify the **Dynamic membership rule syntax**. Active Roles will send the logic configured in this field to Azure to automatically assign or remove members to or from the group later. For more information on how to specify a membership rule, see Dynamic membership rules for groups in Azure AD in the *Microsoft 365 documentation*.
9. To apply your changes, click **Save**.

Adding or removing owners from an M365 Group with the Web Interface

You can use the Active Roles Web Interface to specify owners for a Microsoft 365 (M365) group. Using the applicable options, you can either add or remove owners to or from the selected M365 group.

NOTE: Consider the following when configuring group ownership:
- You cannot specify a group as an owner of another group.
- Although Active Roles and Azure AD support specifying Azure guest users as group owners, One Identity recommends doing so only if assigning the ownership of a specific group to a guest user is in line with the security policies of your organization.

To add owners to an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.
2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. To list the owners of the selected group, click the **Owners** tab of the **Azure Properties** window.
5. Click **Add** to add a new owner (or owners) to the selected group.
6. In the **Select Object** page, use the search field to find the users or guest users in the Azure tenant that you want to specify as owners.

   The users and guest users meeting the search criteria will appear in the **Display Name** column.
7. Select the check boxes of the users or guest users you want to specify as owners of the group. The selected users will be listed in the lower pane of the **Select Object** page.
8. (Optional) To search for additional users or guest users, enter another search string. After that, select the users or guest users you want to add from the updated list.
9. To apply your changes, click **OK**. The **Owners** page will be updated with the new settings.

To remove owners from an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.
2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. To list the owners of the selected group, click the **Owners** tab of the **Azure Properties** window.
5. Select the owners whose ownership you want to revoke, and click **Remove**. The selected owners are removed from the list of owners.
6. To apply your changes, click **OK**. The **Owners** page will be updated with the new settings.

Adding or removing members from an M365 Group with the Web Interface

You can use the Active Roles Web Interface to add members to an existing Microsoft 365 (M365) group with an **Assigned** membership setting. M365 groups support Azure users, Azure guest users, or external users as members.

NOTE: You cannot add or remove members manually to or from an M365 group with dynamic membership. To change the members of a dynamic group manually, first modify its membership type from **Dynamic Members** to **Assigned** membership. For more information, see Modifying an M365 Group with the Web Interface.

NOTE: Azure AD does not support adding M365 groups as members to other M365 groups. For more information, see the Add member page of the *Microsoft GRAPH REST API documentation*.

To add members to an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.
2. Select the group that you want to configure.
3. In the right-side pane, click **Members**.

   The **Members** page then appears with the list of members in the selected group.
4. Click **Add** to add a new member (or members) to the group.
5. In the **Select Object** page, use the search field to find the users or guest users in the Azure tenant that you want to add as members.

   The users and guest users that meet the search criteria will appear in the **Display Name** column.
6. Select the check boxes of the users or guest users you want to add as members to the group. The selected users or guest users will be listed in the lower pane of the **Select Object** page.
7. (Optional) To search for additional users or guest users, enter another search string. After that, select the users or guest users you want to add as members from the updated list.
8. To apply your changes, click **OK**. The **Members** page will be updated with the new membership settings.

To remove members from an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.

2. Select the group that you want to configure.
3. In the right-side pane, click **Members**.

   The **Members** page then appears with the list of members in the selected group.

4. To remove a member (or members) from the selected group, select the members from the **Members Name** list, and click **Remove**.

   The selected members are removed from the **Members Name** list.

5. To apply your changes, click **OK**. The **Members** page will be updated with the new membership settings.

Viewing the members of a dynamic M365 Group with the Web Interface

You can check the members of a Microsoft 365 (M365) group with dynamic membership via the Active Roles Web Interface. This is useful if you want to get a quick update on the current membership status of the dynamic M365 group.

NOTE: You cannot add or remove members manually to or from an M365 group with dynamic membership. To change the members of a dynamic group manually, first modify its membership type from **Dynamic Members** to **Assigned** membership. For more information, see Modifying an M365 Group with the Web Interface.

To view the members of an M365 group with dynamic membership

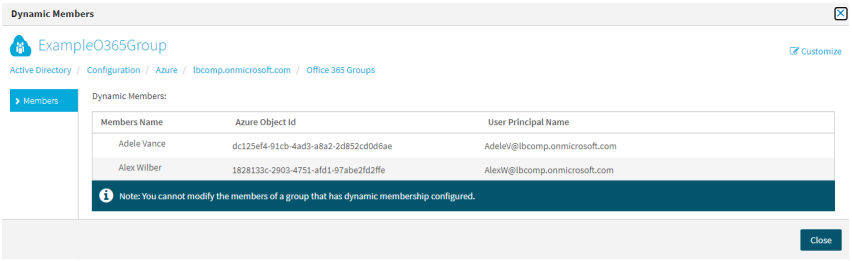
1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.

2. Select the group whose members you want to check.
3. In the right-side pane, click **Dynamic Members**.

   The **Dynamic Members** page then appears with the list of members in the selected group.



4. To exit the **Dynamic Members** window, click **Close**.

Viewing the change history of an M365 Group in the Web Interface

You can check the change history of a Microsoft 365 (M365) group with the Active Roles Web Interface. This is useful if you want to view the list of changes that occurred to the selected M365 group, such as:

- Membership changes (that is, added or removed members).
- Membership type changes (that is, whether the group has been set to assigned or dynamic membership).

NOTE: The **Change History** option of the Active Roles Web Interface lists only group modifications that were performed in Active Roles. It does not list the changes of the group that were performed outside Active Roles, for example in Azure Portal.

To view the change history of an M365 group

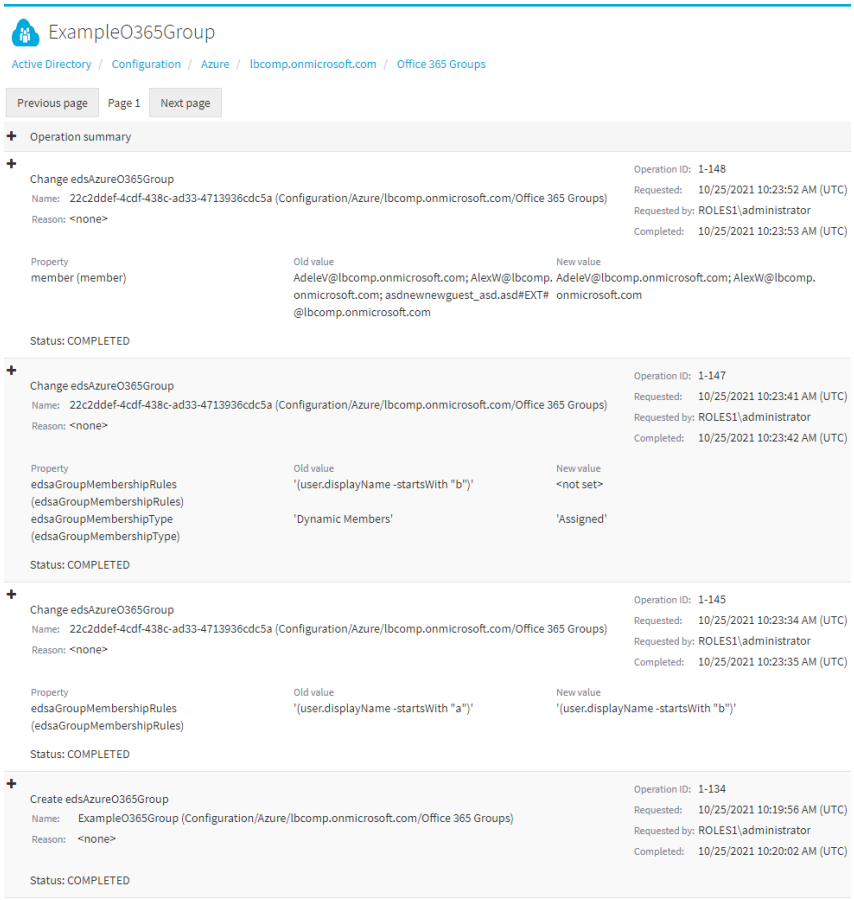
1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The list of existing M365 groups in the selected Azure tenant appears.

   NOTE: When opening the list of **Microsoft 365 Groups** the first time, Active Roles checks and fetches all existing M365 groups that may exist in the Azure cloud. This action is performed automatically and may take a few minutes to complete.

2. Select the group whose change history you want to check.
3. In the right-side pane, click **Change History**.

   The **Change History** page then appears, with the newest change of the group listed at the top of the page.



4. To close the **Change History** window, click any **Tree** node, or any option listed in the right-side pane.

Deleting an M365 Group with the Web Interface

You can use the Active Roles Web Interface to delete a Microsoft 365 (M365) group from an Azure tenant. This is typically required when the M365 group becomes redundant or is otherwise no longer required, for example because of an organizational change.

CAUTION: Deleting an M365 group is a destructive operation that will delete the group from the Azure tenant on the Azure Portal as well.

To delete an M365 group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Microsoft 365 Groups**.

   The **Microsoft 365 Groups** page then opens with the available Azure M365 Groups in the Azure tenant.

2. Select the group that you want to delete.

3. In the right-side pane, click **Delete**.
4. A confirmation dialog appears. To confirm the deletion of the group, click **Yes**.

The selected M365 group is then deleted from the Azure tenant.

Microsoft 365 Group management tasks using Management Shell interface

Active Roles allows you to perform the following management tasks for Office 365 groups using the Management Shell interface:

- Create a new Microsoft 365 Group
- Update the Microsoft 365 Group properties

Create a new Microsoft 365 Group

To create a new group, you can use the Active Roles Management Shell. To create a new group, on the Management Shell interface, run the **New-QADO365Group** cmdlet.

For more information on creating a new Microsoft 365 group using the Management Shell interface, see the *Active Roles Management Shell Help*.

Update the Microsoft 365 Group properties

To modify attributes of an Microsoft 365 group, you can use the Active Roles Management Shell. On the Management Shell interface, run the **Set-QADO365Group** cmdlet.

For more information on modifying an Microsoft 365 user using the Management Shell interface, see the *Active Roles Management Shell Help*.

Delete an Microsoft 365 group

To delete an Microsoft 365 group, you can use the Active Roles Management Shell. To delete an Microsoft 365 group, on the Management Shell interface, run the **Remove-QADO365Group** cmdlet.

For more information on deleting a group from Microsoft 365 using the Management Shell interface, see the *Active Roles Management Shell Help*.

Adding members to an Microsoft 365 Group with the Management Shell

To add new members to an Microsoft 365 (M365) Group, you can use the **Add-QADO365GroupMember** cmdlet on the Active Roles Management Shell.

For more information on adding a member to an M365 Group using the Management Shell interface, see the *Active Roles PowerShell Reference Guide*.

NOTE: Azure AD does not support adding M365 groups as members to other M365 groups. For more information, see the Add member page of the *Microsoft GRAPH REST API documentation*.

Get a member from Microsoft 365 Group

To get a member from the Microsoft 365 group, you can use the Active Roles Management Shell. To get a member from an Microsoft 365 group, on the Management Shell interface, run the **Get-QADO365GroupMember** cmdlet.

For more information on getting a member from an Microsoft 365 group using the Management Shell interface, see the *Active Roles Management Shell Help*.

Get group from Microsoft 365 Group

To get a group from the Microsoft 365 group, you can use the Active Roles Management Shell. To get a group from an Microsoft 365 group, on the Management Shell interface, run the **Get-QADO365Group** cmdlet.

For more information on getting a group from an Microsoft 365 group using the Management Shell interface, see the *Active Roles Management Shell Help*.

Removing members from an Microsoft 365 Group with the Management Shell

To remove members from an Microsoft 365 (M365) Group, you can use the **Remove-QADO365GroupMember** cmdlet on the Active Roles Management Shell interface.

For more information on removing a member from an M365 Group using the Management Shell interface, see the *Active Roles PowerShell Reference Guide*.

Scheduling an Azure object synchronization task

You can use the **Sync Azure O365 Objects** scheduled task of the Active Roles Console (also known as the MMC interface) to synchronize the following Azure objects and Azure tenant information between the Azure Portal and the Active Roles database:

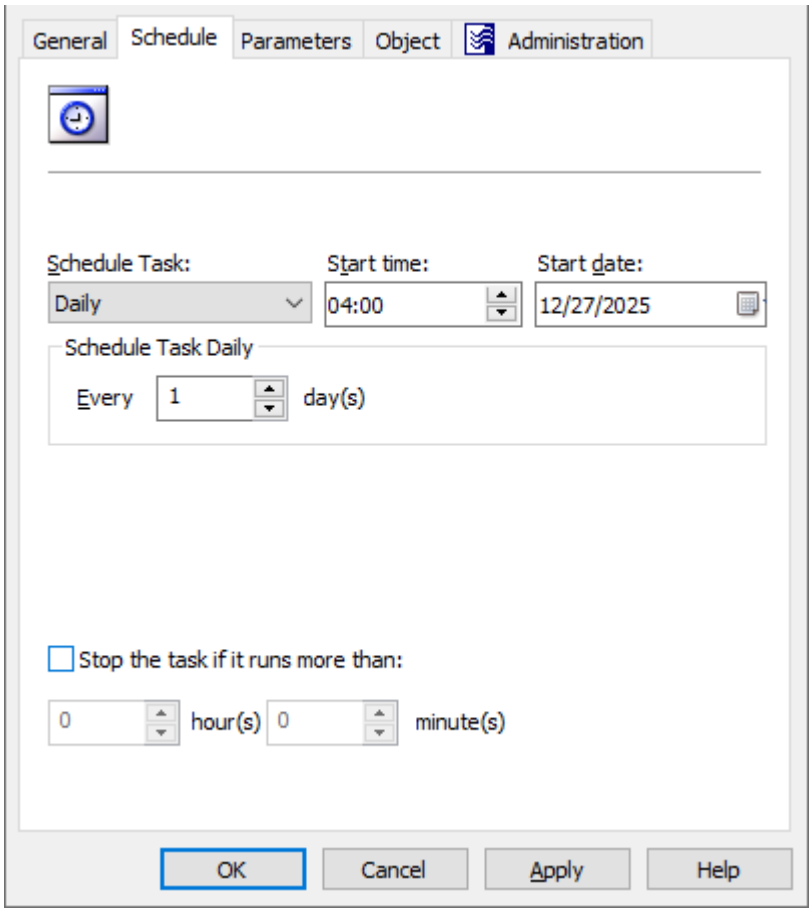
- Azure users
- Azure guest users
- Azure contacts
- Microsoft 365 (M365) groups

- The Azure tenant ID and environment information (that is, whether the tenant is set to a **Non-federated**, **Synchronized identity**, or **Federated** environment configuration.

To configure a scheduled Azure object synchronization task

1. In the Active Roles Console, in the Active Directory (AD) tree, navigate to **Configuration** > **Server Configuration** > **Scheduled Task** > **Builtin**.
2. Open the scheduling properties of the **Sync Azure O365 Objects** built-in scheduled task. To do so, either:
   - Double-click **Sync Azure O365 Objects**, then in the **Properties** window, open the **Schedule** tab.
   - Right-click **Sync Azure O365 Objects**, then click **Properties** > **Schedule**.

Figure 11: Active Roles Console – Scheduling properties of the scheduled task



3. To customize the scheduling settings of the task, open the **Properties** > **Schedule** tab.
4. To change the default scheduling settings of the task for your needs, modify the options of the **Schedule** tab accordingly:

- **Schedule Task**: Specifies how frequently Active Roles runs the task (each hour, every day, or on a weekly/monthly basis). By default, tasks are run on a daily basis.
- **Start time** and **Start date**: These settings specify the time and date of the first scheduled task run. These settings are not available if **Schedule Task** is set to **Once** or **When Service starts**.
- **Schedule Task Hourly** / **Daily** / **Weekly** / **Monthly**: These settings specify the time interval of repeating the configured task.

  For example, setting **Schedule Task** to **Hourly** lets you specify the time interval between two task runs in hours and minutes, while setting it to **Weekly** lets you specify not just the number of weeks between two task runs, but also the days of the week on which Active Roles must run the task.

  NOTE: This setting is not available if **Schedule Task** is set to **Once** or **When Service starts**.
- **Stop the task if it runs more than**: When selected, this setting sets a timeout (in hours and minutes) after which the task stops if it runs longer than the specified interval.

TIP: If the contents of the **Members** and/or **Azure Properties** actions in the Active Roles Web Interface for an Azure object differ from the object information available on the Azure Portal, One Identity recommends running the scheduled **Sync Azure O365 Objects** task manually to synchronize the Azure objects and Azure tenant information.

Managing cloud-only distribution groups

You can use distribution groups (also called mail-enabled universal distribution groups) to distribute messages to a group of people.

In the Active Roles Web Interface, you can create, manage or delete cloud-only distribution groups in **Directory Management** > **Tree**> **Azure** > **<azure-tenant-name>** > **Distribution Groups**. Distribution groups created in the Active Roles Web Interface are synchronized to the Exchange admin center.

For more information about cloud-only distribution groups, see *Create and manage distribution list groups in Exchange Online* in the *Microsoft Exchange Online documentation*.

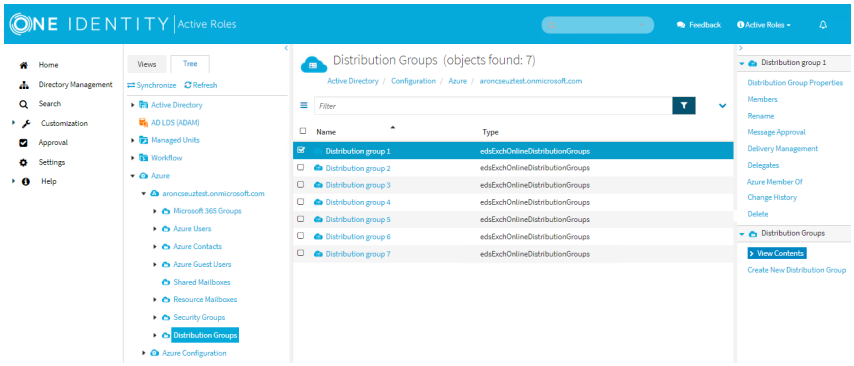
Creating a new distribution group

You can create a new distribution group with the **Create New Distribution Group** action of the Active Roles Web Interface.

To create a new distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 12: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Click **Create New Distribution Group**.
3. In **General**, configure the settings your organization requires for setting up the distribution group.
    - Enter the **Name** of the distribution group.
    - (Optional) Enter the **Display name** of the distribution group.
    - (Optional) Enter a **Description** for the distribution group.
    - **Primary SMTP Address (leave blank for default value)**: Enter the name and select a domain.

      The default value of the primary SMTP address is the name and the domain name of the mailbox. For example, `mailbox1@activeroles.onmicrosoft.com`, where `mailbox1` is the name and `activeroles.onmicrosoft.com` is the domain name.
    - (Optional) **Hide this group from the global address list** (default: selected)

      Select this check box if you do not want the group to appear in the address book and other address lists defined in your Exchange organization.
    - In **Joining the group**, set who can join the distribution group.
        - **Open**: Anyone can join this group without owner approval.
        - **Closed**: Only group owners can add members. All requests to join will be automatically declined.
    - In **Leaving the group**, set who can leave the distribution group.

- **Open**: Anyone can leave this group without owner approval.
- **Closed**: Only group owners can remove members. All requests to leave will be automatically declined.

4. To apply your changes, click **Finish**.

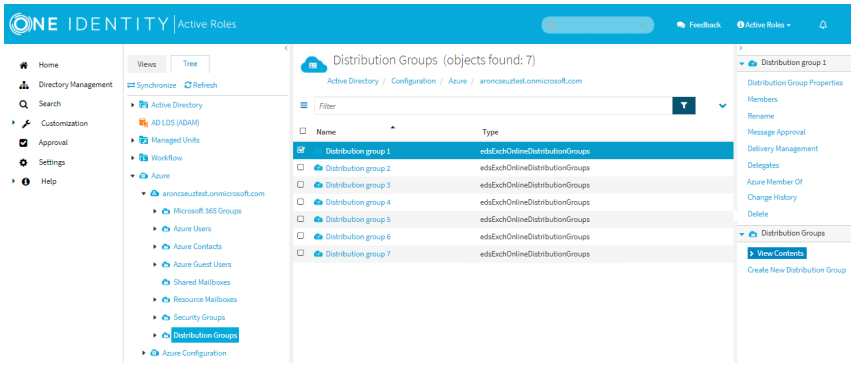
Viewing or modifying the properties of a distribution group

You can view or modify the properties of a distribution group with the **Distribution Group Properties** action of the Active Roles Web Interface.

To view or modify the properties of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 13: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose properties you want to view or modify.
3. Click **Distribution Group Properties**.
4. In **General**, set the following general properties of the distribution group:
   - (Optional) Enter the **Display name** of the distribution group.

     NOTE: This window also shows the **Name** of the distribution group, specifying its unique Exchange Online identity. To change the **Name** of the distribution group, use the **Rename** action.

     For more information, see Renaming a distribution group.
   - (Optional) Enter a **Description** for the distribution group.
   - **Primary SMTP address**: The primary Simple Mail Transfer Protocol (SMTP) address of a user account to be used for server-to-server authorization or access delegation. You cannot modify this value because it is filled

automatically.

- (Optional) **Hide this group from the global address list** (default: selected)

  Select this check box if you do not want the group to appear in the address book and other address lists defined in your Exchange organization.

- In **Joining the group**, set who can join the distribution group.
  - **Open**: Anyone can join this group without owner approval.
  - **Closed**: Only group owners can add members. All requests to join will be automatically declined.
- In **Leaving the group**, set who can leave the distribution group.
  - **Open**: Anyone can leave this group without owner approval.
  - **Closed**: Only group owners can remove members. All requests to leave will be automatically declined.

5. In **Owners**, set the owners of the distribution group.
   - To add owners of the distribution group, click **Add**, select the users and click **OK**.
   - To remove owners from the distribution group, select the users and click **Remove**.
6. To apply your changes, click **Save**.

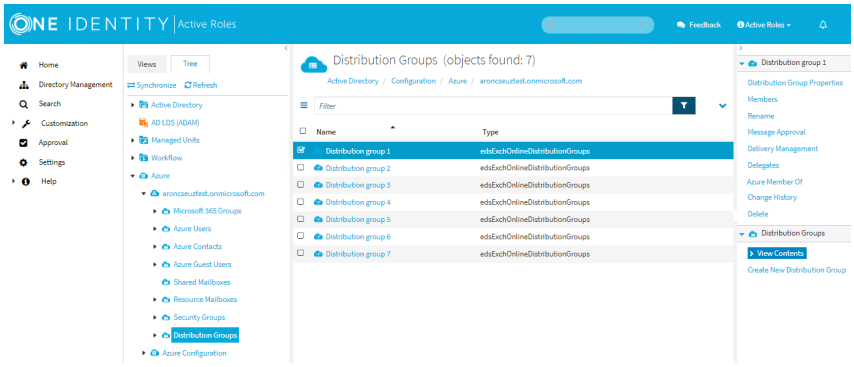
Viewing or modifying the members of a distribution group

You can view or modify the members of a distribution group with the **Members** action of the Active Roles Web Interface.

To view or modify the members of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 14: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose members you want to view or modify.
3. Click **Members**.
4. In **Members**, specify the members of the distribution group.

   NOTE: In the Active Roles Web Interface, adding Azure guest users to a distribution group as members right after assigning them the Exchange Online Plan 2 license will fail because it may take several minutes for the user object(s) to be created in Exchange Online. To add guest users with newly assigned Exchange Online Plan 2 licenses to a distribution group, wait several minutes.

   - To add members to the distribution group, select the users, contacts or distribution groups and click **OK**.
   - To remove members from the distribution group, select the users, contacts or distribution groups and click **OK**.
5. To apply your changes, click **Save**.

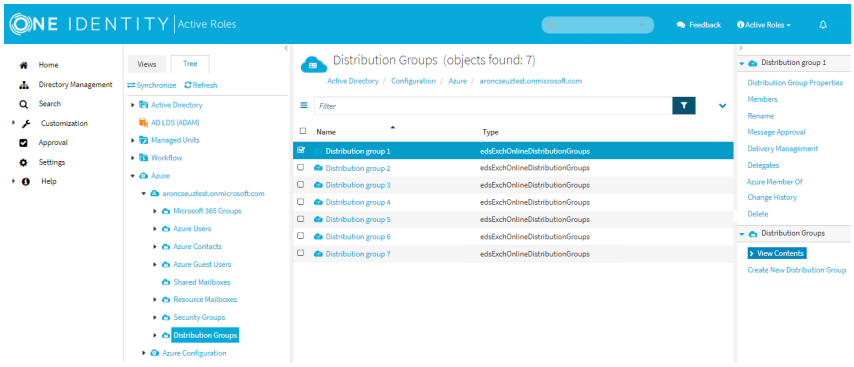
Renaming a distribution group

You can change the Exchange Online identity and/or the display name of a distribution group with the **Rename** action of the Active Roles Web Interface.

To rename a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 15: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group that you want to rename.
3. Click **Rename**.
4. (Optional) In **General**, change the applicable attribute:
    - **Name**: Specifies the Exchange Online identity of the distribution group. The value of this attribute must be unique.
    - **Display name**: Specifies the display name of the distribution group.
5. To apply your changes, click **Finish**.

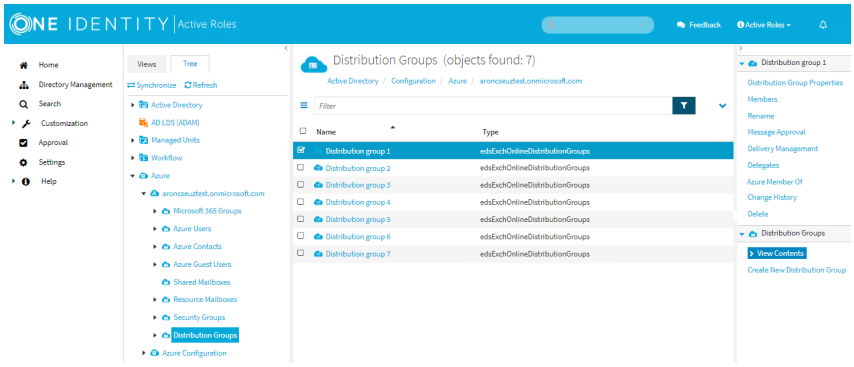
Viewing or modifying the message approval settings of a distribution group

You can view or modify the message approval settings of a distribution group with the **Message Approval** action of the Active Roles Web Interface.

To view or modify the message approval settings of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 16: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose message approval settings you want to view or modify.
3. Click **Message Approval**.
4. In **Message Approval**, set the following message approval settings of the distribution group:
    - **Require moderator approval for messages sent to this group**: Select this check box if group moderators must approve messages to appear. (default: selected)
        - **Group moderators**: If **Require moderator approval for message sent to this group** is selected, add moderators to approve or reject messages.
            - To add users to the list of **Group moderators**, click **Add**, select the user and click **OK**.
            - To remove users from the list of **Group moderators**, select the user and click **Remove**.
    - (Optional) Add senders who don't require message approval: If **Require moderator approval for message sent to this group** is selected, add users whose messages can appear without moderator approval.
        - To add users to the list of **Senders who don't require message approval**, click **Add**, select the users and click **OK**.
        - To remove users from the list of **Senders who don't require message approval**, select the users and click **Remove**.
    - **Notify a sender if their message isn't approved**: If **Require moderator approval for message sent to this group** is selected, specify whether senders receive a notification if their messages get rejected.
        - **Only sender**

- **Only sender in your organization**
- **No notifications**

5. To apply your changes, click **Save**.

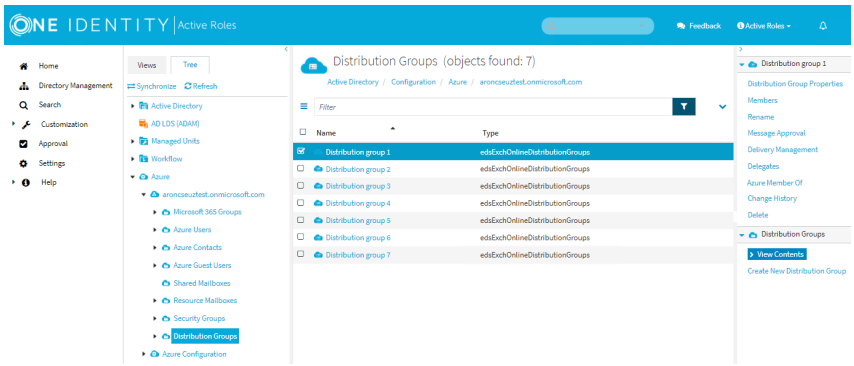
Viewing or modifying the delivery management of a distribution group

You can view or modify the delivery management settings of a distribution group with the **Delivery Management** action of the Active Roles Web Interface.

To view or modify the delivery management of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 17: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose delivery management settings you want to view or modify.
3. Click **Delivery Management**.
4. In **Delivery Management**, set the following delivery management settings of the distribution group.
    - **Only allow messages from people inside my organization**: Clear this check box to allow people outside your organization to send messages to this group. (default: selected)
    - **Accept messages only from these designated senders**: To restrict receiving messages from certain users only, specify the allowed senders in this setting.
        - To add users to the list of **Accept messages only from these designated senders**, click **Add**, select the users and click **OK**.

- To remove users from the list of **Accept messages only from these designated senders**, select the users and click **Remove**.

5. To apply your changes, click **Save**.

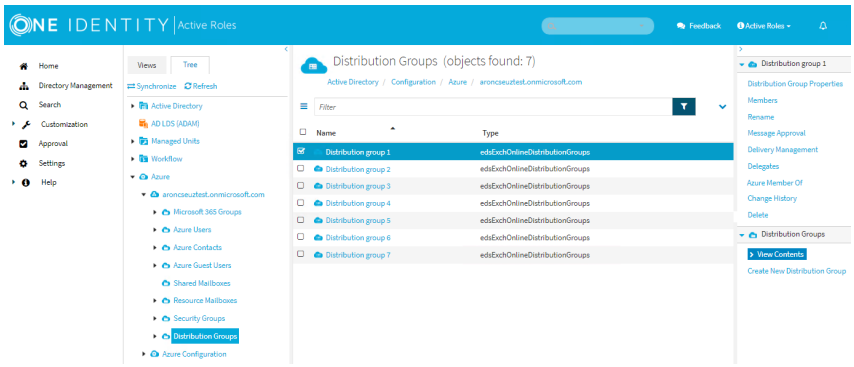
Viewing or modifying delegates of a distribution group

You can view or modify the delegates of a distribution group with the **Delegates** action of the Active Roles Web Interface.

To view or modify the delegates of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 18: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose delegates you want to view or modify.
3. Click **Delegates**.
4. In **Delegates**, set the following delegate settings of the distribution group:
    - **Send on behalf to**

      Only delegates in the **Send on behalf to** list can send messages on behalf of this group.

        - To add delegates to the **Send on behalf to** list, click **Add**, select the users and click **OK**.
        - To remove delegates from the **Send on behalf to** list, select the users and click **Remove**.

    - **Send as**

      Only delegates in the **Send as** list can send messages from this group. To the recipient, the message will appear as a message sent by this group.

- To add delegates to the **Send as** list, click **Add**, select the users and click **OK**.
- To remove delegates from the **Send as** list, select the users and click **Remove**.

5. To apply your changes, click **Save**.

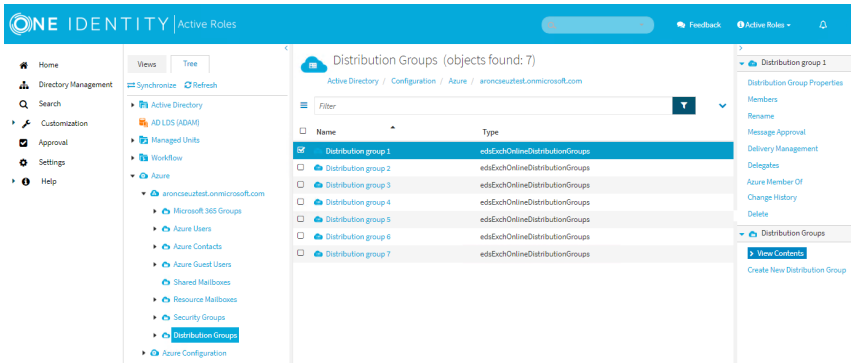
Viewing the change history of a distribution group

You can view the change history of a distribution group in the selected Azure tenant with the **Change History** action of the Active Roles Web Interface.

To view the change history of a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 19: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Select the distribution group whose change history you want to view.
3. Click **Change History**.

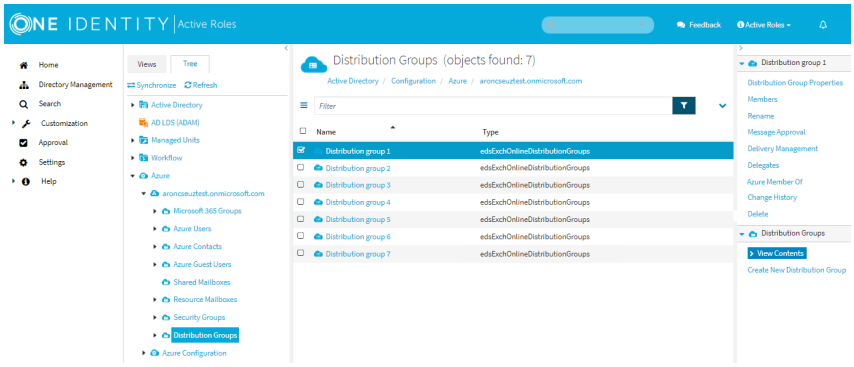
Deleting a distribution group

You can delete a new distribution group with the **Delete** action of the Active Roles Web Interface.

To delete a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Distribution Groups**.

Figure 20: Distribution Groups — Listing the Azure distribution groups in the Azure tenant



2. Click **Delete**.
3. To confirm, click **Yes**.

Managing cloud-only dynamic distribution groups

To distribute messages to a group of users, you can use dynamic distribution groups (mail-enabled Active Directory group objects).

Distribution groups have a defined list of members, but for dynamic distribution groups, you can define filters and conditions. Every time a message is sent to the group, the list of members changes dynamically based on the defined criteria.

In the Active Roles Web Interface, you can create, manage or delete cloud-only dynamic distribution groups in **Directory Management** > **Tree**> **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**. Dynamic distribution groups that are created in the Active Roles Web Interface are synchronized to the Exchange admin center.

For more information about cloud-only dynamic distribution groups, see *Manage dynamic distribution groups in Exchange Online* in the *Microsoft Exchange Online documentation*.

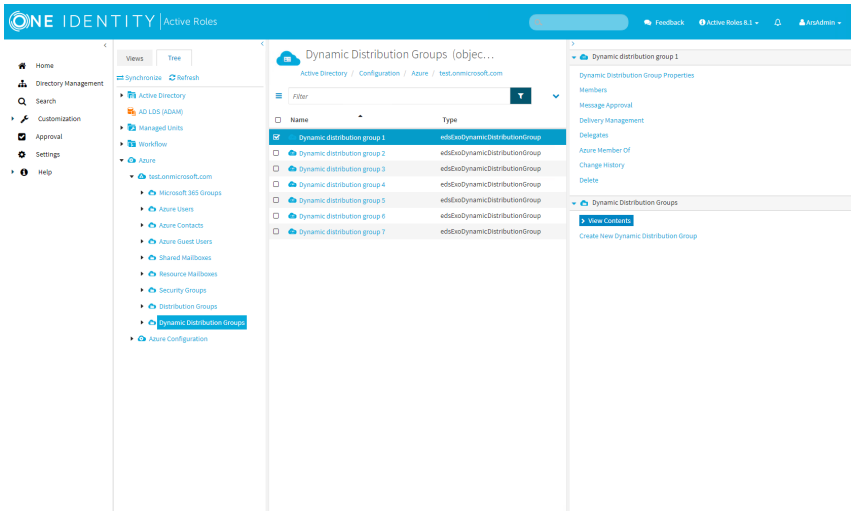
Creating a new dynamic distribution group

You can create a new dynamic distribution group with the **Create New Dynamic Distribution Group** action of the Active Roles Web Interface.

To create a new dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 21: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Click **Create New Dynamic Distribution Group**.
3. In **General**, configure the settings that your organization requires for setting up the dynamic distribution group.
    - Enter the **Name** of the dynamic distribution group.
    - (Optional) Enter the **Display name** of the dynamic distribution group.
    - (Optional) Enter a **Description** for the dynamic distribution group.
    - **Primary SMTP Address (leave blank for default value)**: Enter the name and select a domain.

      The default value of the primary SMTP address is the name and the domain name of the mailbox. For example, `mailbox1@activeroles.onmicrosoft.com`, where `mailbox1` is the name and `activeroles.onmicrosoft.com` is the domain name.
    - (Optional) **Hide this group from the global address list** (default: selected)

      Select this check box if you do not want the group to appear in the address book and other address lists defined in your Exchange organization.
4. To continue, click **Next**.
5. In **Owners**, set the owner of the dynamic distribution group.

   NOTE: You can only set one owner for a dynamic distribution group.
    - To add or change the owner of the dynamic distribution group, click **Modify**, select the user and click **OK**.
    - To view the Azure AD properties of the owner, click **Properties**.

- To remove the owner of the dynamic distribution group, select the users and click **Remove**.

6. In **Members**, set the type of recipients that will be members of the dynamic distribution group.
   - **All recipient types** (default: selected)
   - **Only the following recipient types:**
     - (Optional) Users with Exchange mailboxes
     - (Optional) Mail users with external email addresses
     - (Optional) Resource mailboxes
     - (Optional) Mail contacts with external email addresses
     - (Optional) Mail-enabled groups
7. To apply your changes, click **Finish**.

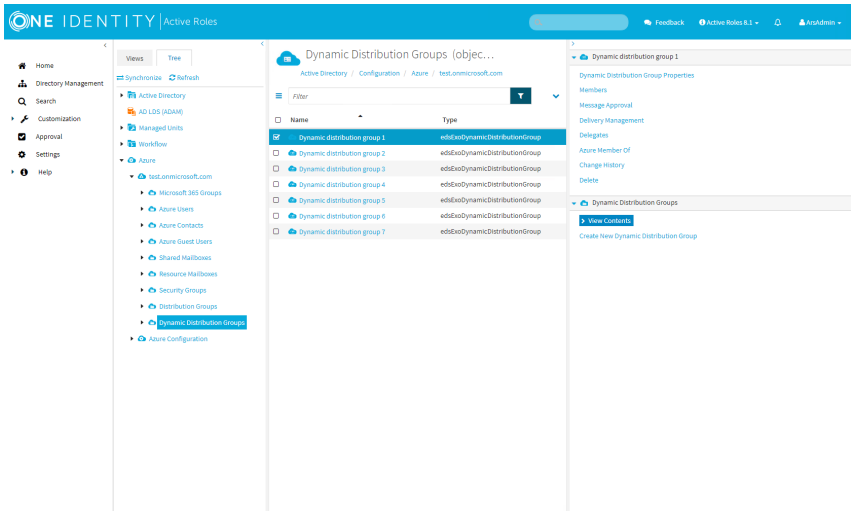
Viewing or modifying the properties of a dynamic distribution group

You can view or modify the properties of a dynamic distribution group with the **Distribution Group Properties** action of the Active Roles Web Interface.

To view or modify the properties of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 22: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group whose properties you want to view or modify.
3. Click **Dynamic Distribution Group Properties**.
4. In **General**, set the following general properties of the dynamic distribution group:
    - Enter the **Name** of the dynamic distribution group.
    - (Optional) Enter the **Display name** of the dynamic distribution group.
    - (Optional) Enter a **Description** for the dynamic distribution group.
    - **Primary SMTP address**: The primary Simple Mail Transfer Protocol (SMTP) address of a user account to be used for server-to-server authorization or access delegation. You cannot modify this value because it is filled automatically.
    - (Optional) **Hide this group from the global address list** (default: selected)

      Select this check box if you do not want the group to appear in the address book and other address lists defined in your Exchange organization.
5. In **Owners**, set the owner of the dynamic distribution group.

   NOTE: You can only set one owner for a dynamic distribution group.

    - To add or change the owner of the dynamic distribution group, click **Modify**, select the user and click **OK**.
    - To view the Azure AD properties of the owner, click **Properties**.
    - To remove the owner of the dynamic distribution group, select the users and click **Remove**.
6. In **Members**, set the type of recipients that will be members of the dynamic distribution group.

- **All recipient types** (default: selected)
- **Only the following recipient types:**
  - (Optional) Users with Exchange mailboxes
  - (Optional) Mail users with external email addresses
  - (Optional) Resource mailboxes
  - (Optional) Mail contacts with external email addresses
  - (Optional) Mail-enabled groups

7. To apply your changes, click **Save**.

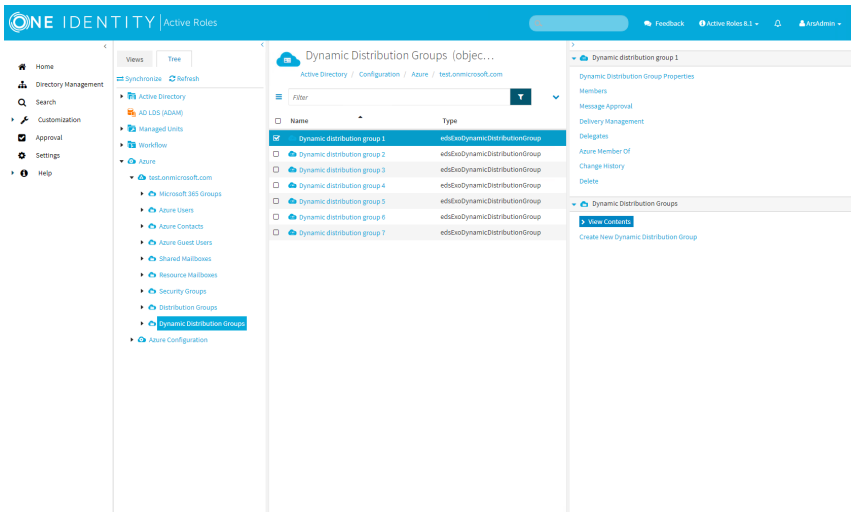
Viewing or modifying the members of a dynamic distribution group

You can view or modify the members of a dynamic distribution group with the **Members** action of the Active Roles Web Interface.

To view or modify the members of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 23: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group whose members you want to view or modify.
3. Click **Members**.

4. In **Members**, set the type of recipients that will be members of the dynamic distribution group.
    - **All recipient types** (default: selected)
    - **Only the following recipient types:**
        - (Optional) Users with Exchange mailboxes
        - (Optional) Mail users with external email addresses
        - (Optional) Resource mailboxes
        - (Optional) Mail contacts with external email addresses
        - (Optional) Mail-enabled groups
5. To apply your changes, click **Save**.

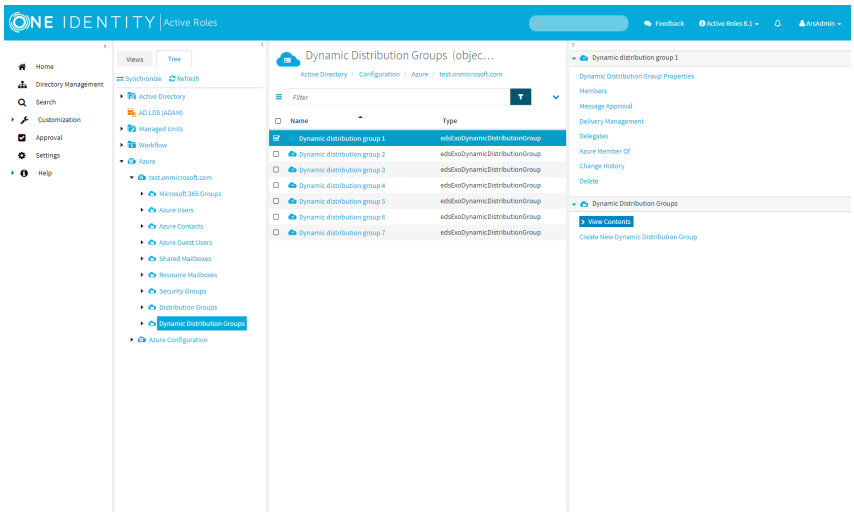
Viewing or modifying the message approval settings of a dynamic distribution group

You can view or modify the message approval settings of a dynamic distribution group with the **Message Approval** action of the Active Roles Web Interface.

To view or modify the message approval settings of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 24: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group whose message approval settings you want to view or modify.
3. Click **Message Approval**.
4. In **Message Approval**, set the following message approval settings of the distribution group:
    - **Require moderator approval for messages sent to this group**: Select this check box if group moderators must approve messages to appear. (default: selected)
        - **Group moderators**: If **Require moderator approval for message sent to this group** is selected, add moderators to approve or reject messages.

          NOTE: You can only add users to the list with an Exchange Online Plan 2 license assigned to them.

            - To add users to the list of **Group moderators**, click **Add**, select the user and click **OK**.
            - To remove users from the list of **Group moderators**, select the user and click **Remove**.
        - (Optional) Add senders who do not require message approval: If **Require moderator approval for message sent to this group** is selected, add users whose messages can appear without moderator approval.

          NOTE: You can only add users to the list with an Exchange Online Plan 2 license assigned to them.

            - To add users to the list of **Senders who don't require message approval**, click **Add**, select the users and click **OK**.
            - To remove users from the list of **Senders who don't require message approval**, select the users and click **Remove**.
        - **Notify a sender if their message isn't approved**: If **Require moderator approval for message sent to this group** is selected, specify whether senders receive a notification if their messages get rejected.
            - **Only sender**
            - **Only sender in your organization**
            - **No notifications**
5. To apply your changes, click **Save**.

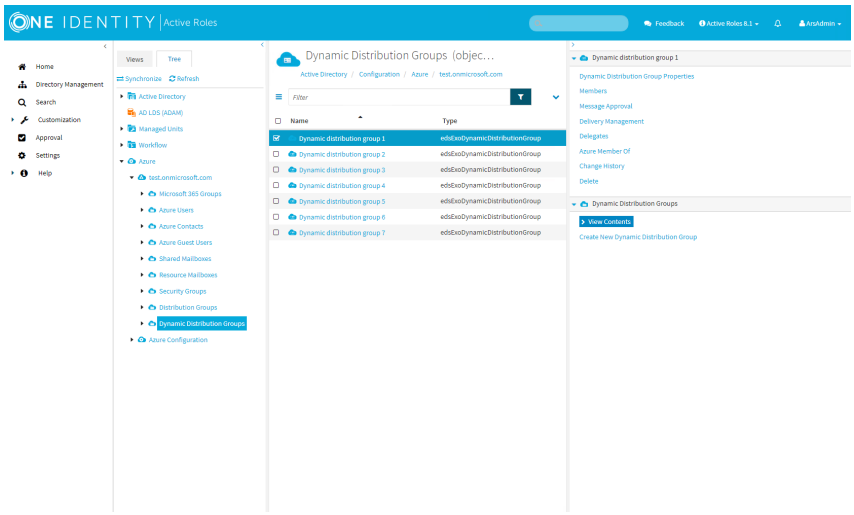
Viewing or modifying the delivery management of a dynamic distribution group

You can view or modify the delivery management settings of a dynamic distribution group with the **Delivery Management** action of the Active Roles Web Interface.

To view or modify the delivery management of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

   Figure 25: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.

2. Select the dynamic distribution group whose delivery management settings you want to view or modify.
3. Click **Delivery Management**.
4. In **Delivery Management**, set the following delivery management settings of the distribution group.
   - **Only allow messages from people inside my organization**: To allow people outside your organization to send messages to this group, clear this check box. (default: selected)
   - **Accept messages only from these designated senders**: To restrict receiving messages from certain users only, specify the allowed senders in this setting.

     NOTE: You can only add users to the list with an Exchange Online Plan 2 license assigned to them.

     - To add users to the list of **Accept messages only from these designated senders**, click **Add**, select the users and click **OK**.
     - To remove users from the list of **Accept messages only from these designated senders**, select the users and click **Remove**.
5. To apply your changes, click **Save**.

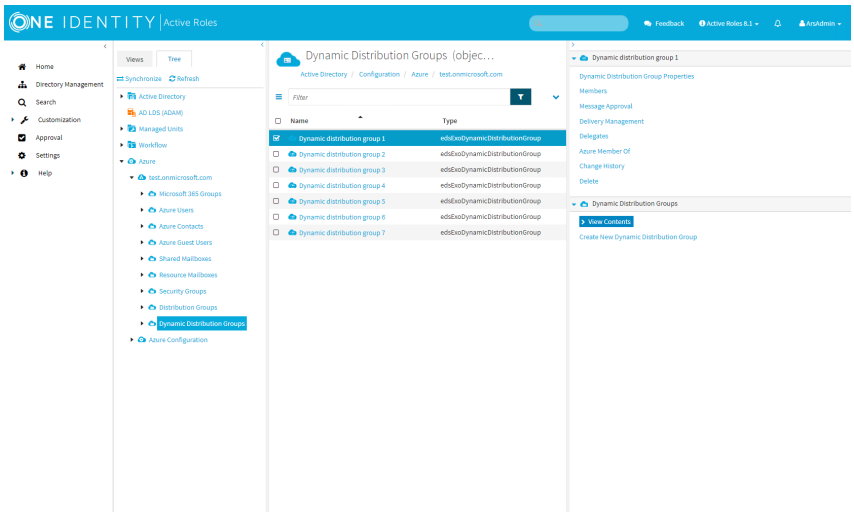
Viewing or modifying delegates of a dynamic distribution group

You can view or modify the delegates of a dynamic distribution group with the **Delegates** action of the Active Roles Web Interface.

To view or modify the delegates of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

   Figure 26: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.

2. Select the dynamic distribution group whose delegates you want to view or modify.
3. Click **Delegates**.
4. In **Delegates**, set the following delegate settings of the distribution group:
   - **Send on behalf to**

     Only delegates in the **Send on behalf to** list can send messages on behalf of this group.

     NOTE: You can only add users to the list with an Exchange Online Plan 2 license assigned to them.

     - To add delegates to the **Send on behalf to** list, click **Add**, select the users and click **OK**.
     - To remove delegates from the **Send on behalf to** list, select the users and click **Remove**.
   - **Send as**

Only delegates in the **Send as** list can send messages from this group. To the recipient, the message will appear as a message sent by this group.

NOTE: You can only add users to the list with an Exchange Online Plan 2 license assigned to them.

- To add delegates to the **Send as** list, click **Add**, select the users and click **OK**.
- To remove delegates from the **Send as** list, select the users and click **Remove**.

5. To apply your changes, click **Save**.

Viewing or modifying the Azure membership of a dynamic distribution group

You can configure and view the Azure group membership(s) of a dynamic distribution group with the **Azure Member Of** option of the Active Roles Web Interface. You can:

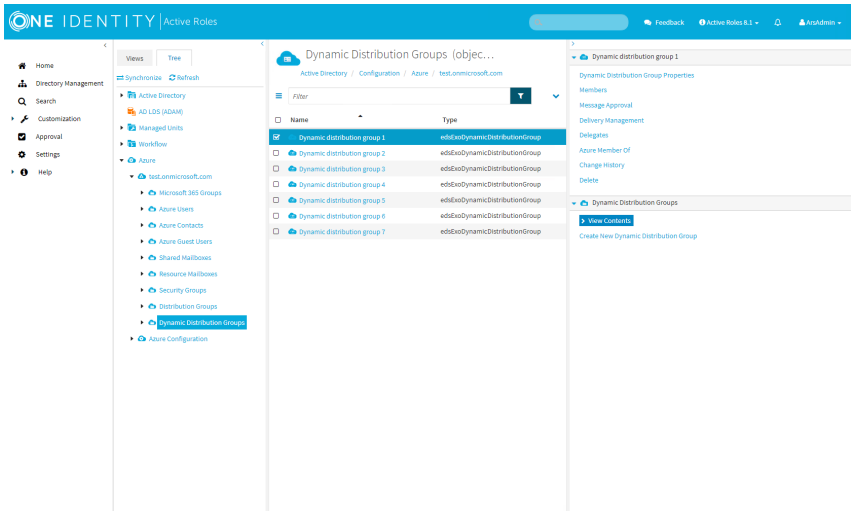
- View the existing distribution group membership(s) of the dynamic distribution group.
- Add or remove the dynamic distribution group to or from the selected Azure distribution group(s).

NOTE: In the Active Roles Web Interface, you can add Azure dynamic distribution groups to Azure distribution groups only, but you cannot add them to Azure O365 groups or Azure security groups. You can add a dynamic distribution group to an Azure O365 group or Azure security group in the Microsoft 365 admin center.

To add or remove an existing dynamic distribution group to or from a distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 27: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group whose membership you want to view or configure.
3. Click **Azure Member Of**. The list of Azure distribution groups where the dynamic distribution group has a membership appears.
    - To add the dynamic distribution group to a new Azure distribution group of the Azure tenant, click **Add**, select the distribution group(s) you want the dynamic distribution group to be a member of, and click **OK**.
    - To remove the dynamic distribution group from any distribution group(s), in **Azure Member Of**, select the distribution group(s), click **Remove**, and click **OK**.

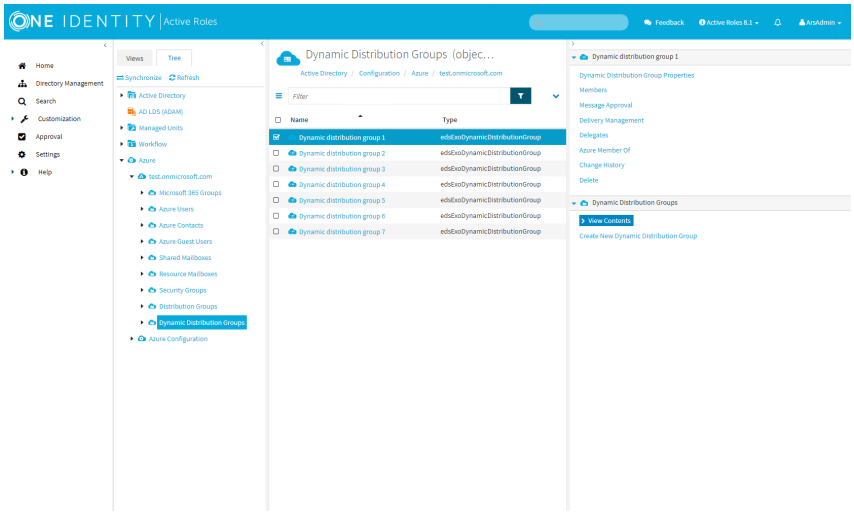
Viewing the change history of a dynamic distribution group

You can view the change history of a dynamic distribution group with the **Change History** action of the Active Roles Web Interface.

To view the change history of a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 28: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group whose change history you want to view.
3. Click **Change History**.

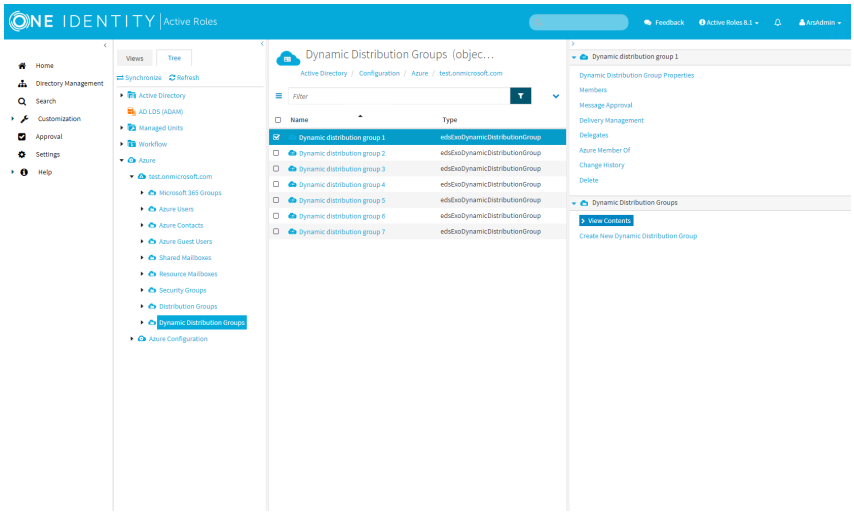
Deleting a dynamic distribution group

You can delete a dynamic distribution group with the **Delete** action of the Active Roles Web Interface.

To delete a dynamic distribution group

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Dynamic Distribution Groups**.

Figure 29: Directory Management > Tree > Azure > <azure-tenant-name> > Dynamic Distribution Groups — Listing the Azure dynamic distribution groups in the Azure tenant.



2. Select the dynamic distribution group(s) you want to delete.
3. Click **Delete**.
4. To confirm, click **Yes**.

Managing Azure security groups

Active Roles supports CRUD (create, read, update and delete) operations for Azure security groups and also lets you specify owners and add/remove members to or from existing Azure security groups in your organization.

Azure security groups are security principals used to secure objects (for example, Azure users, Azure guest users, devices, applications, or other Azure security groups) in Azure AD. Typically, Azure security groups are set up to delegate application licenses or other resource permissions to users based on their group membership. For more information on Azure security groups, see Groups in Microsoft 365 and Azure in the *Microsoft 365 community documentation*.

You can administer Azure security groups via the Active Roles Web Interface.

Creating an Azure security group with the Web Interface

You can use the Active Roles Web Interface to create and enable new Azure security groups.

For more information on Azure security groups, see Groups in Microsoft 365 and Azure in the *Microsoft 365 community documentation*.

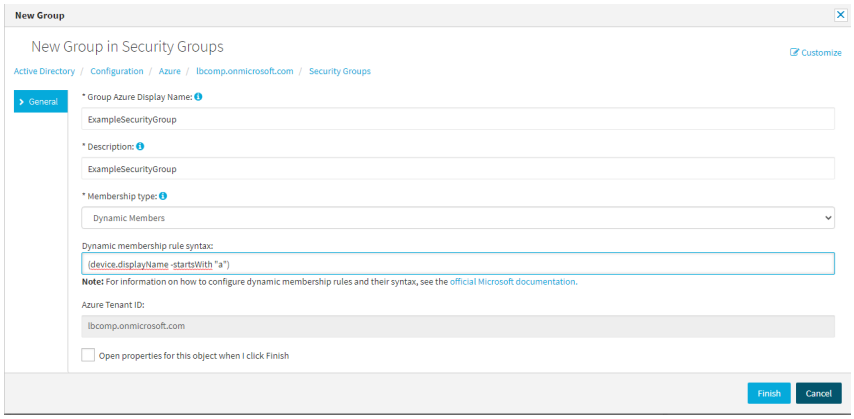
To create a new Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.

2. In the right-side pane, click **New Group**.

   The **New Group in Security Groups** window appears.



3. Specify the **Group Azure Display Name** of the configured group.

   TIP: You can configure multiple groups with the same **Group Azure Display Name** in the same Azure tenant.

4. Provide a short **Description** for the group.

5. Configure the **Membership type** of the group:

   - **Assigned**: When selected, you can add or remove members to or from the group manually later. For more information, see Adding or removing members from an Azure security group with the Web Interface.
   - **Dynamic Members**: When selected, Active Roles sets up the group as a dynamic membership group, and will automatically update group membership based on the configured **Dynamic membership rule syntax**.

   TIP: Consider the following when configuring the **Membership type**:

   - Select **Dynamic Members** to quickly configure a group based on a certain membership logic. For example, if you need to set up a group for employees from the same geographical location, business unit, or functional area, One Identity recommends configuring the group with **Dynamic Members**.
   - If you select **Dynamic Members**, you will not be able to manually add or remove members to or from the Azure security group, unless you change its **Membership type** to **Assigned** later. However, you can still manually configure the owner(s) for a dynamic Azure security group, as described in Adding or removing owners from an Azure security group with the Web Interface.

- Although the **Membership type** drop-down setting does not offer a separate **Dynamic Devices** option, you can actually set up dynamic Azure security groups in Active Roles with the appropriate dynamic device membership rules (such as `device.displayName`). However, the Active Roles Web Interface cannot display member devices and applications.
- You can always change the **Membership type** later by navigating to the **Azure Properties** > **General** page of the selected Azure security group on the Active Roles Web Interface:
- Changing the **Membership type** from **Dynamic Members** to **Assigned** later will keep the last set of members that were dynamically assigned to the group.

6. If you set the **Membership type** to **Dynamic Members**, specify the **Dynamic membership rule syntax**. Active Roles will send the logic configured in this field to Azure to automatically assign or remove members to or from the group later.

   NOTE: Consider the following when using the **Dynamic membership rule syntax** setting:

   - This setting is enabled only if **Membership type** is set to **Dynamic Members**. However, in that case, it is mandatory and cannot be empty.
   - The specified dynamic membership rule must meet all rule syntax requirements, otherwise the window will return an error. For more information on the available membership rule properties, operators and values, see Dynamic membership rules for groups in Azure AD in the *Microsoft 365 documentation*.
   - Whenever you modify the dynamic membership rule of a dynamic M365 group, it can take several minutes for Azure to update the list of group members in the **Dynamic Members** window of the selected Azure security group.

7. To complete the configuration of the new Azure security group, click **Finish**.

   The new Azure security group will appear under the **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups** node.

Modifying an Azure security group with the Web Interface

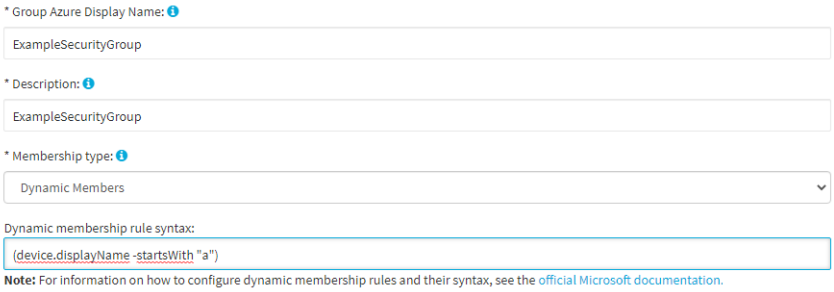
You can use the Active Roles Web Interface to modify the Azure properties of an existing Azure security group in your Azure tenant. This is typically useful if you have to:

- Modify the display name of the Azure security group, for example because of an organizational or security policy change.
- Change the configured membership type (manually assigned or dynamic) of the Azure security group.

To modify the Azure properties of an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. In the left-side pane of the **Azure Properties** window, click **Properties**.



5. (Optional) Specify the **Group Azure Display Name** of the configured group.

   TIP: You can configure multiple groups with the same **Group Azure Display Name** in the same Azure tenant.
6. (Optional) Provide a short **Description** for the group.
7. (Optional) Configure the **Membership type** of the group:
   - **Assigned**: When selected, you can add or remove members to or from the group manually later. For more information, see Adding or removing members from an Azure security group with the Web Interface.
   - **Dynamic Members**: When selected, Active Roles sets up the group as a dynamic membership group, and will automatically update group membership based on the configured **Dynamic membership rule syntax**.

   TIP: Consider the following when configuring the **Membership type**:
   - Select **Dynamic Members** to quickly configure a group based on a certain membership logic. For example, if you need to set up a group for employees from the same geographical location, business unit, or functional area, One Identity recommends configuring the group with **Dynamic Members**.
   - If you select **Dynamic Members**, you will not be able to manually add or remove members to or from the Azure security group, unless you change its **Membership type** to **Assigned** later. However, you can still manually configure the owner(s) for a dynamic Azure security group, as described in Adding or removing owners from an Azure security group with the Web Interface.

- Changing the **Membership type** from **Dynamic Members** to **Assigned** later will keep the last set of members that were dynamically assigned to the group.

8. (Optional) If you set the **Membership type** to **Dynamic Members**, specify the **Dynamic membership rule syntax**. Active Roles will send the logic configured in this field to Azure to automatically assign or remove members to or from the group later. For more information on how to specify a membership rule, see Dynamic membership rules for groups in Azure AD in the *Microsoft 365 documentation*.
9. To apply your changes, click **Save**.

Adding or removing owners from an Azure security group with the Web Interface

You can use the Active Roles Web Interface to specify owners for an Azure security group. Using the applicable options, you can either add or remove owners to or from the selected Azure security group.

NOTE: Consider the following when configuring group ownership:

- You cannot specify a group as an owner of another group.
- Although Active Roles and Azure AD support specifying Azure guest users as group owners, One Identity recommends doing so only if assigning the ownership of a specific group to a guest user is in line with the security policies of your organization.

To add owners to an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. To list the owners of the selected group, click the **Owners** tab of the **Azure Properties** window.
5. Click **Add** to add a new owner (or owners) to the selected group.
6. In the **Select Object** page, use the search field to find the users or guest users in the Azure tenant that you want to specify as owners.

   The users and guest users meeting the search criteria will appear in the **Display Name** column.
7. Select the check boxes of the users or guest users you want to specify as owners of the group. The selected users will be listed in the lower pane of the **Select Object** page.

8. (Optional) To search for additional users or guest users, enter another search string. After that, select the users or guest users you want to add from the updated list.
9. To apply your changes, click **OK**. The **Owners** page will be updated with the new settings.

To remove owners from an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to configure.
3. In the right-side pane, click **Azure Properties**.
4. To list the owners of the selected group, click the **Owners** tab of the **Azure Properties** window.
5. Select the owners whose ownership you want to revoke, and click **Remove**. The selected owners are removed from the list of owners.
6. To apply your changes, click **OK**. The **Owners** page will be updated with the new settings.

Adding or removing members from an Azure security group with the Web Interface

You can use the Active Roles Web Interface to add members to an existing Azure security group with an **Assigned** membership setting.

NOTE: Consider the following when managing the members of an Azure security group in Active Roles:

- In the Active Roles Web Interface, you can only specify Azure users, Azure guest users, other Azure security groups and external users as group members for Azure security groups with an **Assigned** membership setting. You cannot specify devices and applications. However, you can:
  - Configure Azure security groups in the Active Roles Web Interface to have dynamic device membership by using the appropriate dynamic membership rules (such as `device.displayName`). For more information on the applicable membership rule syntax, see Dynamic membership rules for groups in Azure AD in the *Microsoft 365 documentation*.
  - Configure device and application memberships later in Azure Portal for Azure security groups created in Active Roles.
- You cannot add or remove members manually to or from an Azure security group with dynamic membership. To change the members of a dynamic group manually, first modify its membership type from **Dynamic Members** to **Assigned** membership. For more information, see Modifying an Azure security group with the Web Interface.

- Although you can use the Active Roles Web Interface to manage Azure security groups that also contain devices and applications, the Active Roles Web Interface cannot display the member devices and applications of such groups.

To add members to an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to configure.
3. In the right-side pane, click **Members**.

   The **Members** page then appears with the list of members in the selected group.
4. Click **Add** to add a new member (or members) to the group.
5. In the **Select Object** page, use the search field to find the users, guest users or Azure security groups in the Azure tenant that you want to add.

   The users, guest users and Azure security groups that meet the search criteria will appear in the **Display Name** column.
6. Select the check boxes of the users, guest users or Azure security groups that you want to add to the group. The selected objects will appear in the lower pane of the **Select Object** page.
7. (Optional) To search for additional users, guest users or Azure security groups, enter another search string. After that, select the objects you want to add from the updated list.
8. To apply your changes, click **OK**. The **Members** page will be updated with the new membership settings.

To remove members from an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to configure.
3. In the right-side pane, click **Members**.

   The **Members** page then appears with the list of members in the selected group.
4. To remove a member (or members) from the selected group, select the members from the **Members Name** list, and click **Remove**.

   The selected members are removed from the **Members Name** list.
5. To apply your changes, click **OK**. The **Members** page will be updated with the new membership settings.

Viewing the members of a dynamic Azure security group with the Web Interface

You can check the member users, guest users and Azure security groups of an Azure security group with dynamic membership via the Active Roles Web Interface. This is useful if you want to get a quick update on the current membership status of the dynamic Azure security group.

NOTE: Consider the following when using dynamic Azure security groups in Active Roles:

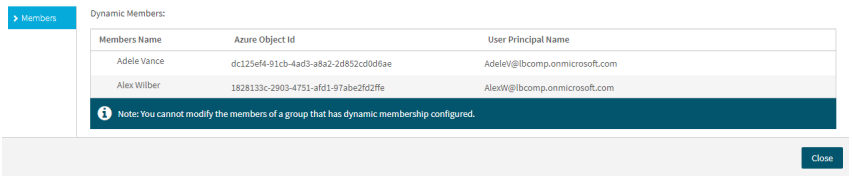
- You cannot add or remove members manually to or from an Azure security group with dynamic membership. To change the members of a dynamic group manually, first modify its membership type from **Dynamic Members** to **Assigned** membership. For more information, see Modifying an Azure security group with the Web Interface.
- Although you can use the Active Roles Web Interface to manage Azure security groups that also contain devices and applications, the Active Roles Web Interface cannot display the member devices and applications of such groups.

To view the members of an Azure security group with dynamic membership

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group whose members you want to check.
3. In the right-side pane, click **Dynamic Members**.

   The **Dynamic Members** page then appears with the list of members in the selected group.



4. To exit the **Dynamic Members** window, click **Close**.

Viewing the change history of an Azure security group in the Web Interface

You can check the change history of an Azure security group with the Active Roles Web Interface. This is useful if you want to view the list of changes that occurred to the selected Azure security group, such as:

- Membership changes (that is, added or removed members).
- Membership type changes (that is, whether the group has been set to assigned or dynamic membership).

NOTE: The **Change History** option of the Active Roles Web Interface lists only group modifications that were performed in Active Roles. It does not list the changes of the group that were performed outside Active Roles, for example in Azure Portal.

To view the change history of an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group whose change history you want to check.
3. In the right-side pane, click **Change History**.

   The **Change History** page then appears, with the newest change of the group listed at the top of the page.
4. To close the **Change History** window, click any **Tree** node, or any option listed in the right-side pane.

Deleting an Azure security group with the Web Interface

You can use the Active Roles Web Interface to delete an Azure security group from an Azure tenant. This is typically required when the group becomes redundant or is otherwise no longer required, for example because of a security policy change.

CAUTION: Deleting an Azure security group is a destructive operation that will delete the group from the Azure tenant on the Azure Portal as well.

To delete an Azure security group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Security Groups**.

   The list of existing Azure security groups in the selected Azure tenant appears.
2. Select the group that you want to delete.
3. In the right-side pane, click **Delete**.
4. A confirmation dialog appears. To confirm the deletion of the group, click **Yes**.

The selected Azure security group is then deleted from the Azure tenant.

Managing cloud-only Azure users

Active Roles supports managing cloud-only Azure users. Using the Active Roles Web Interface, you can:

Create, view, update, or delete cloud-only Azure users in the Azure AD of your organization.

- Check the Azure membership details, Azure properties, Exchange Online properties, or the change history of Azure users.
- Perform administrative operations on Azure users, such as rename them or reset their password.

When you create a new cloud-only Azure user for your organization, you must:

1. Specify a User Principal Name (UPN) and password for the Azure user.
2. Select the organization domain where the Azure user will be located within the Azure tenant.

Viewing cloud-only Azure user

To view cloud-only Azure user information, you can use the Active Roles Web Interface.

To view cloud-only Azure user

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.

   NOTE: Active Roles lists the available cloud-only Azure users, Azure guest users, and Azure contacts on the Active Roles Web Interface with the following restrictions:

   - Active Roles can initially list 999 items.
   - The items listed in the list have a sliding expiry of 8 hours, after which the objects that have not been accessed will be flushed.
   - Whenever you perform a search in the list, Active Roles will always fetch the list of objects from Azure to update the cache.

Creating a new cloud-only Azure user

You can use the Active Roles Web Interface to create and enable a new cloud-only Azure user.

To create a new cloud-only Azure user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Users**.

   The list of cloud-only Azure users in your Azure tenant then appears.
2. To start creating a new Azure user, in the right-side pane, click **New User**.
3. In the **New User** window, on the **General** tab, specify the details of the new Azure user (**First name**, **Last name**, **Display name**, **User principal name**, **Alias**, and **Description**).

   > **CAUTION:** Hazard of data loss!
   >
   > The **Display Name** field supports special characters. However, to avoid any potential problems in Active Roles when managing the Azure object, do not use any semicolons (**;**) in the specified display name.

   NOTE: In accordance with Microsoft 365, Azure users may share the same name. However, their aliases must be different.
4. To apply your changes and create the new Azure user, click **Finish**.

   The new cloud-only user then appears in the **Azure Users** list of the Active Roles Web Interface.

Viewing or modifying the properties of a cloud-only Azure user

You can use the Active Roles Web Interface to modify the properties of existing Azure users.

To view or modify the properties of a cloud-only Azure user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Users**.

   The list of cloud-only Azure users in your Azure tenant then appears.
2. From the list of **Azure Users**, select the user you want to modify.
3. To open the properties dialog of the Azure user, in the right-side pane, click **Azure properties**.
4. Use the tabs of the **Azure Properties** wizard to view or modify properties of the cloud-only Azure user.

   > **CAUTION:** Hazard of data loss!
   >
   > The **Display Name** field supports special characters. However, to avoid any potential problems in Active Roles when managing the Azure object, do not use any semicolons (**;**) in the specified display name.
5. To apply your changes, click **Save**.

Configuring Microsoft OneDrive for cloud-only Azure users

For cloud-only Azure users, to configure Microsoft OneDrive, you can use the Active Roles Web Interface.

To configure Microsoft OneDrive

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab, click **Azure Users** > **Azure** > **Azure Configuration** > **<Azure tenant>**.
3. Select the tenant and then click **OneDrive Configuration** available on the **Command** pane.
4. Provide the details in the **OneDrive Configuration**wizard and click **Save**.

IMPORTANT: The OneDrive configuration here is applicable for cloud-only users. For OneDrive configuration for hybrid users, see *Configuring Active Roles to manage Hybrid AD objects* in the *Active Roles Administration Guide*.

Blocking a cloud-only Azure user

To block a cloud-only Azure user, you can use the Active Roles Web Interface.

To block previously unblocked cloud-only user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. Select the Azure user that you want to block.
4. In the **Command** pane, click **Disable**.

   The account is blocked and marked with a blocked icon.

Unblocking a cloud-only Azure user

To unblock a cloud-only Azure user, you can use the Active Roles Web Interface.

To unblock a previously blocked cloud-only user for Azure

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. Select the Azure user that you want to unblock.
4. To unblock a blocked account, select the blocked account and in the **Command** pane click **Enable**.

   NOTE: The **Enable** command only appears for a blocked account.

   The account is unblocked again.

Viewing and modifying Exchange Online properties

To create and view and modify the Exchange Online properties of the new cloud-only Azure user, you can use the Active Roles Web Interface.

To view the Exchange Online properties of a cloud-only Azure user

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. Select the check box corresponding to the specific cloud-only Azure user with Exchange Online license for which you want to view the properties.
4. In the **Command** pane, click **Exchange Online Properties**.

   The **Exchange Online Properties** wizard displays the following Exchange Online properties for the cloud-only Azure user:

   - Mail Flow Settings
   - Delegation
   - E-mail Addresses
   - Mailbox Features
   - Mailbox Settings
5. To view the following Exchange Online properties of the cloud-only Azure user, use the tabs in the **Exchange Online Properties** dialog:

- Mail Flow Settings
    - Message Size restrictions
        - Sending Message size
        - Receiving Message size.
    - Delivery Options
        - Send On behalf
        - Forwarding Address
        - Enabling or disabling of Delivery messages to the forwarding address and mailbox.
- Delegation
- E-mail Addresses
- Mailbox Features
    - Exchange ActiveSync
    - Outlook Web App
    - MAPI
    - IMAP
    - POP3
    - Archive
- Mailbox Settings
    - Messaging Records management

Resetting password for a cloud-only Azure user

To reset the password for a cloud-only Azure user, you can use the Active Roles Web Interface.

To reset password of the cloud-only Azure user

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. In the **Command** pane, under Azure Users, click **Reset Password**.
4. In the **Password** field, provide the new password.
5. Reenter the password in the **Confirm password** field.

6. Select the relevant check box if you want users to change password during next sign-in.
7. Click **Finish**.

   The password is reset for the cloud-only Azure user.

Renaming a cloud-only Azure user

You can use the Active Roles Web Interface to rename an existing cloud-only Azure user.

To rename an Azure user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Users**.

   The list of cloud-only Azure users in your Azure tenant then appears.
2. From the list of **Azure Users**, select the user you want to rename.
3. To open the **Rename** dialog, in the right-side pane, click **Rename**.
4. Enter the new name of the Azure user.

   CAUTION: Hazard of data loss!

   The **Display Name** field supports special characters. However, to avoid any potential problems in Active Roles when managing the Azure object, do not use any semicolons (**;**) in the specified display name.
5. To apply your changes, click **Finish**. The **Azure Users** list is then updated with the new name of the user.

Viewing Azure membership

To view the Azure membership details of an cloud-only Azure user, you can use the Active Roles Web Interface.

Viewing cloud-only Azure user membership details

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. In the **Command** pane, click **Azure member of**.

   You can view the Azure group to which the cloud-only Azure user is associated.

Viewing Change History and User Activity

To view the **Change History** and **User Activity** for a cloud-only Azure user, you can use the Active Roles Web Interface.

To view the Change History and User Activity of a cloud-only Azure user

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. To view the history, select the Azure user.
4. In the **Command** pane, click **Change History** or **User Activity**.

   Selecting **Change History** displays the information on changes that were made to the user through Active Roles.

Deleting an Azure user account

To delete an Azure user , you can use the Active Roles Web Interface.

To delete an Azure user account

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. Select the Azure user that you want to delete.
4. In the **Command** pane, click **Delete**.

   A message prompts you to confirm the action.
5. Click **Yes** to continue.

   The Azure user that are selected are deleted.

Managing cloud-only Azure guest users

You can invite (or re-invite), modify and remove cloud-only Azure guest users in the Azure AD of your organization with the Active Roles Web Interface.

An Azure guest user is a type of cloud-only Azure user that is not part of the organization domain for which you configure it.

When you create a new cloud-only Azure user for your organization, you must:

1. Specify a User Principal Name (UPN) and password for the Azure user.
2. Select the organization domain where the Azure user will be located within the Azure tenant.

However, when you create an Azure guest user, no domains are assigned to the user within the Azure tenant. Instead, the procedure has the following main steps:

1. You specify the basic permissions of the guest user, along with an email address to which Active Roles will send an invitation.
2. Using the link in the invitation email, the guest user can gain the configured access with their account upon joining the organization.
3. Once the guest accepted the invitation, you can assign additional permissions (like roles, licenses, storage space, and so on) to the user, similarly to a regular cloud-only Azure user.

NOTE: Active Roles does not restrict the type of permissions that you can assign to Azure guest users. However, for security reasons, One Identity recommends that you assign only the rights and resources to guest users that external contractors typically receive in your organization.

Inviting an Azure guest user

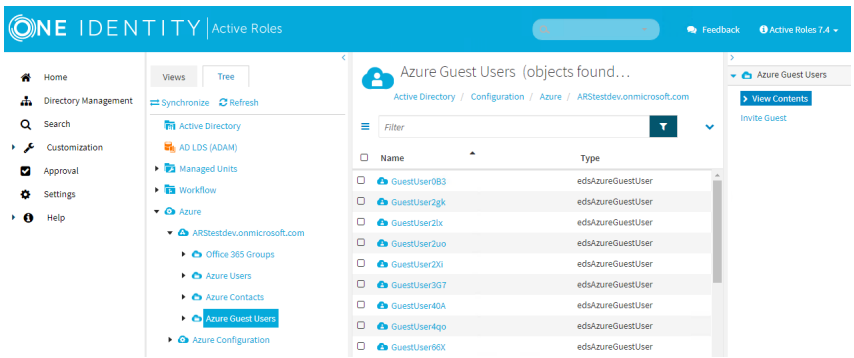
If an external user (such as a contractor, or other non-employee resource with limited permissions) must be added to the organization, invite them as Azure guest users to the Azure tenant of the organization using the Active Roles Web Interface.

To invite an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

   Figure 30: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant

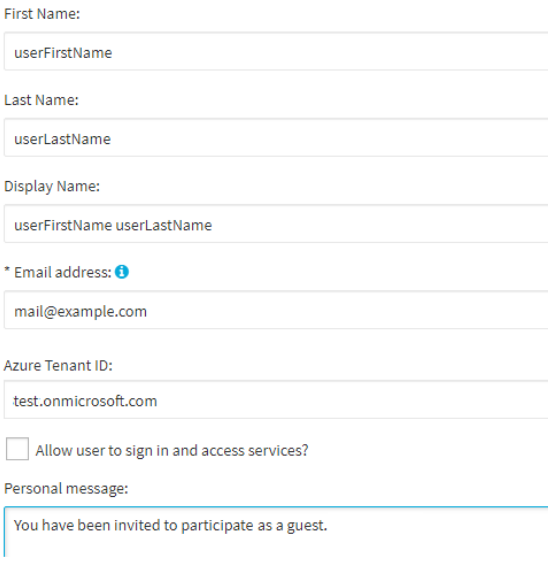
2. In the right-side pane, click **Invite Guest**.

You will invite a new guest user, and set up their account, application licenses and various admin roles, too.

3. **Identity**

   Configure the settings required by your organization for setting up the identity of the guest user.

Figure 31: Azure Guest Users > Invite Guest > Identity – Configuring basic user account settings for the Azure guest user



   a. (Optional) Enter the **First Name** of the Azure guest user.

      NOTE: If you do not enter a **First Name**, Active Roles will fill this field with the local part of the specified **Email address**.

   b. (Optional) Enter the **Last Name** of the Azure guest user.

   c. (Optional) Enter the **Display Name** of the Azure guest user.

      TIP: By default, the **Display Name** is automatically generated from the specified **First Name** and **Last Name**, but you can modify it to something else (such as a nickname).

      CAUTION: Hazard of data loss!

      The **Display Name** field supports special characters. However, to avoid any potential problems in Active Roles when managing the Azure object, do not use any semicolons (**;**) in the specified display name.

   d. Enter the **Email address** where Active Roles will send out the invitation. This field is mandatory and must be unique.

   e. (Optional) Enter the **Azure Tenant ID** of the Azure tenant that will contain the guest user.

f. To grant the Azure guest user access to the configured licenses and admin roles, select **Allow user to sign in and access services**.

- If this setting is selected during this step, the guest user will receive access as soon as they accept the invitation.
- If left clear, you must manually grant access later by enabling this setting in the **Azure Properties** page of the guest user. For more information, see Viewing and updating the properties of an Azure guest user.

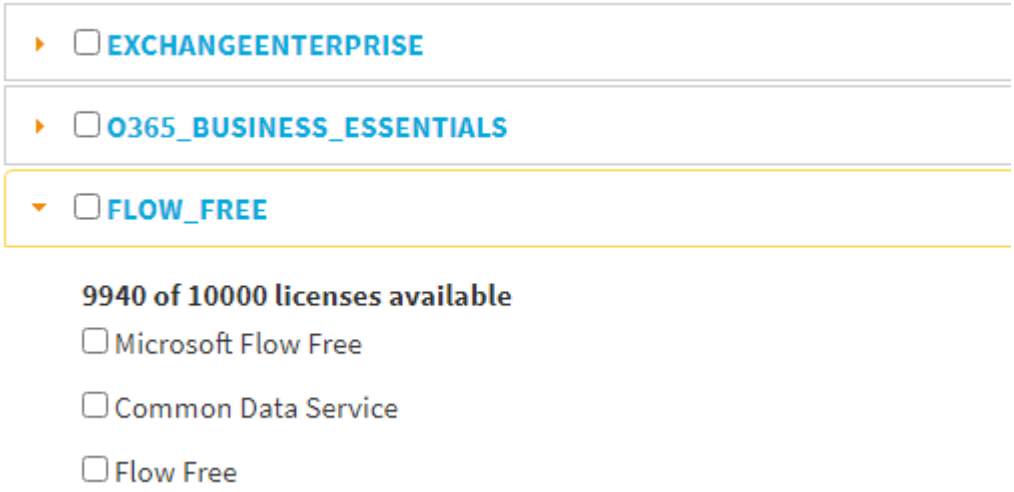
> TIP: Leaving this setting clear is useful if the account of the Azure guest user is created in advance, and they require access to the assigned resources only later (for example, because their contract project starts only at a later date).

g. (Optional) Enter a unique **Personal message** that the invitation email will contain.

4. **Licenses**

Select the Microsoft application resources licensed in your organization that you want to assign to the configured Azure guest user.

Figure 32: Azure Guest Users > Invite Guest > Licenses – Assigning application licenses to the Azure guest user



5. **O365 Admin Roles**

Select the O365 role(s) that you want to grant for the Azure guest user.

Figure 33: Azure Guest Users > Invite Guest > O365 Admin Roles – Assigning Office 365 administrator roles to the Azure guest user

NOTE: You can assign roles to the Azure guest user in Active Roles without any limitation. However, One Identity recommends that you assign Azure guest users only the admin roles that external contractors typically receive in your organization.

6. (Optional) **Job Info**

   Enter the **Job Title** and the assigned **Department** of the guest user, if needed.

Figure 34: Azure Guest Users > Invite Guest > Job Info – Specifying organizational information for the Azure guest user

7. To save your changes and send the invite email to the guest user, click **Finish**.

   NOTE: Consider the following when administering cloud-only Azure guest users:

   - You can resend the invitation later for the guest user, if needed. For more information, see Resending the invitation to an Azure guest user.

- You can modify the user account settings later, if needed. For more information, see Viewing and updating the properties of an Azure guest user.

Viewing Azure guest users

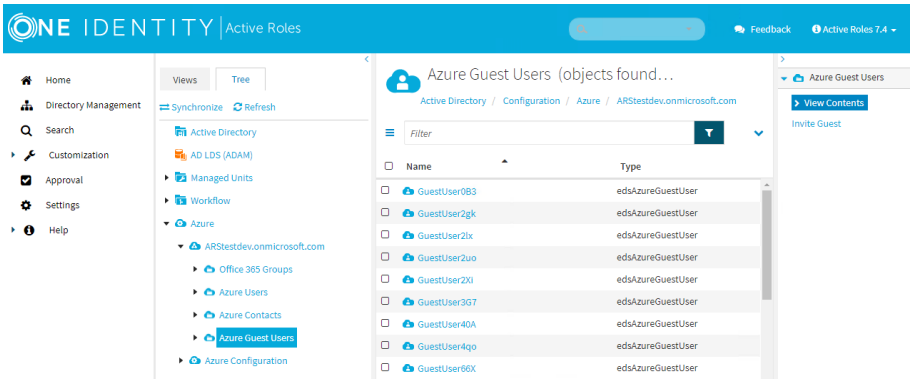
To list the configured cloud-only Azure guest users of an Azure tenant, and access their available configuration actions, expand the **Azure Guest Users** node of the Active Roles Web Interface.

To view the configured Azure guest users in an Azure tenant

Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

The list of Azure guest users of the selected tenant is displayed.

Figure 35: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



NOTE: Active Roles lists the available cloud-only Azure users, Azure guest users, and Azure contacts on the Active Roles Web Interface with the following restrictions:

- Active Roles can initially list 999 items.
- The items listed in the list have a sliding expiry of 8 hours, after which the objects that have not been accessed will be flushed.
- Whenever you perform a search in the list, Active Roles will always fetch the list of objects from Azure to update the cache.

Disabling or Enabling an Azure guest user

If you want to revoke the access of an Azure guest user from the resources, applications and roles assigned to them, you can disable their account without deleting them with the **Disable Account** action.

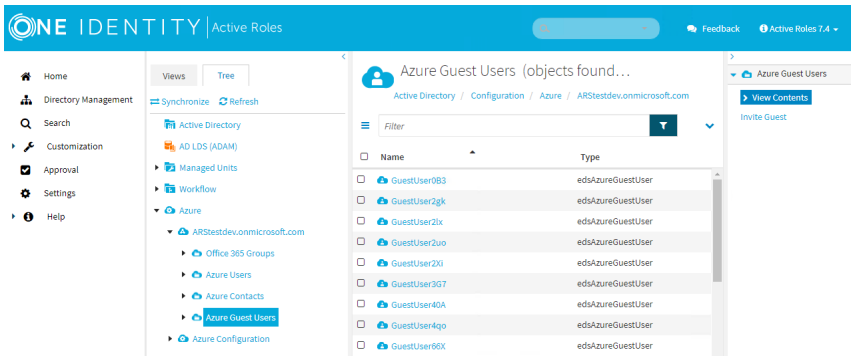
Likewise, once the revoked access rights of a disabled Azure guest user can be reinstated, you can re-enable them with the **Enable Account** action.

To disable or enable a cloud-only Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

   Figure 36: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user that you want to enable or disable from the list.
3. Click the applicable option:
   - If the selected Azure guest user is enabled, click **Disable Account**.
   - If the selected Azure guest user is disabled, click **Enable Account**.

   NOTE: The available option changes depending on the state of the selected guest user account.
4. To confirm disabling/enabling the selected Azure guest user, click **Save**.

Revoking the session of an Azure guest user

You can revoke the current session of any selected cloud-only Azure guest user of an Azure tenant. When doing so, Active Roles clears the active login tokens of the guest user on all devices they have previously logged in from, forcing them to log in again and validate their credentials.

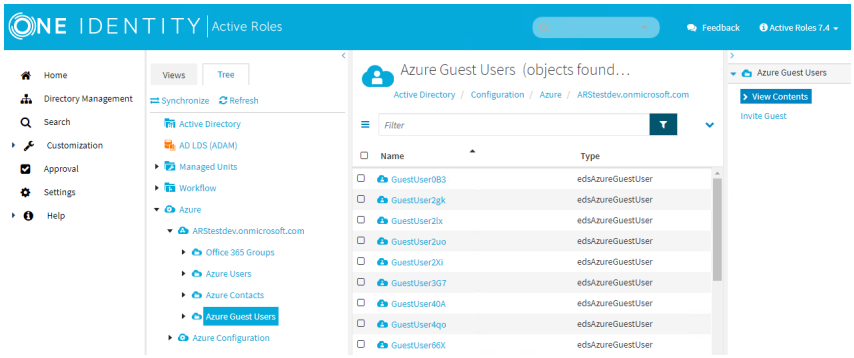
TIP: If any device that the Azure guest user has been previously logged in from has been compromised (for example, because the guest user has lost their notebook or cellphone), then One Identity recommends revoking their current session.

To revoke the active session of an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

Figure 37: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user whose session you want to revoke.
3. Click **Revoke Session**.
4. To confirm revoking the session of the selected Azure guest user, click **Save**.

Resending the invitation to an Azure guest user

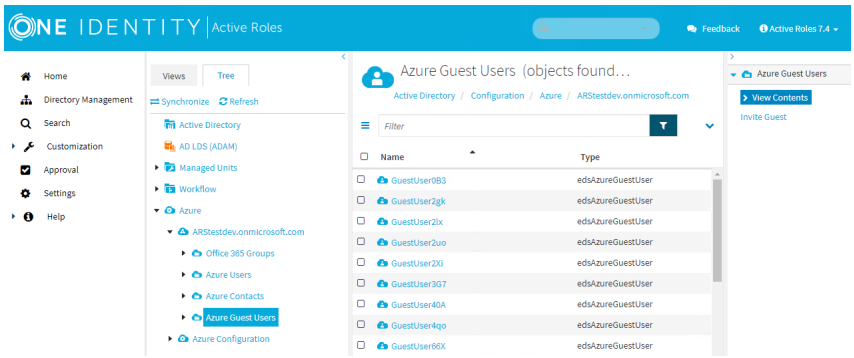
It can happen that the invitation email sent out at the end of the Inviting an Azure guest user procedure must be sent again to the Azure guest user (for example, because the guest user cannot access the specified email address for some reason, or because the previous invitation was accidentally deleted). In such cases, you can resend the invitation email.

To resend the invitation to an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

Figure 38: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user for which you want to resend the invitation.

3. Click **Resend Invitation**.

   Active Roles will then resend the invitation to the email address previously specified with the **Invite Guest** > **Email address** property.

Renaming an Azure guest user

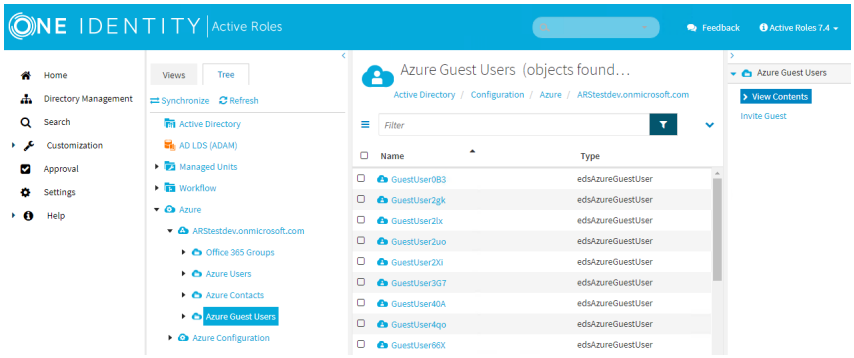
If an Azure guest user account must be renamed for any reason (for example, to fix a typo or an incorrect first/last name), you can use the **Rename** option of the Active Roles Web Interface.

To rename an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

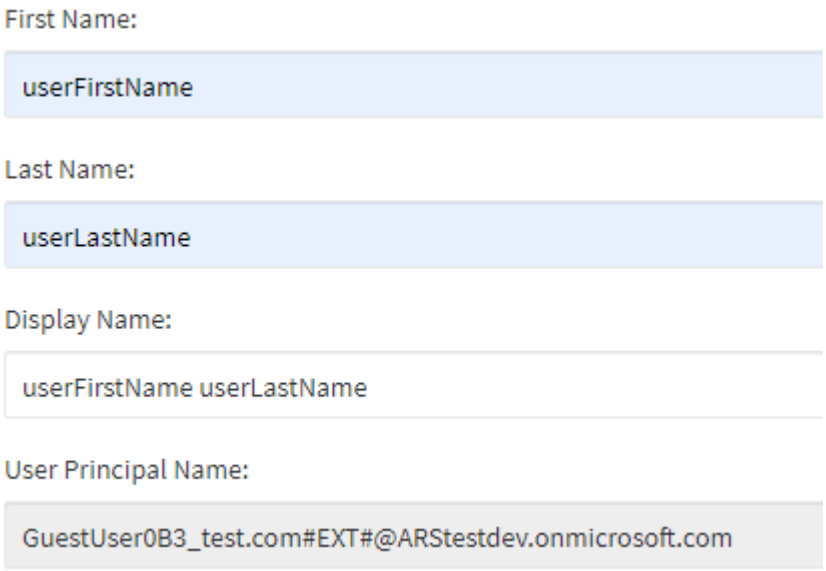
   The list of Azure guest users of the selected tenant is displayed.

   Figure 39: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user that you want to rename.
3. To open the rename form, click **Rename**.

Figure 40: Azure Guest Users > Rename – Renaming an Azure guest user



4. Update the **First Name**, **Last Name** or **Display Name** of the guest user as needed.

   CAUTION: Hazard of data loss!

   The **Display Name** field supports special characters. However, to avoid any potential problems in Active Roles when managing the Azure object, do not use any semicolons (**;**) in the specified display name.

5. To apply your changes, click **Finish**.

Viewing and updating the properties of an Azure guest user

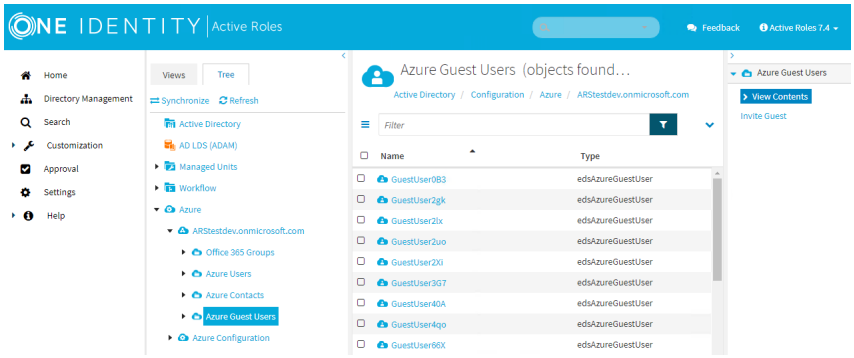
Once you configured and invited a new Azure guest user as described in Inviting an Azure guest user, you can modify their account settings with the **Azure Properties** option later if any change occurred to the user that must be reflected in their account.

To view and update the properties of an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

Figure 41: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. In the available **Azure Properties** pages, configure the Azure guest user settings that you want to change.

Table 2: Available Azure properties

Page	Description
Identity	View and configure user identity settings and information in this tab.
Settings	View and configure user authentication settings in this tab.
Job Info	View and configure job and organizational information in this tab.
Contact Info	View and configure contact and location information in this tab. NOTE: You can only update certain **Contact Info** properties (such as phone numbers or email addresses) for non-administrator Azure guest users, or for Azure guest users with a specific set of limited administrator roles. For more information on these roles, see the Update User page of the official Microsoft documentation. Attempting to update these properties for an Azure guest user with different administrative roles assigned to it will result in failure, and the following error log message appearing in the Windows Event Log: `Post-processing operation on object caused a policy violation.`
Licenses	View and configure the Microsoft application resources available in the organization to the Azure guest user.
O365 Admin Roles	View and configure the O365 roles in the organization granted for the guest user.

5. To apply your changes, click **Save**.

NOTE: Active Roles lists the available cloud-only Azure users, Azure guest users, and Azure contacts on the Active Roles Web Interface with the following restrictions:

- Active Roles can initially list 999 items.
- The items listed in the list have a sliding expiry of 8 hours, after which the objects that have not been accessed will be flushed.
- Whenever you perform a search in the list, Active Roles will always fetch the list of objects from Azure to update the cache.

Configuring the Identity settings of an Azure guest user

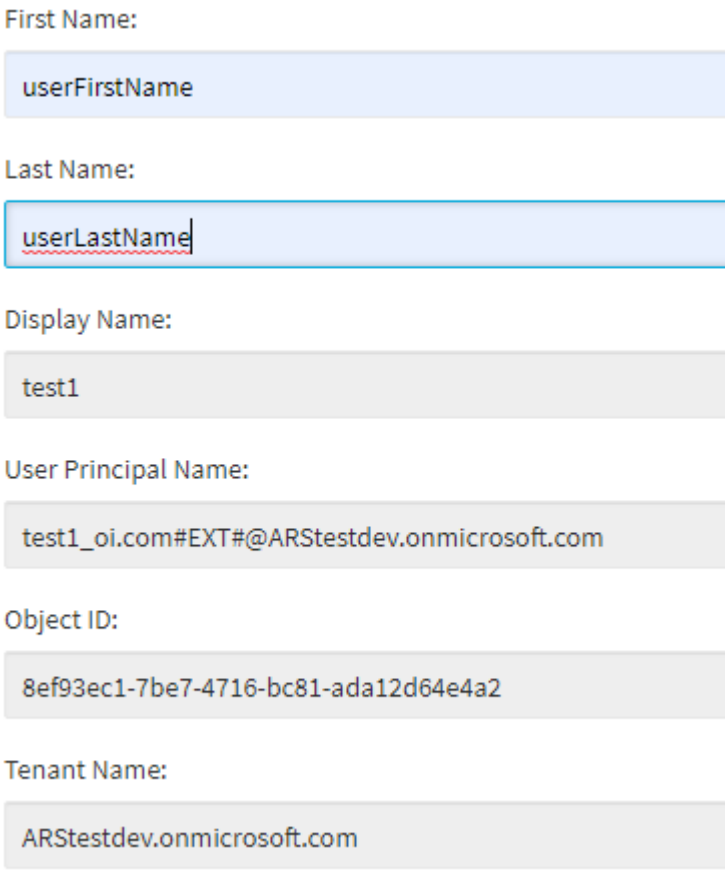
You can update the name settings of an Azure guest user in an Azure tenant with the **Azure Properties** > **Identity** tab.

NOTE: You can only change the **First Name** and **Last Name** settings of the guest user on this tab. You can change the rest of the identity settings when inviting the guest user. For more information, see Inviting an Azure guest user.

To update the settings of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the name settings, click the **Identity** tab.

Figure 42: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > Identity — Configuring the identity-related information of an Azure Guest user



5. Enter the **First Name** of the Azure guest user. If no first name has been specified in this field when inviting the Azure guest user, this text box contains the local-part of the email address where the invite has been sent.
6. Enter the **Last Name** of the Azure guest user.
7. To apply your changes, click **Save**.

NOTE: You can also view the following identity properties of the selected Azure guest user on this page:

- **Display Name**: Shows the display name of the Azure guest user. By default, the display name consists of the specified **First Name** and **Last Name**.

  TIP: You cannot directly modify the **Display Name** of the guest user on this tab. To do that, use the **Rename** action. For more information, see Renaming an Azure guest user.

- **User Principal Name**: Displays the User Principal Name (UPN) of the Azure guest user. The UPN has the following syntax:

```
<azure-guest-user-email-address>#EXT#@<azure-tenant>
```

- **Object ID**: Displays the object ID of the Azure guest user
- **Tenant Name**: Displays the Azure tenant containing the Azure guest user.

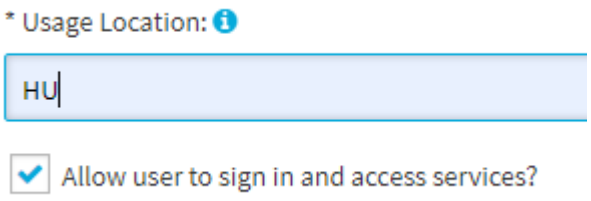
Configuring the Settings of an Azure guest user

You can update the authentication settings of an Azure guest user in an Azure tenant with the **Azure Properties** > **Settings** tab. You must modify these settings typically when the geographical location of the guest user has changed (for example, because they have moved to an office located in another country), or if the guest user has received no access to the configured roles and licenses when their account has originally been created.

To configure the authentication settings of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the user authentication settings, click the **Identity** tab.

Figure 43: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > Settings — Accessing the authentication settings of an Azure Guest user



5. To restrict the login attemps with the configured Azure guest user account to a specific geographical location, enter the corresponding ISO 3166 country code in the **Usage Location** field. Active Roles will then only allow the guest user to log in, if the login attempt occurs from the country that you specified.
6. (Optional) To grant the Azure guest user access to the configured licenses and admin roles, select **Allow user to sign in and access services**. If access has been granted previously, and must be revoked, then deselect this option.

   TIP: Leaving this setting clear is useful if the account of the Azure guest user is created in advance, and they require access to the assigned resources only later (for example, because their contract project starts only at a later date).
7. To apply your changes, click **Save**.

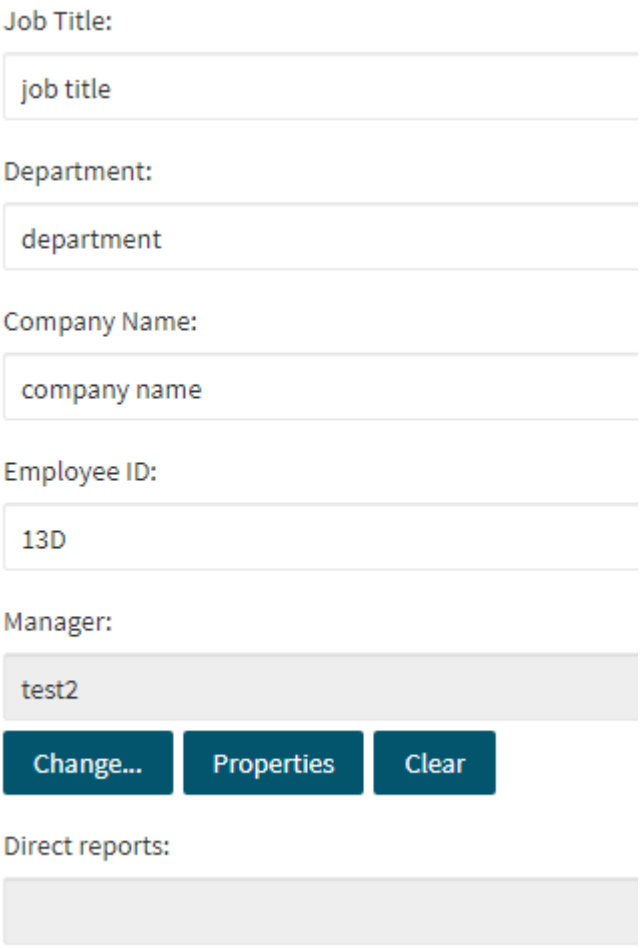
Configuring the Job Info settings of an Azure guest user

You can configure job and organizational information for an existing Azure guest user in an Azure tenant with the **Azure Properties** > **Job Info** tab. This is typically required if the employment status of the guest user changes, for example their position, assigned department or employee ID is modified for some reason.

To modify the job information of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the job information settings, click the **Job Info** tab.

Figure 44: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > Job Info — Accessing the organizational settings of an Azure Guest user



5. (Optional) Specify the **Job Title** of the guest user.
6. (Optional) Specify the **Department** of the guest user to which they are assigned.
7. (Optional) Specify the assigned company of the guest user with the **Company Name** setting. For example, this can be either the external company that employs the guest user, or a specific company-size unit within your organization that is contracting them.
8. (Optional) Specify the **Employee ID** of the guest user, if they have one issued.
9. (Optional) Specify the **Manager** the guest user reports to. Use **Change...** to specify or change the manager, click **Properties** to view information about the currently specified manager, or click **Clear** to remove the current selection.
10. To apply your changes, click **Save**.

NOTE: The **Job Info** also has a **Direct reports** field that lists the employees or other guest users reporting to the selected guest user, if there are any.

Configuring the Contact Info settings of an Azure guest user

You can modify the contact and location information (such as phone number, address, office location) of an Azure guest user in an Azure tenant with the **Azure Properties** > **Contact Info** tab. This is typically required if the organization requires detailed contact information for the guest user, or if any previously-configured contact information has been changed.

NOTE: You can only update certain **Contact Info** properties (such as phone numbers or email addresses) for non-administrator Azure guest users, or for Azure guest users with a specific set of limited administrator roles. For more information on these roles, see the Update User page of the official Microsoft documentation.

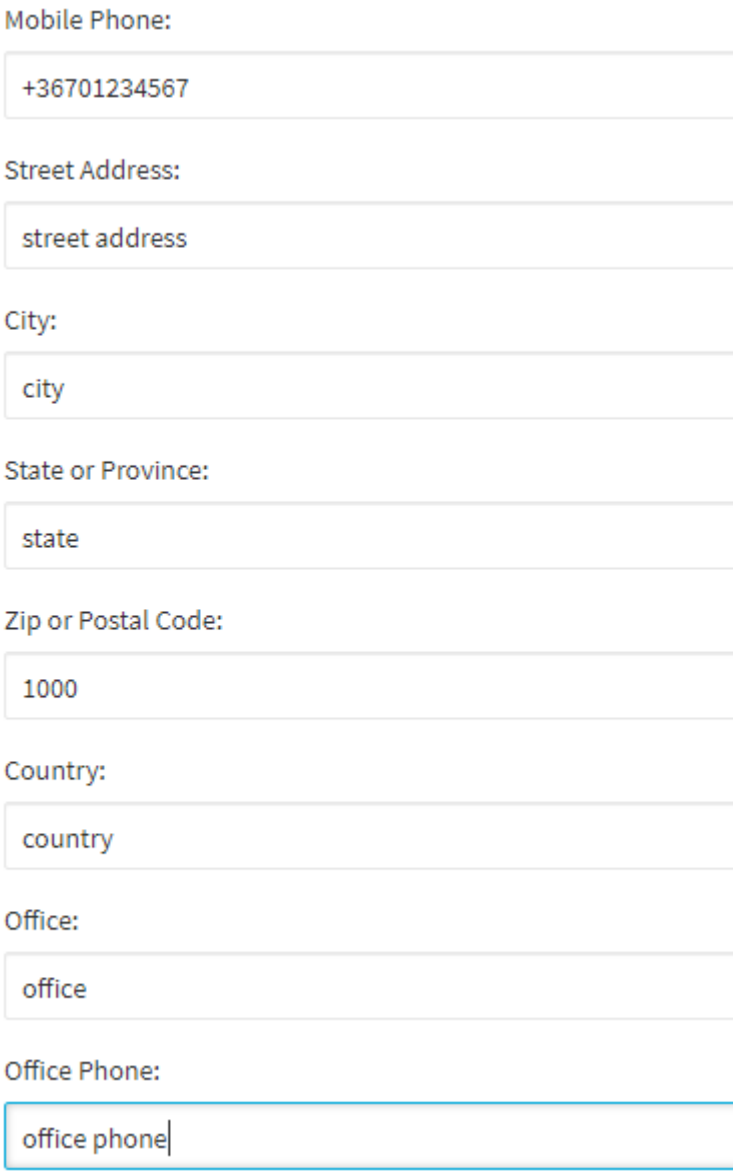
Attempting to update these properties for an Azure guest user with different administrative roles assigned to it will result in failure, and the following error log message appearing in the Windows Event Log:

```
Post-processing operation on object caused a policy violation.
```

To modify the contact information of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the contact information settings, click the **Contact Info** tab.

Figure 45: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > Contact Info — Accessing the contact and location settings of an Azure Guest user



5. (Optional) Specify the **Mobile Phone** number of the guest user.
6. (Optional) Specify the **Street Address** of the guest user.
7. (Optional) Specify the **City** where the guest user is located.
8. (Optional) Specify the **State or Province** where the guest user is located.
9. (Optional) Specify the **Zip or Postal Code** of the location of the guest user.
10. (Optional) Specify the **Country** where the guest user is located.
11. (Optional) Specify the **Office** where the guest user is located.

12. (Optional) Specify the **Office Phone** number of the guest user, if one is issued to them.
13. To apply your changes, click **Save**.

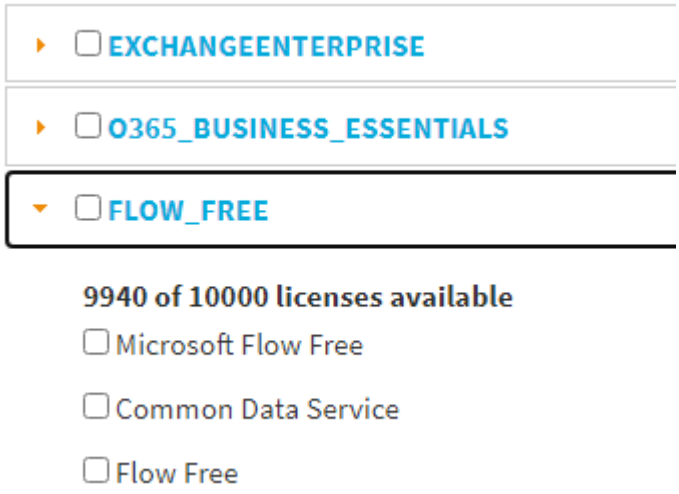
Configuring the Licenses settings of an Azure guest user

You can assign or unassign any of the Microsoft application resources in an organization to an existing Azure guest user in the **Azure Properties** > **Licenses** tab. This is typically required if the previously-configured application licenses must be modified, for example because of changes in the assignment of the guest user.

To configure the application licenses of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the application license settings, click the **Licenses** tab.

Figure 46: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > Licenses — Accessing the application license settings of an Azure Guest user



5. (Optional) If the available licenses are categorized into various headings, expand the list of the license(s) you want to add or remove from the guest user.
6. Select the license(s) you want to assign to the guest user, or deselect the one(s) you want to remove from them.
7. To apply your changes, click **Save**.

Configuring the O365 Admin Roles settings of an Azure guest user

You can grant (or revoke) O365 administration roles to (or from) an existing Azure guest user in the **Azure Properties** > **O365 Admin Roles** tab. This is typically required either when the assignment of a guest user changes, or when it is finished.

To configure the O365 admin roles of an existing Azure guest user

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Guest Users**.
2. From the list in the middle pane, select the Azure guest user that you want to update.
3. To open the properties of the selected Azure guest user, click **Azure Properties** on the right pane.
4. To open the administration role settings, click the **O365 Admin Roles** tab.

   Figure 47: Directory Management > Tree View > Azure > *<azure-tenant>* > Azure Guest Users > *<azure-guest-user>* > Azure Properties > O365 Admin Roles — Accessing the administrator role settings of an Azure Guest user

5. Select the administrator role(s) you want to grant for the guest user, or deselect the role(s) you want to revoke.

   NOTE: You can assign roles to the Azure guest user in Active Roles without any limitation. However, One Identity recommends that you assign Azure guest users only the admin roles that external contractors typically receive in your organization.

6. To apply your changes, click **Save**.

Viewing or updating the Exchange Online properties of an Azure guest user

You can create, modify or view the Exchange Online properties of an existing Azure guest user with the **Exchange Online** option of the Active Roles Web Interface. With the Exchange Online properties, you can configure various mailbox-related settings for the guest user, such as:

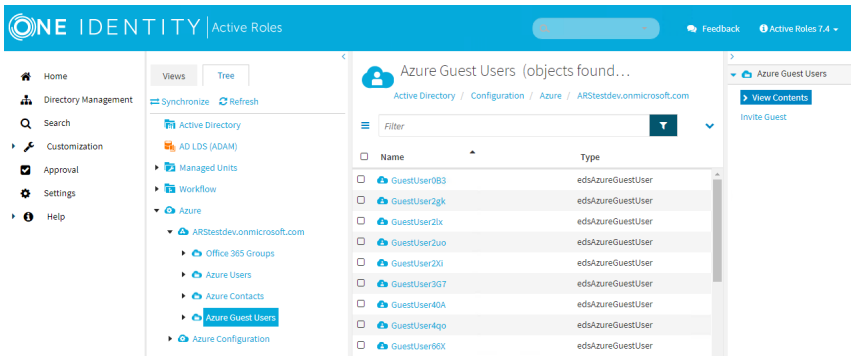
- The name of the email address.
- Message size and delivery rules.
- Setting up the guest user mailbox as a shared mailbox.
- Enabling or disabling various applications (such as Outlook Web App) or protocols (such as MAPI, IMAP4, or POP3) for the mailbox.
- Configuring Messaging Records Management (MRM) settings for the guest user mailbox.

To view and update the Exchange Online properties of an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

   Figure 48: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant

2. Select the guest user whose Exchange Online properties you want to check or update.
3. To access the Exchange Online-specific mailbox settings, click **Exchange Online Properties**.
4. In the available **Exchange Online Properties** tabs, configure the Exchange Online

mailbox settings as you need.

Table 3: Available Exchange Online properties

Page	Description
Mail Flow Settings	View and configure rules for the emails that the mailbox sends or receives via the Exchange Online service.
Delegation	Configure the email account as a shared mailbox.
General	View and configure the email addresses associated with the mailbox.
Mailbox Features	View and configure various Exchange Online mailbox features, for example mobile access, additional mailbox protocols, or archival settings.
Mailbox Settings	View and configure Messaging Records Management (MRM) settings for the mailbox.

5. To apply your changes, click **Close**.

Configuring the mail flow settings of an Exchange Online mailbox

You can set up rules for the emails that Exchange Online mailboxes send or receive in the organization with the **Exchange Online Properties** > **Mail Flow Settings** tab of the Active Roles Web Interface. Active Roles supports setting up two types of such rules:

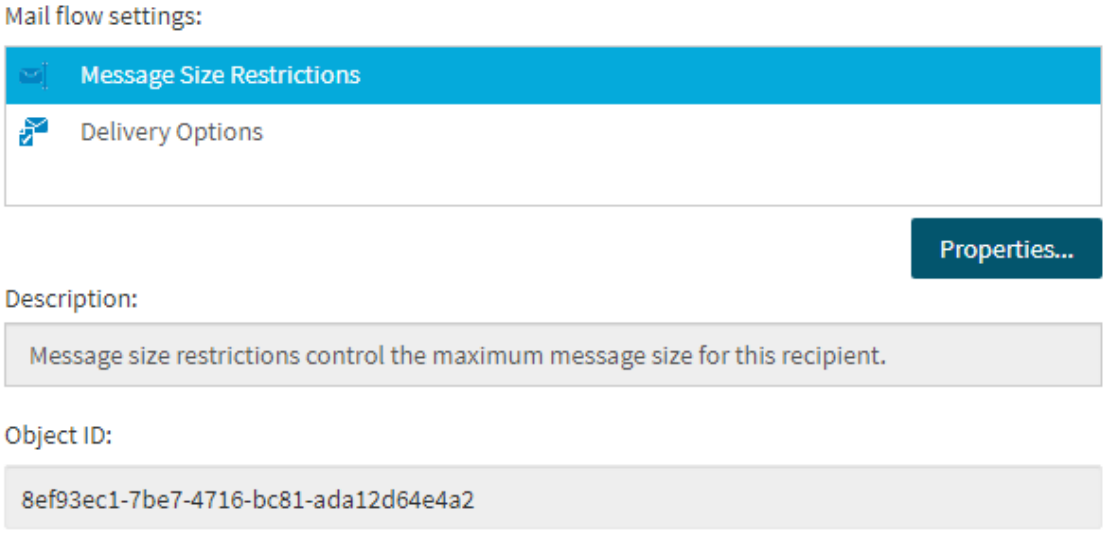
- Message size settings, specifying the size of the emails that the guest user can send or receive.
- Email delivery and forwarding settings, allowing the guest user to send emails on behalf of a specified group, or have their received emails automatically forwarded to an additional specified address.

Such mail flow settings are typically configured if the organization enforces specific email messaging policies for users and guest users.

To configure the mail flow settings for an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the mail flow settings, click the **Mail Flow Settings** tab.

Figure 49: Exchange Online Properties > Mail Flow Settings — Configuring the message size and forwarding settings of an Exchange Online mailbox



5. Select **Message Size Restrictions**, and click **Properties...**.
6. Configure the size of the emails (in KB) that are sent or received by the mailbox. By default, both the **Sending message size** and the **Receiving message size** settings use the default limit of the Azure tenant.
7. To apply your changes and close the **Message Size Restrictions** dialog, click **Save**.
8. Select **Delivery Options**, and click **Properties** to configure the following email delivery and forwarding settings.
    - **Send on Behalf**: When configured, the mailbox can send emails on behalf of the specified mailbox or group.
    - **Forwarding Address**: When configured, the emails received by the mailbox are always forwarded to the specified email address.
9. To apply any changes you made in the **Delivery Options** dialog, click **Save**.
10. To close the **Exchange Online Properties** window, click **Close**.

Configuring the delegation settings of an Exchange Online mailbox

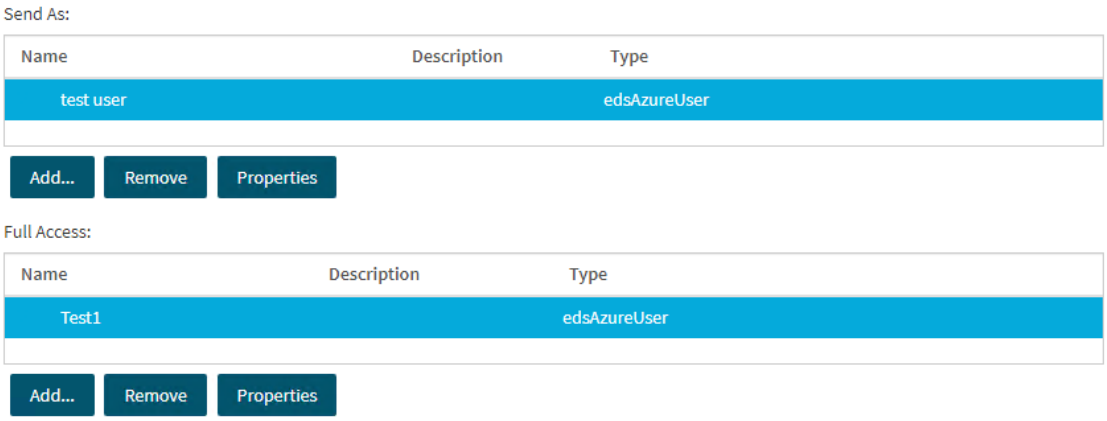
You can set up an Exchange Online mailbox as a shared mailbox in the **Exchange Online Properties** > **Delegation** tab of the Active Roles Web Interface. This is typically performed if the configured email account is used as a group account, such a common support or information email address.

The Active Roles Web Interface supports granting *Send as* and *Full access* permissions to the specified users and guest users. For more information on shared mailboxes and these permissions, see Shared mailboxes in Exchange Online in the *Microsoft Exchange documentation*.

To configure the email delegation settings of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the delegation settings, click the **Delegation** tab.

Figure 50: Exchange Online Properties > Delegation — Accessing the email account delegation settings of an Exchange Online mailbox



5. To delegate *Send as* permission to a user (or users), click **Add...** under the **Send As** list.
6. Select the user(s) you want to grant *Send as* rights for the email address, then click **OK**.
7. To delegate *Full Access* permission to a user (or users) click **Add...** under the **Full Access** list.
8. Select the user(s) you wish to grant *Full access* rights for the email address, then click **OK**.
9. To remove a delegated user either from the **Send As** or **Full Access** list, click **Remove** and select the user(s) you want to revoke the permission from.
10. To apply your changes, click **Save**, then **Close**.

Configuring the general email address settings of an Exchange Online mailbox

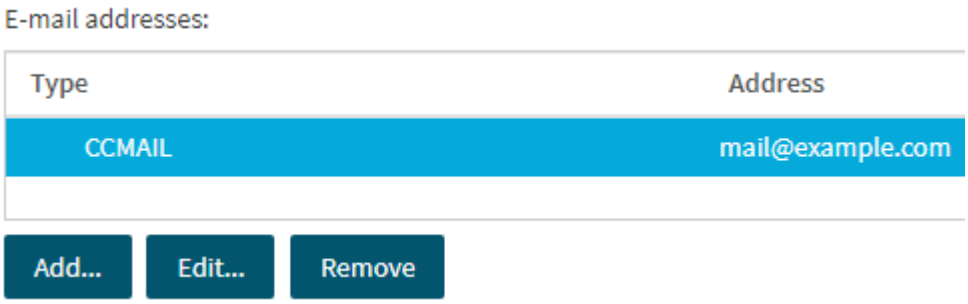
You can add, edit or remove email addresses to or from an Exchange Online mailbox in the **Exchange Online Properties** > **General** tab of the Active Roles Web Interface. Adding, editing, or removing email addresses is typically required in case of organizational changes

(for example, the mailbox user is assigned to a new project, or the contract of a guest user ends within the organization).

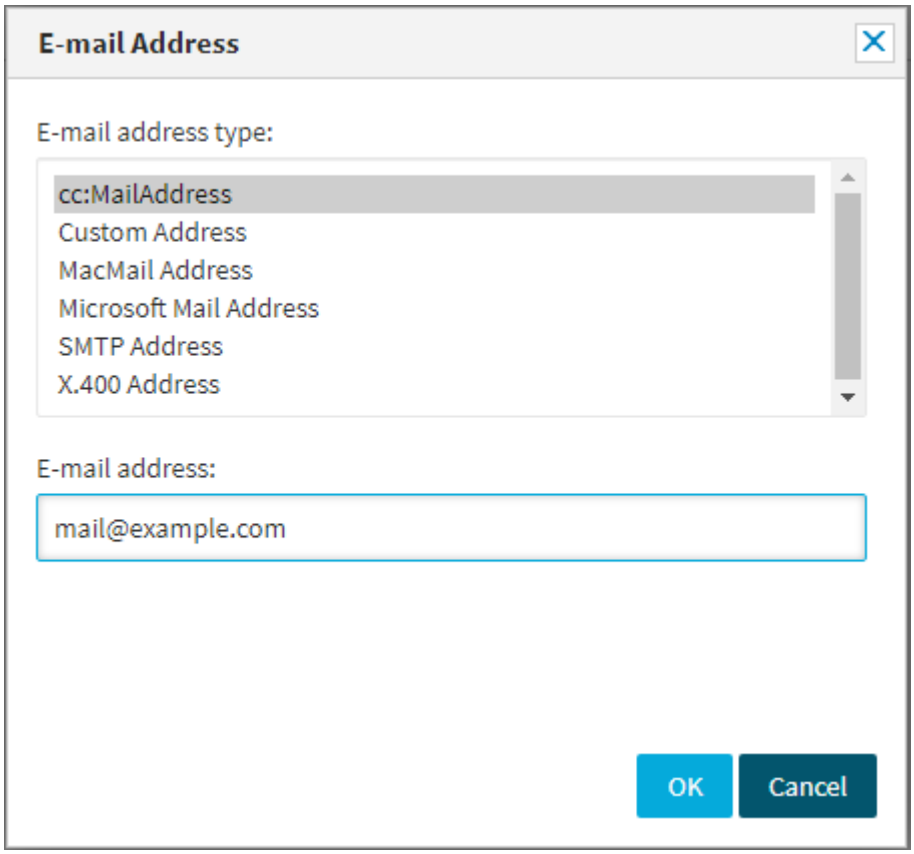
To add a new email address to an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.

Figure 51: Exchange Online Properties > General — Accessing the email account settings of an Exchange Online mailbox



5. Click **Add...**. The **E-mail Address** dialog then opens.



6. From the **E-mail address type** list, select the email account type applicable to your organization.
7. In the **E-mail address** text box, specify the address of the new account.
8. To apply your changes and create the new email account, click **OK**.
9. To close the **Exchange Online Properties** window, click **Close**.

To edit an existing email address of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.
5. To open the settings of an email address, select the email address, then click **Edit...**.
6. In the **E-mail address** text box, modify the current email address.

   NOTE: You cannot modify the **E-mail address type** of an existing email account. You can only change the name of the existing address.

7. To apply your changes, click **OK**.
8. To close the **Exchange Online Properties** window, click **Close**.

To remove an existing email address of an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the email address settings, click the **General** tab.
5. In the **E-mail addresses** list, select the address you want to remove.
6. Click **Remove** and confirm the deletion of the email address.
7. To close the **Exchange Online Properties** window, click **Close**.

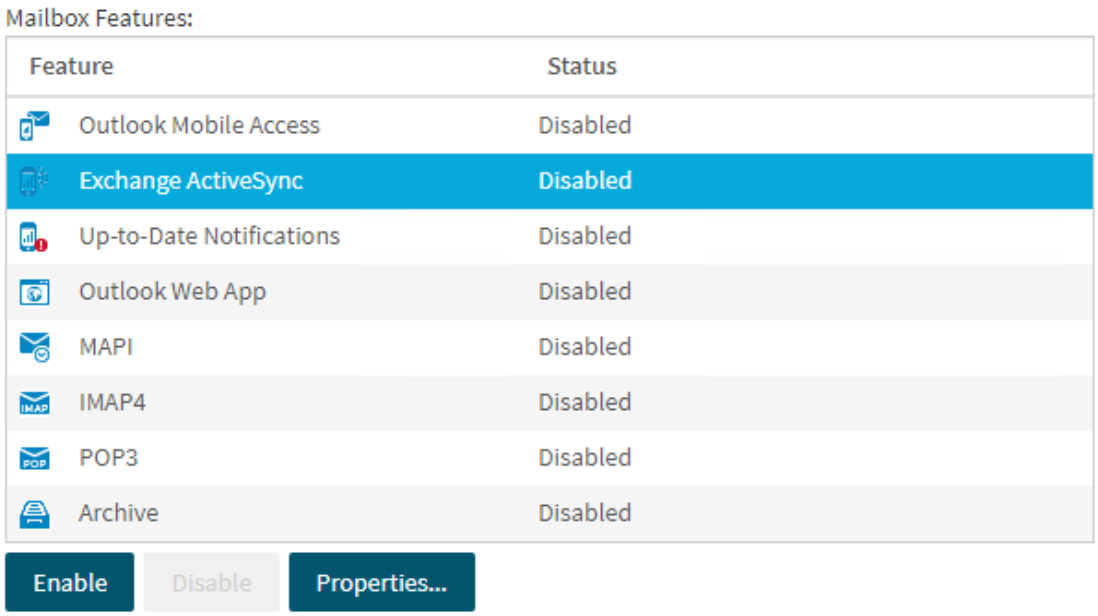
Configuring the mailbox features of an Exchange Online mailbox

You can enable or disable various Exchange Online mailbox features for an Exchange Online mailbox (such as Outlook Mobile Access or support for messaging protocols like IMAP4 or POP3) in the **Exchange Online Properties** > **Mailbox Features** tab of the Active Roles Web Interface. This is typically required if the organization supports specific applications and protocols for its Exchange mailboxes.

To enable or disable Exchange Online mailbox features for an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the mailbox feature settings, click the **Mailbox Features** tab.

Figure 52: Exchange Online Properties > Mailbox Features — Configuring mailbox features for an Exchange Online mailbox



5. Select the Exchange Online mailbox feature that you want to enable or disable:
   - **Outlook Mobile Access**: Enables or disables the Outlook Mobile Access (OMA) mobile browsing service for the mailbox. Enabling this settings allows the mailbox user use OMA on their mobile device to access their account.
   - **Exchange ActiveSync**: Enables or disables the Exchange ActiveSync synchronization protocol for the mailbox. Enabling this setting allows the mailbox user synchronize their configured mobile device with their mailbox.
   - **Up-to-Date Notifications**: Enables or disables the Up-to-date (UTD) feature notifications for the mailbox.
   - **Outlook Web App**: Enables or disables access to the browser-based Outlook Web App for the mailbox user.
   - **MAPI**, **IMAP4**, **POP3**: Enables or disables support for the MAPI, IMAP4 or POP3 protocols for the mailbox user. If MAPI is enabled, the mailbox user can access their mailbox through the Outlook desktop app (or other MAPI clients). If IMAP4 or POP3 is enabled, they are also able to access their mailbox with any IMAP4 or POP3 email client.
   - **Archive**: Enables or disables the archive mailbox feature for the mailbox.
6. Click **Enable** to enable the selected mailbox feature, or **Disable** to disable it.
7. Once you are done with the configuration, click **Close**.
8. To close the **Exchange Online Properties** window, click **Close**.

Configuring the mailbox settings of an Exchange Online mailbox

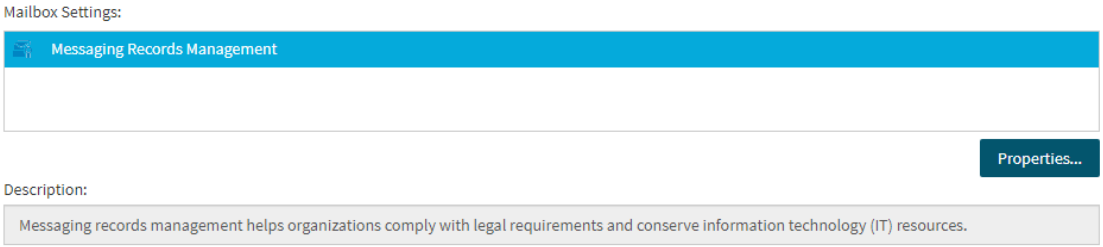
You can configure settings related to Messaging Records Management (MRM) for an Exchange Online mailbox in the **Exchange Online Properties** > **Mailbox Settings** tab of the Active Roles Web Interface. MRM settings are typically configured to meet mailbox archiving policies in effect within the organization.

For more information about MRM in Exchange Online, see Messaging records management in the *Microsoft Exchange Online documentation*.

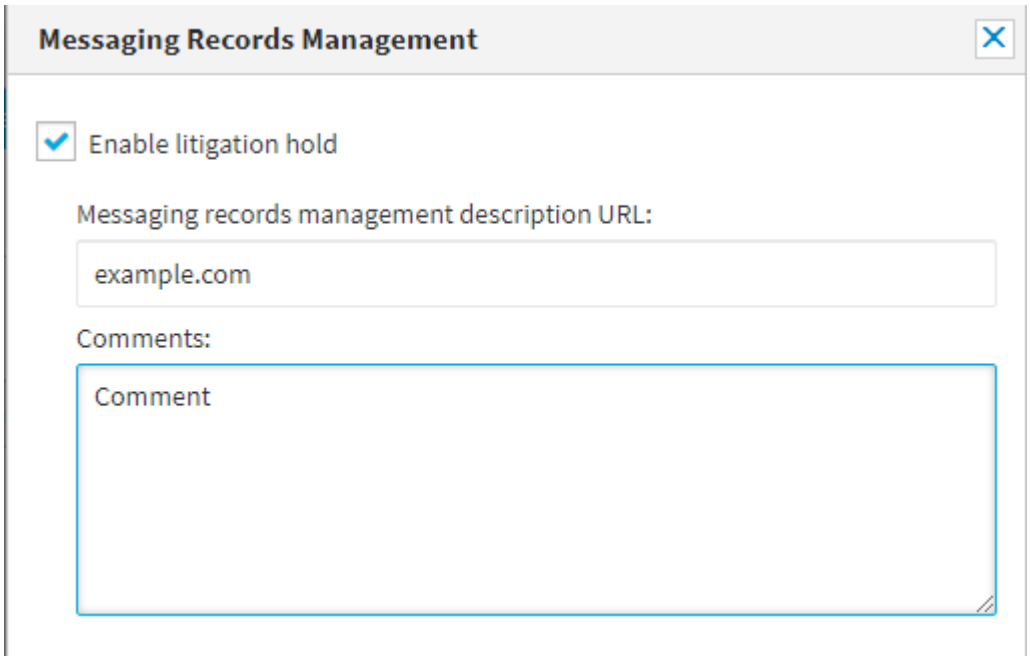
To configure Messaging Records Management settings for an Exchange Online mailbox

1. On the Active Roles Web Interface, navigate to **Directory Management** > **Tree View** > **Azure** > **<azure-tenant>** > **Azure Users** (or **Azure Guest Users**).
2. From the list in the middle pane, select the Azure user or Azure guest user that you want to update.
3. To open the Exchange Online properties of the selected Azure user or guest user, click **Exchange Online Properties** on the right pane.
4. To open the MRM settings, click the **Mailbox Settings** tab.

Figure 53: Exchange Online Properties > Mailbox Settings — Accessing the MRM settings of an Exchange Online mailbox



5. Under **Mailbox Settings**, make sure that **Messaging Records Management** is selected, then click **Properties**. The **Messaging Records Management** dialog opens.



6. To enable placing the entire contents of the user mailbox on hold, enable the **Enable litigation hold** check box. For more information on the Litigation Hold feature of Exchange Online, see the In-Place Hold and Litigation Hold page of the official Microsoft documentation.
7. (Optional) If your organization has an internal resource on the litigation hold practices, specify its URL in the **Messaging records management description URL** text box.
8. (Optional) If you want to display a customized message in Outlook for the mailbox user on the litigation hold, write the message in the **Comments** text box.
9. Click **Save** to apply your changes and close the **Messaging Records Management** dialog.
10. To close the **Exchange Online Properties** window, click **Close**.

Resetting the password of an Azure guest user

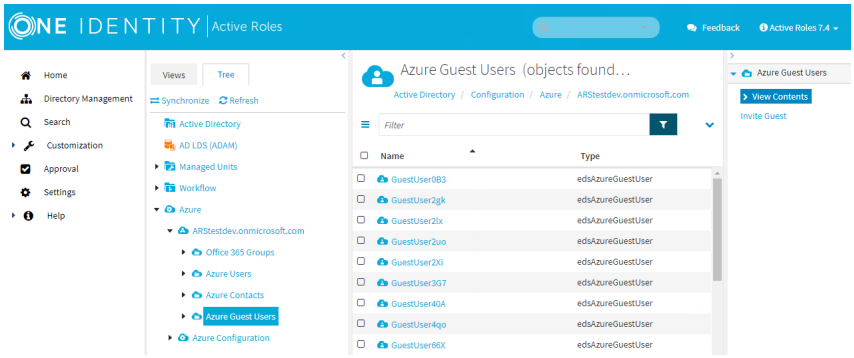
You can reset the password of an existing Azure guest user in the selected Azure tenant with the **Reset Password** option of the Active Roles Web Interface. This is typically performed if the guest user forgot their password.

To reset the password of an Azure guest user

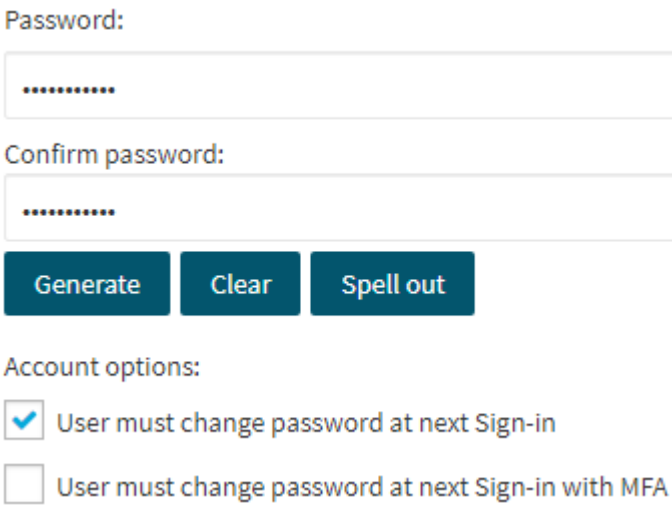
1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

Figure 54: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user whose password you want to reset.
3. Click **Reset Password**.



4. Specify a new password either manually or by generating a new one.
   a. **Configure the Password**

      Under **Password**, specify the new password of the Azure guest user with one of the available methods:

      - **Configure the password manually**

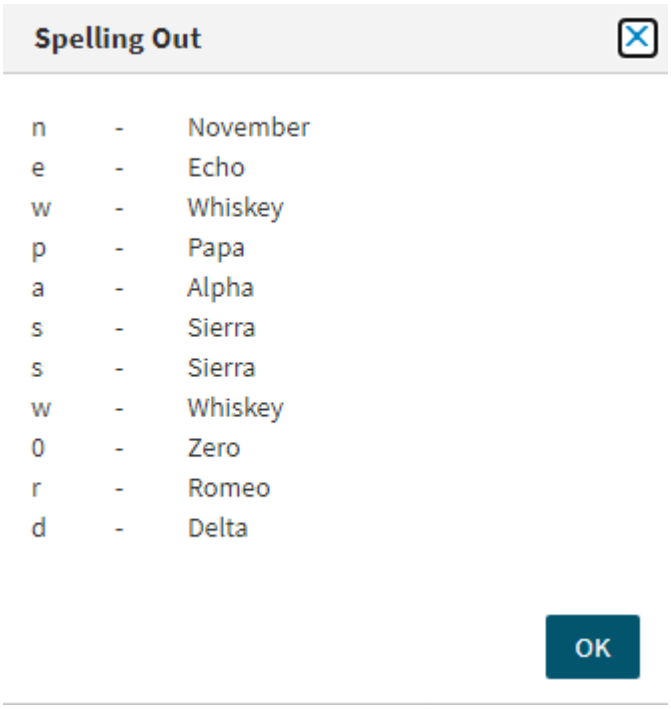
        To specify the new password manually, enter it into the **Password** and **Confirm password** fields.

      - **Generate the password automatically**

        To generate a new password with Active Roles automatically, click **Generate**. The generated password will meet the policy requirements of both your organization and Azure AD.

        To clear the currently specified password, click **Clear**.

To spell out each character of the specified password for clarification, click **Spell out**.



b. **Configure Account Options**

Under **Account options**, configure the password change settings.

- To enforce password change after the first successful login, select **User must change password at next Sign-in**.

5. To apply your changes, click **Finish**.

Deleting an Azure guest user

You can delete an Azure guest user in the selected Azure tenant with the **Delete** option of the Active Roles Web Interface. This is typically performed if the guest user no longer works for the organization.

NOTE: You can only remove certain Azure guest users (for example, Global Administrators) if you have sufficient administrator roles. For more information on these role requirements, see the official Microsoft documentation.

Attempting to delete an Azure guest user without sufficient administrative privileges will result in failure, and the following error log message appearing in the Windows Event Log:

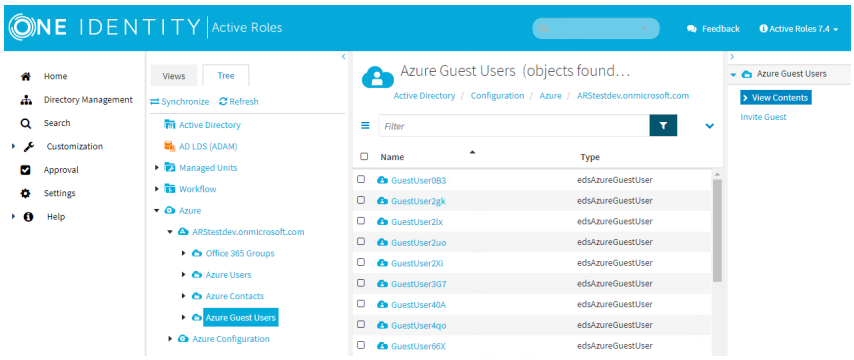
```
Post-processing operation on object caused a policy violation.
```

To delete an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

   Figure 55: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user that you want to delete.
3. Click **Delete**.
4. To confirm the removal of the guest user, click **Yes**.

Configuring the O365 Group membership of an Azure guest user

You can configure and view the Azure group membership(s) of an Azure guest user with the **Azure Member Of** option of the Active Roles Web Interface. Using this option, you can:

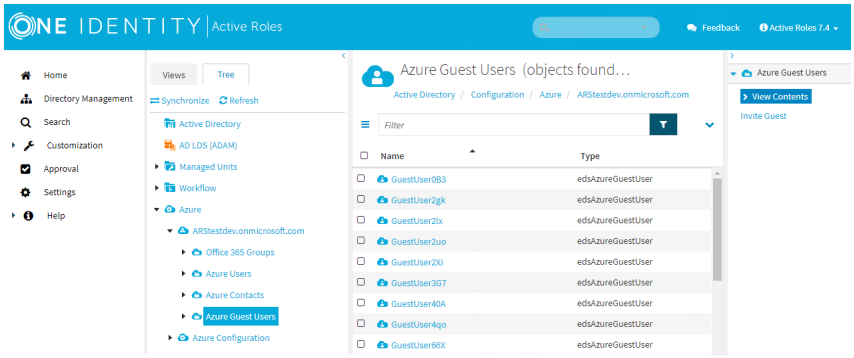
- View the existing O365 group membership(s) of the Azure guest user.
- Add or remove the Azure guest user to or from the selected Azure O365 Group(s).

To add or remove an existing Azure guest user to or from an O365 Group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

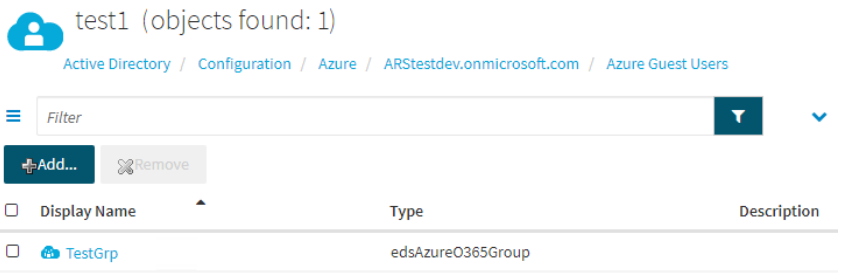
   The list of Azure guest users of the selected tenant is displayed.

Figure 56: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. In the middle pane, select the Azure guest user whose membership you want to view or configure.
3. In the right pane, click **Azure Member Of**. The list of Azure O365 groups where the guest user has a membership then appears.

Figure 57: Directory Management > Tree View > Azure > <azure-tenant> > Azure Guest Users > Azure Member Of – Listing the Azure groups of the selected Azure Guest user



4. To add the Azure guest user to a new Azure O365 group of the Azure tenant, click **Add**.
5. In the **Select Object** page, select the O365 Group(s) you want the Azure guest user to be a member of, then click **OK** to apply your changes and return to the **Azure Member Of** page. The list is then updated with the new groups that you selected previously.
6. To remove the Azure guest user from any O365 Group(s), select the group(s) in the **Azure Member Of** page, and then click **Remove**. Click **OK** to confirm the removal from the group.

Viewing the change history of an Azure guest user

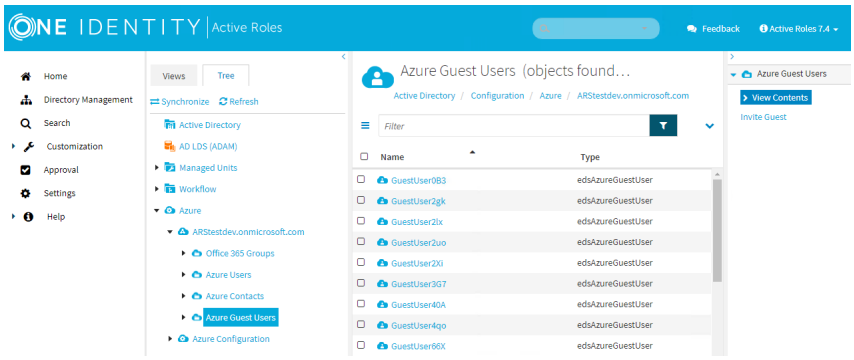
You can view the change history of an Azure guest user in the selected Azure tenant with the **Change History** option of the Active Roles Web Interface.

To view the change history of an Azure guest user

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Azure Guest Users**.

   The list of Azure guest users of the selected tenant is displayed.

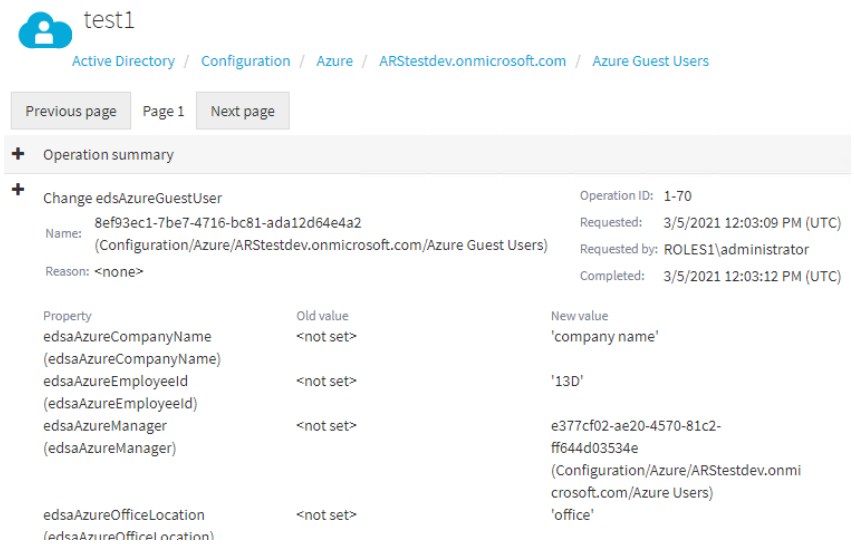
Figure 58: Directory Management > Tree View > Azure > <azure-tenant-name> > Azure Guest Users — Listing the Azure guest users in the tenant



2. Select the Azure guest user whose change history you want to check.
3. Click **Change History**.

   The change history of the Azure guest user then appears.

Figure 59: Directory Management > Tree View > Azure > <azure-tenant> > Azure Guest Users > Change History – Viewing the change history of the selected Azure guest user



Managing cloud-only Azure contacts

Active Roles provides the facility to perform administrative tasks such as create, read, update, and delete Azure contact on cloud through web interface. You can also perform other operations such as viewing and modifying the Azure cloud-only contact, view change history, and other operations related to Azure cloud-only contacts.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

View cloud-only Azure contacts

You can use the Active Roles Web Interface to view the cloud-only Azure contacts.

To view the cloud-only Azure contacts

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Contacts**.

   The **Azure Contacts** page is displayed and lists the Azure cloud-only contacts available in Azure.

   NOTE: Active Roles lists the available cloud-only Azure users, Azure guest users, and Azure contacts on the Active Roles Web Interface with the following restrictions:

   - Active Roles can initially list 999 items.
   - The items listed in the list have a sliding expiry of 8 hours, after which the objects that have not been accessed will be flushed.
   - Whenever you perform a search in the list, Active Roles will always fetch the list of objects from Azure to update the cache.

Create new cloud-only Azure contacts

You can use the Active Roles Web Interface to create and enable new cloud-only Azure contacts.

To create a new cloud-only Azure contact

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Contacts**.

The **Azure Contacts** page is displayed and lists the Azure cloud-only contacts available in Azure.

3. In the **Command** pane, under **Azure Contacts**, click **New Contact**.
4. In the **New Contact** window, on the **General** tab, enter the appropriate text in the **Name**, **Alias**, and **Description** fields.
5. Click **Finish**.

   The **Azure Contacts** page displays the newly added Azure contact.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

View or modify Azure contacts properties

For an existing Azure cloud-only contact, you can use the Active Roles Web Interface to view or modify the properties.

To view or modify the Azure contacts properties

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Users**.

   The **Azure Users** page is displayed and lists the Azure users that are available in Azure.
3. Select the Azure contact for which you want to view or modify the properties.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** wizard for the contact is displayed.
5. To view or modify properties of the Azure cloud-only contact, use the tabs in the **Azure Properties** wizard.
6. After setting all the required properties, click **Save**.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

Renaming Azure cloud contacts

You can use the Active Roles Web Interface to rename an Azure cloud contacts.

To rename an Azure cloud contacts account

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Contacts**.

   The **Azure Contacts** page is displayed and lists the Azure cloud-only contacts available in Azure.
3. Select the Azure contact that you want to rename.
4. In the **Command** pane, click **Rename**.
5. Enter the required name.
6. Click **Yes** to continue.

   The Azure cloud contacts that you have selected are renamed.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

Viewing and modifying Exchange Online properties

You can use the Active Roles Web Interface to create and view and modify the Exchange Online properties of the new cloud-only Azure Contacts.

To view the Exchange Online properties of a cloud-only Azure Contacts

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Contacts**.

   The **Azure Contacts** page is displayed and lists the Azure cloud-only contacts available in Azure.
3. Select the specific cloud-only Azure contacts for which you want to view the properties.
4. In the **Command** pane, click **Exchange Online Properties**.

   The **Exchange Online Properties** wizard displays the following Exchange Online properties for the cloud-only Azure contact.

   - General
   - Mail tip
5. Use the tabs in the **Exchange Online Properties** dialog to view the following Exchange Online properties of the cloud-only Azure contact:

- **General**

  In the **Alias** field, enter an Exchange Online alias name. You can also choose to hide the alias name from the organizational address list.

- **Mail tip**

  In the **Mail tip text** field, enter an optional mail tip.

NOTE: When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.

Viewing the change history of cloud-only Azure contacts

You can use the Active Roles Web Interface to view the change history and user activity for cloud only Azure contacts.

To view the change history and user activity of cloud only Azure contacts

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Active Directory**.

   The list of Active Directory domains is displayed.
3. To view the history, select the Azure contact.
4. In the **Command** pane, click **Change History** or **User Activity**.

   The information on changes that were made to the contact through Active Roles is displayed.

Deleting an Azure contact

You can use the Active Roles Web Interface to delete an Azure contact.

To delete an Azure contact

1. On the Active Roles Web Interface navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure** > **<Azure tenant>** > **Azure Contacts**.

   The **Azure Contacts** page is displayed and lists the Azure cloud-only contacts available in Azure.
3. Select the Azure contact that you want to delete.
4. In the **Command** pane, click **Delete**.

   A message prompts you to confirm the action.

5. Click **Yes** to continue.

   The Azure contacts that you have selected are deleted.

Viewing or modifying the Exchange Online properties of a remote mailbox

When creating a remote mailbox for an on-premises user, Active Roles creates an Azure user entry for the mailbox in the Azure tenant where the remote mailbox is stored. The Azure user entry of the remote mailbox is listed in the **Azure** > **<azure-tenant-name>** > **Azure Users** node of the Active Roles Web Interface, and its name takes the value of the `Name` attribute of the remote mailbox.

You can view or modify the Exchange Online settings of the remote mailbox with the **Exchange Online Properties** action of the Azure user entry of the remote mailbox in the Active Roles Web Interface. Changing these properties is typically required if the user mailbox is affected by an IT infrastructural or organizational change, or the personal information of the user has changed.

NOTE: Although the on-premises user also has an **Exchange Properties** action when selecting it in the Active Roles Web Interface, you cannot use that action to modify the settings of the remote mailbox assigned to the on-premises user.

To modify the Exchange Online settings of a remote mailbox assigned to an on-premises user, always use the **Exchange Online Properties** of the Azure user entry of the remote mailbox instead.

To view or modify the Exchange Online properties of a remote mailbox

1. In the Active Roles Web Interface, under **Directory Management** > **Tree** > **Active Directory**, navigate to **Azure** > **<azure-tenant-name>** > **Azure Users**.

   NOTE: **<azure-tenant-name>** is the Azure tenant storing the remote mailbox.
2. Select the Azure user entry of the remote mailbox you want to view or modify, then click **Exchange Online Properties**.
3. In the available **Exchange Online Properties** tabs, configure the Exchange Online mailbox settings as you need.

Table 4: Available Exchange Online properties

Page	Description
Mail Flow Settings	View and configure rules for the emails that the mailbox sends or receives via the Exchange Online service.
Delegation	Configure the email account as a shared mailbox.
General	View and configure the email addresses associated with the

Page	Description
	mailbox.
Mailbox Features	View and configure various Exchange Online mailbox features, for example mobile access, additional mailbox protocols, or archival settings.
Mailbox Settings	View and configure Messaging Records Management (MRM) settings for the mailbox.

4. To apply your changes, click **Save**.

Managing room mailboxes

Room mailbox is a type of Exchange Online resource mailbox assigned to a physical location, such as a meeting room. Using room mailboxes that an administrator creates, users can reserve rooms by adding room mailboxes to meeting requests as an attendee or location.

In the Active Roles Web Interface, you can create, manage or delete room mailboxes in **Directory Management** > **Tree**> **Azure** > **Resource Mailboxes**. Room mailboxes created in the Active Roles Web Interface are synchronized to the Exchange admin center (admin.exchange.microsoft.com), where you can find them in **Home** > **Resources**.

For more information about room mailboxes, see Manage resource mailboxes in Exchange Online in the *Microsoft Exchange Online documentation*.

Creating a new room mailbox

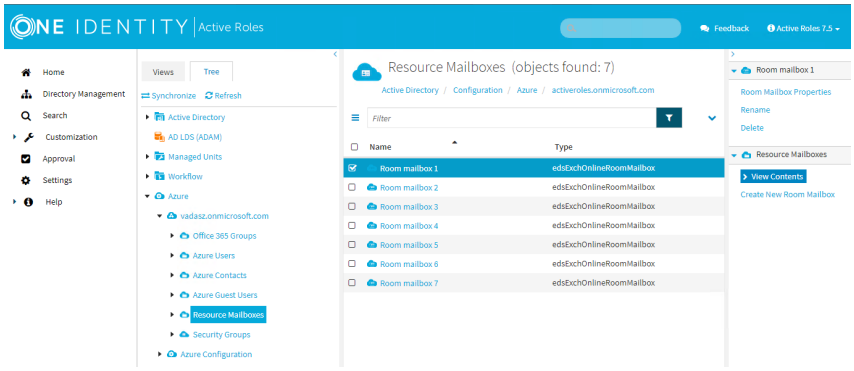
To create a new room mailbox in the Active Roles Web Interface, follow the steps.

To create a new room mailbox

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree**> **Azure** > **Resource Mailboxes**.

   The list of resource mailboxes of the selected tenant is displayed.

Figure 60: Directory Management > Tree View > Azure > Resource Mailboxes — Listing the resource mailboxes in the tenant



2. In the right pane, click **Create New Room Mailbox.**

   The **Create New Room Mailbox** window opens.

3. On the **General** tab, set the following general details of the room:

   - (Optional) **Display name**
   - **Name**: Enter a name for the room.

     NOTE: If you enter a name that is already used, you will receive an error message and Exchange Online will not allow you creating the new room mailbox. To create a new room mailbox, enter a different name.

     NOTE: To change the name of an existing room mailbox:

     1. In the right pane, click **Rename**.
     2. **Display name**: Enter a new display name for the room.
     3. **Name**: Enter a new name for the room.
     4. Click **Finish**.

   - (Optional) **Primary SMTP Address (leave blank for default value)**

     To specify the domain, use the drop-down.

     The default value of the Primary SMTP Address is the name and the domain name of the room mailbox. For example, `roommailbox1@activeroles.onmicrosoft.com`, where `roommailbox1` is the name and `activeroles.onmicrosoft.com` is the domain name.

   - (Optional) **Capacity**
   - (Optional) **Hide from global address lists**

     Select this check box if you do not want the room mailbox to appear in the address book and other address lists defined in your Exchange organization.

     By default, this check box is not selected.

4. (Optional) On the **Calendar Processing** tab, set the following optional details of the room:

- **Maximum duration (hours)**
- **Booking window (days)**
- **Allow repeating meetings**

  By default, this check box is selected.
- **Allow scheduling only during work hours**

  By default, this check box is selected.

5. (Optional) On the **Location** tab, set the following optional details of the company:
   - **Department**
   - **Company Name**
   - **Street Address**
   - **City**
   - **State or Province**
   - **Zip or Postal Code**
   - **Country**: You must enter a valid country code or country name, for example: `US` or `United States of America (the)`.
6. Click **Finish**.

If the operation is successful, the newly-created room mailbox appears in the list of **Resource Mailboxes**.

The newly-created room mailbox also appears in the Exchange admin center, in **Home** > **Resources**.

Viewing or modifying a room mailbox

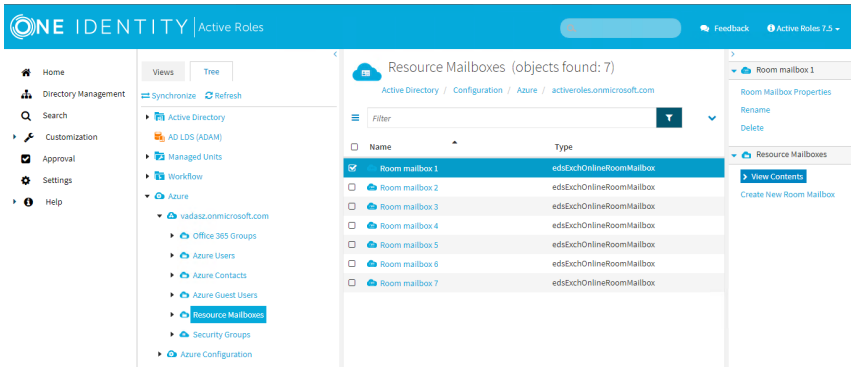
To view or modify the properties of a room mailbox in the Active Roles Web Interface, follow the steps.

To view or modify the properties of a room mailbox

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree**> **Azure** > **Resource Mailboxes**.

   The list of resource mailboxes of the selected tenant is displayed.

Figure 61: Directory Management > Tree View > Azure > Resource Mailboxes — Listing the resource mailboxes in the tenant



2. Select the room mailbox you want to view or modify.

   In the right pane, the name of the room mailbox appears with the following available actions:

   - **Room Mailbox Properties**
   - **Rename**
   - **Delete**

3. In the right pane, click **Room Mailbox Properties**.

   The **Room Mailbox Properties** window opens.

4. On the **General** tab, view or modify the following general details of the room:

   - **Display name**

     NOTE: To change the name of an existing room mailbox:

     1. In the right pane, click **Rename**.
     2. **Display name**: Enter a new display name for the room.
     3. **Name**: Enter a new name for the room.
     4. Click **Finish**.

   - **Object GUID**: The Exchange Online GUID of the mailbox object in the Exchange Cloud. By default, this check box is not selected.
   - **External directory ID**: The Azure Active Directory (Azure AD) object of the user object connected to the mailbox object in Azure AD. You cannot modify this value because it is filled automatically.
   - **User Principal Name**: The room mailbox address in User Principal Name (UPN) format. By default, this check box is not selected.
   - **Primary SMTP Address**: By default, this check box is not selected.
   - **Capacity**
   - **Hide from global address lists**

Select this check box if you do not want the room mailbox to appear in the address book and other address lists defined in your Exchange organization.

By default, this check box is not selected.

5. On the **Calendar Processing** tab, view or modify the following optional details of the room:
   - **Maximum duration (hours)**
   - **Booking window (days)**
   - **Allow repeating meetings**

     By default, this check box is selected.
   - **Allow scheduling only during work hours**

     By default, this check box is selected.
6. On the **Location** tab, view or modify the following optional details of the company:
   - **Department**
   - **Company Name**
   - **Street Address**
   - **City**
   - **State or Province**
   - **Zip or Postal Code**
   - **Country**: You must enter a valid country code or country name, for example: `US` or `United States of America (the)`.
7. To close the **Room Mailbox Properties** window:
   a. To update the properties of the room mailbox, click **Save**.
   b. To close the window without saving the changes, click **Cancel**.

Deleting a room mailbox

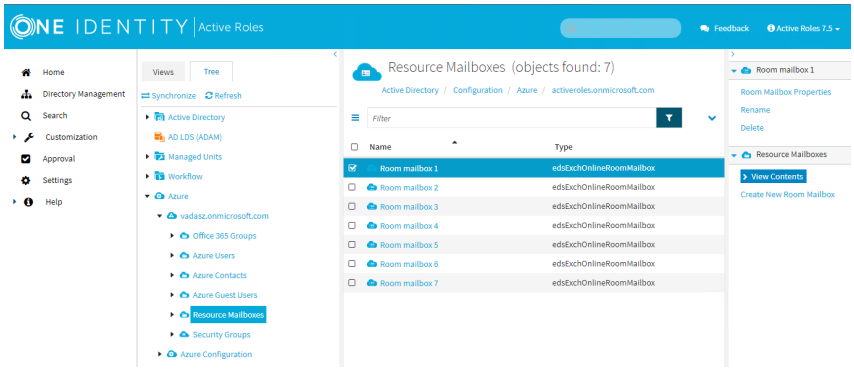
To delete a room mailbox in the Active Roles Web Interface, follow the steps.

To delete a room mailbox

1. In the Active Roles Web Interface, navigate to **Directory Management** > **Tree**> **Azure** > **Resource Mailboxes**.

   The list of resource mailboxes of the selected tenant is displayed.

Figure 62: Directory Management > Tree View > Azure > Resource Mailboxes — Listing the resource mailboxes in the tenant



2. Select the room mailbox that you want to delete.

   In the right pane, the name of the room mailbox appears with the following available actions:

   - **Room Mailbox Properties**
   - **Rename**
   - **Delete**

3. Click **Delete**.

   The following dialog appears:

   ```
   Are you sure you want to delete <room mailbox>?
   ```

4. Click **Yes**.

If the operation has been successful, the room mailbox is deleted and it disappears both from the **Resource Mailboxes** list in the Active Roles Web Interface, and from the **Resources** list in the Exchange admin center.

Managing cloud-only shared mailboxes

A cloud-only shared mailbox is a type of user mailbox in Exchange Online that you can use when multiple people need access to the same mailbox to read and send messages. In an organization, functions such as technical support or company information use shared mailboxes with a generic email address, for example, **`info@company.com`**. After you create a shared mailbox, you must assign permissions to all users that you want to have access to the shared mailbox.

In the Active Roles Web Interface, you can create, manage or delete cloud-only shared mailboxes in **Directory Management** > **Tree**> **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**. Shared mailboxes created in the Active Roles Web Interface are synchronized to the Exchange admin center, where you can find them in **Teams & Groups** > **Shared mailboxes**.

For more information about shared mailboxes, see Shared mailboxes in the *Microsoft 365 documentation*.

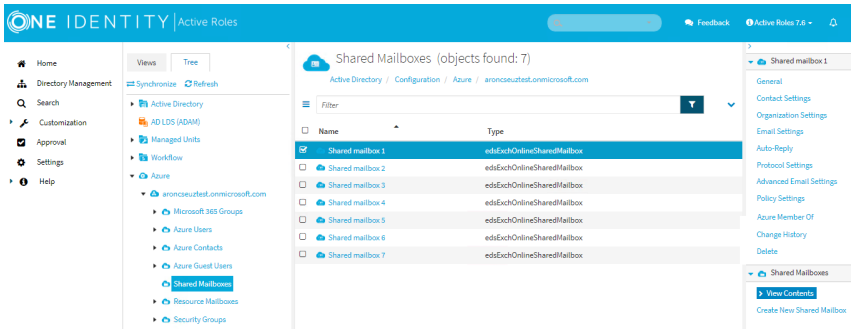
Creating a new shared mailbox

You can create a new shared mailbox with the **Create New Shared Mailbox** option of the Active Roles Web Interface.

To create a new shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

   Figure 63: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant

2. Click **Create New Shared Mailbox**.
3. In **General**, configure the settings your organization requires for setting up the shared mailbox.
   - Enter the **Display name** of the shared mailbox.
   - Enter the **Name** of the shared mailbox.
   - **Primary SMTP Address (leave blank for default value)**: Enter the name and select a domain.

     The default value of the primary SMTP address is the name and the domain name of the mailbox. For example, `mailbox1@activeroles.onmicrosoft.com`, where `mailbox1` is the name and `activeroles.onmicrosoft.com` is the domain name.
   - (Optional) Enter an Exchange Online **Alias** for the shared mailbox.
4. To apply your changes, click **Finish**.

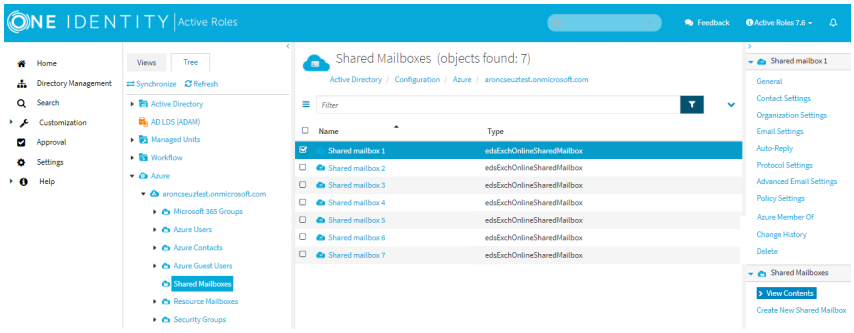
Viewing or modifying the general properties of a shared mailbox

You can view or modify the general properties of a shared mailbox with the **General** option of the Active Roles Web Interface.

To view or modify the general properties of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

   Figure 64: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant

2. Select the shared mailbox whose general properties you want to view or modify.
3. In **General**, set the following general properties of the shared mailbox:
   - Enter the **Display name** of the shared mailbox.
   - Enter the **Name** of the shared mailbox.
   - **Primary SMTP address**: The primary Simple Mail Transfer Protocol (SMTP) address of a user account to be used for server-to-server authorization or access delegation. You cannot modify this value because it is filled automatically.
   - **External directory ID**: The Azure Active Directory (Azure AD) object of the user object connected to the mailbox object in Azure AD. You cannot modify this value because it is filled automatically.
   - (Optional) Enter an Exchange Online **Alias** for the shared mailbox.
   - (Optional) **Hide from global address lists** (default: selected)

     Select this check box if you do not want the mailbox to appear in the address book and other address lists defined in your Exchange organization.
4. To apply your changes, click **Save**.

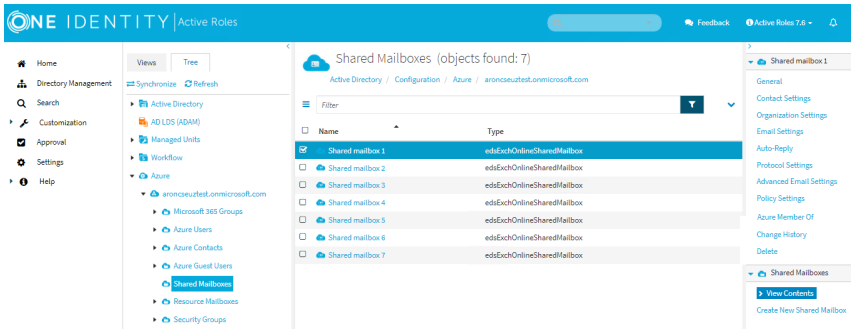
Viewing or modifying the contact settings of a shared mailbox

You can view or modify the contact settings of a shared mailbox with the **Contact Settings** option of the Active Roles Web Interface.

To view or modify the contact settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

   Figure 65: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant

2. Select the shared mailbox whose contact settings you want to view or modify.
3. Click **Contact Settings**.
4. In **Contact Settings**, set the following contact settings of the shared mailbox:
   - (Optional) **Office**
   - (Optional) **Office phone**
   - (Optional) **Mobile phone**
   - (Optional) **Home phone**
   - (Optional) **Fax number**
   - (Optional) **Street address**
   - (Optional) **City**
   - (Optional) **Country**: You must enter a valid country code or country name, for example: `US` or `United States of America (the)`.
   - (Optional) **State or province**
   - (Optional) **ZIP or postal code**
   - (Optional) **Notes**: Enter a customized message about the contact settings of the shared mailbox for users that will appear in Outlook.
5. To apply your changes, click **Save**.

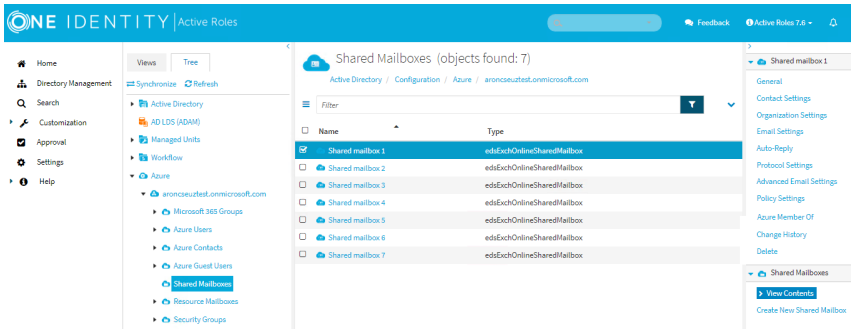
Viewing or modifying the organization settings of a shared mailbox

You can view or modify the organization settings of a shared mailbox with the **Organization Settings** option of the Active Roles Web Interface.

To view or modify the organization settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

   Figure 66: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant

2. Select the shared mailbox whose organization settings you want to view or modify.
3. In **Organization Settings**, set the following organization settings of the shared mailbox:
   - (Optional) **Job title**
   - (Optional) **Department**
   - (Optional) **Company name**
   - (Optional) **Manager**:
     - To add or change the manager of the shared mailbox, click **Modify**, select the user and click **OK**.
     - To view or modify the Azure properties of the user, click **Properties**.
     - To delete the manager of the shared mailbox, click **Remove**.
4. To apply your changes, click **Save**.

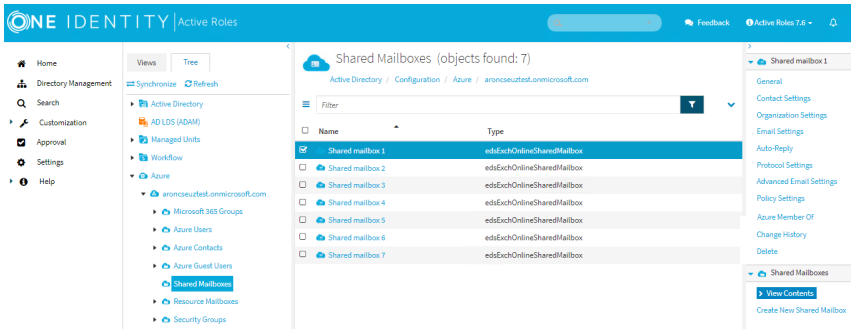
Viewing or modifying the email settings of a shared mailbox

You can view or modify the email settings of a shared mailbox with the **Email Settings** option of the Active Roles Web Interface.

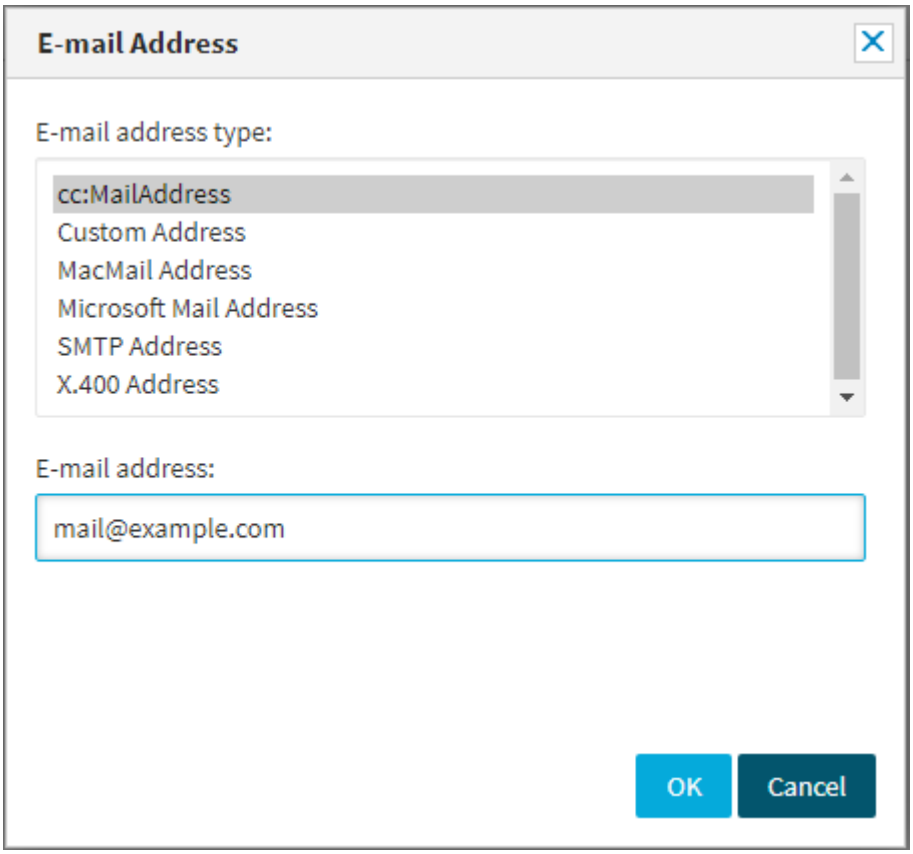
To view or modify the email settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 67: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose email settings you want to view or modify.
3. In **Email Settings**, set the following email settings of the shared mailbox:
    - **Primary SMTP address**: The primary Simple Mail Transfer Protocol (SMTP) address of a user account to be used for server-to-server authorization or access delegation. You cannot modify this value because it is filled automatically.
    - **Email addresses**:



  - To add additional email addresses (also called proxy addresses) for the shared mailbox, click **Add**, select the **E-mail address type**, enter the **E-mail address**, and click **OK**.

    NOTE: The first SMTP address that you add will be the primary SMTP address (also called the primary email address or the default reply address).

  - To modify an email address that is already added to the list of email addresses, select it and click **Edit**, modify the **E-mail address**, and click **OK**.
    NOTE: You cannot modify the **E-mail address type** of an existing email account. You can only modify the existing address.

  - To remove an email address that is already added to the list email addresses, select it and click **Remove**.

- **Accept messages from all senders** (default: selected)
  - To only accept messages from selected senders, clear the check box and click **Add**. Select the users you want to accept messages from, and click **OK**.
  - To remove senders from the list of users you want to accept messages from, select the users and click **Remove**.
- **Block messages from none** (default: selected)

- To block messages from selected senders, clear the check box and click **Add**. Select the users you do not want to accept messages from, and click **OK**.
- To remove senders from the list of users you do not want to accept messages from, select the users and click **Remove**.

- **Send message maximum size (0-150 000 KB)**: Set the maximum size of messages in KB. The default value is **35840** KB.
- **Received message maximum size (0-150 000 KB)**: Set the maximum size of received messages in KB. The default value is **36864** KB.
- **Maximum recipients (0-1000)**: Set the maximum number of recipients. The default value is **500**.
- **Forwarding address**: Specify whether to forward received messages from the shared mailbox to another email address.
  - To disable message forwarding, select **None** (default: selected).
  - To enable message forwarding, select **Forward to**, and enter the email address you want the shared mailbox to forward received messages to.
  - To modify the forwarding address, click **Modify**.
- **Deliver messages to both forwarding address and mailbox** (default: not selected)

  To forward messages that the shared mailbox receives to the forwarding address you set, select this check box.

4. To apply your changes, click **Save**.

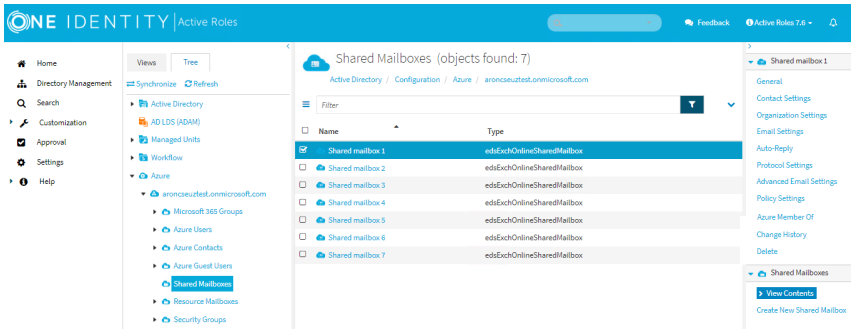
Viewing or modifying the auto-reply settings of a shared mailbox

You can view or modify the automatic reply (out of office) settings of a shared mailbox with the **Auto-Reply** option of the Active Roles Web Interface.

To view or modify the auto-reply settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 68: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose automatic reply settings you want to view or modify.
3. In **Auto-Reply**, set the following automatic reply settings of the shared mailbox:
   - **Automatic replies** (default: not selected)

     To send an automatic reply to all senders inside your organization from the shared mailbox, select this check box and enter an automatic reply.
   - **Send automatic replies to senders outside this organization** (default: not selected)

     To send an automatic reply to all senders outside of your organization from the shared mailbox, select this check box and enter an automatic reply.

     To specify the senders outside of your organization, you can set one of the following:
     - **Only reply to senders in this mailbox's contact list**
     - **Reply to all senders**
4. To apply your changes, click **Save**.

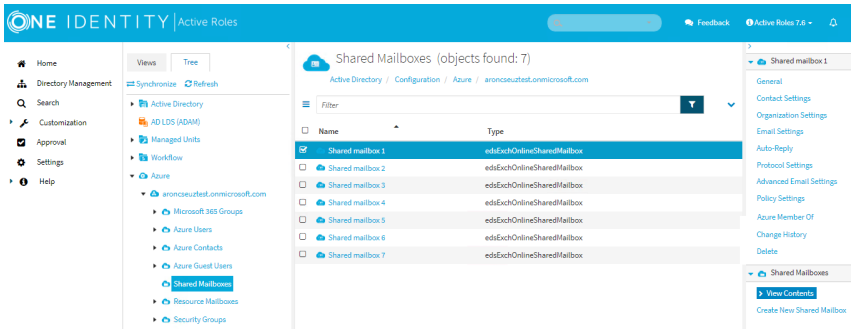
Viewing or modifying the protocol settings of a shared mailbox

You can view or modify the protocol settings of a shared mailbox with the **Protocol Settings** option of the Active Roles Web Interface.

To view or modify protocol settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 69: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose protocol settings you want to view or modify.
3. In **Protocol Settings**, set the following protocol settings of the shared mailbox:
    - **Outlook Web** (default: selected)
    - **Outlook Desktop** (default: selected)
    - **Exchange Web Services** (default: selected)
    - **Mobile Exchange** (default: selected)
    - **IMAP** (default: selected)
    - **POP3** (default: selected)
4. To apply your changes, click **Finish**.

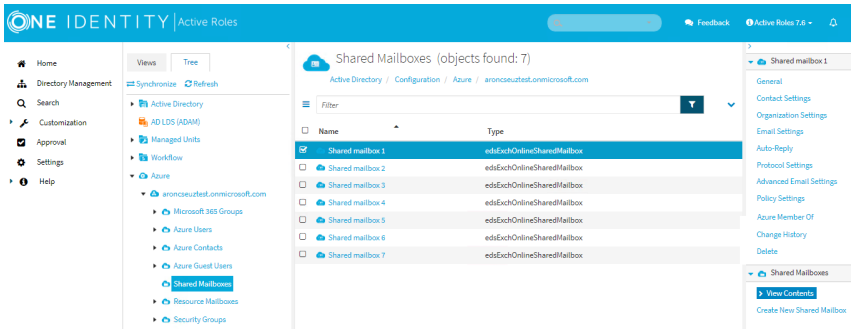
Viewing or modifying the advanced email settings of a shared mailbox

You can view or modify the advanced email settings of a shared mailbox with the **Advanced Email Settings** option of the Active Roles Web Interface.

To view or modify the advanced email settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 70: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose advanced email settings you want to view or modify.
3. Click **Advanced Email Settings**.
4. In **Advanced Email Settings**, set the following advanced email settings of the shared mailbox:
    - **Send as**

      Only the users in the **Send as** list have permission to send emails from this shared mailbox that will appear as emails sent by the owner of the mailbox.
        - To add users to the **Send as** list, click **Add**, select the users and click **OK**.
        - To remove users from the **Send as** list, select the users and click **Remove**.
    - **Read and manage (Full control)**

      Only the users in the **Read and manage** list have full administrator access to the shared mailbox.
        - To add users to the **Read and manage** list, click **Add**, select the users and click **OK**.
        - To remove users from the **Read and manage** list, select the users and click **Remove**.
    - **Mailbox archive** (default: selected)
    - **Convert mailbox from shared to regular** (default: not selected)

      NOTE: After you convert a mailbox from shared to regular, you can only convert it back to shared in the Exchange admin center.
    - **Litigation hold** (default: not selected)

      Litigation hold places all contents of the shared mailbox on hold. For more information on litigation hold, see *In-Place Hold and Litigation Hold* in the *Microsoft Exchange Online documentation*.

NOTE: To place an Exchange Online mailbox on litigation hold, it must be assigned an Exchange Online Plan 2 license.

- **Date hold created**: You cannot modify this value because it is filled automatically.
- **Hold started by**: You cannot modify this value because it is filled automatically.
- (Optional) **Hold duration (days). Leave blank for no limit**: Enter the number of days. For example: **`180`**.
- (Optional) **Note (visible to the user)**: Enter a customized message for users about the litigation hold that will appear in Outlook.
- (Optional) **Web page with more information for the user**: If your organization has an internal website about litigation hold practices, enter its URL.

5. To apply your changes, click **Save**.

Viewing or modifying the policy settings of a shared mailbox

You can view or modify the policies available in your Azure Active Directory (Azure AD) environment for a shared mailbox with the **Policy Settings** option of the Active Roles Web Interface.

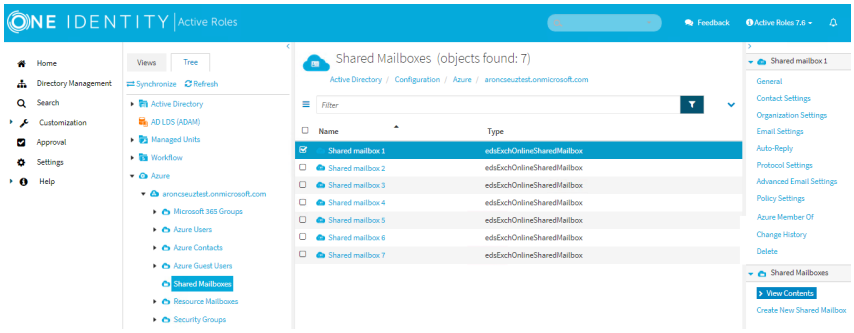
Prerequisites

NOTE: To modify the default policy settings, you must run PowerShell command **`Enable-OrganizationCustomization`** for the Azure tenant of the shared mailbox. It can take up to 10-15 minutes for the command to take effect before you can save the policy changes.

To view or modify policy settings of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 71: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose policy settings you want to view or modify.
3. In **Policy Settings**, select the following policies available in your Azure AD environment for the shared mailbox:
    - **Sharing policy**: Sets how users can share information with other users in your organization.
    - **Role assignment policy**: Sets the permissions assigned to the users of the shared mailbox.
    - **Retention policy**: Sets the time period in which users can manage email in the shared mailbox.
    - **Address book policy**: Sets the default address book in your organization.
4. To apply your changes, click **Save**.

Configuring the distribution group membership of a shared mailbox

You can configure and view the Azure group membership(s) of a shared mailbox with the **Azure Member Of** option of the Active Roles Web Interface. You can:

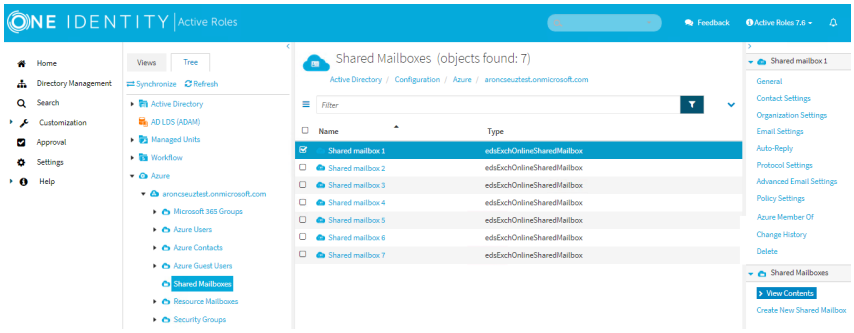
- View the existing distribution group membership(s) of the shared mailbox.
- Add or remove the shared mailbox to or from the selected Azure distribution group(s).

NOTE: In the Active Roles Web Interface, you can add shared mailboxes to Azure distribution groups only, but you cannot add them to Azure O365 groups or Azure security groups. You can add a shared mailbox to an Azure O365 group or Azure security group in the Microsoft 365 admin center.

To add or remove an existing shared mailbox to or from a distribution group

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 72: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose membership you want to view or configure.
3. Click **Azure Member Of**. The list of Azure distribution groups where the shared mailbox has a membership appears.
4. To add the shared mailbox to a new Azure distribution group of the Azure tenant, click **Add**.
5. Select the distribution group(s) you want the shared mailbox to be a member of, and click **OK**.
6. To remove the shared mailbox from any distribution group(s), in **Azure Member Of**, select the group(s), click **Remove**, and click **OK**.

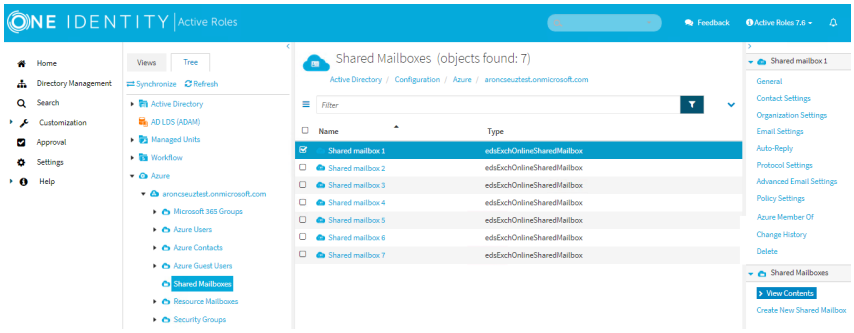
Viewing the change history of a shared mailbox

You can view the change history of a shared mailbox in the selected Azure tenant with the **Change History** option of the Active Roles Web Interface.

To view the change history of a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 73: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox whose change history you want to view.
3. Click **Change History**.

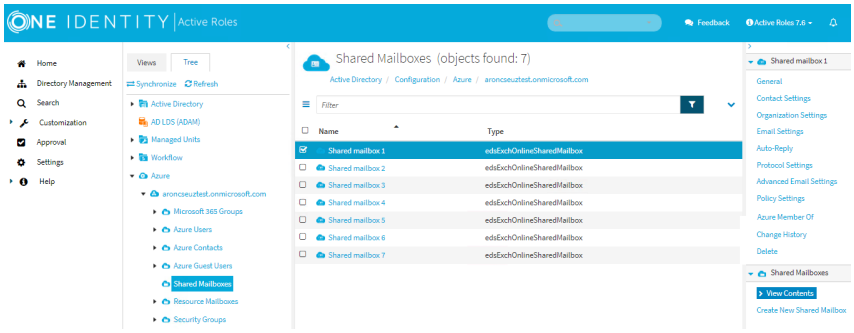
Deleting a shared mailbox

You can delete a shared mailbox in the selected Azure tenant with the **Delete** option of the Active Roles Web Interface.

To delete a shared mailbox

1. Navigate to **Directory Management** > **Tree** > **Azure** > **<azure-tenant-name>** > **Shared Mailboxes**.

Figure 74: Shared Mailboxes — Listing the shared mailboxes in the Azure tenant



2. Select the shared mailbox that you want to delete.
3. Click **Delete**.
4. To confirm, click **Yes**.

Deleting or changing the remote mailbox of an on-premises user

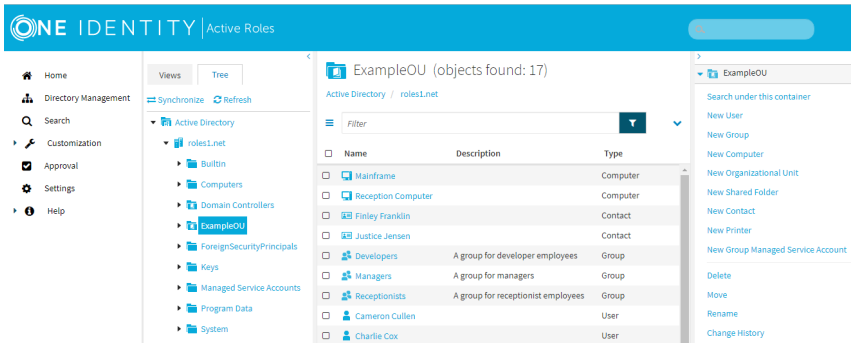
You can remove the remote mailbox (that is, the assigned Exchange Online mailbox) of an on-premises user with the Active Roles Web Interface and the Active Roles Console.

Deleting the remote mailbox of a user is typically required in case of an organizational or infrastructural change, but is also a mandatory prerequisite if you want to change the current remote mailbox of the user.

To delete the remote mailbox of an on-premises user

1. In the Active Roles Web Interface, under **Directory Management** > **Tree** > **Active Directory**, navigate to the OU of the on-premises user whose remote mailbox you want to delete.

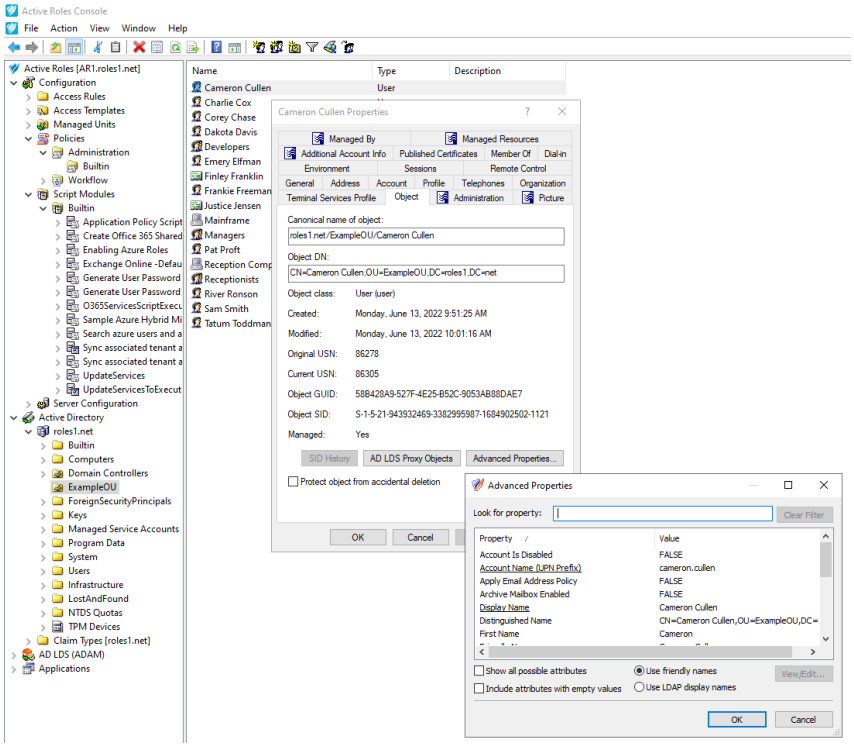
   Figure 75: Active Roles Web Interface – Navigating to the OU of the user

2. Select the user and click **Delete E-mail Addresses**.
3. To confirm the deletion of the email address, click **OK**.

   After clicking **OK**, Active Roles deletes the remote mailbox of the on-premises user. However, this change does not reset the value of the **edsvaMsExchEnableRemoteMailRoutingAddress** property of the user. While this does not cause any operational issues, Active Roles recommends updating this value manually for consistency as described in the next step.
4. (Optional) Open the **Advanced Properties** of the on-premises user. In the Active Roles Console, in the Active Directory (AD) tree, navigate to the Organizational Unit (OU) where the user is located, double-click the user, then in the **Properties** window, click **Object** > **Advanced Properties**.

Figure 76: Active Roles Console– Opening the Advanced Properties of a user



5. Search for the **edsvaMsExchEnableRemoteMailRoutingAddress** property.

   TIP: To find the property faster, enter its name (or part of its name) in the **Look for property** field. If you cannot find the property, select **Show all possible attributes** and **Include attributes with empty values**, too.

   After you found the property, open its settings by double-clicking it.

6. In the **Edit Attribute** dialog, in **Value**, delete the configured remote mailbox.
7. To apply your changes, click **OK** in each open window.

To change the remote mailbox of an on-premises user

1. In the Active Roles Web Interface, delete the current remote mailbox of the on-premises user as described in the To delete the remote mailbox of an on-premises user procedure.
2. Open the **Advanced Properties** of the on-premises user. In the Active Roles Console, in the Active Directory (AD) tree, navigate to the Organizational Unit (OU) where the user is located, double-click the user, then in the **Properties** window, click **Object** > **Advanced Properties**.
3. Search for the **edsvaMsExchEnableRemoteMailRoutingAddress** property.

   TIP: To find the property faster, enter its name (or part of its name) in the **Look for property** field. If you cannot find the property, select **Show all possible**

attributes and **Include attributes with empty values**, too.

After you found the property, open its settings by double-clicking it.

4. In the **Edit Attribute** dialog, in **Value**, specify the new remote mailbox for the user.
5. To apply your changes, click **OK** in each open window.

Managing AD LDS data

You can use the Web Interface to manage directory data in Microsoft Active Directory Lightweight Directory Services (AD LDS). Similarly to Active Directory domains, directory data can be managed in only the AD LDS instances that are registered with Active Roles (that is, in managed AD LDS instances).

The application directory partitions found on the managed AD LDS instances are grouped together in the **AD LDS (ADAM)** container, thus making it easy to locate the AD LDS data. Each directory partition is represented by a separate container (node) so you can browse the partition tree the same way you do for an Active Directory domain.

The Web Interface supports a wide range of administration operations on AD LDS users, groups and other objects, so you can create, view, modify, and delete directory objects, such as users, groups, containers and Organizational Units in AD LDS the same way you do when managing data in Active Directory.

To browse the directory tree in AD LDS directory partitions

1. On the Navigation bar, click **Directory Management**.
2. In the Browse pane, click the **Tree** tab.
3. On the **Tree** tab, do the following:
    a. Expand the **AD LDS (ADAM)** container.
    b. Under **AD LDS (ADAM)**, expand a directory partition object to view its top-level containers.
    c. Expand a top-level container to view the next level of objects in that container.
4. Do one of the following:
    - To move down a directory tree branch, continue expanding the next lowest container level on the **Tree** tab.
    - To administer a directory object at the current directory level, click a container on the **Tree** tab and perform the following instructions.

To manage directory data in AD LDS

On the **Tree** tab in the Browse pane, under **AD LDS (ADAM)**, click the container that holds the data you want to manage.

1. In the list of objects, select the object that represents the directory data you want to manage.
2. Use commands in the Command pane to perform management tasks.

NOTE: In the list of objects, clicking the name of a leaf object, such as a user or group will display the properties page of the object. Clicking a container object, such as a partition or an organizational unit, will display a list of objects held in that container.

Managing computer resources

You can use the Web Interface to manage the following computer resources:

- **Services**: Start or stop a service, view or modify properties of a service.
- **Network file shares**: Create a file share, view or modify properties of a file share, stop sharing a folder.
- **Logical printers**: Pause, resume or cancel printing, list documents being printed, view or modify properties of a printer.
- **Documents being printed (print jobs)**: Pause, resume, cancel or restart printing of a document, view or modify properties of a document being printed.
- **Local groups**: Create or delete a group, add or remove members from a group, rename a group, view or modify properties of a group.

  NOTE: This task is not available on Domain Controllers (DCs).
- **Local users**: Create or delete a local user account, set a password for a local user account, rename a local user account, view or modify properties of a local user account.

  NOTE: This task is not available on DCs.
- **Devices**: View or modify properties of a logical device, start or stop a logical device.

To manage computer resources

1. In the Web Interface, locate the computer that hosts resources you want to manage. For more information on how to locate objects in the Web Interface, see Locating directory objects.
2. Select the computer in the list of objects, then click **Manage** in the Command pane.
3. In the list of resource types, click the type of resource you want to manage.
4. In the list of objects that appears, select the resource you want to manage.
5. Use commands in the Command pane to perform management tasks on the selected resource.

To manage print jobs

1. To start managing computer resources, repeat Steps 1 and 2 of the previous procedure.
2. To view the list of printers found on the selected computer, in the list of resource types, click **Printers**.
3. In the list of printers, select a printer whose print jobs you want to manage.
4. To view the list of documents being printed, in the Command pane, click **Print Jobs**.
5. In the list of documents, select a document to pause, resume, restart, or cancel printing.
6. To perform management tasks on the selected document, use the available commands in the Command pane.

Restoring deleted objects

The Web Interface can be used to restore deleted objects in any managed domain that has the Active Directory Recycle Bin feature enabled.

To undo deletions, Active Roles relies on the ability of Active Directory Recycle Bin to preserve all attributes, including the link-valued attributes, of the deleted objects. This makes it possible to restore deleted objects to the same state they were in immediately before deletion. For example, restored user accounts regain all group memberships that they had at the time of deletion.

This section provides instructions on how to restore deleted objects by using the Web Interface. For more information, see *Recycle Bin* in the *Active Roles Administration Guide*.

Locating deleted objects

If Active Directory Recycle Bin is enabled in a managed domain, the Web Interface provides access to the **Deleted Objects** container that holds the deleted objects from that domain. On the **Tree** tab in the Browse pane, the **Deleted Objects** container appears at the same level as the domain object, under the **Active Directory** node. If multiple managed domains have Active Directory Recycle Bin enabled, then a separate container is displayed for each domain. To tell one container from another, the name of the container includes the domain name (for example, **MyDomain.MyCompany.com - Deleted Objects**).

When you select the **Deleted Objects** container, the Web Interface lists all the deleted objects that exist in the corresponding domain. For more information on how to sort or filter the list to find specific objects, see Managing the list of objects. If you click an object in the list, a menu appears that displays all actions you can perform on that object.

Searching the Deleted Objects container

You can search for deleted objects in your Active Directory domain by searching the contents of the **Deleted Objects** container.

To locate deleted objects in the Deleted Objects container

1. On the **Tree** tab in the Browse pane, click the **Deleted Objects** container.
2. In the Command pane, click **Search under this container**.
3. Specify criteria for the deleted 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.
4. To start the search, press **Enter**.

Locating objects deleted from a certain OU or MU

To view a list of objects that were deleted from a particular Organizational Unit (OU) or Managed Unit (MU), use the **View or Restore Deleted Objects** command. The command opens a page that lists the deleted objects that were direct children of the corresponding OU or MU at the time of deletion.

To view a list of objects that were deleted from a certain OU or MU

1. Select the OU or MU that held deleted objects you want to view.
2. In the Command pane, click **View or Restore Deleted Objects**.

The Web Interface lists the objects that were deleted from the OU or MU you selected. The list can be sorted or filtered as appropriate to locate particular objects (see Managing the list of objects earlier in this document).

NOTE: The **View or Restore Deleted Objects** command is also available on domain and container objects.

Restoring a deleted object

You can restore deleted objects by using the **Restore** command that is available in the Command pane when you select a deleted object in the Web Interface.

To restore a deleted object

1. In a list of deleted objects, select the object you want to undelete. For more information on how to prepare a list of deleted objects, see Locating deleted objects.
2. In the Command pane, click **Restore**.
3. Review and, if necessary, change the settings in the **Restore Object** dialog box, then click **OK** to start the restore process.

The **Restore Object** dialog box prompts you to choose whether the deleted child objects (descendants) of the deleted object should also be restored. The **Restore child objects** check box is selected by default, which ensures that the **Restore** command applied on a deleted container restores the entire contents of the container.

NOTE: When restoring a deleted object, ensure that its parent object is not deleted. You can identify the parent object by viewing properties of the deleted object: the canonical name of the parent object, preceded by the **Deleted from:** label, is displayed beneath the name of the deleted object on the property page for that object. If the parent object is deleted, you need to restore it prior to restoring its children because deleted objects must be restored to a live parent.

4

Using Approval workflows

The Active Roles Web Interface supports approval operations, allowing your organization to control changes to directory data that require monitoring (and therefore, manual approval by organization personnel). For more information, see the following sections.

- Understanding approval workflow
- Locating approval items
- Using "My Tasks"
- Using "My Operations"

Understanding approval workflow

The approval workflow system included with Active Roles provides:

- A point-and-click interface to configure approval rules, available from the Active Roles Console. The approval rules are stored and performed by the Active Roles Administration Service.
- The directory management section of the Web Interface for submitting operation requests for approval. For example, approval rules could be configured so that creation of a user account starts an approval workflow instead of immediately running the user creation operation. For information on how to use the directory management section, see Managing Active Directory objects.
- The **Approval** area of the Web Interface to manage operation requests and approvals. This area includes a "to-do" list of the approval tasks the designated user has to carry out, allowing the user to approve or reject operation requests.

The **Approval** area provides a way to perform change approval actions, allowing you to control changes to directory data that require your approval and monitor your operations that require approval by other persons. You can use the **Approval** area to:

- Perform approval tasks—approve or reject operations so as to allow or deny the requested changes to directory data. Examples of operations include (but not limited to) creation and modification of user accounts or groups.

- Check the status of your operations—examine whether the changes to directory data you requested are approved and applied, or rejected.

When a Web Interface user makes changes to directory data that require permission from other individuals in an organization, the changes are not applied immediately. Instead, an operation is initiated and submitted for approval. This starts a workflow that coordinates the approvals needed to complete the operation. The operation is performed and the requested changes are applied only after approval. An operation may require approval from one person or from multiple persons.

When an operation is submitted for approval, Active Roles tracks the initiator and the approver or approvers. The initiator is the person who requested the changes. Approvers are those who are authorized to allow or deny the changes. An operation that requires approval generates one or more approval tasks, with each approval task assigned to the appropriate approver. Active Roles administrators configure approval workflow by creating approval rules to specify what changes require approval and who is authorized to approve or deny change requests.

In the **Approval** area, you can work with the operations for which you are assigned to the approver role. As an approver, you are expected to take appropriate actions on your approval tasks.

To access the Approval area

1. Open the Active Roles Web Interface.
2. On the Web Interface Home page, click **Approval**.

Locating approval items

The **Approval** area provides a number of views to help you locate approval items (tasks and operations):

- **My Tasks**: Contains detailed entries representing the approval tasks assigned to you. Depending on their status, the approval tasks are distributed into two views. The **Pending** view allows you to manage the approval tasks awaiting your response. The **Completed** view lists your approval tasks that have been completed.
- **My Operations**: The **Recent** view lists your recent operations that required approval, and allows you to examine the status and details pertinent to each operation.

In addition to using the predefined views, you can locate operations and tasks by using the search function.

To search for an operation or task by ID

1. In the right pane of the Web Interface page, under the **Search** label, type the ID number of the operation or task in the **Search by ID** box.
2. Click the button next to the **Search by ID** box to start the search.

You can also search for approval items (operations and tasks) by properties other than ID. For instance, you can find the operations that were initiated by a specific user. Another example is the ability to locate approval tasks generated within a specific time period. To access the advanced search function, click **Advanced Search** under the **Search** label. Then, use the **Advanced Search** page to configure your search settings and start a search.

Advanced search is the most comprehensive way to search for approval items such as operations and tasks. Use it to find approval items based on their properties. You do this by creating queries, which are sets of one or more rules that must be true for an item to be found. An example of a query for operations is `Initiator is (exactly) Sam Smith`. This specifies that you are searching for operations that have the **Initiator** property set to Sam Smith's user account.

With advanced search, you can use conditions and values to search for approval items based on item properties (referred to as **Fields** on the search page). Conditions are limitations you set on the value of a field to make the search more specific. Each type of item has a set of relevant fields and each type of field has a set of relevant conditions that advanced search displays automatically.

Some fields, such as **Target object property** require that you select a property to further define your search. In this case, you configure a query to search for operations or tasks specific to the approval of changes to the objects based on a certain property of those objects. For example, to find the operations that request any changes to the `Description` property, you could select the **Target object property** field, select the **Description** property, then choose the **Modified** condition.

Some conditions require a value. For example, if you select a **Date** field, the `Is between` condition requires a date range value so you have to select a start date and an end date to specify a date range. Another example is the **Initiator** field, which requires that you select a user account of the `Initiator` role holder.

In some cases, a value is not required. For example, if you select the **Modified** condition, no value is necessary, since this condition means that you want your search to be based on any changes to a certain property, without considering what changes were actually requested or made to the property value.

The following topics cover the predefined views of the **Approval** section.

Using "My Tasks"

You can use the **My Tasks** area to work with the approval tasks assigned to you as an approver. According to their status, the tasks are distributed into two views: **Pending** and **Completed**.

For information about the **Pending** view, see Pending tasks.

For information about the **Completed** view, see Completed tasks.

Pending tasks

The **Pending** view contains a list of your approval tasks to be completed. Each task in the list is identified by a header area that provides basic information about the task such as a unique ID number of the task, who requested the operation that is subject to approval, when the task was created, the time limit of the task (if any), and the target object of the operation. In the middle of a task's header area is a section that contains the title of the task (**Approve operation** by default), a label indicating the status of the task, and summary information about the operation that is subject to approval.

The task's header area contains the action buttons you can use to apply the appropriate resolution to the approval task. The action buttons are displayed at the bottom of the header area. Which buttons are displayed depends upon configuration of the approval rule. You may encounter the following action buttons there:

- **Approve**: Allows the requested operation.

  Depending on configuration of the approval and policy rules, the Web Interface may request you to enter additional information that must be added to the operation request. For example, when you approve the operation of creating a user account, you may have to supply certain properties of the user account in addition to those supplied by the administrator who requested creation of that user account. If additional information is required, clicking **Approve** displays a page where you can supply the required information. You can also access that page by clicking the **Examine task** button.
- **Reject**: Denies the requested operation.
- **Escalate**: Assigns the approval task to a higher-level approver.

  This button appears only if the approval rule has one or more additional approver levels (called "escalation levels") configured in addition to the initial approver level. Escalation levels are normally used to assign (escalate) the approval task automatically to a higher-level approver if the task is not completed in time. As such, the approval rule may be configured to allow approvers to escalate approval tasks as needed, in which case the header area of the task also contains the **Escalate** button.
- **Delegate**: Assigns the approval task to a different person. You can select the user to whom you want to assign the task.

  This button appears only if the approval rule is configured with the option to allow approvers to reassign (delegate) their approval tasks to other users.
- **Custom buttons**: The approval rule can include custom buttons to the header area of the task. The action that Active Roles performs when you click a custom button depends upon configuration of the workflow containing the approval rule. The administrator who configures the workflow should normally supply an instruction on the use of custom action buttons. To view the instruction, click the **Examine task** button. This opens a page containing the same action buttons that you see in the task's header area. The instruction text is displayed above the action buttons on that page.

The task's header area contains the **Examine task** button allowing you to get detailed information about the task, review the object properties submitted for approval, and supply

or change additional properties. Clicking the **Examine task** button displays a page containing a replica of the task's header area, the action buttons, and a number of information sections. Review the information on the page, supply or change the object properties for which the task requests your input, then click the appropriate action button.

The page that appears when you click the **Examine task** button includes the following information sections:

- **Object properties**: The contents of this section depend on the configured approval rule. Thus, the approval rule may request you to enter additional information that must be added to the operation request. For example, when you approve the operation of creating a user account, you may have to supply certain properties of the user account in addition to those supplied by the administrator who requested creation of that user account. In this case, enter the requested properties in the fields under **Supply or change the following properties**.

  Normally, the approval rule is configured so that the approver is allowed to review the values of the object properties that were supplied or changed by the operation that is subject to approval. The approval rule may also be configured to allow the approver to change those property values. In either case, you can view or change them in the fields under **Review the properties submitted for approval**.
- **Approvers**: Lists the user accounts or groups to which the approval task is currently assigned. Any of the listed users or members of the listed groups can act as an approver on the task in question.
- **Approval progress**: Provides information on the date and time that the task was created and whether the task was escalated to a higher approver level or reassigned (delegated) to other users. If the task was escalated, you can view when the escalation occurred and what was its cause. If the task was reassigned (delegated), you can view who and when delegated the task and to whom the task was delegated.
- **Details**: Provides aggregated information about the approval task properties and configuration, and some details of the operation that the task is intended to allow or deny. The **Operation ID** filed provides a link to a page where you can examine the operation in more detail.

To complete a pending task

1. Click **Examine task** in the task's header area.
2. On the **Object properties** page, review, supply or change the object properties for which the task requests your input, then click the appropriate action button.

You can also complete a task by clicking the appropriate action button in the task's header area. However, if the current policy and approval rules require the approver to supply some additional information, the Web Interface would open the **Object properties** page, prompting you to configure the required properties.

Completed tasks

The **Completed Tasks** view contains a list of your approval tasks that are completed and do not require approver action. Each task in the list is identified by a header area that provides basic information about the task, such as a unique ID number of the task, who requested the operation that is subject to approval, when the task was created, and the target object of the operation. In the middle of a task's header area is a section that contains the title of the task (**Approve operation** by default), a label indicating the status of the task, and summary information about the operation that was subject to approval. The header area also identifies the approver action that was applied to complete the task and the completion reason, if any, specified by the approver who completed the task.

The task's header area contains the **Examine task** button allowing you to get detailed information about the task and review the object properties that were submitted for approval or changed by the approver who completed the task. Clicking the **Examine task** button displays a page containing a replica of the task's header area and the following information sections:

- **Object properties**

  The contents of this section heavily depends upon configuration of the approval rule. Thus the approval rule may request the approver to enter additional information that must be added to the operation request. For example, when you approve the operation of creating a user account, you may have to supply certain properties of the user account in addition to those supplied by the administrator who requested creation of that user account. The values of the properties supplied by the approver are displayed in the fields under **Supply or change the following properties**.

  Normally, the approval rule is configured so that the approver is allowed to review the values of the object properties that were supplied or changed by the operation that is subject to approval. The approval rule may also be configured to allow the approver to change those property values. In either case, you can view them in the fields under **Review the properties submitted for approval**.

- **Approvers**

  This section displays a list of the user accounts or groups to which the approval task was assigned.

- **Approval progress**

  This section provides information on the date and time that the task was created, and whether the task was escalated to a higher approver level or reassigned (delegated) to other persons. If the task was escalated, you can view when escalation occurred and what caused escalation. If the task was reassigned (delegated), you can view who and when delegated the task and to whom the task was delegated.

  The **Task completed** sub-section indicates the date and time that the task was completed, identifies the approver who completed the task and the approver action that was applied to complete the task, and lists the values of the object properties that were supplied or changed by the approver.

- **Details**

This section lets you view aggregated information about the approval task properties and configuration, and some details of the operation that was allowed or denied by the completed task. The filed **Operation ID** provides a link to a page where you can examine the operation in more detail.

Using "My Operations"

In the **My Operations** area, the **Recent** view lists your operation requests that are waiting for approval from other individuals, as well as those allowed (approved) or denied (rejected) by the approver. You can use this view to monitor the status of your requests. You also have the option to cancel any of your requests that are not yet approved or rejected.

Each operation listed in the **Recent** view is identified by a header area that provides basic information about the operation such as a unique ID number of the operation, when and by whom the operation was requested, and the target object of the operation. A section in the middle of the operation header contains a summary of the operation, operation status and an operation reason that was supplied when the operation was submitted for approval.

The operation summary identifies the operation type (such as **Create user** or **Change user**) and may provide information about the changes to the object properties that result from the operation. From the operation status you can tell whether the operation is waiting for approval (pending), allowed (completed), denied (rejected) or canceled. If a given operation is waiting for approval, you can remove the operation request by clicking the **Cancel operation** button.

The operation header contains the **View operation details** button allowing you to get detailed information about the operation and review the object properties that were submitted for approval or changed by the approver who allowed the operation. Clicking the **Examine task** button displays a page that contains a replica of the operation header and the following information sections under the operation header:

- **Properties changed during this operation**: This section lists the object property values that were changed as a result of the operation, new values assigned to the properties, and identifies who made the changes.
- **Workflow activities and policy actions**: This section provides detailed information about all policies and workflows that Active Roles performed when processing the operation request, including information about the approval tasks created as a result of approval workflow activities. For each approval task, you can view the status of the task along with aggregated information about the properties and configuration of the task.

  From the task status, you can tell whether the task is waiting for completion (pending), completed to allow the operation or rejected to deny the operation. From the additional information about a task, you can identify, for instance, the approvers to whom the task is assigned, the due date of the task, the approver who allowed or denied the operation and what changes, if any, the approver made to the original operation request.

- **Operation details**: This section contains additional information about the operation, including when and by whom the operation was requested, the target object of the operation, the current status of the operation, and the date and time that the record of the operation was last updated.

About us

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

Contacting us

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

Technical support resources

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

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

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

Glossary

Index