One Identity Active Roles 7.3

Azure AD and Office 365 Management Administration Guide

Legend

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

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

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

Active Roles Azure AD and Office 365 Management Administration Guide
Updated - May 2019
Version - 7.3

Contents

1

Overview

Active Roles (formerly known as ActiveRoles®) is an administrative platform that facilitates administration and provisioning for Active Directory, Exchange, and Azure Active Directory (Azure AD) in a hybrid environment. Active Roles enables the organization to manage through the web interface and to develop a flexible administrative structure that suits their needs, while ensuring secure delegation of tasks, reduced workloads, and lower costs.

Active Roles enables synchronization of the on-premises Active Directory objects to the Azure AD.

This guide is designed for individuals responsible for performing administrative tasks using the Active Roles web interface for Azure Active Directory and Office 365. The document includes instructions to help delegated administrators and help-desk operators perform day-today Azure AD administrative activities.

NOTE: Azure AD related operations are supported only on Active Roles web interface with sites for Administrators template. Some of the operations are also supported through the Management Shell. This guide provides detailed information on the Azure AD operations.

2

Configuring Active Roles to Manage Hybrid AD Objects

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

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

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

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

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

- Configuring Active Roles to manage Hybrid AD using Web Interface
- Configuring Active Roles to manage Hybrid AD using Management Shell
- Active Roles Configuration steps to manage Hybrid AD objects
- Active Roles Configuration to synchronize existing AD objects to Azure AD

Configuring Active Roles to manage Hybrid AD using Web Interface

Active Roles Web interface enables you to perform the following configuration tasks to manage Hybrid AD:

- Add an Azure AD tenant
- View or modify the Azure AD tenant properties
- View the Domains associated to an Azure AD tenant
- Delete an Azure AD tenant
- Add an Azure AD Application
- View the Azure AD Application properties
- Provide Administrator Consent for Azure AD application to access Active Directory
- Delete an Azure AD Application
- View Azure Health for Azure AD tenants and applications
- View Azure Licenses Report

Add an Azure AD tenant

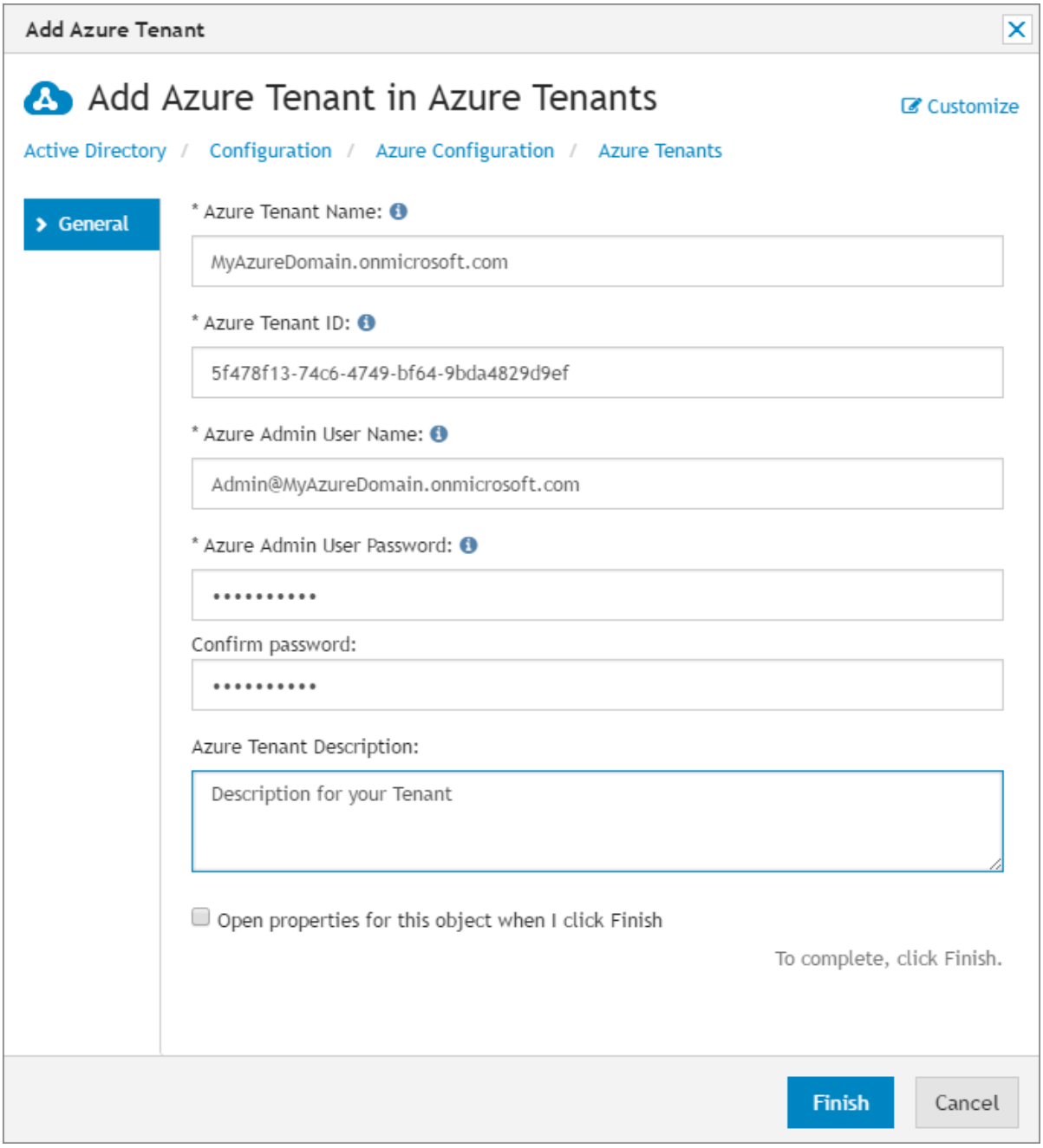
You can use the Active Roles Web Interface to add an Azure AD tenant.

NOTE: Currently, Active Roles supports single Azure AD tenant model. Make sure to add only one tenant with correct Azure AD related details.

To add an Azure AD tenant

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration**.
3. In the **Command** pane, click **Add Azure Tenant**.
4. In the **General** properties **Add Azure Tenant** window, enter the following details:

Figure 1: Azure Tenant Configuration



- **Azure Tenant Name**: Enter the name of the Azure AD tenant
- **Azure Tenant ID**: Enter the Azure AD tenant ID obtained from the default tenant created after subscribing for Microsoft Azure.

NOTE:

- The first time you sign up for a Microsoft cloud service such as Azure, Microsoft Office 365, or Microsoft Intune, you are prompted to provide details about your organization and your organization's Internet domain name registration. This information is then used to create a new Azure directory instance for your organization. That same directory is used to authenticate sign in attempts when you subscribe to multiple Microsoft cloud services.
- In Active Roles Web interface, the values entered for configuring Azure AD tenant must exactly match the values configured for Azure AD, else Azure AD application creation and management of Azure AD objects fail.

- **Azure Admin User Name**: Enter the administrative user name of Azure AD.

  It is recommended to use the Global Administrator account . However, Active Roles requires the following minimal role permission to manage Users and Groups along with Exchange Online permission:

  - User management Administrator
  - Exchange Administrator
- **Azure Admin User Password**: Enter the password provided for the administrative user.
- **Confirm Password**: Re-enter the password provided for the administrative user.
- **Azure Tenant Description**: Enter the required description for the Azure AD tenant.

5. Click **Next**.

   The Azure AD Tenant Type properties wizard is displayed with the following types of domains:

   - Non Federated Domain: On-premises Domains are not registered in Azure AD and AADconnect is not configured. Users are typically created with **onmicrosoft.com** UPN suffix.
   - Federated Domain: On-premises Domains are registered in Azure AD, AADconnect and ADFS is configured. Users are typically created with selected on-premises domain's UPN suffix.
   - Synchronized Identity Domain: On-premises Domains may or may not be registered in Azure AD and AADconnect is configured. Users may typically be created with selected on-premises domain's or **onmicrosoft.com** UPN suffix.
6. Select the appropriate domain type and click **Finish**.

   The newly added Azure AD tenant is displayed in the **Azure Tenants** list.

NOTE: If the Tenant type is selected as Federated Domain or Synchronized Identity Domain, the Azure properties fields on **Azure properties** wizard of the Azure User, Group, or Contacts that are created are greyed out and cannot be edited.

View or modify the Azure AD tenant properties

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

To view or modify the Azure AD tenant properties

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Tenants**.

   The list of existing Azure AD tenants are displayed.
3. Select the check box corresponding to the specific Azure AD tenant 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 tenant is displayed.
5. Use the fields in the **Azure Properties** wizard to view or modify the password or description of the Azure AD tenant.

   NOTE:

   - If the Tenant type is selected as Federated Domain or Synchronization Identity domain while creating the Azure User, Group, or Contact, the Azure properties fields on **Azure properties** wizard of the that Azure object are greyed out and cannot be edited.
   - You cannot modify the Azure AD tenant ID.
6. Click **Azure AD Tenant Type**, and modify the modify type od domain assigne dto the Azure tenant.
7. After setting all the required properties, click **Save**.

View the Domains associated to an Azure AD tenant

For every Azure AD tenant created there are domains associated with the tenants. You can use the Active Roles Web Interface to view the domains associated to the Azure AD tenant.

To view the Azure AD tenant associated domains

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration ->**

Azure Domains.

The list of domains associated to the Azure AD tenant are displayed.

Delete an Azure AD tenant

You can use the Active Roles Web Interface to delete an Azure AD tenant.

To delete an Azure AD tenant

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Tenants**.

   The list of existing Azure AD tenants are displayed.
3. Select the check box corresponding to the specific Azure AD tenant which you want to delete.
4. In the **Command** pane, click **Delete**.

   A message is displayed prompting you to confirm if you want to delete the tenant.
5. Click **Yes**.

   The Azure AD tenant and all the related domains and applications are deleted and can be verified by navigating to **Azure Configuration -> Azure Tenants** and **Azure Configuration -> Azure Domains.**

NOTE: The domains are deleted only from the Active Roles database. However, the applications are deleted from the Active Roles database and Azure AD.

Add an Azure AD Application

You can use the Active Roles Web Interface to add an Azure AD application to the Azure AD tenant.

To add an Azure AD application

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration**.
3. In the **Command** pane, click **Add Azure Application**.
4. In the **General** properties **Add Azure Application** window, enter the following details:

- **Name**: Enter a name for the Azure AD application
- **Display Name**: Enter the name to be displayed

- **Azure Tenant ID**: Enter the Azure AD tenant ID obtained from the default tenant created in the Azure Portal after Azure subscription.

NOTE: In Active Roles Web interface, the values entered for creating Azure AD tenant must exactly match the values configured for Azure AD, else Azure AD application creation and management of Azure AD objects fail.

5. Click **Finish**.

   The newly added Azure AD application is displayed in the **Azure Applications** list.

View the Azure AD Application properties

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

To view the Azure AD application properties

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Application**.

   The list of existing Azure AD applications are displayed.
3. Select the check box corresponding to the specific Azure AD application for which you want to view or update the Azure properties.
4. In the **Command** pane, click **Azure properties**.

   The **Azure Properties** wizard for the Azure AD application is displayed.
5. Use the fields in the **Azure Properties** wizard to view the properties of the Azure AD application.

NOTE: You cannot modify the Azure AD application properties.

Provide Administrator Consent for Azure AD application to access Active Directory

After an application is created for the Azure AD tenant, the administrator with the Global Administrators group privileges must provide consent for communication between the application and Active Roles Server for the permission scopes that are configured for the application.

To provide Administrator consent for an application

1. On the Active Roles Web interface Navigation bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Application**.

   The list of existing Azure AD applications are displayed.
3. Select the check-box corresponding to the specific Azure AD application for which you want to provide consent to Microsoft Azure AD, and click **Azure Properties**.
4. From the **Azure Properties** wizard, copy the URL displayed in the **Consent URL** field, open a new Web Browser tab or window, enter the URL and press **Enter.**
5. On the Microsoft Azure login page, enter the Azure AD administrator credentials.
6. Click **Accept** to provide consent to Microsoft Azure to grant access to the Active Roles Active Directory resources.

   On successful completion of the task the Local host window is displayed.

Azure AD Application Permissions

When an Azure AD application is registered, the administrator defines the permission scope for the application. By default, minimal permissions are assigned to every application. To add additional permissions to the Azure application, go to the Azure Portal and add the required permissions. To add the additional permissions for all the users in the organization, click **Accept**.

During an in-place upgrade of Active Roles to version 7.3, delete the existing Tenant and then add a new Tenant and Application. This ensures that the Application has the minimal permissions assigned by default.

Deleting the Azure AD Tenant and application, does not delete the application from Azure. To remove the application completely, go to the Azure portal and delete the application.

Delete an Azure AD Application

You can use the Active Roles Web Interface to delete an Azure AD application.

To delete an Azure AD application

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Applications**.

   The list of existing Azure AD applications are displayed.
3. Select the check box corresponding to the specific Azure AD application which you want to delete.
4. In the **Command** pane, click **Delete**.

A message is displayed prompting you to confirm if you want to delete the application.

5. Click **Yes**.

   The Azure AD application is deleted and can be verified by navigating to **Azure Configuration -> Azure Applications.**

NOTE: The Azure AD application is deleted from the Active Roles database and Azure AD.

View Azure Health for Azure AD tenants and applications

Azure Health Check informs you about the Active Roles to Azure AD connectivity status, and the Active Roles Azure AD tenant and application heath status.

To view the Azure AD health status in Active Roles

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Health Check**.

   The health status for the following services and resources is displayed:

   - **Graph Connectivity** – Green status indicates that the Active Roles connectivity to the Microsoft Graph API is successful
   - **Tenant Connectivity** – The tenant username and password are validated. Green status indicates that the Azure AD Tenant credentials are valid. The tenant connectivity is successful only if the Graph connectivity is successful
   - **Azure Application Connectivity** – The Azure AD applications are validated and verified if the applications are consented. Green status indicates that the Azure AD applications connectivity is successful. The application connectivity is successful only if both the Graph connectivity and tenant connectivity are successful.

View Azure Licenses Report

Azure Licenses Report displays the Office 365 licenses that are available and assigned to a user.

To view the Azure AD licenses report

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Licenses Report**.

   The Azure Licenses Report wizard displays the list of Office 365 licenses available for the Azure AD domain. For each license the following information is displayed:

   - **Valid** – The total number of a specific license available for the Azure AD domain.
   - **Expired** – The number of licenses of a specific license type that are in renewal period or have expired.
   - **Assigned** – The number of licenses of a specific license type that have been assigned to any users in the domain.

Configuring Active Roles to manage Hybrid AD using Management Shell

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

- Add an Azure AD Tenant
- Add an Azure AD Application

Add an Azure AD Tenant

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

To add an Azure AD tenant

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

Synopsis

This cmdlet enables you to add an Azure AD tenant to Active Directory.

Syntax

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

Description

Use this cmdlet to add an Azure AD tenant using the tenant ID provided by Microsoft for the default tenant created at the time of Microsoft Azure subscription.

Parameters

- type (string)

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

NOTE: AzureADTenantType can be Federated, Non Federated, or Synchronized depending on the customer's environment.

Table 1: Parameters: type (string)

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

- name (string)

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

Table 2: Parameters: name (string)

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

- AzureTenantId (string)

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

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

Table 3: Parameters: AzureTenantId (string)

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

- AzureTenantDescription

  Use this parameter to specify the required description for the Azure AD tenant.

Table 4: AzureTenantDescription

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

- AzureAdminUserID

  Use this parameter to specify the administrative user name for Microsoft Azure AD.

NOTE: The Administrative user must have the required privileges to perform license management and Azure user and group management.

Table 5: Parameters: AzureAdminUserID

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

- AzureAdminPassword

  Use this parameter to specify the administrative user name for Microsoft Azure AD.

Table 6: Parameters: AzureAdminPassword

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

Table 7: Parameters: AzureADTenantType

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

Example

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

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

Example

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

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

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

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

C:\PS> disconnect-qadService
```

Add an Azure AD Application

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

To add an Azure AD application

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

Synopsis

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

Syntax

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

Description

Use this cmdlet to add an Azure AD application.

Parameters

- type (string)

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

  Table 8: Parameters: type (string)

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

- name (string)

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

  Table 9: Parameters: name (string)

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

- AzureTenantId (string)

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

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

  Table 10: Parameters: AzureTenantId (string)

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

- Displayname (string)

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

  Table 11: Parameters: Displayname (string)

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

- AzureAppPermissions

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

  Table 12: Parameters:AzureAppPermissions

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

- AzureApplicationDescription

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

Table 13: Parameters: AzureApplicationDescription

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

Example

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

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

Example

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

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

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

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

C:\PS> disconnect-qadService
```

Active Roles Configuration steps to manage Hybrid AD objects

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

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

5. Edit the **edsvaAzureOffice365Enabled** attribute for the Azure OU and set the value to "True".
    a. In the console tree, go to the Organizational Unit you want to modify.
    b. Right-click the Organizational Unit, and then click **Properties** to display the **Properties** dialog box for that Organizational Unit.
    c. On the **Properties** dialog box, go to the **Object** tab and click **Advanced Properties**.
    d. From the list of available attributes, search and click on the attribute **edsvaAzureOffice365Enabled**.
    e. In the **Edit Attribute** dialog box, set the value to **True**.
    f. To set the attribute for all the Child organizational units, select the check box corresponding to All Child Organizational Units, and click **OK**.

Active Roles Configuration to synchronize existing AD objects to Azure AD

In any hybrid environment, on-premises Active Directory objects are synchronized to Azure AD using some means such as Azure AD Connect. When Active Roles 7.3 is deployed in such a hybrid environment, the existing users and groups' information, such as Azure objectID, must be synchronized back from Azure AD to on-premises AD to continue using the functionality. To synchronize existing AD users and groups from Azure AD to Active Roles we must use the back-synchronization operation.

The back-synchronization operation can be perfomed automatically or manually using the Active Roles Synchronization Service Web interface:

- Automatic Back Synchronization is performed using the **Azure Backsync Configuration** feature in Active Roles Synchronization Service that allows you to configure the backsync operation in Azure with on-premises Active Directory objects through the Synchronization Service Web interface. After the backsync operation is completed successfully the Azure application registration and the required connections, mappings, and sync workflow steps are created automatically.

  For information on configuring the backsync operation automatically using the Active Roles Synchronization Service web interface, see Configuring Sync Workflow to back-synchronize Azure AD Objects to Active Roles automatically using the Synchronization Service Web interface.

  For more information on the results of the backsync operation see the *One Identity Active Roles Synchronization Service Administration Guide*.
- Manual Back Synchronization is performed by leveraging the existing functionality of Synchronization Service component of Active Roles. Synchronization workflows are configured to identify the Azure AD unique users or groups and map them to the on-

premises AD users or groups. After the back-synchronization operation is completed, Active Roles displays the configured Azure attributes for the synchronized objects.

For information on configuring Synchronization workflows for Azure AD, see *One Identity Active Roles Synchronization Service Administration Guide*.

Configuring Sync Workflow to back-synchronize Azure AD Objects to Active Roles automatically using the Synchronization Service Web interface

Pre-requisites to configure the back-synchronization:

- The hybrid environment must have Azure AD Connect installed and configured.
- The user account used to perform Back sync configuration must have the following privileges:
  - User Administrator
  - Privileged Role Administrator
  - Exchange Administrator
  - Application Administrator
- The Windows Azure Active Directory (Azure AD) module version 2.0.0.131 or later must be installed for the backsync feature to work successfully.
- Directory Writers Role must be enabled in Azure Active Directory. To enable the role use the following script:

```
$psCred=Get-Credential

Connect-AzureAD -Credential $psCred

$roleTemplate = Get-AzureADDirectoryRoleTemplate | ? { $_.DisplayName -eq
"Directory Writers" }

# Enable an instance of the DirectoryRole template

Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId
```

To configure Azure backsync in Active Roles Synchronization Service

1. In the upper right corner of the Synchronization Service Administration Console, select **Settings** | **Configure Azure BackSync**.

   The Configure BackSync operation in Azure with on-prem Active Directory objects dialog box is displayed.

2. In the dialog box that opens:
   a. Enter the Azure domain valid Account ID credentials, and click **Test Office 365 Connection**.

b. Specify whether you want to use a proxy server for the connection. You can select one of the following options:

- **Use Internet Explorer settings**: Causes the connector to automatically detect and use the proxy server settings specified in Microsoft Internet Explorer installed on the Synchronization Service computer.
- **Use WinHTTP settings**: Causes the connector to use the proxy server settings configured for Windows HTTP Services (WinHTTP).
- **Automatically detect**: Automatically detects and uses proxy server settings.
- **Do not use proxy settings**: Specifies to not use proxy server for the connection.

On successful validation, the success message that the Office 365 Connection settings are valid is displayed.

c. Enter the valid Active Roles account details and click **Test Active Roles Connection**.

On successful validation the success message that the Active Roles connection settings are valid is displayed.

3. Click **Configure BackSync**.

The Azure App registration is done automatically. The required connections, mappings, and workflow steps are created automatically. For more information on the automatically created backsync settings, see Settings updated after Azure backsync configuration operation.

On successful configuration the success message is displayed.

If the Azure BackSync settings are already configured in the system, a warning message is displayed to confirm if you want to override the existing backsync settings with the new settings. If yes, click **Override BackSync Settings**. Else, click **Cancel** to retain the existing settings.

Configuring Sync Workflow to back-synchronize Azure AD Objects to Active Roles manually

Pre-requisites to configure the back-synchronization manually:

- The hybrid environment must have Azure AD Connect installed and configured.
- Synchronization Service Component must be installed and configured for Active Roles.
- Azure AD configuration and the Administrator Consent for Azure AD application through web interface must be complete.

- Azure AD built-in policy must be enforced and the attribute ***edsvaazureOffice365enabled*** must be set to **true** for the container where the back-synchronization is performed.

NOTE: Before adding a replication partner in a Replication environment, make sure to perform back-synchronization in the Service that is configured with the Publisher database.

Configuring Sync Workflow to back-synchronize Azure AD users and groups to Active Roles manually

To configure sync workflow to back-synchronize users and groups perform the following steps:

Step 1: Create Connection to Azure AD in the hybrid environment

Create a connection to Azure AD using the Azure AD Connector. The configuration requires the Azure domain name, the Client ID of an application in Azure AD, and the Client Key to establish the connection with Azure AD.

To configure an application:

1. Create an Azure Web application (or use any relevant existing Azure Web Application) under the tenant of your Windows Azure Active Directory environment.

   The application must have "Application Permissions" to "read" and "write" directory data in Windows Azure Active Directory.

   NOTE: Alternatively, to assign the required permissions to the application by running a Windows PowerShell script, see the Creating a Windows Azure Active Directory connection section in Sync Service Guide.

2. Open the application properties and copy the following:

- Client ID
- Valid key of the application

3. You need to supply the copied client ID and key when creating a new or modifying an existing connection to Windows Azure Active Directory in the Synchronization Service Administration Console.

NOTE: The Web Application that is created or is already available for Sync Service Azure AD Connector, is different from the application that is created while configuring Azure AD using Active Roles Web interface. Both the applications must be available for performing back-sync operations.

Step 2: Create Connection to Active Roles in the hybrid environment

Create a connection to Active Roles using the Active Roles Connector. The configuration requires the local domain details and Active Roles version used. Define the scope to select the container from which the objects for synchronization must be selected.

Step 3: Create Sync Work flow

Create a Sync Workflow using the Azure AD and Active Roles connections. Add a Synchronization step to Update Azure User/Group to Active Roles User/Group. Configure the **Forward Sync Rule** to synchronize the following:

- Azure **ObjectID** property of a user/group to the Active Roles user/group **edsvaAzureObjectID** property.
- Set the **edsvaAzureOffice365Enabled** attribute in Active Roles user/group to **True**.

Step 4: Create Mapping

Create a Mapping Rule which identifies the user/group in Azure AD and on-premises AD uniquely and map the specified properties from Azure AD to Active Roles appropriately.

For example, the property **userprincipalname** can be used to map users between on-premises AD and Azure AD in a federated environment.

NOTE:

- Based on the environment, make sure to create the correct Mapping rule to identify the user or group uniquely. In-correct mapping rule may create duplicate objects and the back-sync operation may not work as expected.
- Initial configuration and execution of back-sync operation for Azure AD users ID is a one-time activity.
- In Federated or Synchronized environments, Azure AD group creation is not supported. The group is created in Active Roles and 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.
- Sync engine must be configured to synchronize the data back to AD based on the frequency of groups creation.

Configuring Sync Workflow to back-synchronize Office 365 Contacts to Active Roles

To configure sync workflow to back-synchronize contacts perform the following steps:

Step 1: Create Connection to Office 365 in the hybrid environment

Create a connection to Office 365 using the Microsoft Office 365 Connector. The configuration requires Microsoft Online Services ID, Password, Proxy server (if required) and Exchange Online services.

NOTE: Back synchronization of contacts uses Microsoft Office 365 Connector to establish connection to Office 365. Back synchronization of users and groups uses the Azure AD Connector to establish connection to Azure AD.

Step 2: Create Connection to Active Roles in the hybrid environment

Create a connection to Active Roles using the Active Roles Connector. The configuration requires the local domain details and Active Roles version used. Define the scope to select the container from which the objects for synchronization must be selected.

Step 3: Create Sync Workflow

Create a Sync Workflow using the Office 365 and Active Roles connections. Add a Synchronization step to Update Office 365 Contacts to Active Roles Contacts. Configure the **Forward Sync Rule** to synchronize the following:

- Azure **ExternalDirectoryObjectId** property of a contact to the Active Roles contact **edsaAzureContactObjectId** property.
- Set the **edsvaAzureOffice365Enabled** attribute in Active Roles contact to **True**.

Step 4: Create Mapping

Create a Mapping Rule, which identifies the contact in Office 365 and on-premises AD uniquely and map the specified properties from Office 365 to Active Roles appropriately.

NOTE:

- Based on the environment, make sure to create the correct Mapping rule to identify the contacts uniquely. In-correct mapping rule may create duplicate objects and the back-sync operation may not work as expected.
- In Federated or Synchronized environments, Office 365 contact creation is not supported. The contact is created in Active Roles and is synchronized eventually to Office 365 using Microsoft Native tools, such as AAD Connect. To manage the Office 365 contact through Active Roles, you must perform periodic back-synchronization to on-premise AD.

Managing Hybrid AD Users

The Active Roles web interface enables you to perform administrative tasks such as create, read, update, deprovision, undo-deprovison, and delete Azure AD users in Hybrid environment. You can also perform other operations such as 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 Sell to manage Azure AD users.

- Azure AD user management tasks using Web interface
- Hybrid User Management tasks using web interface
- Azure AD user management tasks using Management Shell interface
- Office 365 license management for hybrid environment users

Azure AD user management tasks using Web interface

Active Roles web interface enables you to perform the following management tasks for Azure AD users:

- Create a new Azure AD user
- View or update the Azure AD user properties
- Modify the Azure AD user Manager
- Disable or re-enable an Azure AD user
- Deprovision or undo deprovision of a Azure AD user
- Add or remove a Azure AD user from a group
- View the Change History and User Activity for an Azure AD user
- Delete an Azure AD user

Create a new Azure AD user

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

To create a new 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 domain in which you need to create a new user.
4. In the list of objects displayed, 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 such as **First Name**, **Last Name**, **Initials, and User logon name.**
7. Click **Next**.
8. In the **Account** properties wizard, click **Generate** to generate a password for the Account, 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 re-set the password for the Azure AD account if required.
10. From the **User Principal Name** drop-down list,select the AD domain to which you want to associate the Azure AD user.
11. In the **Usage Location** field, enter the two-letter location code of the location where the product will be used.

    NOTE: The **Usage Location** field is a mandatory field. The licenses cannot be assigned to the product if the product usage location information is not available. The local rules and regulations for usage of the product and services may vary based on the location.
12. Click **Next**.

    The **Licenses** wizard displays the Office 365 licenses, for example the Office 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 **Finish**.

    The licenses assigned can be viewed on the user's **Azure Properties->Licenses** wizard.

View or update the Azure AD user properties

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

1. On the Active Roles Web interface **Navigation** bar, click **Directory Management**.
2. On the **Views** tab in the **Browse** pane, click **Azure Configuration -> Azure Tenants**.

   The list of existing Azure AD tenants are displayed.
3. Select the check box corresponding to the specific Azure AD tenant 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 tenant is displayed.
5. Use the fields in the **Azure Properties** wizard to view or modify the password or description of the Azure AD tenant.

   NOTE:

   - If the Tenant type is selected as **Federated Domain** or **Synchronized Identity** domain while creating the Azure User, Group, or Contact, the **Azure properties** fields on **Azure properties** wizard of the that Azure object are greyed out and cannot be edited.
   - If Tenant type is selected as **Federated Domain** or **Synchronized Identity** domain, it enables the user to create Azure User even when Azure AD Connect is enabled.
   - You cannot modify the Azure AD tenant ID.
6. Click **Azure AD Tenant Type**, and modify type of domain assigned to the Azure tenant.
7. After setting all the required properties, click **Save**.

Modify the Azure AD user Manager

For an existing Azure AD user, you can use the Active Roles Web Interface to modify the Azure AD user Manager.

To view or modify the Azure AD user 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 user for which you want to view or update the Manager information.
4. In the **Command** pane, click **General properties**.

   The **General Properties** dialog box for the user is displayed.
5. Navigate to the **Managed by** tab, and in the **Manager** field, click **Change**.
6. Use the **Select Objects** dialog box, to locate and select the Manger to assign to the user and click **OK**.

   The newly added Manager name is displayed in the **Manager** field.
7. Click **Save**.

   The **Manager ID** field in the **Azure Properties** wizard for the user is populated with the new Manager information.

   NOTE: To verify the changes in Microsoft Azure, go to the Azure Portal and view the Manger ID information for the specific user in the Work Info tab.

Disable or re-enable 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 or re-enable 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 to be disabled.
4. In the **Command** pane, click **Disable**.

   The account is disabled and marked with a disabled icon.
5. To enable a disabled account, select the check-box corresponding to 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.

Deprovision or undo deprovision of a 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.

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

Add or remove a Azure AD user from a group

You can use the Active Roles Web Interface to add or remove an existing Azure AD user from 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 check-box corresponding to 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, click **Add** to add the user to another group.
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.

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 add to a group.
4. Select the check-box corresponding to 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.

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 for 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**.

   Selecting **Change History** displays the information on changes that were made to the user through Active Roles.

   Selecting **User Activity** displays information on management actions that were performed by a given user.

Delete an Azure AD user

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

To delete 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 to be deleted.
4. In the **Command** pane, click **Delete**.

   The account is deleted.

NOTE:

- Deleting a user is an irreversible operation. A new user with the same name as a deleted user does not automatically assume the permissions and memberships of the deleted account. For this reason, it is advisable to disable rather than delete accounts.
- 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.

Hybrid User Management tasks using web interface

Active Roles web interface enables you to perform the following Hybrid management tasks for hybrid users:

- Create a new Hybrid user using web interface
- Migrate an Exchange on-premise user to a Hybrid user
- View or modify the Exchange Online properties of an Office 365 User
- View the Mail Flow settings of an Office 365 User
- View or modify the Email Address settings for an Office 365 User
- View or modify the MailBox features for an Office 365 User
- View or modify the MailBox settings for an Office 365 User
- View or Modify the MailBox Delegation settings for an Office 365 User

Create a new Hybrid user using web interface

You can use the Active Roles web interface to create and manage Hybrid users.

To create a new hybrid 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 domain in which you need to create a new user.
4. In the list of objects displayed, 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 such as **First Name**, **Last Name**, **Initials, and User logon name.**
7. Click **Next**.
8. In the **Account** properties wizard, click **Generate** to generate a password for the Account, 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. Select the check box to create Exchange mailbox on premise.
10. 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 re-set the password for the Azure AD account if required.
11. From the **User Principal Name** drop-down list, select the AD domain to which you want to associate the Azure AD user.
12. In the **Usage Location** field, enter the two-letter location code of the location where the product will be used.

    NOTE: The **Usage Location** field is a mandatory field. The licenses cannot be assigned to the product if the product usage location information is not available. The local rules and regulations for usage of the product and services may vary based on the location.
13. Click **Next**.
14. Select the Exchange Online license from the listed subscription in the Licenses wizard and click **Finish.**

    The assigned license can be viewed on the user's **Azure properties->Licenses** wizard.

Migrate an Exchange on-premise user to a Hybrid user

An Exchange on-premise user can be converted to a hybrid user by migrating the Exchange on premise mailbox to Exchange Online.

To migrate an Exchange on-premise user in a Synchronized or Federated Environment to a Hybrid 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 domain in which you need to create a new user.
4. In the list of objects displayed, click the required **Container** or the **Organizational Unit**.
5. Select an existing user with Exchange on premise and click **Azure Properties**.
6. In the **Azure Properties** wizard, select the **Licenses** wizard.
7. Select Exchange Online Plan from the License subscription list and click **Finish**.

   An Exchange online mailbox for the user is created.

   The Exchange Online created is available only after migration.

   Refer the Microsoft link to perform migration from Exchange on premise to Exchange Online mailbox.

   After the migration, the Exchange on premise properties updated in Web interface are synced to Office 365 portal through Microsoft Native Tools and can be viewed using Exchange Online Properties.

NOTE: Exchange Online properties in Web interface in Synchronized and Federated environments are non-editable and can be used only to view the properties.

View or modify the Exchange Online properties of an Office 365 User

For an existing Office 365 user, you can use the Active Roles Web Interface to view or modify the Exchange Online properties.

NOTE:

- The Exchange online settings are read-only in Synchronized Identity and Federated environments. The modify option is applicable for Office 365 users in non-federated environment only.
- To manage Exchange or Exchange Online properties in Hybrid Exchange environment, Administrators must set the corresponding properties using the Exchange Properties tab. These properties are eventually synchronized to Exchange Online through Microsoft Native tools.

To view the Exchange Online properties of an Office 365 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 select the check-box corresponding to the specific 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 Office 365 user.
   - Mail Flow Settings
   - Delegation
   - E-mail Addresses
   - Mailbox Features
5. Use the tabs in the **Exchange Online Properties** dialog box to view the following Exchange Online properties of the Office 365 user:
   - 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

View the Mail Flow settings of an Office 365 User

For an existing Office 365 user, you can use the **Mail Flow settings** tab in the Exchange Online Properties wizard to view or set the message size restrictions and delivery options.

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

To view and modify the message size restrictions for an Office 365 user

1. In the Exchange Online Properties wizard of an Office 365 user, click **Mail Flow Settings**.
2. Under Mail flow settings, click **Message Size Restrictions** and then **Properties**.

   The Message Size Restrictions dialog box displays the sending and receiving message size restrictions.
3. In non-federated environment, to set or modify the sending and receiving message size restrictions, select one of the following in the Message Size Restrictions dialog box:
   - Use default limit – Allows you to set the maximum size for the outgoing or incoming messages to the default value used in Exchange Online, which is applied through the built-in policy "**Built-in Policy - Exchange Online - Default Message Size Restrictions**" enforced on the container.
   - Maximum (KB) – Allows you to specify the maximum value for the outgoing or incoming message size.
4. Click **Save**.
5. Close the dialog box and click **Save**.

NOTE: The changes made to message size restrictions settings for the Office 365 user can be verified in the Microsoft Office 365 portal.

To view or modify the message delivery options for an Office 365 user

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

1. In the Exchange Online Properties wizard of an Office 365 user, click **Mail Flow Settings**.
2. Under Mail flow settings, click **Delivery Options** and then **Properties**.
3. To allow one or more users to send messages on behalf of the Office 365 user, in the Delivery Options dialog box, click **Add**, select one or more users from the **Select Object** list, and then click **OK**.
4. To limit users from sending messages on behalf of the Office 365 user, select the users in the **Name** list and click **Remove**.
5. To specify a forwarding address for messages addressed to the Office 365 user, select **Forward to**, and click **Modify**.

   Alternatively, to change the current forwarding address, click **Modify**.
6. From the Select Object wizard, select the users to whom the messages addressed to the mailbox can be forwarded and click **OK**.
7. Click **Save**.
8. Close the dialog box and click **Save**.

NOTE: The changes made to message delivery options for the Office 365 user can be verified in the Microsoft Office 365 portal.

View or Modify the MailBox Delegation settings for an Office 365 User

For an existing Office 365 user, you can use the MailBox delegation settings tab in the Exchange Online Properties wizard to view or modify other users or groups who can send mails or be provided full access to the user's mailbox.

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

To view or modify the MailBox delegation settings for an Office 365 user

1. In the Exchange Online Properties wizard of an Office 365 user, click **Delegation**.
2. To specify or modify the list of users or groups who can send mail from the Office 365 user’s mailbox, under **Send as**, click **Add**.
3. Select one or more users or groups from the **Select Object** list, and then click **OK**.
4. Alternatively, to limit users who can send emails from the Office 365 user’s mailbox, select the users in the **Name** list and click **Remove**.
5. Click **Properties** to view the general properties of the user added under the **Send as** option.
6. To specify Office 365 users or groups who can be provided full access to the user’s

mailbox, under **Full Access**, click **Add**, select one or more users or groups from the **Select Object** list, and then click **OK**.

7. Alternatively, to limit users who can be provided full access to the user's mailbox, select the users in the **Name** list and click **Remove**.
8. Click **Properties** to view the general properties of the user added under **Full Access** option.
9. Click **Save**.
10. Close the dialog box and click **Save**.

NOTE: The changes made to MailBox delegation settings for the Office 365 user can be verified in the Microsoft Office 365 portal.

View or modify the Email Address settings for an Office 365 User

For an existing Office 365 user, you can use the E-mail Address settings tab in the Exchange Online Properties wizard to view or set the email address settings.

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

To view or modify the email address settings for an Azure AD user

1. In the Exchange Online Properties wizard of an Office 365 user, click **E-mail Settings**.
2. To add email addresses, click **Add**.
3. In the E-mail Addresses dialog box, select the email address type, add the email address, and click **OK**.
4. To modify a selected email address, click **Edit**.
5. In the E-mail Addresses dialog box, edit the selected email address, and click **OK**.
6. To delete a selected email address, click **Remove**.
7. Click **Save**.
8. Close the dialog box and click **Save**.

NOTE: The changes made to email address settings for the Office 365 user can be verified in the Microsoft Office 365 portal.

View or modify the MailBox features for an Office 365 User

You can use the Exchange Features tab to manage a variety of mailbox features for the Office 365 mailbox user.

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

To view or modify the Mailbox features for an Office 365 user

1. In the Exchange Online Properties wizard of an Office 365 user, click **Mailbox Features**.

   The following mailbox features are displayed and can be managed for the Office 365 mailbox user:

   - **Exchange ActiveSync**: Allows the user to access the mailbox from a mobile device.
   - **Outlook Web App**: Allows the user to browse the mailbox with a cell phone or other wireless devices.
   - **MAPI**: Allows the user to access the mailbox from a MAPI client such as Microsoft Outlook.
   - **IMAP4**: Allows the user to access the mailbox from an IMAP4 client such as Outlook Express.
   - **POP3**: Allows the user to access the mailbox from a POP3 client such as Outlook Express.
   - **Archive**: If the mailbox is archive-enabled, you can view or change the archive properties.
2. Under Mailbox Features, select the required feature you want to enable or disable for the Office 365 mailbox user, and then click **Enable** or **Disable** respectively.
3. Click **Save**.
4. Close the dialog box and click **Save**.

NOTE: The changes made to MailBox Features for the Office 365 mailbox user can be verified in the Microsoft Office 365 portal.

View or modify the MailBox settings for an Office 365 User

For an existing Office 365 user, you can use the MailBox settings tab in the Exchange Online Properties wizard to view or modify the messaging records management settings.

NOTE: The modify option is applicable for Office 365 users in non-federated environment only.

To view or modify the messaging records management settings for an Office 365 user

1. In the Exchange Online Properties wizard of an Office 365 user, click **Mail Flow Settings**.
2. Under **Messaging Records Management**, click **Properties**.
3. To place the user mailbox on litigation hold, select the **Enable litigation hold** check box.
4. In the **Messaging records management description URL** text box, enter URL of the location where the deleted mailbox items are preserved and changes made to mailbox items are recorded.
5. In the **Comments** text box, enter the mailbox comments.
6. Click **Save**.
7. Close the dialog box and click **Save**.

NOTE: The changes made to MailBox settings for the Office 365 user can be verified in the Microsoft Office 365 portal.

Azure AD user management tasks using Management Shell interface

Active Roles enables you to perform the following management tasks for Azure AD users:

- Create a new Azure AD user
- Update the Azure AD user properties
- View the Azure AD user properties
- Delete an Azure AD user

Active Roles Management Shell enables you to perform the following management tasks for Azure AD users:

Create a new Azure AD user

You can use the Active Roles Management Shell to create a new user. To create a new user, on the Management Shell interface, run the **New-QADUser** cmdlet. Use this cmdlet with the additional Boolean parameters *AzureUserAccountEnabled* and *AzureOffice365Enabled* to create and enable a new Azure AD user. To retrieve and update Azure properties *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

Create 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'
```

Example

You can add 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' -attr @
{edsaAzureUserGivenName='user64';edsaAzureUserUsageLocation='IN'}
```

Update the Azure AD user properties

You can use the Active Roles Management Shell to modify attributes of an Azure AD user in Active Directory. 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: Set-QADUser cmdlet does not work for Azure attributes in Synchronized and Federated environment.

View the Azure AD user properties

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

You can use the Active Roles Management Shell to delete a user from Azure. To delete an Azure AD user, 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.

Office 365 license management for hybrid environment users

Active Roles enables you to perform the following Office 365 license management tasks for hybrid users:

- Assign Office 365 licenses to new hybrid users
- Assign Office 365 licenses to existing hybrid users
- Modify or remove Office 365 licenses assigned to hybrid users
- Update Office 365 licenses display names
- Office 365 Granular user license management

Assign Office 365 licenses to new hybrid users

To assign Office 365 license to new hybrid users

1. On the Active Roles Web interface, Create a new Azure AD user.
2. In the **Create Azure Account**| **Usage Location** field, enter the two-letter location code of the location where the product will be used.

NOTE: The **Usage Location** field is a mandatory field. The licenses cannot be assigned to the user if the product usage location information is not available. The local rules and regulations for usage of the product and services may vary based on the location.

3. Click **Next**.

   The **Licenses** wizard displays the Office 365 licenses, for example the Office 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 corresponding to the licenses that need to be assigned to the user, and click **Finish**.

   The licenses assigned can be viewed on the user's**Azure Properties**| **Licenses** wizard.

Assign Office 365 licenses to existing hybrid users

To assign Office 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 check-box corresponding to 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 box for the user is displayed.
5. In the Azure Properties dialog box, click **Settings.**
6. If the usage location is not entered in the **Usage Location** field, enter the two-letter location code of the location where the product will be used, and click **Save**.

   NOTE: The **Usage Location** field is a mandatory field. The licenses cannot be assigned to the user if the product usage location information is not available. The local rules and regulations for usage of the product and services may vary based on the location.

   Alternatively, if the product usage location is entered for the user earlier, navigate to the **Licenses** wizard to assign the Office 365 license to the user.
7. Re-open the Azure Properties dialog box for the user, and click **Licenses.**

   The Licenses wizard displays the Office 365 licenses, for example Office 365 Business Essentials and Business Premium licenses, that are available for assigning to the user.
8. Select the check box corresponding to the license that is to be assigned to the user.
9. Click the drop-down arrow corresponding to the selected license to view the products included in the license.

   By default, all the products are enabled for the user.
10. De-select the check boxes corresponding to the products in the license that are to be disabled for the user.
11. Click **Save**.

Modify or remove Office 365 licenses assigned to hybrid users

To modify or remove the Office 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 check-box corresponding to 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 box, click **Licenses.**

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

   The products that are included and assigned to the user in the license are displayed.
7. Select or de-select the check box corresponding to the product included in the license that needs to be enabled or removed for the user.
8. Click **Save**.

NOTE:

- When a user is de-provisioned or deleted, all the licenses that were assigned to the user are removed and can be assigned to other hybrid users.
- On performing an undo-deprovision operation on a hybrid user, the license assignment gets restored to the user on successful completion of the operation.
- For information on Azure AD user De-provisioning policy for Office 365 licenses management see the Office 365 Licenses Retention section in the *Active Roles Administration Guide*.

Update Office 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, go to **..\One Identity\Active Roles\7.3\Service\AzureLicenses.xml**..
2. Open the xml file and edit the required SKU with the new license display name.

NOTE: If the xml file with Azure licenses is not available or 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 licenses display names can be viewed on the user's **Azure Properties| Licenses** wizard.

Office 365 Granular user license management

Office 365 license assignment to Azure AD users is controlled or restricted by creating a new provisioning policy and applying the policy to the Organizational Unit.

To create and apply the new policy

1. From the Active Roles Console, create a Policy Object. For instructions on creating a policy object, see the section **Creating a Policy Object**, in the *Active Roles Administration Guide*.

NOTE: In Active Roles Console, select **Office 365 License Management** as the **Policy to Configure** page.

2. From the Web interface, assign or modify the Office 365 license for an Azure AD User.

   The Policy is triggered for any Azure AD user in the Organization Unit for which the **Office 365 License Management** policy is applied.

   If the policy conditions are not satisfied while assigning or modifying Azure AD User licenses, the following policy violation error is displayed:

   Provisioning policy failure. The Office365 License Management policy encountered an error. Excepton in Office365 License Management Policy violation: The Azure user License(s) O365_BUSINESS_ESSENTIALS-INTUNE_O365, can be assigned. The policy prescribes that this Azure User requires only the specified license in the policy object to be assigned.

3. To check for policy violations, access the object in the Active Roles Console, right-click and click **Check Policy**.

   For a container object, this displays the **Check Policy** dialog box.

4. Review the options in the Check Policy dialog box and click **OK**.

   The Policy Check Results window is displayed.

NOTE: For information on Azure AD user provisioning policy for Office 365 licenses management see the Office 365 License Management section in the *Active Roles Administration Guide*.

Managing Office 365 Contacts

The Active Roles web interface enables you to perform administrative tasks such as create, read, update, and delete Office 365 contacts in Hybrid environment. You can also perform other operations such as add and remove Office 365 contacts to Groups.

Office 365 contact management tasks using Web interface

Active Roles web interface enables you to perform the following management tasks for Office 365 contacts:

- Create a new Office 365 contact
- Modify the Office 365 Contact Properties
- View the Change History for an Office 365 contact
- Delete an Office 365 contact

Create a new Office 365 contact

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

To create a new Office 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 need to create a new contact.
4. In the list of objects displayed, click the required **Container** or the **Organizational Unit**.
5. In the **Command** pane, click **New Contact**.
6. In the **New Conatct in <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** option.
9. In the **External e-mail address** field, enter the email address for the contact, and click **Finish**.

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

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

Modify the Office 365 Contact Properties

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

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

View the Change History for an Office 365 contact

You can use the Active Roles Web Interface to view the Change History for an Office 365 contact.

To view the Change History of an Office 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**.

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

Delete an Office 365 contact

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

To delete an Office 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 to be deleted.
4. In the **Command** pane, click **Delete**.

   The contact is deleted.

Managing Hybrid AD Groups

Active Roles provides the facility to perform administrative tasks such as create, read, update, and delete Groups in Azure AD through web interface. You can also perform other operations like 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 interfcae.The following section guides you through the Active Roles web interface and Management Sell to manage Azure AD groups.

- Azure AD Group management tasks using the Web interface
- Azure AD Group management tasks using Management Shell interface

Azure AD Group management tasks using the Web interface

Active Roles enables you to perform the following management tasks for Azure AD groups:

- Create an Azure AD group
- View or modify Azure AD group properties
- Add or remove members to an Azure AD group
- View the Change History for an Azure AD Group
- Delete an Azure AD group

Create an Azure AD group

You can use the Active Roles Web Interface to create and enable a new Azure AD group.

To create a new Azure AD 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 domain in which you need to create a new group.
4. In the list of objects displayed, click the required **Container** or the **Organizational Unit**.
5. In the **Command** pane, click **New Group**.
6. In the **General** properties **New Group in <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 the option **Create Azure Group**.

   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 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.

View or modify Azure AD group properties

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

To view or modify the Azure AD group 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 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. Use the tabs in the **Azure Properties** wizard to view or modify properties of the Azure AD group.
6. After setting all the required properties, click **Save**.

Add or remove members to an Azure AD group

You can use the Active Roles Web Interface to add or remove members from an Azure AD group.

To add a member to an Azure AD 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 group to which you want to add members.
4. Select the check-box corresponding to 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, click **Add** to add a user to the group.
6. In the **Select Object** wizard, search and select the members you want to add to the group.

   NOTE: Click **Temporal Membership Settings** to specify the date and time when the selected members should be added or removed from the group.
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

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 from which you want to remove a member.
4. Select the check-box corresponding to the member 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 to be removed 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.

View the Change History for an Azure AD Group

You can use the Active Roles Web Interface to view the Change History for an Azure AD group.

To view the Change History of an Azure AD 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.
4. In the **Command** pane, click **Change History**.

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

Delete an Azure AD group

You can use the Active Roles Web Interface to delete an Azure AD group.

To delete an Azure AD 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 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.

   NOTE: Deleting a group account is an irreversible operation. A new group account with the same name as a deleted group account does not automatically assume the permissions and memberships of the deleted account. For this reason, it is advisable to disable rather than delete accounts.

Azure AD Group management tasks using Management Shell interface

Active Roles enables you to perform the following management tasks for Azure AD groups using the Management Shell interface:

- Create a new Azure AD Group
- Update the Azure AD Group properties
- Delete an Azure AD group

Active Roles Management Shell enables you to perform the following management tasks for Azure AD users:

Create a new Azure AD Group

You can use the Active Roles Management Shell to create a new user. To create a new group, on the Management Shell interface, run the **new-qadGroup** cmdlet. Use this cmdlet with the additional Boolean parameter **AzureOffice365Enabled** to create and enable a new Azure AD group.

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

Update the Azure AD Group properties

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

Delete an Azure AD group

You can use the Active Roles Management Shell to delete an Azure AD group. To delete an Azure AD group, 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*.

About us

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

Contacting us

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

Technical support resources

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

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

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