INTEGRATION PACK FOR MICROSOFT ENTRA ID

For Microsoft System Center Orchestrator

For System Center 2016 and 2019, you must use the 32-bit version of the integration pack, which has the name **Kelverion_Integration_Pack_for_Microsoft_Entra_ID_3.1**

For System Center 2022 and later, you must use the 64-bit version of the integration pack, which has the name **Kelverion_IP_Microsoft_Entra_ID_x64_3.1**

User Guide

Version 3.1

Kelverion Integration Pack for Microsoft Entra ID

Released: December 2023

Feedback

Send suggestions and comments about this document to support@kelverion.com

Contents

Kelverion Integration Pack for Microsoft Entra ID

The Integration Pack for Microsoft Entra ID is an add-on for System Center Orchestrator that enables you to integrate and automate user management functionality in your Entra ID environment.

System Requirements

The Integration Pack for Microsoft Entra ID requires the following software to be installed and configured prior to implementing the integration. For more information about installing and configuring Orchestrator and Microsoft Entra ID, refer to the respective product documentation.

Kelverion_Integration_Pack_for_Microsoft_Entra_ID (32-bit)

- Microsoft System Center Orchestrator 2016, 2019
- Microsoft .NET Framework 4.6.2
- Microsoft Azure or Office 365 Subscription

Kelverion_Integration_Pack_for_Microsoft_Entra_ID (64-bit)

- Microsoft System Center Orchestrator 2022
- Microsoft .NET Framework 4.6.2
- Microsoft Azure or Office 365 Subscription

Registering and Deploying the Integration Pack

After you download the integration pack file, you must register it with the Orchestrator management server and then deploy it to Runbook Servers and Runbook Designers. For more information about how to install integration packs, see the How to Install an Integration Pack (https://technet.microsoft.com/en-us/library/hh420346.aspx).

IMPORTANT: Ensure that you are deploying the correct version of the Integration Pack.

- For System Center 2016 and 2019, you must use the 32-bit version of the integration pack, which has the name **Kelverion_Integration_Pack_for_Microsoft_Entra_ID**
- For System Center 2022 and later, you must use the 64-bit version of the integration pack, which has the name **Kelverion_IP_Microsoft_Entra_ID_x64**

To register the integration pack:

1. On the management server, copy the **.OIP** file for the integration pack to a local hard drive or network share.
2. Confirm that the file is not set to **Read Only** to prevent unregistering the integration pack later.
3. Start the **Deployment Manager**.
4. In the navigation pane of the Deployment Manager, expand **Orchestrator Management Server**, right-click **Integration Packs** to select **Register IP with the Orchestrator Management Server**. The **Integration Pack Registration Wizard** opens.

5. Click **Next**.
6. In the **Select Integration Packs or Hotfixes** dialog box, click **Add**.
7. Locate the **.OIP** file that you copied locally from step 1, click **Open** and then click **Next**.
8. In the **Completing the Integration Pack Wizard** dialog box, click **Finish**.
9. On the **End User Agreement** dialog box, read the Kelverion License Terms**,** and then click **Accept**.
10. The **Log Entries** pane displays a confirmation message when the integration pack is successfully registered.

To deploy the integration pack:

1. In the navigation pane of the **Deployment Manager**, right-click **Integration Packs**, click **Deploy IP to Runbook Server or Runbook Designer**.
2. Select the integration pack that you want to deploy, and then click **Next**.
3. Enter the name of the runbook server or computers with the Runbook Designer installed, on which you want to deploy the integration pack, click **Add**, and then click **Next**.
4. Continue to add additional runbook servers and computers running the Runbook Designer, on which you want to deploy the integration pack. Click **Next**.
5. In the **Installation Options** dialog box, configure the following settings.
6. To choose a time to deploy the integration pack, select the **Schedule installation** check box, and then select the time and date from the **Perform installation** list.
7. Click one of the following:
    a. **Stop all running runbooks before installing the integration pack** to stop all running runbooks before deploying the integration pack.
    b. **Install the Integration Packs without stopping the running Runbooks** to install the integration pack without stopping any running runbooks.
8. Click **Next**.
9. In the **Completing Integration Pack Deployment Wizard** dialog box, Click **Finish**.
10. When the integration pack is deployed, the **Log Entries** pane displays a confirmation message.

Licensing the Integration Pack

After you register and deploy the integration pack you must provide a valid Kelverion license before running any runbooks that contain activities from the integration pack

To deploy the integration pack license file to System Center Orchestrator 2019 or earlier:

1. Copy the .KAL license file to %PROGRAMFILES(X86)%\Kelverion Automation\Licenses
2. Repeat for each Orchestrator Runbook Server and Runbook Designer host system.

To deploy the integration pack license file to System Center Orchestrator 2022 or later:

1. Copy the .KAL license file to %PROGRAMFILES%\Kelverion Automation\Licenses

2. Repeat for each Orchestrator Runbook Server and Runbook Designer host system.

Configuring the Integration Pack

A connection establishes a reusable link between Orchestrator and a Microsoft Entra ID. You can create as many connections as you require by specifying links to multiple Entra ID accounts. You can also create multiple connections to the same AD to allow for differences in security permissions for different user accounts.

To set up a Microsoft Entra ID configuration:

1. In the Orchestrator Runbook Designer, click the **Options** menu, and select *KA Microsoft Entra ID*. The **KA Microsoft Entra ID** dialog box appears.
2. On the **Configurations** tab, click **Add** to begin the configuration setup. The **Add Configuration** dialog box appears.
3. In the **Name** box, enter a name for the configuration. This could be the name of the Microsoft Entra ID server or a descriptive name to distinguish the type of configuration.
4. Click the ellipsis button (…) next to the **Type** box and select ***Azure AD Configuration***.
5. In the **Tenant ID** box enter the tenant identifier for your Microsoft Entra ID environment.
6. In the **Client ID** box enter the client ID for the application that you registered in your Microsoft Entra ID environment, to communicate with the integration pack. For details, see Connecting to Entra ID.
7. **(Optional)** In the **Client Secret** box enter the client secret for the application identified in the **Client ID** box. When not specified, the integration pack will use the specified **Username** and **Password** credentials to connect to Microsoft Entra ID.

   Note: Integration pack activities that set user passwords, such as **Update User Password** and **Update User UPN**, must connect to Microsoft Entra ID using Username and Password. Using Client Secret credentials to perform these operations will result in the activities failing with insufficient privileges error.
8. **(Optional)** In the **Username** box enter a user with permissions to administer the Microsoft Entra ID environment. This should be a WAAD user from the domain you intend to manage with the IP, for example john.smith@mydomain.onmicrosoft.com. The integration pack will only use **Username** and **Password** to connect to Microsoft Entra ID when the **Client Secret** is not specified.
9. **(Optional)** In the **Password** box enter the password for user specified in **Username**.
10. Click **OK** to close the configuration dialog box, and then click **Finish**.

Connecting to Microsoft Entra ID

The Kelverion Integration Pack for Microsoft Entra ID is using the *Microsoft Graph REST API* to communicate with Microsoft Entra ID. You will need to create and configure an application in your Microsoft Entra ID environment, which will allow the integration pack to connect and communicate with Microsoft Entra ID. Once your app configuration is complete, you must provide the app registration settings in integration pack configuration options.

1. Create a new application. In your Entra ID, go to **App Registrations** and click **New Registration**. Type in a name for the new app, for example "Kelverion Integration Pack", and click **Register**.
2. After the application is created, copy the **Application (client) ID** from the **Overview** page, and enter it in the **Client ID** box, in your integration pack connection. See Configuring the Integration Pack.
3. Configure Authentication. In your app registration, under **Authentication**, enable **Allow Public Client Flows**, in the Advanced Settings section.
4. **(Optional)** Create a new client secret. In your app registration, under **Certificates & Secrets**, create a new client secret. Copy the secret value and enter it in the **Client Secret** box, in your integration pack connection. You can skip this step if you are planning for the integration pack to connect to Azure with Username and Password.
   Note: Integration pack activities that set user passwords, such as **Update User Password** and **Update User UPN**, must connect to Microsoft Entra ID using Username and Password credentials. Using Client Secret credentials to perform these operations will result in the activities failing with insufficient privilege errors.
5. Add permissions and grant consent. In your app registration, under **API Permissions**, configure the following Microsoft Graph permissions. Make sure to grant admin consent for each permission.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	Granted
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes	Granted
Directory.ReadWrite.All	Application	Read and write directory data	Yes	Granted
User.ReadWrite.All	Delegated	Read and write all users' full profiles	Yes	Granted
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	Granted

Microsoft Entra ID Activities

This integration pack adds the KA Microsoft Entra ID category to the **Activities** pane in the Client.

This Integration Pack contains the following activities:

- Add Group Member
- Add User
- Add User License
- Get Groups
- Get Group Members
- Get User
- Get User License
- Get Users
- Remove Group Member
- Remove User
- Remove User License
- Update User
- Update User Password
- Update User UPN

Common Configuration Instructions for All Activities

The following configuration instructions apply to all activities in this integration pack. Links to this section are included in the configuration instructions for each activity.

Activity Properties

Each activity has a set of required or optional properties that define the configuration of that activity. This includes how it connects to other activity or how the activity performs its actions. You can view or modify activity properties in the Orchestrator Client.

To configure the properties for an activity:

1. Double-click the activity. Alternatively, you can right-click the activity, and then click **Properties**.
2. To save your configuration entries, click **Finish**.

In the activity properties dialog box, several tabs along the left side provide access to general and specific settings for the activity. Although the number of available tabs for activity properties differs from activity to activity, all activities will have a **General** tab, a **Properties** tab and/or **Filters** tab, and a **Run Behavior** tab. Some activities may have additional tabs.

General Tab

This tab contains the **Name** and **Description** properties for the activity. By default, the **Name** of the activity is the same as its activity type, and the **Description** is blank. You can modify these properties to create more descriptive names or provide detailed descriptions of the actions of the activity.

Properties/Filters Tab

These tabs contain properties that are specific to the activity.

All activities in this integration pack have the **Configuration Name** property at the top of the **Properties** tab. This property is used to specify the connection to a Microsoft System Center.

To configure the Configuration Name property:

- Click the ellipsis **(…)** button next to the **Name** field, and then select the applicable connection name. Connections displayed in the list have been previously configured as described in Configuring the Microsoft System Center Connections.

Filter Behavior

The Monitor and Get activities use filters to determine the values that will invoke a runbook or retrieve activities. Property values of potential candidates are compared to the values of the filters to determine if they meet the criteria. When matching against values, you select one of the available methods of comparison. An option is provided to either match or not match the filter using each method. For example, the "Does not" version of a method causes alerts that do not match the filter to trigger the runbook.

- **Equals**: the property of the object exactly matches the text or number specified in the filter.

- **Does not equal**: the property of the object does not exactly match the text or number specified in the filter.
- **Is less than**: the property of the object is less than the number specified in the filter.
- **Is less than or equal to**: the property of the object is less than or equal to the number specified in the filter.
- **Is greater than**: the property of the object is greater than the number specified in the filter.
- **Is greater than or equal to**: the property of the object is greater than or equal to the number specified in the filter.
- **Contains**: the property of the object contains the exact text specified in the filter. Unlike the Equals behavior, there can be other text surrounding the matching text.
- **Does not contain**: the property of the object does not contain the exact text specified in the filter. Unlike the Equals behavior, there can be other text surrounding the matching text.
- **Starts with**: the property of the object starts with the exact text specified in the filter. Unlike the Equals behavior, there can be other text following the matching text.
- **Ends with**: the property of the object ends with the exact text specified in the filter. Unlike the Equals behavior, there can be other text preceding the matching text.
- **Matches**: the property of the object matches the regular expression specified in the filter.
- **Matches**: the property of the object does not match the regular expression specified in the filter.

Server-Side and Client-Side Filtering

Some of the integration pack activity filtering operations are performed server-side, through the capabilities provided by the Microsoft Graph REST API. The integration pack can also perform client-side filtering, for operations that are not supported by the API for server-side filtering. In the case of client-side filtering, larger data sets are first retrieved from Microsoft Entra ID, and then filtered down by the integration pack before publishing onto the Orchestrator data bus.

It is recommended that you use server-side filtering whenever possible, to reduce the amount of data that the integration pack retrieves from Microsoft Entra ID. Be sure to refer to activity inputs and filters, to determine which operations are supported for server-side filtering. If a filter operator is not specified in the list of server-side filters, then that filtering operation is performed client-side.

Run Behavior Tab

This tab contains the properties that determine how the activity handles multi-value published data and what notifications will be sent if the activity fails or runs for an excessive period of time.

Multi-Value Published Data Behavior

The Get activities retrieve information from another activity or outside source, and can return one or more values in the published data. For example, when you use the Get Collection Member activity, the data output from that activity might be a list of computers that belong to the specified collection.

By default, the data from the Get activity will be passed on as multiple individual outputs. This invokes the next activity as many times as there are items in the output. Alternatively, you can

provide a single output for the activity by enabling the **Flatten** option. When you enable this option, you also choose a formatting option:

- **Separate with line breaks**. Each item is on a new line. This format is useful for creating human-readable text files for the output.
- **Separate with _** . Each item is separated by one or more characters of your choice.
- **Use CSV format**. All items are in CSV (comma-separated value) format. This format is useful for importing data into spreadsheets or other applications.

The activity will produce a new set of data every time it runs. The **Flatten** feature does not flatten data across multiple instances of the same activity.

Event Notifications

Some activities are expected to take a limited amount of time to complete. If they do not complete within that time they may be stalled or there may be another issue preventing them from completing. You can define the number of seconds to wait for completion of the action. After this period a platform event will be sent and the issue will be reported. You can also choose whether to generate a platform event if the activity returns a failure.

To be notified when the activity takes longer than a specified time to run or fails to run:

1. In the **Event Notifications** box, enter the **number of seconds** of run time before a notification is generated.
2. Select **Report if activity fails to run** to generate run failure notifications.

For more information about Orchestrator events, see the “Event Notifications " topics in the Runbook Properties (https://technet.microsoft.com/en-us/library/hh489610.aspx#Event Notifications).

Published Data

Published data is the foundation of a working runbook. It is the data produced as a result of the actions of an activity. This data is published to an internal data bus that is unique for each runbook. Subsequent activities in the runbook can subscribe to this data and use it in their configuration. Link conditions also use this information to add decision-making capabilities to runbooks.

An activity can only subscribe to data from the activities that are linked before it in the runbook. You can use published data to automatically populate the property values needed by activities.

To use published data:

1. Right-click the property value box, click **Subscribe**, and then click **Published Data**.
2. Click the **Activity** drop-down box and select the activity from which you want to obtain the data.
3. To view additional data elements common to all activities, select **Show Common Published Data**.
4. Click the published data element that you want to use, and then click **OK**.

For a list of the data elements published by each activity, see the Published Data tables in the activity topic. For information about the common published data items, see the Published Data (http://technet.microsoft.com/en-us/library/hh403821.aspx).

Add Group Member Activity

The **Add Group Member** activity is used in a runbook to assign a new member to an existing group.

Note: *This activity starts the member assignment operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Group Object ID	Identifies the group to which the member is to be added.
Group Member Object ID	Identifies the member that will be added to the group.

Add User Activity

The **Add User** activity is used in a runbook to add new users to your Microsoft Entra ID environment.

Note: *This activity starts the user creation operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Display Name	The display name of the user.
Mail Alias	The mail alias for the user. Maximum length is 64 characters.
Password	The new password for the user. The password must satisfy the strong password requirements according to the **Strong Password Required** setting. For more details see Microsoft Entra ID password policies.
Password Confirm	Confirm the user Password.
User Principal Name	The UPN of the new user.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

Alternate Email Addresses	Alternate email addresses for the user. Separate multiple values with comma (,) character.
Block Credential	When true, the user will not be able to log on using their user ID. Defaults to false when not specified.
City	The city of the user.
Country	The country of the user.
Department	The department of the user.

Fax	The fax number of the user.
First Name	The first name of the user.
Force Change Password	When true, the user will be required to change their password the next time they sign in.
Immutable ID	The immutable ID of the user's federated identity. This should be omitted for users with standard identities.
Last Name	The last name of the user.
Mobile Phone	The mobile phone number of the user.
Office	The office of the user.
Password Never Expires	Specifies whether or not the user's password will expire periodically. When not specified, password expiration will be in effect.
Phone Number	The office phone number of the user.
Postal Code	The postal code of the user.
Preferred Language	The preferred language of the user. Should follow ISO 639-1 Code; for example "en-US".
State	The state or province where the user is located.
Street Address	The street address of the user.
Strong Password Required	Specifies whether or not the user requires a strong password. When not specified, a strong password is required.
Title	The job title of the user.
Usage Location	The location of the user where services are consumed. Must be a two-letter country code (ISO standard 3166).

Published Data

The activity also publishes the following properties:

User Principal Name	UPN of the user.
Object ID	Object ID of the user.

Add User License Activity

The **Add User License** activity is used in a runbook to assign one or more licenses to an existing Microsoft Entra ID user.

Note: *This activity starts the user creation operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Note: *The user Usage Location should be configured before adding the user license.*

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user is to be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.
License SKU ID	One or more licenses (Account SKU IDs) which are to be assigned to the user. Separate multiple values with comma (,) character. For more details on license SKU IDs see Product Names and Service Plan Identifiers for Licensing.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

Disabled Plans	Specifies one or more service plans IDs (GUIDs), which are to be disabled for the specified license. Separate multiple values with comma (,) character. ***Note:*** Disabled plans cannot be specified when **License SKU ID** property specifies multiple licenses.

Published Data

The activity also publishes the following properties:

User Principal Name	UPN of the user. Available only when *Identify By = User Principal Name*.
Object ID	Object ID of the user. Available only when *Identify By = Object ID*.

Get Groups Activity

The **Get Groups** activity is used in a runbook to retrieve Microsoft Entra ID groups.

Note: This activity supports both server-side and client-side filtering. It is recommended to use server-side filtering whenever possible, in order to minimize the volume of data retrieved from Microsoft Entra ID.

Optional Properties

You can use the following optional properties to control the behavior of the activity:

Descending	Specifies if the returned records are ordered in ascending or descending error. Only used when the **Order By** property is specified.
Group Type	Specifies the type of groups to be returned. Valid values are: • DistributionList • Security • MailEnableSecurity • Microsoft365 When not specified, the activity will return all group types.
Return Max Results	Specifies the maximum number of results to be returned.
Search String	Specifies a string for searching groups. Only groups with a display name starting with this value will be returned.
Object ID	Specifies the **Object ID** of a specific group to be returned.
Order By	Specifies the sort field for the returned records. Valid values are: • Display Name

Published Data

The activity also publishes the following properties:

Description	Group description.
Display Name	Group display name.
Email Address	Group email address.
Group Count	Number of group records returned by the activity.
Group Type	The group type. Valid values are: • DistributionList • Security • MailEnableSecurity • Microsoft365
Group Types	Comma(,) separated string collection denoting the group type and its membership. If this collection contains **Unified**, the group is a Microsoft 365 group, otherwise, it is either a security group or distribution group. Valid values are: • Unified

	• DynamicMembership For details, see Group Types in Microsoft Entra ID and Microsoft Graph.
Mail Enabled	Indicates if the group is mail-enabled.
Object ID	Group object ID.
Security Enabled	Indicates if the group is security enabled.

Filters

Use the following filters to determine which groups to retrieve.

Display Name	Filter by Display Name. Server-side operators: *Equals, Does not equal, Starts with*.
Email Address	Filter by Email Address. Server-side operators: *Equals, Does not equal, Starts with, Ends with*.
Group Types	Filter by Group Types containing the specified filter value. Server-side operators: *Contains, Does not contain*. Valid values are: • Unified • DynamicMembership
Mail Enabled	Filter by Mail Enabled. Server-side operators: *Equals, Does not equal*.
Security Enabled	Filter by Security Enabled. Server-side operators: *Equals, Does not equal*.

Get Group Members Activity

The **Get Group Members** activity is used in a runbook to retrieve members of a group.

Note: This activity supports both server-side and client-side filtering. It is recommended to use server-side filtering whenever possible, in order to minimize the volume of data retrieved from Microsoft Entra ID.

Required Properties

You must configure the following properties:

Group Object ID	Identifies the group for which to members are to be returned.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

Group Member Type	Specifies the type of group members to be returned. Valid values are: • User • Group

	When not specified, the activity will return all group member types.
Return Max Results	Specifies the maximum number of results to be returned.

Published Data

The activity also publishes the following properties:

Display Name	Member display name.
Email Address	Member email address.
Group Member Count	Number of group member records returned by the activity.
Group Member Type	Member type.
Group Member Object ID	Group member object ID.
Is Licensed	Indicates if this is the member is licensed or not.

Filters

Use the following filters to determine which group members to retrieve:

Display Name	Filter by Display Name. Server-side operators: *Equals, Does not equal, Starts with*.
Email Address	Filter by Email Address. Server-side operators: *Equals, Does not equal, Starts with, Ends with*.
Is Licensed	Filter licensed members. Server-side operators: none, client-side only.
Group Member Object ID	Filter by member Object ID. Server-side operators: *Equals*.

Get User Activity

The **Get User** activity is used in a runbook to retrieve a specific Microsoft Entra ID user.

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the specific user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.

Published Data

The activity also publishes the following properties:

Account Enabled	Indicates if the user account is enabled or not.
Alternate Email Addresses	Alternate email addresses for the user.
Assigned Licenses	List of license SKU IDs that the user has been assigned.
Block Credential	Specifies whether user credentials are blocked or not.
City	Specifies user city.
Country	Specifies user country.
Department	Specifies user department.
Display Name	User display name.
Fax	User fax number.
First Name	User first name.
Immutable ID	The immutable ID of the user's federated identity.
Is Licensed	Specifies whether this user is licensed or not.
Last Name	User last name.
Last Password Change Timestamp	Date and time when user password was last changed.
Mobile Phone	User mobile phone number.
Object ID	User Object ID.
Office	Specifies office of the user.
Password Never Expires	Specifies whether or not user password never expires.
Password Reset Not Required During Activate	Specifies whether or not user password reset is not required during activate.
Phone Number	User phone number.
Postal Code	User postal code.
Preferred Language	User preferred language.
State	User state.
Street Address	User street address.
Strong Password Required	Specifies whether or not this user requires a strong password.
Title	User title.
Usage Location	The location of the user where services are consumed.
User Count	Number of user records returned by the activity.
User Principal Name	User UPN.
User Type	User Type.
When Created	Date and time when user was created.

Get User License Activity

The **Get User License** activity is used in a runbook to retrieve licenses assigned to a specific Microsoft Entra ID user.

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.

Published Data

The activity also publishes the following properties:

License Count	Number of license records returned by the activity.
License SKU ID	License SKU identifier.
Object ID	Object ID of the user.
SKU Part Number	Specifies the SKU part for the license.
User Principal Name	UPN of the user.

Filters

Use the following filters to select which user licenses to retrieve:

SKU Part Number	Filter by user SKU Part Number. Server-side filters: none, all client-side.
License SKU ID	Filter by user License SKU ID. Server-side filters: none, all client-side.

Get Users Activity

The **Get Users** activity is used in a runbook to retrieve and filter users from your Microsoft Entra ID environment.

Note: This activity supports both server-side and client-side filtering. It is recommended to use server-side filtering whenever possible, in order to minimize the volume of data retrieved from Microsoft Entra ID.

Optional Properties:

You must configure the following properties:

City	When specified, the activity will only return results with this city.
Country	When specified, the activity will only return results with this country.
Department	When specified, the activity will only return results with this department.
Descending	
Enabled Status	Specifies whether the activity should return only enabled users, only disabled users, or all users.
Order By	
Return Max Results	Specifies the maximum number of results to be returned, when *Return All Results* is set to *False.*
Search String	Specifies a string to search for users. Only users with an email address or display name starting with this string will be returned.
State	When specified, the activity will only return results with this state.
Title	When specified, the activity will only return results with this title.
Unlicensed Users	Specifies whether the activity should return or not only the users who are not assigned a license.
Usage Location	The filter for the country where the user consumes the services. This must be a two-letter country code.

Published Data

The activity also publishes the following properties:

Account Enabled	Indicates if the user account is enabled or not.
Alternate Email Addresses	Alternate email addresses for the user.
Assigned Licenses	List of license SKU IDs that the user has been assigned.
Block Credential	Specifies whether user credentials are blocked or not.
City	Specifies user city.
Country	Specifies user country.
Department	Specifies user department.

Display Name	User display name.
Fax	User fax number.
First Name	User first name.
Immutable ID	The immutable ID of the user's federated identity.
Is Licensed	Specifies whether this user is licensed or not.
Last Name	User last name.
Last Password Change Timestamp	Date and time when user password was last changed.
Mobile Phone	User mobile phone number.
Object ID	User Object ID.
Office	Specifies office of the user.
Password Never Expires	Specifies whether or not user password never expires.
Password Reset Not Required During Activate	Specifies whether or not user password reset is not required during activate.
Phone Number	User phone number.
Postal Code	User postal code.
Preferred Language	User preferred language.
State	User state.
Street Address	User street address.
Strong Password Required	Specifies whether or not this user requires a strong password.
Title	User title.
Usage Location	The location of the user where services are consumed.
User Count	Number of user records returned by the activity.
User Principal Name	User UPN.
User Type	User Type.
When Created	Date and time when user was created.

Filters

Use the following filters to determine which users to retrieve:

Account Enabled	Filter enabled/disabled user accounts. Server-side filters: *Equals, Does not equal*.
Block Credential	Filter users with blocked credentials. Server-side filters: *Equals, Does not equal*.
City	Filter by user city. Server-side filters: *Equals, Does not equal, Starts with*.
Country	Filter by user country. Server-side filters: *Equals, Does not equal, Starts with*.
Department	Filter by user department. Server-side filters: *Equals, Does not equal, Starts with*.
Display Name	Filter by user display name. Server-side filters: *Equals, Does not equal, Starts with*.
Email Address	Filter by user email address. Server-side filters: *Equals, Does not equal, Starts with, Ends with*.
Fax	Filter by user fax number. Server-side filters: *Equals, Does not equal, Starts with*.
First Name	Filter by user first name. Server-side filters: *Equals, Does not equal, Starts with*.
Immutable ID	Filter by immutable ID value. Server-side filters: *Equals, Does not equal*.
Is Licensed	Filter users that are licensed or not. Server-side filters: *Equals, Does not equal*.
Last Name	Filter by user last name. Server-side filters: *Equals, Does not equal, Starts with*.
Last Password Change Timestamp	Filter by user DateTime value when user password was last changed. Server-side filters: none, all client-side.
Mobile Phone	Filter by user mobile phone value. Server-side filters: *Equals, Does not equal, Starts with*.
Object ID	Filter by user Object ID. Server-side filters: *Equals*.
Office	Filter by user office. Server-side filters: *Equals, Does not equal, Starts with*.
Password Never Expires	Filter by user Password Never Expires value. Server-side filters: none, all client-side.

Password Reset Not Required During Activate	Filter by user Password Reset Not Required During Activate value. Server-side filters: none, all client-side.
Phone Number	Filter by user phone number. Server-side filters: *Equals, Does not equal*.
Postal Code	Filter by user postal code. Server-side filters: *Equals, Does not equal, Starts with*.
Preferred Language	Filter by user Preferred Language. Server-side filters: *Equals, Does not equal, Starts with*.
State	Filter by user state. Server-side filters: *Equals, Does not equal, Starts with*.
Street Address	Filter by user street address. Server-side filters: *Equals, Does not equal, Starts with*.
Strong Password Required	Filter by user Strong Password Required value Server-side filters: none, all client-side.
Title	Filter by user title. Server-side filters: *Equals, Does not equal, Starts with*.
Usage Location	Filter by user Usage Location. Server-side filters: *Equals, Does not equal, Starts with*.
User Principal Name	Filter by user UPN. Server-side filters: *Equals, Does not equal, Starts with, Ends with*.
User Type	Filter by User Type. Valid values are: • Member • Guest • Viral • Other Server-side filters: *Equals, Does not equal*.
When Created	Filter by user created DateTime. Server-side filters: *Equals, Does not equal, Is greater than, Is greater than or equal to, Is less than, Is less than or equal to*.

Remove Group Member Activity

The **Remove Group Member** activity is used in a runbook to remove a member from a group.

Note: *This activity starts the member removal operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Group Object ID	Identifies the group from which the member will be removed.
Group Member Object ID	Identifies the member that is to be removed from the group.

Remove User Activity

The **Remove User** activity is used in a runbook to remove users from your Microsoft Entra ID environment.

Note: *This activity starts the user removal operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Object ID	The Object ID of the user to be removed.

Published Data

The activity also publishes the following properties:

Object ID	Object ID of the user.

Remove User License Activity

The **Remove User License** activity is used in a runbook to remove one or more licenses from an existing Microsoft Entra ID user.

Note: *This activity starts the license removal operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.
License SKU ID	One or more licenses (SKU IDs) which are to be removed from the user. Separate multiple values with comma (,) character.

Published Data

The activity also publishes the following properties:

User Principal Name	UPN of the user.
Object ID	Object ID of the user.

Update User Activity

The **Update User** activity is used in a runbook to update properties of existing users in your Microsoft Entra ID environment.

Note: *This activity starts the user update operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

Alternate Email Addresses	Alternate email addresses for the user. Separate multiple values with comma (,) character.
Block Credential	When true, the user will not be able to log on using their user ID.
City	The city of the user.
Country	The country of the user.
Department	The department of the user.
Fax	The fax number of the user.
First Name	The first name of the user.
Immutable ID	The immutable ID of the user's federated identity. This should be omitted for users with standard identities.
Last Name	The last name of the user.
Mobile Phone	The mobile phone number of the user.
Office	The office of the user.
Password Never Expires	Sets whether or not the user's password will expire periodically.
Phone Number	The phone number of the user.
Postal Code	The postal code of the user.
Preferred Language	The preferred language of the user.
State	The state where the user is located.
Street Address	The street address of the user.

Strong Password Required	Sets whether or not the user requires a strong password.
Tenant ID	The unique ID of the tenant to perform the operation on. If this is not provided, then the value will default to the tenant of the current user.
Title	The title of the user.
Usage Location	The location of the user where services are consumed. Must be a two-letter country code.

Published Data

The activity also publishes the following properties:

User Principal Name	UPN of the user. Available only when *Identify By = User Principal Name*.
Object ID	Object ID of the user. Available only when *Identify By = Object ID*.

Update User Password

The **Update User Password** activity is used in a runbook to update the password of an existing Microsoft Entra ID user.

Note: *This activity starts the user update operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Note: *This activity, must connect to Microsoft Entra ID with username and password configuration options. Using client secret credentials when running this activity will result in failure with insufficient privileges error.*

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.
Force Change Password	When true, the user will be required to change their password the next time they sign in.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

New Password	The new password for the user. The password must satisfy the strong password requirements according to the **Strong Password Required** user property. For more details see Microsoft Entra ID password policies.
New Password Confirm	Confirm the user Password.

Update User UPN

The **Update User UPN** activity is used in a runbook to update the UPN of an existing Microsoft Entra ID user.

Note: *This activity starts the user update operation. The operation may not be complete, and may continue, beyond the time when the activity execution finishes.*

Note: *This activity, must connect to Microsoft Entra ID with username and password configuration options, when updating the user password. Using client secret credentials when running this activity will result in failure with insufficient privileges error.*

Required Properties:

You must configure the following properties:

Identify By	Specifies whether the user will be identified by **Object ID** or **User Principal Name**.
Object ID	The Object ID of the user, when **Identify By** is set to **Object ID**.
User Principal Name	The UPN of the user, when **Identify By** is set to **User Principal Name**.
New User Principal Name	The new UPN for the user.

Optional Properties

You can use the following optional properties to further control the behavior of the activity:

Immutable ID	The immutable ID of the user's federated identity. This is required if moving the user from a standard to a federated identity domain.
New Password	The new password for the user. This property is required when moving the user from a federated to a standard identity domain. It has no effect when changing the UPN of a user in a standard identity domain.
New Password Confirm	Confirm the user Password.

Published Data

The activity also publishes the following properties:

New User Principal Name	New UPN of the user.