Oracle® Cloud

Using the Azure Active Directory Adapter with Oracle Integration 3

F86025-11
January 2025

Oracle Cloud Using the Azure Active Directory Adapter with Oracle Integration 3,

F86025-11

Primary Author: Oracle Corporation

Contents

Preface

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

> **Note:**
>
> The use of this adapter may differ depending on the features you have, or whether your instance was provisioned using Standard or Enterprise edition. These differences are noted throughout this guide.

Topics:

Audience

This guide is intended for developers who want to use this adapter in integrations in Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `https://www.oracle.com/corporate/accessibility/`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and

the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

See these Oracle resources:

- Oracle Cloud at `http://cloud.oracle.com`
- *Using Integrations in Oracle Integration 3*
- *Using the Oracle Mapper with Oracle Integration 3*
- Oracle Integration documentation on the Oracle Help Center.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understand the Azure Active Directory Adapter

Review the following topics to learn about the Azure Active Directory Adapter and how to use it as a connection in integrations in Oracle Integration. A typical workflow of adapter and integration tasks is also provided.

Topics:

Azure Active Directory Adapter Capabilities

The Azure Active Directory Adapter enables you to create an integration in Oracle Integration that connects to the Azure Active Directory service. You can configure the Azure Active Directory Adapter as a trigger connection and an invoke connection in an integration in Oracle Integration.

The Azure Active Directory Adapter supports trigger connections with the following capabilities:

- Allows processing of notifications from Azure Active Directory to Oracle Integration.
- Provides support for performing the Create, Update, Delete, and Permanent Delete actions on the selected resource such as User and Group.
- Automatically renews webhook subscriptions every 29 days for activated integrations.
- Supports the Azure AD composite security policy: Digital Signature for incoming requests and OAuth 2.0 Client Credentials for outgoing calls.

The Azure Active Directory Adapter supports invoke connections with the following capabilities:

- Provides support to execute GET operations with query options such as $count, $expand, $filter, $orderby, $search, $select, and $top that are compatible with the OData version 4 query language. You can execute one query or a combination of queries at a time.
- Supports a connectivity agent to provide connectivity with all Azure Active Directory service offerings.
- Supports business objects: User, Organization, Application, and Groups.
- Provides support for performing Create, Update, Get, List, Delete, Add, Remove, and so on operations on the selected business object.
- Retrieves multiple objects from Azure Active Directory through the List operation.
- Retrieves specific objects within Azure Active Directory using the Get operation.
- Supports pagination.

- Supports OAuth 2.0 security policies, including Client Credentials and Authorization Code Credentials for public gateway access.
- Supports Client Credentials as the security policy for accessing an endpoint using a connectivity agent.
- Supports extension attributes: Manage up to 15 extension attributes (`extensionAttributes1` to `extensionAttributes15`) for user objects, allowing storage of additional organization-specific information.
- Supports custom security attributes: Define and manage up to 500 custom security attributes with support for strings, integers, and booleans, offering flexibility for user categorization and other custom scenarios.

The Azure Active Directory Adapter is one of many predefined adapters included with Oracle Integration. See the Adapters page in the Oracle Help Center.

Support for Extension and Custom Security Attributes

The Azure Active Directory Adapter supports extension and custom security attributes.

Extension Attributes Support

The Azure Active Directory Adapter supports managing extension attributes. This feature allows you to use predefined fields to store additional organizational-specific information.

- Supported attributes: Up to 15 attributes are supported (`extensionAttributes1` to `extensionAttributes15`).
- Supported data types: Primarily string data types.
  Example: Store a department code using an attribute such as `extensionAttributes1` with a value such as `HR-001`.

Custom Security Attributes Support

The Azure Active Directory Adapter allows you to define and manage custom security attributes, providing greater flexibility for your data integration needs.

- Supported attributes: Up to 500 custom security attributes.
- Supported data types: Strings, integers, and booleans.
  Example: Use a custom attribute such as `CertificationStatus` with a boolean value to track user certification status.

> **Note:**
>
> To remove the multivalued custom security attribute assignment, a null value must be passed while sending the request.

Azure Active Directory Adapter Restrictions

Note the following Azure Active Directory Adapter restrictions.

- The profile photos operation is not supported.

> **Note:**
>
> There are overall service limits for Oracle Integration. A service limit is the quota or allowance set on a resource. See Service Limits.

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the Connectivity Certification Matrix.

Workflow to Create and Add an Azure Active Directory Adapter Connection to an Integration

You follow a very simple workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

This table lists the workflow steps for both adapter tasks and overall integration tasks, and provides links to instructions for each step.

Step	Description	More Information
1	Create the adapter connections for the applications you want to integrate. The connections can be reused in multiple integrations and are typically created by the administrator.	Create an Azure Active Directory Adapter Connection
2	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Understand Integration Creation and Best Practices in *Using Integrations in Oracle Integration 3* and Add the Azure Active Directory Adapter Connection to an Integration
3	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration 3*
4	(Optional) Create lookups that map the different values used by those applications to identify the same type of object (such as gender codes or country codes).	Manage Lookups in *Using Integrations in Oracle Integration 3*
5	Activate the integration.	Activate an Integration in *Using Integrations in Oracle Integration 3*
6	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*
7	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in *Using Integrations in Oracle Integration 3*
8	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration 3*

2

Create an Azure Active Directory Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate.

Topics:

Prerequisites for Creating a Connection

You must satisfy the following prerequisites to create a connection with the Azure Active Directory Adapter:

Register an Application

Register an application in the Microsoft Entra admin center, and obtain the tenant ID and client ID.

1. Log in to the Microsoft Entra admin center (Azure AD).
2. Navigate to **Identity**, then **Applications**, and then to **App registrations**.
3. Click **New Registrations**.
4. Enter a name for the application, and select a supported account type.
5. Optionally, under **Redirect URI**, enter the redirect URI in the following format:

   ```
   https://OIC_instance_URL/icsapis/agent/oauth/callback
   ```

   > **Note:**
   >
   > A redirect URI is only required if you want to configure Authorization Code Credentials security policy for your Azure Active Directory connection.

6. Click **Register**.

   The tenant ID and client ID are displayed.

7. Copy the values for the tenant ID and client ID.

   You'll need to enter those values on the Connections page when you configure security for your Azure Active Directory Adapter connection in Oracle Integration. See Configure Connection Security.

Create a New Client Secret

Create a new client secret.

1. Log in to the Microsoft Entra admin center.
2. Navigate to **Identity**, then **Applications**, and then to **App registrations**.
3. Select the application that you registered. See Register an Application.
4. Click **Certificates & secrets**.
5. Click **Client secrets**, and then click **New client secret**.
6. Enter a description of the secret, and select a duration.
7. Click **Add**.

   The client secret is displayed in the **Value** column.
8. Copy the client secret from the **Value** column.

   You'll need to enter the client secret on the Connections page when you configure security for your Azure Active Directory Adapter connection in Oracle Integration. See Configure Connection Security.

Assign API Permissions

You must grant API permissions to the application that you created in the Microsoft Entra admin center (Azure AD).

1. Log in to the Microsoft Entra admin center.
2. Navigate to **Identity**, then **Applications**, and then to **App registrations**.
3. Select the application that you registered. See Register an Application.
4. Click **API Permissions**.
5. Add the required permissions. See Microsoft Graph Permissions Reference.

> **Note:**
>
> You must have the mandated API permissions for the specific User, Group, Organization, and Application Business Object.

Refer to the following tables for the required permissions to create an Azure Active Directory Adapter connection.

Table 2-1 Permissions Required for Connections

Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
• User.ReadBasic.All • User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All	Not supported.	• User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All

Table 2-2 Permissions Required for Invoke Actions

Business Object	Action	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
User	Create User	• User.ReadWrite.All • Directory.ReadWriteAll • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All	Not supported.	• User.ReadWrite.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All
	Update User	• User.ReadWrite • User.ManageIdentities.All • User.EnableDisableAccount.All • User.ReadWrite.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All	User.ReadWrite	• User.ManageIdentities.All • User.EnableDisableAccount.All • User.ReadWrite.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All

Table 2-2 (Cont.) Permissions Required for Invoke Actions

Business Object	Action	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
	Get a User	• User.Read • User.ReadWrite • User.ReadBasic.All • User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All	• User.Read • User.ReadWrite	• User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All
	List Users	• User.ReadBasic.All • User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All	Not supported.	• User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • CustomSecAttributeAssignment.Read.All • CustomSecAttributeAssignment.ReadWrite.All • CustomSecAttributeDefinition.Read.All • CustomSecAttributeDefinition.ReadWrite.All
	Delete a User	User.ReadWrite.All	Not supported.	User.ReadWrite.All
	List License Details	• LicenseAssignment.Read.All • Directory.Read.All • Directory.ReadWrite.All • User.Read • User.Read.All • User.ReadWrite.All	User.Read	Not supported.
	Assign and Remove User License	• LicenseAssignment.ReadWrite.All • Directory.ReadWrite.All • User.ReadWrite.All	Not supported.	• LicenseAssignment.ReadWrite.All • Directory.ReadWrite.All • User.ReadWrite.All

Table 2-2 (Cont.) Permissions Required for Invoke Actions

Business Object	Action	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
	List Manager	• User.Read.All • Directory.Read.All • Directory.ReadWrite.All • User.ReadWrite.All	Not supported.	Not supported.
	Get Member Objects User	• User.Read • User.Read.All • Directory.Read.All • User.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• User.Read.All • Directory.Read.All • User.ReadWrite.All • DirectoryReadWrite.All
	Get Member Objects Group	• GroupMember.Read.All • Group.Read.All • Directory.Read.All • Group.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• GroupMember.Read.All • Group.Read.All • Directory.Read.All • Group.ReadWrite.All • Directory.ReadWrite.All
	Create Invitation	• User.Invite.All • Directory.ReadWrite.All • User.ReadWrite.All	Not supported.	• User.Invite.All • Directory.ReadWrite.All • User.ReadWrite.All
	Assign Manager	• User.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• User.ReadWrite.All • Directory.ReadWrite.All
	Remove Manager	• User.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• User.ReadWrite.All • Directory.ReadWrite.All
	List Direct Reports	• User.Read • User.ReadBasic.All • Directory.ReadWrite.All • Directory.Read.All • User.ReadWrite.All • User.Read.All	Not supported.	• User.Read.All • User.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All
	Get Management Chain by ID	• User.Read.All • Directory.Read.All • Directory.ReadWrite.All • User.ReadWrite.All	Not supported.	Not supported.
Groups	Create Group	• Group.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• Group.Create • Directory.ReadWrite.All • Group.ReadWrite.All

Table 2-2 (Cont.) Permissions Required for Invoke Actions

Business Object	Action	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
	List Groups	• GroupMember.Read.All • Group.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • Group.Read.All	Not supported.	• GroupMember.Read.All • Directory.Read.All • Directory.ReadWrite.All • Group.Read.All • Group.ReadWrite.All
	Get Group	• GroupMember.Read.All • Group.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • Group.Read.All	Not supported.	• GroupMember.Read.All • Group.ReadWrite.All • Directory.Read.All • Directory.ReadWrite.All • Group.Read.All
	List Group Members	• GroupMember.Read.All • Directory.Read.All • Group.Read.All • Group.ReadWrite.All • GroupMember.ReadWrite.All	Not supported.	• GroupMember.Read.All • Directory.Read.All • Group.Read.All • Group.ReadWrite.All • GroupMember.ReadWrite.All
	Update Group	• Group.ReadWrite.All • Directory.ReadWrite.All	Not supported.	• Group.ReadWrite.All • Directory.ReadWrite.All
	Delete Group	Group.ReadWrite.All	Not supported.	Group.ReadWrite.All
	Add Members	GroupMember.ReadWrite.All	Not supported.	GroupMember.ReadWrite.All
	Remove Member	• GroupMember.ReadWrite.All • Directory.ReadWrite.All • Group.ReadWrite.All	Not supported.	• GroupMember.ReadWrite.All • Directory.ReadWrite.All • Group.ReadWrite.All
Organization	Get organization	• DeviceManagementServiceConfig.Read.All • DeviceManagementServiceConfig.ReadWrite.All • DeviceManagementConfiguration.Read.All • DeviceManagementConfiguration.ReadWrite.All	Not supported.	• DeviceManagementServiceConfig.Read.All • DeviceManagementServiceConfig.ReadWrite.All • DeviceManagementConfiguration.Read.All • DeviceManagementConfiguration.ReadWrite.All

Table 2-2 (Cont.) Permissions Required for Invoke Actions

Business Object	Action	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
Application	List Applications	• Application.Read.All • Application.ReadWrite.All • Directory.ReadWrite.All • Directory.Read.All	• Application.Read.All and User.Read • Application.ReadWrite.All and User.Read	• Application.Read.All • Application.ReadWrite.OwnedBy • Application.ReadWrite.All • Directory.Read.All

Table 2-3 Permissions Required for Trigger Resources

Resource	Delegated (Work or School Account) Permissions	Delegated (Personal Microsoft Account) Permissions	Application Permissions
User	User.Read.All	User.Read.All	User.Read.All
Group	Group.Read.All	Not supported	Group.Read.All

Create a Connection

Before you can build an integration, you must create the connections to the applications with which you want to share data.

To create a connection in Oracle Integration:

1. In the navigation pane, click **Design**, then **Connections**.
2. Click **Create**.

> **Note:**
>
> You can also create a connection in the integration canvas. See Define Inbound Triggers and Outbound Invokes.

3. In the Create connection panel, select the adapter to use for this connection. To find the adapter, scroll through the list, or enter a partial or full name in the **Search** field.
4. Enter the information that describes this connection.

Element	Description
Name	Enter a meaningful name to help others find your connection when they begin to create their own integrations.
Identifier	Automatically displays the name in capital letters that you entered in the **Name** field. If you modify the identifier name, don't include blank spaces (for example, `SALES OPPORTUNITY`).
Role	Select the role (direction) in which to use this connection. **Note**: *Only* the roles supported by the adapter you selected are displayed for selection. Some adapters support all role combinations (trigger, invoke, or trigger and invoke). Other adapters support fewer role combinations. When you select a role, only the connection properties and security policies appropriate to that role are displayed on the Connections page. If you select an adapter that supports both invoke and trigger, but select only one of those roles, you'll get an error when you try to drag the adapter into the section you didn't select. For example, assume you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an **invoke**. Dragging the adapter to a **trigger** section in the integration produces an error.
Keywords	Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
Description	Enter an optional description of the connection.

Element	Description
Share with other projects	**Note**: This field only appears if you are creating a connection in a project. Select to make this connection publicly available in other projects. Connection sharing eliminates the need to create and maintain separate connections in different projects. When you configure an adapter connection in a different project, the **Use a shared connection** field is displayed at the top of the Connections page. If the connection you are configuring matches the same type and role as the publicly available connection, you can select that connection to reference (inherit) its resources. See Add and Share a Connection Across a Project.

5. Click **Create**.

   Your connection is created. You're now ready to configure the connection properties, security policies, and (for some connections) access type.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.
2. In the **Tenant ID** field, enter the tenant ID that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

Configure Connection Security

Configure security for your Azure Active Directory Adapter connection.

1. Go to the **Security** section.
2. From the **Security Policy** list, select the security policy.
3. (Only for trigger connections) The **Security** field shows the **Azure AD Composite security policy**. This value cannot be changed.
   a. In the **Client Id** field, enter the client ID that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.
   b. In the **Client Secret** field, enter the client secret that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.
   c. In the **Shared Secret** field, enter a meaningful name or key. You can include English alphabetic characters, numbers, underscores, and hyphens.
4. (Only for invoke connections) From the **Security Policy** list, select the security policy.
   - **Client Credentials**: Select this security policy for public gateway access or accessing an endpoint using a connectivity agent.
   - **Authorization Code Credentials**: Select this security policy for public gateway access.
5. If you select **Client Credentials**:

a. In the **Client Id** field, enter the client ID that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

b. In the **Client Secret** field, enter the client secret that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

6. If you select **Authorization Code Credentials**:

a. In the **Client Id** field, enter the client ID that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

b. In the **Client Secret** field, enter the client secret that you obtained after performing the prerequisite steps. See Prerequisites for Creating a Connection.

c. In the **Scope** field, enter the required scopes. See Scopes and permissions in the Microsoft identity platform.

d. Click **Provide Consent** to verify the connection properties.

The Azure Active Directory log in page is displayed.

e. Enter your Azure Active Directory login credentials and click **Accept**.

f. Once you see an `Authenticated` message, you can test your connection.

Understand How the Azure Active Directory Adapter Works with the Connectivity Agent

Understand how the Azure Active Directory Adapter works with the connectivity agent.

- The Azure Active Directory Adapter supports the connectivity agent for invoke connections to provide connectivity with all Azure Active Directory service offerings.
- The Azure Active Directory Adapter does *not* support the connectivity agent for trigger connections.

Configure the Endpoint Access Type

Configure access to your endpoint. Depending on the capabilities of the adapter you are configuring, options may appear to configure access to the public internet, to a private endpoint, or to an on-premises service hosted behind a fire wall.

Select the Endpoint Access Type

Select the option for accessing your endpoint.

Option	This Option Appears If Your Adapter Supports ...
Public gateway	Connections to endpoints using the public internet.

Option	This Option Appears If Your Adapter Supports ...
Connectivity agent	Connections to on-premises endpoints through the connectivity agent. 1. Click **Associate agent group**. The Associate agent group panel appears. 2. Select the agent group, and click **Use**. To configure an agent group, you must download and install the on-premises connectivity agent. See Download and Run the Connectivity Agent Installer and About Creating Hybrid Integrations Using Oracle Integration in *Using Integrations in Oracle Integration 3*.

Test the Connection

Test your connection to ensure that it's configured successfully.

1. In the page title bar, click **Test**. What happens next depends on whether your adapter connection uses a Web Services Description Language (WSDL) file. Only some adapter connections use WSDLs.

If Your Connection...	Then...
Doesn't use a WSDL	The test starts automatically and validates the inputs you provided for the connection.
Uses a WSDL	A dialog prompts you to select the type of connection testing to perform: • **Validate and Test**: Performs a full validation of the WSDL, including processing of the imported schemas and WSDLs. Complete validation can take several minutes depending on the number of imported schemas and WSDLs. No requests are sent to the operations exposed in the WSDL. • **Test**: Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.

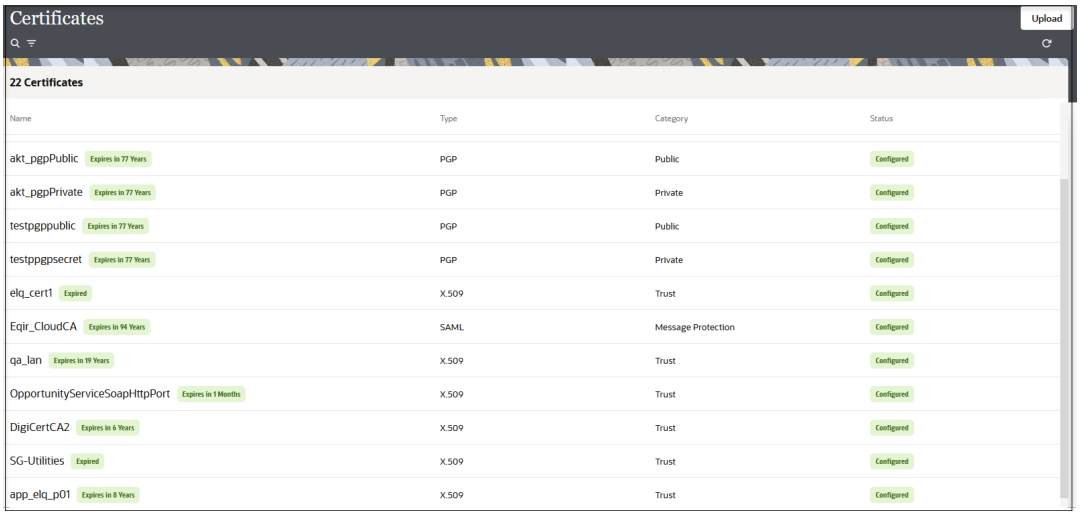
2. Wait for a message about the results of the connection test.
   - If the test was successful, then the connection is configured properly.
   - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload a Certificate to Connect with External Services

Certificates allow Oracle Integration to connect with external services. If the external service/endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception error is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

1. Sign in to Oracle Integration.
2. In the navigation pane, click **Settings**, then **Certificates**.
   All certificates currently uploaded to the trust store are displayed on the Certificates page.
3. Click **Filter** to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.



4. Click **Upload** at the top of the page.
   The Upload certificate panel is displayed.
5. Enter an alias name and optional description.
6. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
   - Digital Signature
   - X.509 (SSL transport)
   - SAML (Authentication & Authorization)
   - PGP (Encryption & Decryption)
   - Signing key

Digital Signature

The digital signature security type is typically used with adapters created with the Rapid Adapter Builder. See Learn About the Rapid Adapter Builder in Oracle Integration in *Using the Rapid Adapter Builder with Oracle Integration 3*.

1. Click **Browse** to select the digital certificate. The certificate must be an X509Certificate. This certificate provides inbound RSA signature validation. See RSA Signature Validation in *Using the Rapid Adapter Builder with Oracle Integration 3*.
2. Click **Upload**.

X.509 (SSL transport)

1. Select a certificate category.
   a. **Trust**: Use this option to upload a trust certificate.

i. Click **Browse**, then select the trust file (for example, `.cer` or `.crt`) to upload.

b. **Identity**: Use this option to upload a certificate for two-way SSL communication.

i. Click **Browse**, then select the keystore file (`.jks`) to upload.

ii. Enter the comma-separated list of passwords corresponding to key aliases.

> **Note:**
>
> When an identity certificate file (`.jks`) contains more than one private key, all the private keys must have the same password. If the private keys are protected with different passwords, the private keys cannot be extracted from the keystore.

iii. Enter the password of the keystore being imported.

c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available certificate category and cannot be deselected. Use this option to upload a keystore certificate with SAML token support. Create, read, update, and delete (CRUD) operations are supported with this type of certificate.
2. Click **Browse**, then select the certificate file (`.cer` or `.crt`) to upload.
3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for communication. PGP is used for signing, encrypting, and decrypting files. You can select the private key to use for encryption or decryption when configuring the stage file action.

a. **Private**: Uses a private key of the target location to decrypt the file.

i. Click **Browse**, then select the PGP file to upload.

ii. Enter the PGP private key password.

b. **Public**: Uses a public key of the target location to encrypt the file.

i. Click **Browse**, then select the PGP file to upload.

ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**.

- **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content.
- **No** causes the message to be sent in binary format.

iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text. The following supported cipher algorithms are FIPS-compliant:

- AES128
- AES192

- AES256
- TDES

c. Click **Upload**.

Signing key

A signing key is a secret key used to establish trust between applications. Signing keys are used to sign ID tokens, access tokens, SAML assertions, and more. Using a private signing key, the token is digitally signed and the server verifies the authenticity of the token by using a public signing key. You must upload a signing key to use the OAuth Client Credentials using JWT Client Assertion and OAuth using JWT User Assertion security policies in REST Adapter invoke connections. Only PKCS1- and PKCS8-formatted files are supported.

1. Select **Public** or **Private**.
2. Click **Browse** to upload a key file.
   If you selected **Private**, and the private key is encrypted, a field for entering the private signing key password is displayed after key upload is complete.
3. Enter the private signing key password. If the private signing key is not encrypted, you are not required to enter a password.
4. Click **Upload**.

Refresh Integration Metadata

You can manually refresh the currently-cached metadata available to adapters that have implemented metadata caching.

Metadata changes typically relate to customizations of integrations, such as adding custom objects and attributes to integrations. There may also be cases in which integrations have been patched, which results in additional custom objects and attributes being added. This option is similar to clearing the cache in your browser. Without a manual refresh, a staleness check is only performed when you drag a connection into an integration. This is typically sufficient, but in some cases you may know that a refresh is required. For these cases, the **Refresh Metadata** menu option is provided.

> **Note:**
>
> The **Refresh Metadata** menu option is only available with adapters that have implemented metadata caching.

1. In the navigation pane, click **Design**, then **Connections**.
2. Hover over the connection to refresh.
3. Click **Actions** ..., then select **Refresh metadata**.

   A message is displayed indicating that the refresh was successful.

3

Add the Azure Active Directory Adapter Connection to an Integration

When you drag the Azure Active Directory Adapter into the trigger or invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the Azure Active Directory Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the Azure Active Directory Adapter as a trigger or an invoke in an integration.

Topics:

Trigger Basic Info Page

Specify a name and description on the Basic Info page of each trigger connection in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and hyphens in the name. You can't include the following characters: • No blank spaces (for example, `My Inbound Connection`) • No special characters (for example, `#;83&` or `righ(t)now4`) except underscores and hyphens • No multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities.

Trigger Configuration Page

Specify the conditions that must be met for the trigger to run.

Element	Description
Select a Resource	Select a resource. The supported resources are: • **User** • **Group**

Element	Description
Available Options	Select an operation to perform for the selected resource, such as **Create**, **Update**, **Delete**, or **Permanent Delete**. The options available for selection are based on the resource selected.
Selected Options	Displays the selected options.
Subscription Expiry (in days)	Enter a value between `1` and `29`. The maximum expiration date for subscriptions per resource in Microsoft Graph is 29 days. **Note**: When setting an expiration date for **User** and **Group** resources, ensure that the selected date falls within a 29-day limit. Webhooks subscriptions expire in 29 days. The Azure Active Directory Adapter automatically renews webhook subscriptions every 29 days for activated integrations.
Subscription expiration date and time (UTC Time)	Displays a subscription expiration date based on the days selected in the **Subscription Expiry (in days)** field. It displays the date and time in the `YYYY-MM-DDTHH:MM:SS.SSS` format. For example, `2023-12-20T11:00:00Z`.

Invoke Basic Info Page

Specify a name, description, business object, and action type on the Basic Info page of each invoke connection in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and hyphens in the name. You can't include the following characters: • No blank spaces (for example, `My Inbound Connection`) • No special characters (for example, `#;83&` or `righ(t)now4`) except underscores and hyphens • No multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities.
Select Business Object	Select a business object: • **Application** • **Groups** • **Organization** • **User**
Action	Select the type of operation for this connection to perform, such as Create User, Assign Manager, Get Management Chain by id, Update Group, Delete Group, Add Members, Remove Member, Get Organization, List Applications, and so on. The operations available for selection are based on the business object selected.

Invoke Configuration Page

If the **Get Management Chain by Id** operation is selected on the Basic Info page, the Configuration page is displayed. Specify a numeric value and select the necessary options to execute the Get Management Chain by Id operation and receive a response.

Element	Description
Enter a numeric value for Manager Hierarchy Level (1-35)	Enter a number value between 1 and 35. The default value is 1.
Available Options	Select the Manager fields, such as **ID**, **Company Name**, **Assigned Plans**, and others to display in the response.
Selected Options	Displays the selected options.

Summary Page

You can review the specified adapter configuration values on the Summary page.

Element	Description
Summary	Displays a summary of the configuration values you defined on previous pages of the wizard. The information that is displayed can vary by adapter. For some adapters, the selected business objects and operation name are displayed. For adapters for which a generated XSD file is provided, click the XSD link to view a read-only version of the file. To return to a previous page to update any values, click the appropriate tab in the left panel or click **Go back**. To cancel your configuration details, click **Cancel**.

4

Implement Common Patterns Using the Azure Active Directory Adapter

You can use the Azure Active Directory Adapter to implement the following common pattern.

Topics:

> **Note:**
>
> Oracle Integration offers a number of prebuilt integrations, known as *recipes*, that provide you with a head start in building your integrations. You can start with a recipe, and then customize it to fit your needs and requirements. Depending upon the solution provided, a variety of adapters are configured in the prebuilt integrations. See the Recipes and Accelerators page on the Oracle Help Center.

Extract Employee Details from Workday and Create a New User in Azure Active Directory

This use case provides an overview of how to extract employee details from Workday and create a new user in Azure Active Directory.

This use case uses the following operations:

- **Enterprise Interface Builder (EIB-based Reports)**: Extracts the details of an employee from Workday.
- **Create User**: Creates a user in Azure Active Directory.

1. Create a schedule integration.
2. Drag and drop an assign action and create two variables:
   - `fileDir= "fileDir"`
   - `fileName= "filename"`
3. Add a scope and drag the Workday Adapter into the integration canvas.
4. Configure the Workday Adapter as follows:
   a. On the Basic Info page, name the adapter (for this example, `Launch_EIB`).
   b. On the Action page, select **Extract Bulk data from Workday**.
   c. On the RaaS/EIB Services page, select **Enterprise Interface Builder (EIB-based Reports)** as the type of Workday report.
   d. Select **Launch an EIB Integration** as the integration operation.
   e. Select an EIB integration configured in Workday.

5. Drag and drop an assign action and create a variable:

   ```
   status= Processing
   ```

6. Drag a while action and specify the condition as follows:

   ```
   status= Processing
   ```

7. Drag a wait action.
8. Drag a second Workday Adapter connection into the integration canvas and specify the following details in the Adapter Endpoint Configuration Wizard.
   a. On the Basic Info page, name the adapter (for this example, `Monitor_event`).
   b. On the Action page, select **Extract Bulk data from Workday**.
   c. On the RaaS/EIB Services page, select **Enterprise Interface Builder (EIB-based Reports)** as the type of Workday report.
   d. Select **Monitor EIB Integration Progress** as the integration operation.
9. Drag a switch action and specify the IF condition:

   ```
   ID= Completed AND type= Background_Process_Instance_Status_ID
   ```

10. Drag and drop an assign action and update the variable:

    ```
    status= Completed
    ```

11. Drag a third Workday Adapter connection outside the while action in the integration canvas.
12. Specify the following details in the Adapter Endpoint Configuration Wizard.
    a. On the Basic Info page, name the adapter (for this example, `extract_file`).
    b. On the Action page, select **Extract Bulk data from Workday**.
    c. On the RaaS/EIB Services page, select **Enterprise Interface Builder (EIB-based Reports)** as the type of Workday report.
    d. Select **Download file generated by EIB integration** as the integration operation.
13. Perform mapping for the Workday endpoints.
14. Drag and drop an assign action and update two variables with **fileDetails** from the Workday endpoint.
    - `fileDir = fileDir`
    - `filename = fileName`
15. Drag a stage file action. The stage file action reads the CSV format data from Oracle Integration at the downloaded location.
    a. Name the action.
    b. Specify the delimited data file name and directory name.
16. Drag a for-each action into the canvas, select **record** as the repeating element from the stage file response, provide a name, and provide a current element name.
17. Drag an Azure Active Directory Adapter into the integration canvas and configure it with the **Create User** action.

a. On the Basic Info page, provide a name.

b. Select **Business Object** as **User** and **Action** as **Create User**.

c. Review your selections on the Summary page.

18. In the mapper, perform the required mappings to create a user in Azure Active Directory.

19. Activate the integration.

5

Troubleshoot the Azure Active Directory Adapter

Review the following topic to learn about troubleshooting issues with the Azure Active Directory Adapter.

Topics:

Custom Security Attributes Support

As per the latest enhancements, new features have been introduced to support custom security attributes. For these newly added features, you need the following additional API permissions for User, Group, Organization, and Application Business Object.

- CustomSecAttributeAssignment.Read.All
- CustomSecAttributeAssignment.ReadWrite.All
- CustomSecAttributeDefinition.Read.All
- CustomSecAttributeDefinition.ReadWrite.All