

Oracle® Construction and Engineering Using the Oracle Primavera Unifier Adapter with Oracle Integration 3



F78935_03
December 2023



Oracle Construction and Engineering Using the Oracle Primavera Unifier Adapter with Oracle Integration 3,
F78935_03

Copyright © 1998, 2023, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

Contents

Preface

Audience	iv
Documentation Accessibility	iv
Diversity and Inclusion	iv
Related Resources	v
Conventions	v

1 Understand the Primavera Unifier Adapter

Primavera Unifier Adapter Capabilities	1-1
Primavera Unifier Adapter Restrictions	1-1
What Application Version Is Supported?	1-2
Workflow to Create and Add a Primavera Unifier Adapter Connection to an Integration	1-2

2 Create a Primavera Unifier Adapter Connection

Prerequisites for Creating a Connection	2-1
Create a Connection	2-1
Configure Connection Properties	2-2
Configure Connection Security	2-2
Test the Connection	2-3
Upload an SSL Certificate	2-3

3 Add the Primavera Unifier Adapter Connection to an Integration

Basic Info Page	3-1
Trigger BP Selection Page	3-3
Invoke BP Selection Page	3-3
Summary Page	3-4

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](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)

Audience

This guide is intended for developers who want to use the Primavera Unifier Adapter 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 in the Oracle Help Center.
- [Oracle Primavera Unifier Documentation](#) on 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.
<i>italic</i>	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 Primavera Unifier Adapter

Review the following topics to learn about the Oracle Primavera Unifier 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:

- [Primavera Unifier Adapter Capabilities](#)
- [Primavera Unifier Adapter Restrictions](#)
- [What Application Version Is Supported?](#)
- [Workflow to Create and Add a Primavera Unifier Adapter Connection to an Integration](#)

Primavera Unifier Adapter Capabilities

The Primavera Unifier Adapter enables you to set up a connection with Primavera Unifier. You can use this connection in integrations to connect with Unifier.

You can use the Unifier Adapter to fetch, create, or update a Business Process (BP) record (without attachments) in Unifier. It provides for an easy selection of the BP needed for integration. Based on the BP you select, the fields defined in the integration interface of that BP are available for mappings.

The Unifier Adapter provides trigger (inbound) and invoke (outbound) support. As a trigger, the adapter enables you to send the BP record data to Oracle Integration for further processing. As an invoke, the adapter enables you to create, update, and fetch records from and into Unifier.

The Unifier Adapter is one of many predefined adapters included with Oracle Integration. You can configure the Unifier Adapter as an invoke or trigger connection in an integration in Oracle Integration.

Primavera Unifier Adapter Restrictions

Note the following Primavera Unifier Adapter restrictions.

- The adapter does not support Business Process (BP) record data deletion in Unifier.
- The adapter supports synchronizing only one type of BP record at a time.

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 a Primavera Unifier 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	Access Oracle Integration.	Go to https://instance_URL/ic/home
2	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 a Primavera Unifier Adapter Connection
3	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Create Integrations in <i>Using Integrations in Oracle Integration 3</i> and Add the Primavera Unifier Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration 3</i>
5	(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 <i>Using Integrations in Oracle Integration 3</i>
6	Activate the integration.	Activate an Integration in <i>Using Integrations in Oracle Integration 3</i>
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in <i>Using Integrations in Oracle Integration 3</i>
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in <i>Using Integrations in Oracle Integration 3</i>

Step	Description	More Information
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration 3</i>

 **Note:**

Visit My Oracle Support (MOS) if you have a technical issue and/or if you have a question about the Primavera Unifier Adapter that you cannot resolve using information on the Manage Errors page.

2

Create a Primavera Unifier 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](#)
- [Create a Connection](#)
- [Upload an SSL Certificate](#)

Prerequisites for Creating a Connection

You must satisfy the following prerequisites to create a connection with the Primavera Unifier Adapter:

- **Create an account in Primavera Unifier:** Purchase a subscription to Primavera Unifier. When you subscribe, you receive the Primavera Unifier instance URL for your region and administrator credentials.
- **Set up an Integration User Account with OAuth or Basic Authentication Type:** An integration user account is a generic user account used to manage integrations between Unifier and other applications. You must set up an integration account with an OAuth-based or Basic authentication type. Refer to the [V1 and V2 OAuth Authentication Setup and Details](#) and [V1 and V2 Basic Authentication Setup and Details](#) topics in the *Primavera Unifier Help Documentation* for instructions on OAuth and Basic Authentication setups, respectively.

Note:

Use a dedicated integration user account for all Primavera Unifier Adapter connections within Oracle Integration. Ensure that the integration user account has the *Admin > Get* permission and the *Get, Create, and Update Business Process (BP)* permissions if you intend to use the Primavera Unifier Adapter for performing GET, POST, and PUT operations on BPs.

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.
 - a. Enter a meaningful name to help others find your connection when they begin to create their own integrations. The name you enter is automatically added in capital letters to the **Identifier** field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).
 - b. Select the role (direction) in which to use this connection (trigger, invoke, or both). Only the roles supported by the adapter are displayed for selection. 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.
 - c. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
 - d. Enter an optional description of the connection.
5. Click **Create**.

Your connection is created. You're now ready to configure the connection properties, security policies, and (for certain connections) agent group.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.
2. In the **Connection URL** field, specify your Primavera Unifier URL.

Configure Connection Security

Configure security for your Primavera Unifier Adapter connection.

1. Go to the **Security** section.
2. In the **User Name** field, enter the Primavera Unifier integration user account username.
3. In the **Password** field, enter the Primavera Unifier integration user account password.

 **Note:**

The Unifier Adapter uses the username and password to obtain and refresh the OAuth token used to connect with Unifier.

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: <ul style="list-style-type: none"> • 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 an SSL Certificate

Certificates are used to validate outbound SSL connections.

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.

Name	Type	Category	Status
akt_ppgPublic <small>Expires in 77 Years</small>	PGP	Public	Configured
akt_ppgPrivate <small>Expires in 77 Years</small>	PGP	Private	Configured
testppgpublic <small>Expires in 77 Years</small>	PGP	Public	Configured
testppgsecret <small>Expires in 77 Years</small>	PGP	Private	Configured
elq_cert1 <small>Expired</small>	X.509	Trust	Configured
Eqir_CloudCA <small>Expires in 94 Years</small>	SAML	Message Protection	Configured
qa_lan <small>Expires in 77 Years</small>	X.509	Trust	Configured
OpportunityServiceSoapHttpPort <small>Expires in 1 Months</small>	X.509	Trust	Configured
DigiCertCA2 <small>Expires in 4 Years</small>	X.509	Trust	Configured
SG-Utilities <small>Expired</small>	X.509	Trust	Configured
app_elq_p01 <small>Expires in 8 Years</small>	X.509	Trust	Configured

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.
 - X.509 (SSL transport)
 - SAML (Authentication & Authorization)
 - PGP (Encryption & Decryption)
 - Signing key

X.509 (SSL transport)

1. Select a certificate category.
 - a. **Trust:** Use this option to upload a trust certificate.
 - i. Click **Choose File**, 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 **Choose File**, 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 **Choose File**, 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 **Choose File**, 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 **Choose File**, 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 **Choose file** 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.

3

Add the Primavera Unifier Adapter Connection to an Integration

When you select and place the Primavera Unifier 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 Unifier Adapter endpoint properties.

The following wizard pages that guide you through configuration of the Unifier Adapter as an invoke in an integration.

Topics:


- [Basic Info Page](#)
- [Trigger BP Selection Page](#)
- [Invoke BP Selection Page](#)
- [Summary Page](#)

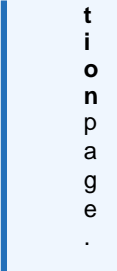
Basic Info Page

You can enter a name and description on the Basic Info page of each adapter 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: <ul style="list-style-type: none">• 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. For example: <code>This connection receives an inbound request to synchronize account information with the cloud application.</code>
Select Level	Select the level within Unifier where you want to execute the service. You can select Company or Shell .

Element	Description
What action do you want to perform on the endpoint?	Select the HTTP action you want to perform. Select GET to retrieve an existing record, POST to create a new record, and PUT to update an existing record.

 **N**
o
t
e
:
T
h
i
s
f
i
e
l
d
i
s
o
n
l
y
a
v
a
i
l
a
b
l
e
f
o
r
t
h
e
l
n
v
o
k
e
B
P
S
e
l
e
c

Element	Description
	

Trigger BP Selection Page

Select the Business Process (BP) record that you want to create in Unifier.

Element	Description
Select BP at Company/Shell Level	Select the BP record you want to create in Unifier.



Note:

Based on the BP you select, the fields defined in the integration interface of that BP are available for mappings.

Invoke BP Selection Page

Select the Business Process (BP) record you want to fetch.

Element	Description
Select BP at Company/Shell Level	Select the BP record you want to fetch from Unifier.



Note:

Based on the BP you select, the fields defined in the integration interface of that BP are available for mappings.

Summary Page

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

Element	Description
Summary	<p>Displays a summary of the configuration values you defined on previous pages of the wizard.</p> <p>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.</p> <p>To return to a previous page to update any values, click the appropriate tab in the left panel or click Back.</p> <p>To cancel your configuration details, click Cancel.</p>