

Developer Guide | PUBLIC
Document Version: 1.0 – 2023-06-27

Integration with SAP S/4HANA and SAP S/4HANA Cloud

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 About. . . . 3
1.1 Component Overview. . . . 3
1.2 User Identity Mapping. . . . 5
1.3 Technical Requirements. . . . 6

2 Prerequisites. . . . 8
2.1 Create SAP Conversational AI Enterprise Tenant. . . . 8
Create a New Global Account. . . . 8
Create a New Subaccount. . . . 9
Enable Cloud Foundry for Subaccount. . . . 9
Subscribe to SAP Conversational AI. . . . 9
2.2 Configure SAML Trust between SAP BTP Subaccount and IAS. . . . 12
Export SAML 2.0 IdP Metadata from IAS. . . . 12
Configure SAP BTP Subaccount to Trust IAS as SAML IdP and Export SP Metadata. . . . 13
Configure IAS as SAML IdP to Trust BTP Subaccount as SP. . . . 14
2.3 Configure SAML Trust between SAP S/4HANA System and IAS. . . . 15
2.4 (Optional) Configure IAS as SAML proxy to Corporate IdP. . . . 16
Configure the Corporate Identity Provider. . . . 16
Configure the Identity Authentication Tenant as a Proxy. . . . 17
Configure Trust Between Subaccount and Proxy. . . . 20

3 Runtime Set Up. . . . 21
3.1 Connect SAP BTP Subaccount to SAP S/4HANA ABAP System. . . . 21
3.2 Configure Destinations. . . . 22
3.3 Configure SAP Conversational AI Web Client and FLP Plugin. . . . 23
3.4 Maintain Custom Content Security Policy. . . . 24
3.5 Allowlisting the FLP Domain. . . . 24
Custom FLP Domain (SAP S/4HANA On-Premise Only). . . . 24
XSUAA Service (SAP S/4HANA Cloud and On-Premise). . . . 25
3.6 Verify SAP Conversational AI Web Client Plugin. . . . 29
3.7 Access OData Services From A Chatbot. . . . 30

4 Designtime Set Up. . . . 31
4.1 Assign Roles in SAP Conversational AI. . . . 31
4.2 Create Organizations and Teams. . . . 31
4.3 Import SAP S/4HANA Template Chatbot in SAP Conversational AI Enterprise Tenant. . . . 32
4.4 Connect Chatbot to Web Client. . . . 34

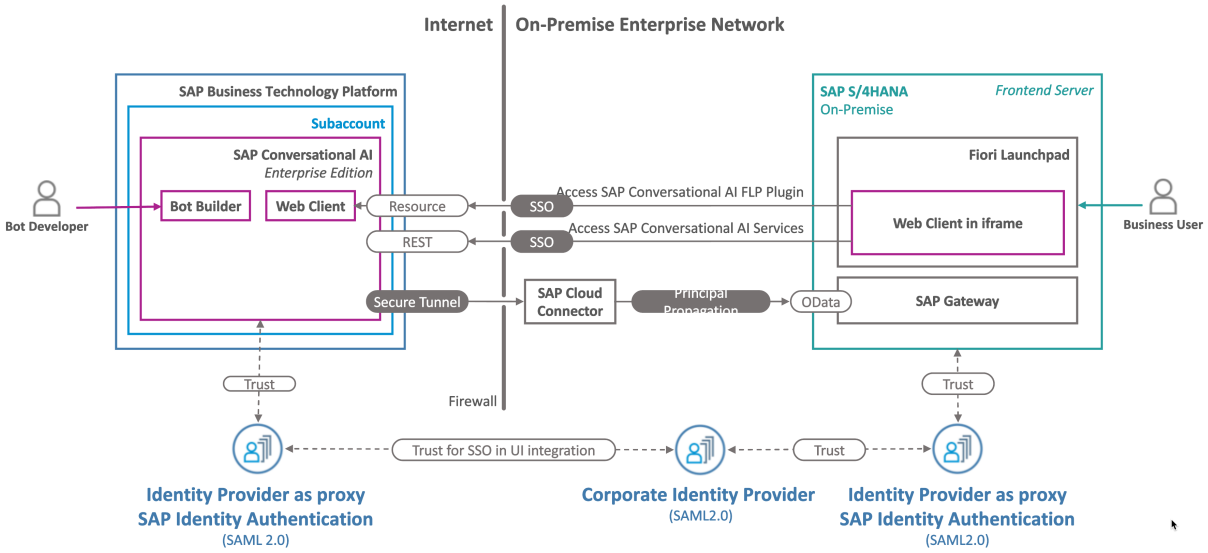
1 About

This guide mainly applies to customers using the on-premise or Cloud solution of SAP S/4HANA, who want to enable chatbot capabilities by integrating the solution with the enterprise version of SAP Conversational AI. This guide is intended for system administrators and technical consultants who are assisting customers with the initial set up and management of existing integration.

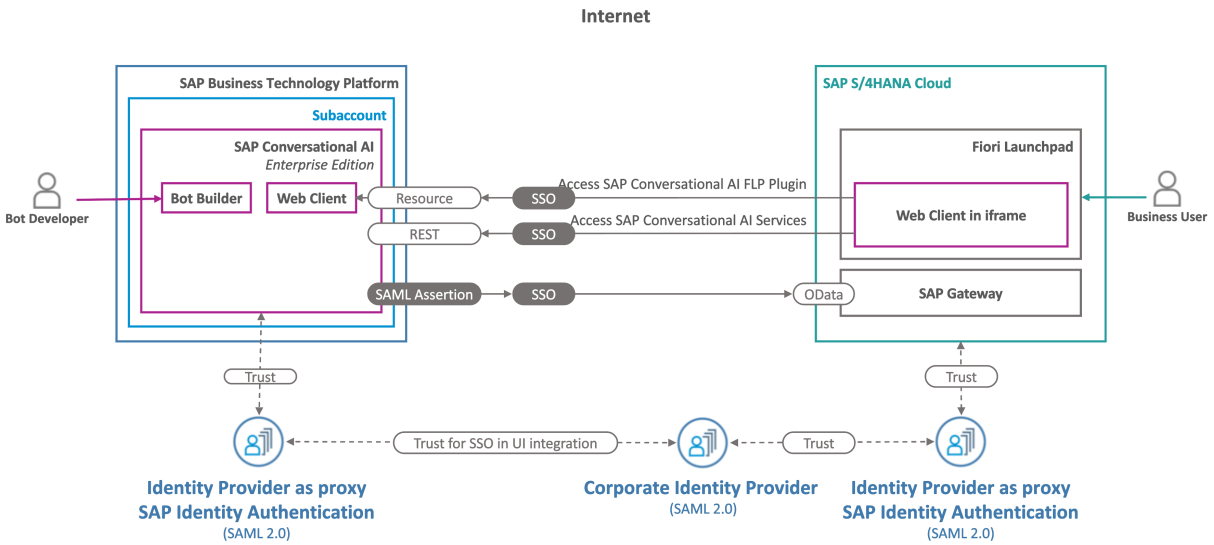
1.1 Component Overview

The following diagrams shows a high-level overview of the components and how they interact with each other.

Components of S/4HANA On-Premise Integration



Components of S/4HANA Cloud Integration



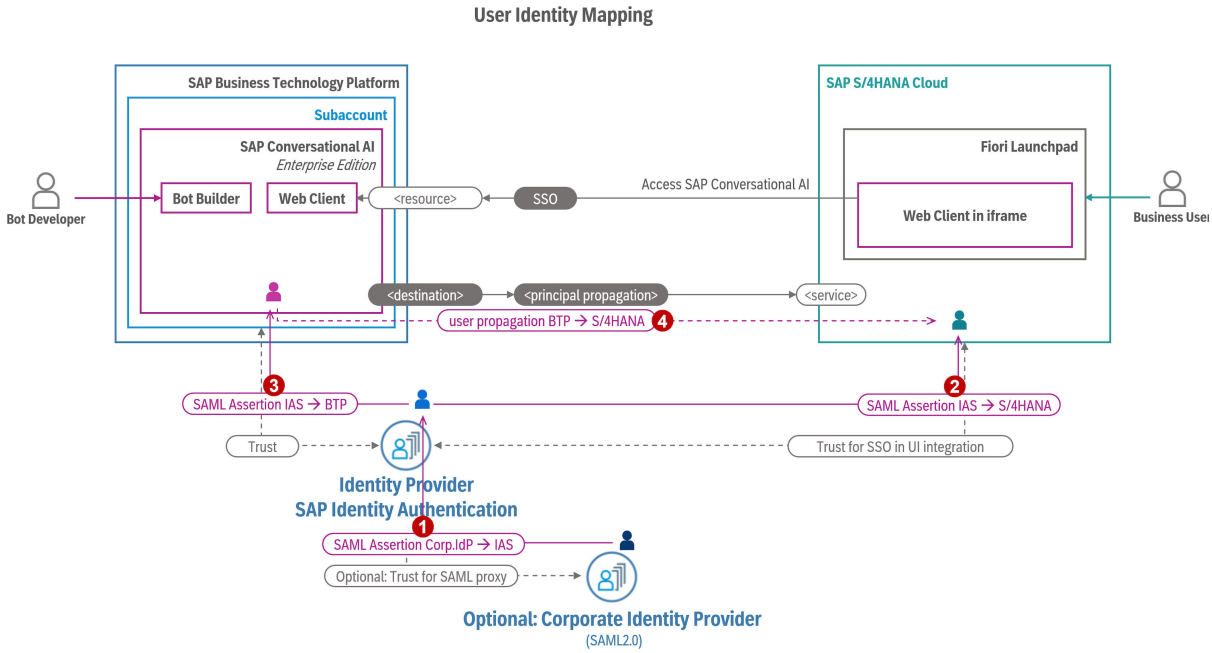
> ### i Note
>
> Single sign-on for the UI integration of SAP Conversational AI Web Client with SAP Fiori Launchpad on SAP S/4HANA system relies on the same SAML identity provider that is used for both systems.
>
> Since SAP Conversational AI Web Client is displayed in an iFrame, the SAML identity provider must also support its authentication UIs being rendered in an iFrame (frameablity).

Optional

Using SAP Identity Authentication Service (IAS) as SAML 2.0 identity provider ensures frameablity. However, corporate users are usually managed in an existing directory or a Corporate Identity Provider. IAS supports both scenarios, to either connect to an existing directory, or to act as a SAML proxy for the Corporate Identity Provider. For more information, see User Identity Mapping [page 5].

1.2 User Identity Mapping

The following figure shows the different user identities, which represent the actual user in the components and how these identities are mapped:



The SAP Identity Authentication Service (IAS) is the central identity provider for the SAP components. Depending on your landscape, the user identities are stored in the IAS directory, or IAS is connected to a Corporate User Store, or it acts as a proxy for a Corporate Identity Provider. For more information, go to the SAP Help Portal documentation for SAP Cloud Identity Services - Identity Authentication, see sections Corporate User Store and Corporate Identiy Providers in the Operation Guide.

If your landscape includes a Corporate Identity Provider, the SAML assertion issued by the Corporate Identity Provider for the IAS as proxy must contain the required attributes for the user identity, that are passed on from IAS to SAP BTP and SAP S/4HANA when the IAS issues the SAML assertion for the respective service provider. For more information, see Configure IAS as SAML proxy.

SAP S/4HANA uses its own user store, therefore the user identity from the SAML assertion issued by IAS for SAP S/4HANA must be mapped to the local user identity in the SAP S/4HANA ABAP system.

SAP BTP supports user federation, thus the user identity from the *Subject Name ID* attribute of the SAML assertion issued by IAS for SAP BTP will be used as user identity in SAP BTP.

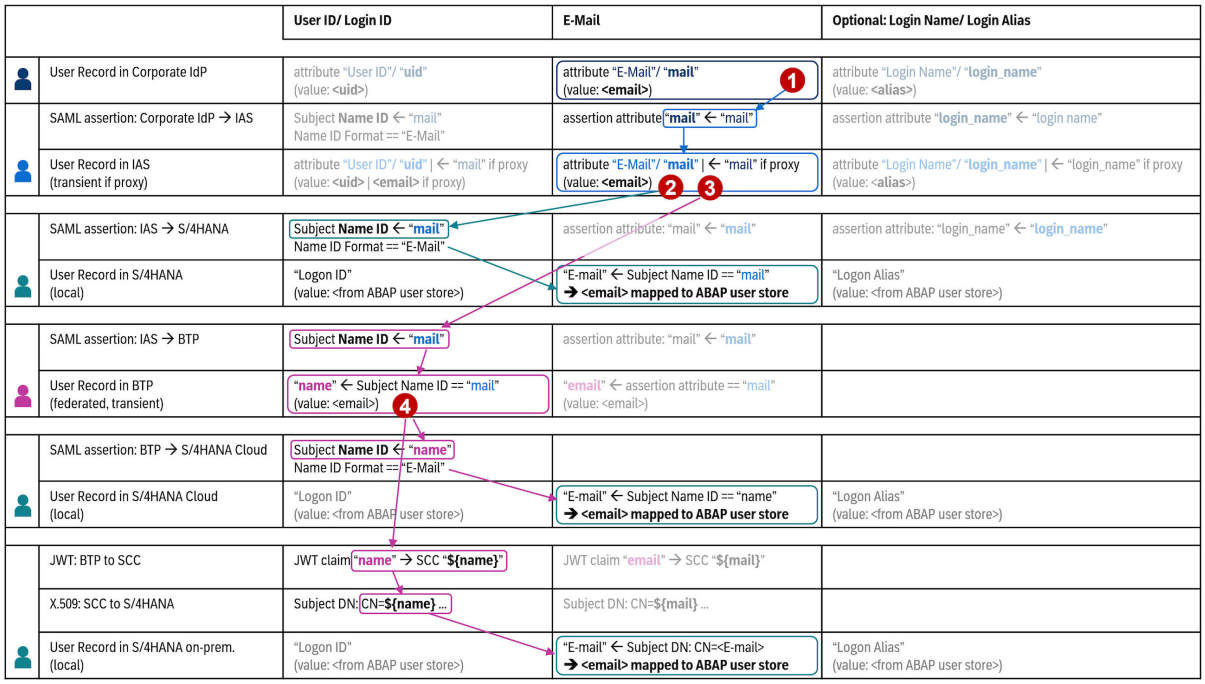
For the system-to-system communication, for example, when a chat bot retrieves data from an OData service on SAP S/4HANA, the user identity from SAP BTP (as received from the SAML assertion from IAS) must be mapped to the corresponding ABAP user identity for principal propagation to work. For more information, see Configure Principal Propagation from BTP to SAP S/4HANA.

We recommend using the email address as user identifier in the following scenarios:

- Optional for the SAML assertion from Corporate Identity Provider to IAS: email address sent as assertion attribute, with mapping on IAS to *E-Mail*.

- SAML assertion from IAS to SAP S/4HANA: *E-Mail* as *Subject Name Identifier*; with mapping configured for *E-Mail* in SAML service provider configuration on SAP S/4HANA.
- SAML assertion from IAS to SAP BTP: *E-Mail* as *Subject Name Identifier*; no mapping on SAP BTP.
- User propagation from SAP BTP to SAP S/4HANA: *User ID* in SAP BTP is *Email*, mapping on SAP S/4HANA to email address:
  - For SAP S/4HANA on-premise via SAP Cloud Connector (SCC): On SCC, the SAP BTP *User ID* (email address) is mapped via X.509 Principal Propagation pattern to subject distinguished name of the X.509 user certificate, for example, CN=email. On SAP S/4HANA on-premise, the subject distinguished name of the certificate is mapped to the user via transaction `CERTRULE`.
  - For SAP S/4HANA Cloud: The SAP BTP *User ID* (email address) is mapped to the *Subject Name Identifier* of the SAML assertion, which is issued by the SAP BTP connectivity service for the SAP S/4HANA system. Mapping is handled by communication arrangement `SAP_COM_0676`.

The following figure illustrates the recommended usage of user identities and their mapping:



The actual mappings depend on your system landscape. For example, if you use the *Logon Alias* in your SAP S/4HANA system as user identifier, you need to adapt the user mappings accordingly.

1.3 Technical Requirements

A specific set of components and configurations are required to integrate SAP Conversational AI Web Client with SAP S/4HANA on-premise and SAP S/4HANA Cloud.

Technical Requirements

Requirement	Details
SAP Business Technology Platform account	SAP BTP global account and subaccount
SAP Conversational AI tenant	SAP Conversational AI Enterprise tenant as application subscription in SAP BTP subaccount
SAP Identity Authentication Service (IAS)	Recommended as SAML 2.0 identity provider (IdP), frameable
SAP Cloud Connector (SCC)	2.11.03 or higher, with X.509 Principal Propagation enabled (for SAP S/4HANA on-premise only).
SAP S/4HANA system	• **On-premise** SAP S/4HANA 1909 and higher • **Cloud** SAP S/4HANA Cloud 2108

Admin Permissions

The following Administrators are involved in the configuration:

Role	Task
IAS Tenant Administrator	manages SAML trust setup to SAP BTP subaccount and SAP S/4HANA system
SAP BTP Account Administrator	manages SAP BTP subaccount, subscriptions, destinations
SAP BTP Account Security Administrator	manages SAML trust configuration to IAS, roles, role collections and assignments to users
SAP Cloud Connector Administrator (S/4HANA OP only)	manages X.509 principal propagation setup
Web Dispatcher Administrator (S/4HANA OP only, optional)	manages X.509 principal propagation setup (if a Web Dispatcher is used between SCC and SAP S/4HANA)
SAP S/4HANA OP Administrator (SAP S/4HANA OP only)	manages SAML trust configuration to IAS and X.509 principal propagation from SAP Cloud Connector
One SAP S/4HANA Cloud Tenant Business Administrator (SAP S/4HANA Cloud only)	manages communication setup and content security policy

2 Prerequisites

Based on your landscape, you must have the following configured:

1. SAP Conversational AI tenant as a subscription in SAP BTP subaccount with Cloud Foundry enabled
2. SAP BTP subaccount configured with IAS as SAML Id to authenticate bot developers and business users
3. SAP S/4HANA system configured with IAS as SAML IdP to authenticate SAP Fiori Launchpad business users
4. (Optional) IAS configured as SAML proxy to a Corporate Identity Provider
5. SAP BTP subaccount connected to SAP S/4HANA system for usage of OData services with propagated user context

Based on this, you configure the SAP Conversational AI design-time to let bot developers create and build new bots or deploy pre-built bots. You then configure the SAP Conversational AI runtime to make the bots available to the business users.

2.1 Create SAP Conversational AI Enterprise Tenant

To integrate SAP Conversational AI with SAP S/4HANA, you need your own SAP Conversational AI enterprise tenant in SAP BTP. For more information, see Configuring the Enterprise Edition

> **i Note**
>
> SAP Conversational AI Community Edition does not support Single Sign-On and principal propagation with SAP S/4HANA.

Please note that SAP Conversational AI Enterprise Edition is available in the following data centers and the subaccount in SAP BTP that serves as the tenant account for SAP Conversational AI must be assigned to at least **one** of the regions:

- Europe (eu10)
- US (us10)

2.1.1 Create a New Global Account

It is important to either:

- Re-use an existing customer managed global account, or
- Create a new global account

For more information see, Getting a Global Account under SAP Business Technology Platform documentation.

> **i Note**
>
> There's currently no trial account available for SAP Conversational AI in SAP BTP .

> **i Note**
>
> External customers must contact their account executive for creating a new global account.

2.1.2 Create a New Subaccount

Subscriptions in SAP Business Technology Platform are only possible at subaccount level.

> **→ Remember**
>
> You can either:
>
> - use an existing subaccount for bot provisioning only if it was created after January 2020 as XSUAA instances (configured implicitly for a subaccount) created before 2001 release, are not OIDC compliant or
> - create a new subaccount in the appropriate region.

As a global account administrator, you create subaccounts in your global account. Once you create a new subaccount, you see a tile for it in the global account view, and you are automatically assigned to it as an administrator.

1. From your global account, choose *New Subaccount*.
2. Provide the necessary details and click *Create*.
   A new tile appears in the global account page with the subaccount details. For more details, see SAP Business Technology Platform documentation.

2.1.3 Enable Cloud Foundry for Subaccount

Once you have created the subaccount, you must enable cloud foundry for your subaccount.

1. In the SAP Business Technology Platform Cockpit, navigate to your subaccount created for Cloud Foundry.
2. Choose *Enable Cloud Foundry*.
3. You can either accept the suggested *Organization Name* or adjust it according to your preferences. For more information, see Orgs, Spaces, Roles, and Permissions in the Cloud Foundry documentation.
4. Choose *Create*.
   You have now enabled Cloud Foundry for your subaccount.

2.1.4 Subscribe to SAP Conversational AI

You need to first subscribe to the relevant service in SAP Business Technology Platform.

> **Note**
>
> You need to be a global account administrator to perform the following tasks.

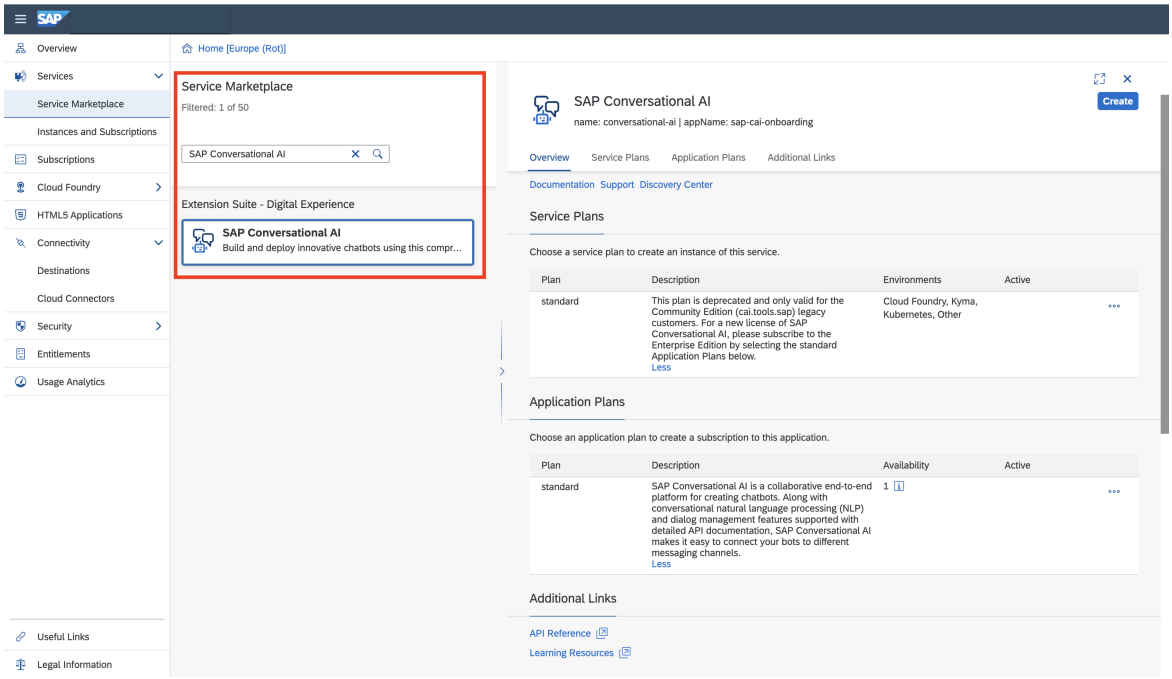
1. In the SAP BTP Cockpit, open your subaccount.

   > **Note**
   >
   > Ensure that the name of the subaccount subdomain and Cloud Foundry organization should be same.

2. Choose *Security* > *Trust Configuration*. Click *Establish Trust* and select an identity provider from the list of available and choose *Establish Trust*.
   Depending on the data center region of your IAS tenant, it may take upto twenty four hours for replication of the trust setup. However, if your IAS tenant is in Europe – ROT, you should be able to subscribe immediately after the trust setup.

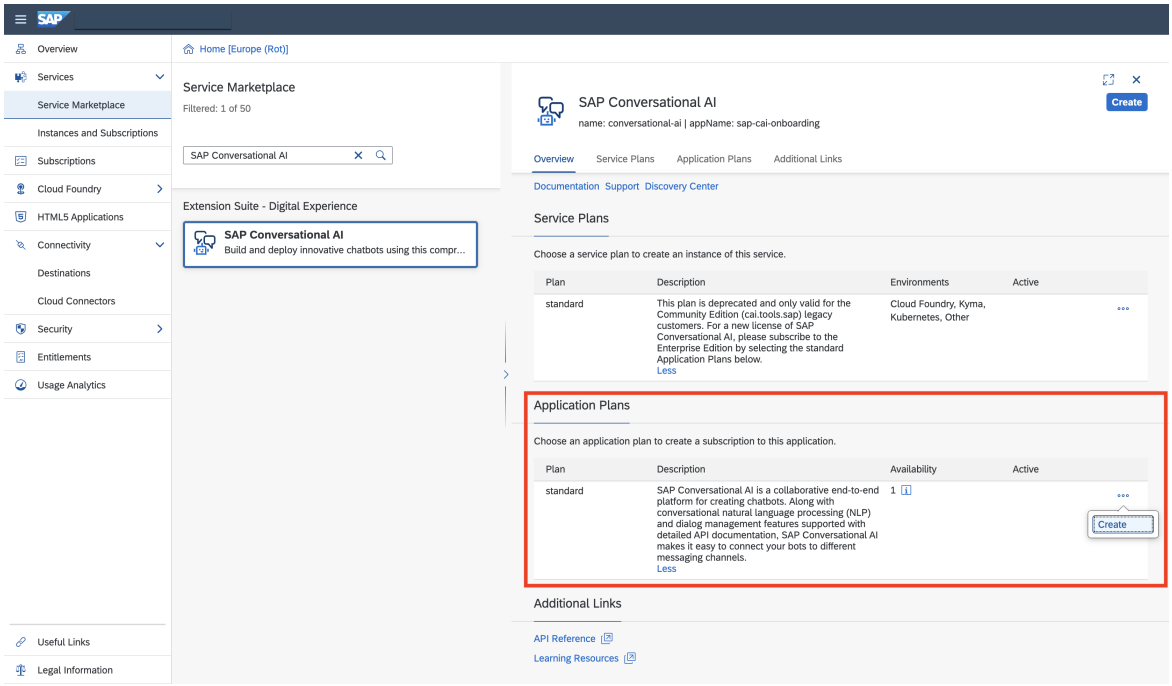
   > **Note**
   >
   > To obtain a new tenant of Identity Authentication, see Tenant Model and Licensing.
   >
   > If you already have IAS tenant/s, you can view all SAP Cloud Identity Services tenants that are assigned to your customer ID. For more information, see Viewing Assigned Tenants and Administrators.

3. Open your *Subaccount* tile and click *Service Marketplace* in the left navigation pane.
4. Look for the application *SAP Conversational AI* and click the tile to open it.

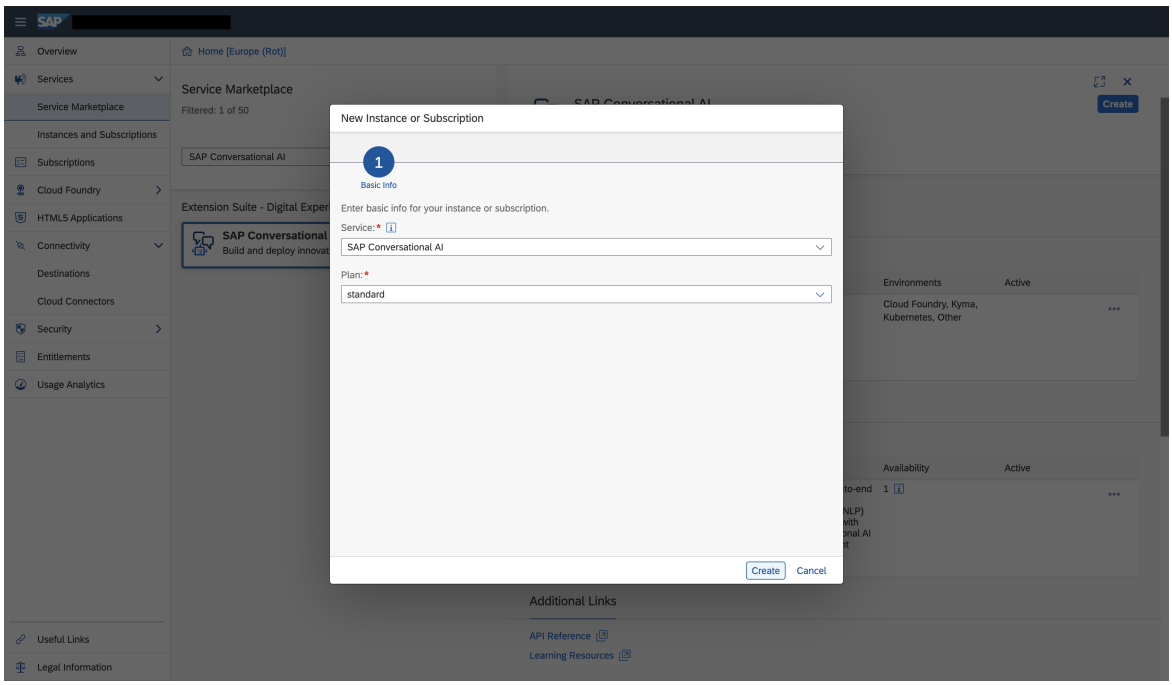


5. Under *Application Plans*, click the overflow menu (three dots) on the right and select *Create*. Note that the plans are visible according to your global account or sub-account entitlements.

   > **Note**
   >
   > The standard plan under *Service Plans* is currently not available. It is only available for Community edition legacy customers. You must select the standard plan under *Application Plans* to subscribe to the Enterprise edition of SAP Conversational AI.



6. Select the relevant plan in the popup and click *Create*.
   You can find the newly subscribed application under *Instances and Subscriptions*.



> ## Note
>
> All the bot conversations in an enterprise tenant are billed by SAP Conversational AI.

Related Information

Subscribe to Multitenant Applications Using the Cockpit

2.2 Configure SAML Trust between SAP BTP Subaccount and IAS

You need to set up SAML 2.0 trust between SAP Conversational AI subaccount inSAP BTP as service provider and SAP Identity Authentication Service (IAS) as identity provider.

For more information, see SAP Authorization and Trust Management Service in the Cloud Foundry Environment under section Security and Operation Guide for SAP Cloud Identity Services - Identity Authentication.

> **i** Note
>
> SAP BTP account does not support mapping of SAML Assertion attributes to the user identifier for the Cloud Foundry account. It uses the SAML Assertion's *Name ID Attribute*, hence it is recommended to configure the user's email address as *Subject Name Identifier* in the IAS configuration.

For more information, see Manually Establish Trust and Federation Between UAA and Identity Authentication.

2.2.1 Export SAML 2.0 IdP Metadata from IAS

As a tenant administrator view and download the tenant SAML 2.0 metadata.

Context

To view and download the tenant SAML 2.0 metadata, proceed as follows:

Procedure

1. Access the tenant's administration console for Identity Authentication by using the console's URL.

   The URL has the following pattern:

   ```
   https://<tenant ID>.accounts.ondemand.com/admin
   ```
2. Under *Applications and Resources*, choose the *Tenant Settings* tile.
3. Choose the *SAML 2.0 Configuration* list item.

4. To download the identity provider's metadata, click the *Download Metadata File* button or download from URL `https://<ias-tenant>.accounts.ondemand.com/saml2/metadata`.

   For more information, see Tenant SAML 2.0 Configuration.

2.2.2 Configure SAP BTP Subaccount to Trust IAS as SAML IdP and Export SP Metadata

You must establish a trust relationship with an SAML 2.0 identity provider in your subaccount in SAP BTP.

Context

The following procedure guides you though the trust configuration in your SAML 2.0 identity provider.

Procedure

1. Go to your subaccount (see Navigate to Orgs and Spaces) and choose *Security* > *Trust Configuration* in the SAP BTP cockpit.
2. Choose *New Trust Configuration*.
3. Upload the SAML 2.0 IdP metadata (that you downloaded in step Export SAML 2.0 IdP Metadata from IAS [page 12]).
4. Provide a suitable name and a description.
5. (Optional) Consider changing the *Origin Key* and make sure that *Available for User Logon* is checked
6. (Optional) Provide a *Link Text for User Logon* to overwrite the default *Name*.

   Whenever business users want to log on to their application, they see the logon link of the custom identity provider that they should use. It has the caption you entered in *Link Text for User Logon*.
7. Save your changes.
8. To export the SAP BTP subaccount's SAML 2.0 SP metadata, click *SAML Metadata*. Specify a file name and save the metadata locally to your hard drive.

   For more information, see Establish Trust and Federation with UAA Using Any SAML Identity Provider

2.2.3 Configure IAS as SAML IdP to Trust BTP Subaccount as SP

Create and configure an application to represent the Cloud Foundry account in the Identity Authentication Service tenant as SAML 2.0 service provider.

Procedure

1. Log on to the tenant's administration console for the Identity Authentication service at `https://<tenant ID>.accounts.ondemand.com/admin` as administration user.
2. Create an SAML Application for the Cloud Foundry Account.
   a. In the navigation area, choose *Applications & Resources* > *Applications*.
   b. Choose *+ Add*.
   c. Provide a suitable *Application Display Name*, for example your SAP BTP subaccount name and select *SAP BTP* solution as *Application Type*.
   d. Choose *Save*.
3. Configure the SAML 2.0 trust with the subaccount as a service provider. To do so, proceed as follows:
   a. On the left-hand side, choose the newly created application, and then choose *Trust*.
   b. Choose *SAML 2.0 Configuration*.
   c. Upload the metadata XML file of your subaccount that you have downloaded in step Configure SAP BTP Subaccount to Trust IAS as SAML IdP and Export SP Metadata [page 13].

      On service provider metadata upload, the fields are populated with the parsed data from the XML file.
   d. Save the configuration settings.
4. Configure the *Subject Name Identifier* sent to Cloud Foundry.
   a. Under *Applications*, choose the entry for the Cloud Foundry application that you have just created.
   b. Choose *Subject Name Identifier*.
   c. Choose *Basic Configuration* and select *E-Mail* from the dropdown list.
   d. Choose *Save*.
5. Configure the *Default Name ID Format* for the Cloud Foundry Application.
   a. Under *Applications*, choose the entry for the Cloud Foundry application in the Identity Authentication service.
   b. Choose *Default Name ID Format*.
   c. Choose *E-Mail* radio button.
   d. Choose *Save*.
6. Configure the SAML Assertion Attributes for Cloud Foundry. This is an optional step, but recommended for the mapping of groups to role collections.
   a. Under *Applications*, choose the entry for the Cloud Foundry application.
   b. Choose *Assertion Attributes*.
   c. Choose *+Add* to enter the following user attributes and their corresponding assertion attributes (if they don't already exist).

User Attribute	Assertion Attribute
First Name	**`first_name`**
Last Name	**`last_name`**
E-Mail	**`mail`**
Groups	**`Groups`**

Make sure that you enter **`Groups`** (with upper case **`G`**), not **`groups`**, as assertion attribute.

d. Choose *Save*.

2.3 Configure SAML Trust between SAP S/4HANA System and IAS

SAP S/4HANA on-premise: Configure SAML Trust for AS ABAP

Since SAP S/4HANA on-premise is built on SAP Netweaver Application Server for ABAP, you use the AS ABAP transaction `SAML2` to configure the trust setup to IAS.

1. Export SAML 2.0 IdP metadata from IAS.
   For more information, see Export SAML 2.0 IdP Metadata from IAS [page 12].
2. Configure AS ABAP client to trust IAS as IdP.
   For more information, see Configuring AS ABAP as a Service Provider.

> **i Note**
>
> Before Trusting an Identity Provider, make sure that you have enabled Security Assertion Markup Language (SAML) 2.0 support and made the basic configurations for a SAML 2.0 service provider. For more information, see Enabling the SAML Service Provider.

3. Configure IAS as SAML IdP to trust AS ABAP client as SP. You can use the *SID* + *client ID* as application name.
   For more information, see Configure IAS as SAML IdP to Trust BTP Subaccount as SP [page 14].

> **i Note**
>
> Adding the assertion attribute **`Groups`** is not required.
>
> If you select *E-Mail* as Subject Name Identity for the SAML Assertion via the IAS application configuration to AS ABAP, make sure to select the appropriate Name ID Format *E-Mail* on AS ABAP too and the ABAP user record should contain an email address, or a user mapping in `USREXTID` that can be used.
>
> For more information, see Managing Name IDs.

SAP S/4HANA Cloud: Validate Pre-configured SAML

For your SAP S/4HANA Cloud tenant, the IAS tenant and mutual SAML 2.0 trust are pre-configured. To validate this, check if you can login to the SAP Fiori Launchpad of your SAP S/4HANA Cloud tenant.

For more information, see User Administration and Authentication.

2.4 (Optional) Configure IAS as SAML proxy to Corporate IdP

In this scenario, single sign on is achieved by configuring trust between the subaccount and the proxy to the corporate IdP, which then forwards the request to the corporate IdP to authenticate the SAP S/4HANA Cloud and SAP S/4HANA OP business users.

Perform the following steps to configure SSO using an identity provider proxy:

1. Configure the Corporate Identity Provider [page 16]
2. Configure the Identity Authentication Tenant as a Proxy [page 17]
3. Configure Trust Between Subaccount and Proxy [page 20]
4. Configure Destinations [page 22]
5. Connect SAP BTP Subaccount to SAP S/4HANA ABAP System [page 21]

2.4.1 Configure the Corporate Identity Provider

Configure the corporate identity provider (IdP).

The corporate IdP is already configured to send the *login name* as the subject name identifier, that is the *User Alias* of the business users in the SAP S/4HANA Cloud tenant.

You need to configure the corporate IdP to send also the *E-Mail* as the *mail* attribute in the SAML assertion to the Identity Authentication tenant that serves as a proxy.

Prerequisite

You have a corporate IdP. In this procedure, the corporate IdP is an Identity Authentication tenant.

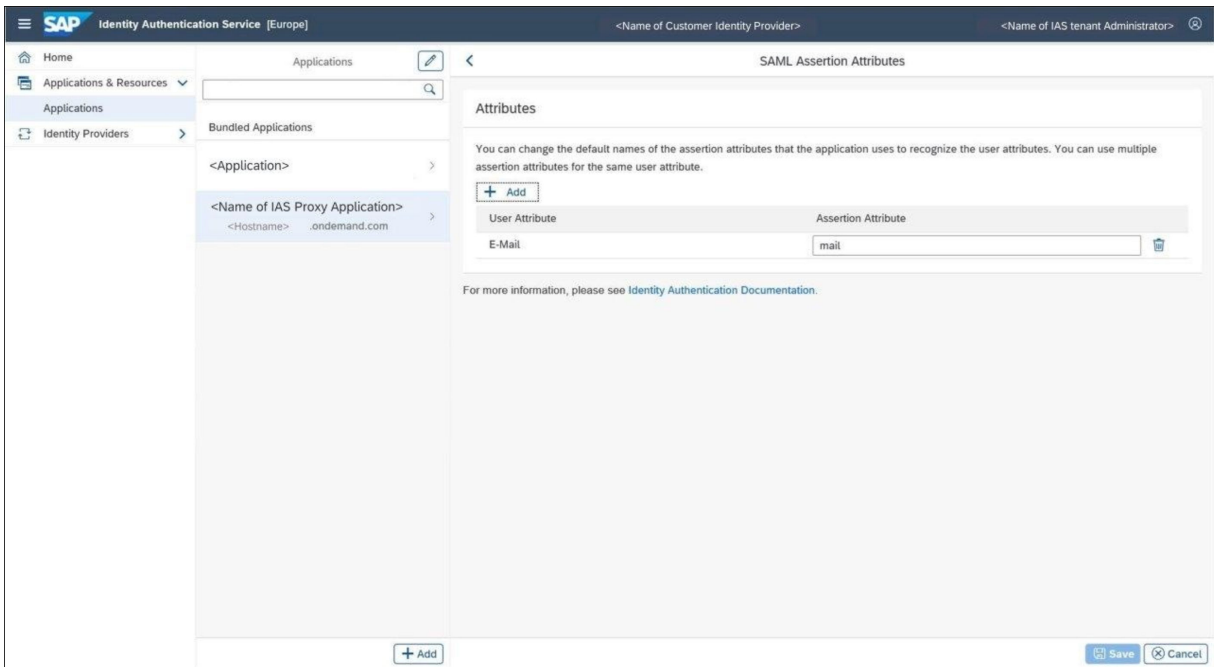
> **i** Note
>
> Using an Identity Authentication tenant as the corporate IdP is an example. Other corporate IdPs can also be used.

Procedure

1. In the Administration Console of your corporate IdP (Identity Authentication tenant), navigate to *Applications & Resources* > *Applications*.
2. Select the application that represents the proxy Identity Authentication tenant of your SAP BTP subaccount.

3. In the *Trust* tab, open the *Assertion Attributes* option.
4. Add the *User Attribute* - *E-Mail*, which is mapped by default to the *Assertion Attribute* - *mail*.
5. Save.

The following screenshot shows the mapped attribute:



2.4.2 Configure the Identity Authentication Tenant as a Proxy

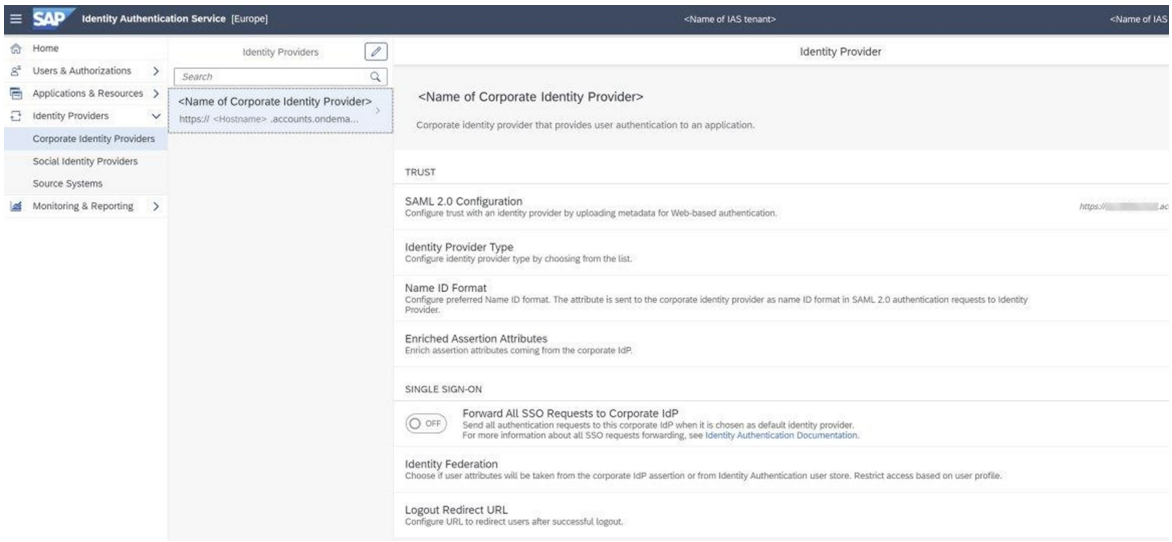
Configure the Identity Authentication tenant as a proxy to the corporate identity provider (IdP) for the SAP Conversational AI subaccount.

Overview

The Identity Authentication tenant serves as a proxy between the subaccount on SAP BTP on one side, and the corporate IdP on the other side. In the previous step, you configured the corporate identity provider to send the *E-Mail* as the *mail* attribute in the SAML assertion. In this step, you configure the Identity Authentication tenant to map between the *mail* assertion attribute and the subject name identifier for the application in the the SAP Conversational AI subaccount.

Prerequisites

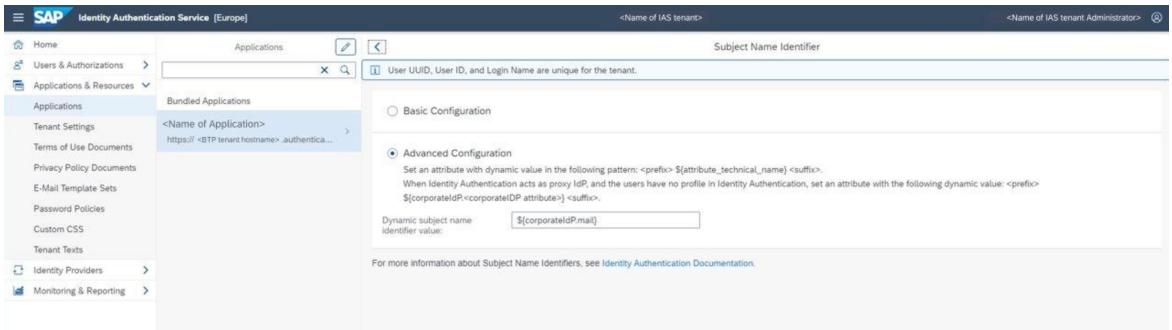
- Your IdP is configured as the corporate IdP with SAML 2.0 configuration. For example:



- In the SAP BTP cockpit, navigate to your subaccount, select *Security* > *Trust Configuration* from the navigation panel, and then download the SAML metadata from the SAP Conversational AI subaccount.

Procedure

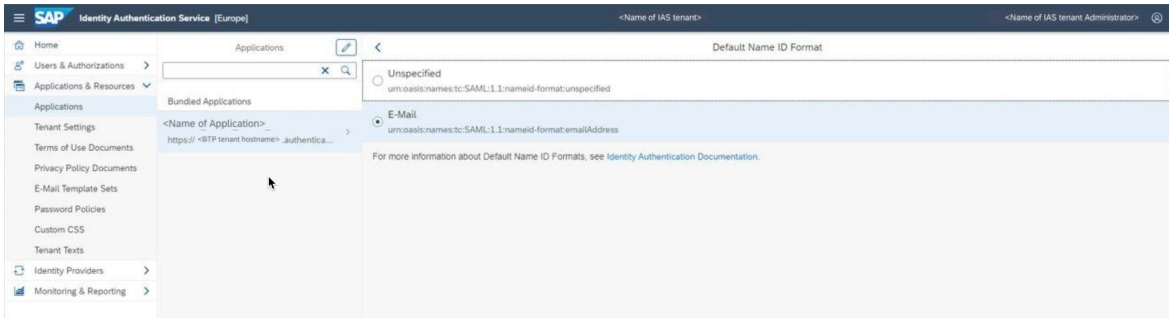
1. In the Identity Authentication tenant, navigate to *Applications & Resources* > *Applications*, and click *+Add* to create an application for the SAP Conversational AI subaccount.
2. Select the application you just created, and click *SAML 2.0 Configuration*.
3. Under *Define from Metadata*, browse for the metadata file that you downloaded from the SAP BTP cockpit.
4. Save and use the back arrow to go back to the main screen.
5. Click *Subject Name Identifier*, select *Advanced Configuration*, and in the *Dynamic subject name identifier value* field, enter the following value:
   `${corporateIdP.mail}`
   For example:



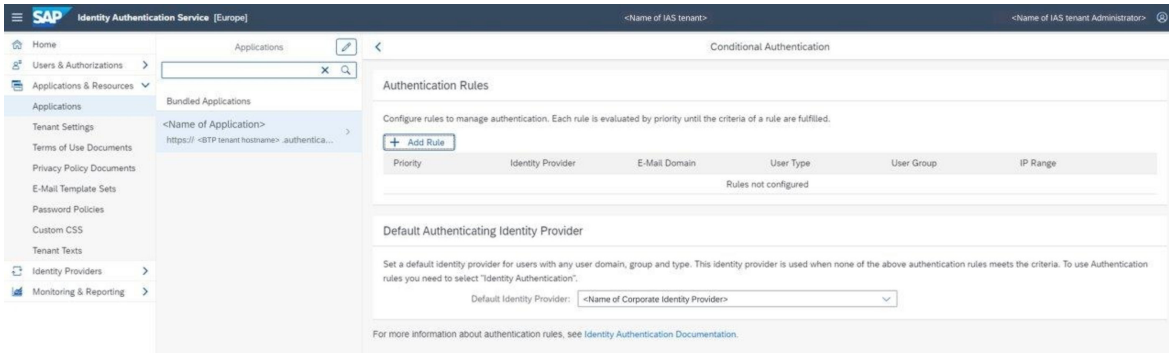
> ### Note
>
> When using the Identity Authentication tenant as a proxy to the IdP, and the users do not have profiles in Identity Authentication, set an attribute with the following dynamic value:
>
> **`<prefix> ${corporateIdP.<corporateIDP attribute>} <suffix>`**
>
> For more information, see Configure the Subject Name Identifier Sent to the Application.

6. Save and use the back arrow to go back to the main screen.

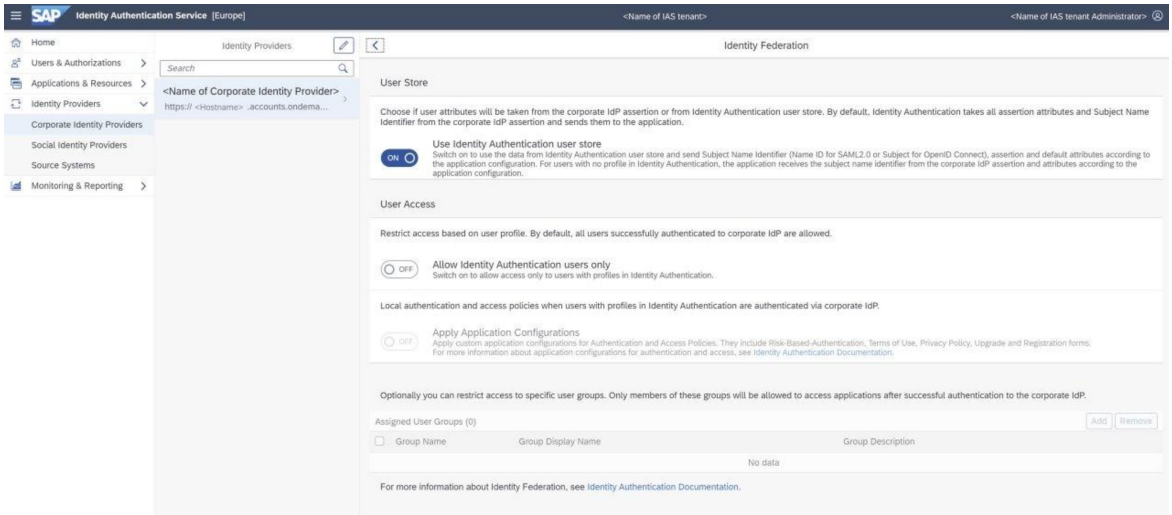
7. Click *Default Name ID Format* and select the *E-Mail (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress)* option.
   For example:



8. Save and use the back arrow to go back to the main screen.
9. Click *Conditional Authentication* and from the *Default Identity Provider* drop-down list, select your corporate IdP.
   For example:



10. Save and use the back arrow to go back to the main screen.
11. In the Identity Authentication tenant, navigate to *Identity Providers* > *Corporate Identity Providers* and select your corporate IdP.
12. Click *Identity Federation* and set the *User Store* option to **ON**.
    For example:



> **i Note**
>
> The *User Store* setting is required to map the *mail* attribute of the corporate IdP SAML assertion to the subject name identifier for the application in the SAP Conversational AI subaccount. It is **not** necessary to create user profiles in the Identity Authentication tenant as proxy.
>
> The application of the SAP S/4HANA Cloud tenant uses the *login name* as the subject name Identifier.
>
> For more information about the *User Store* option, see Configure Identity Federation.

2.4.3 Configure Trust Between Subaccount and Proxy

Configure trust between your subaccount and the Identity Authentication tenant as proxy.

SAP S/4HANA Cloud business users are authenticated using the Identity Authentication tenant as proxy that forwards the request to the customer IdP, to enable the users to log on.

Prerequisite

You have downloaded the SAML 2.0 metadata file from the Identity Authentication tenant as proxy.

For more information, see Manually Establish Trust and Federation Between UAA and Identity Authentication.

Procedure

1. In the SAP BTP cockpit, navigate to your subaccount and select *Security* > *Trust Configuration* > *New Trust Configuration*.
2. In the *Metadata* field, upload the SAML 2.0 metadata file that you downloaded, and select the *Available for User Logon* option.

3 Runtime Set Up

3.1 Connect SAP BTP Subaccount to SAP S/4HANA ABAP System

Configure Communication from SAP BTP Subaccount to SAP S/4HANA On-Premise

1. Install and configure the SAP Cloud Connector as a link between your SAP BTP subaccount and the on-premise SAP S/4HANA system.
   For more information, see Principal Propagation SSO Authentication for HTTP.
2. Configure the SAP Fiori Launchpad plugin to display SAP Conversational AI Web Client in the SAP Fiori Launchpad.
   For more information, see Configure SAP Conversational AI Web Client and FLP Plugin [page 23].

Configure Communication from SAP BTP Subaccount to SAP S/4HANA Cloud Tenant

In the SAP S/4HANA Cloud ABAP Tenant, the customer administrator creates a communication arrangement and a communication system for SAP Conversational AI communication scenario SAP_COM_0676. Set up a SAML Bearer Assertion Provider and the corresponding SAML2.0 configurations that enable trust by both E-Mail and User Alias.

Prerequisite

- Communication scenario SAP_COM_0676 is available
- You have downloaded, in the SAP BTP cockpit, the trust certificate from SAP Conversational AI subaccount destinations, by navigating to *Connectivity* > *Destinations* and selecting *Download Trust*. For more information, see Configure Destinations [page 22].

Procedure

1. Log in to SAP Fiori Launchpad as an administrator.
2. Launch the app *Communication Arrangements*.
3. Create a new communication arrangement and select **`SAP_COM_0676`** as the *Scenario* and provide a name. Click *Create*.
4. Create new communication system from the communication arrangement, as follows:
   1. Specify the *System ID* and *System Name*.
   2. Click *Create*.
   3. In the *Host Name* field, enter the host name of your SAP Conversational AI tenant URL.
   4. Set *SAML Bearer Assertion Provider* to *ON*.

5. Keep the *User ID Mapping Mode* setting to *User Name*.
6. Upload the certificate file that you downloaded from your SAP Conversational AI subaccount as the *Signing Certificate*.
7. Specify a unique *Provider Name*.
8. Add a new user for the outbound communication by clicking + button.
9. Select the *Authentication Method* as *None*.
10. Click *Create*.
11. Save the communication system to return to the communication arrangement.

5. Select the outbound user in the communication arrangement. Click the value help for *User Name* and choose *None*.
6. Save the communication arrangement.

3.2 Configure Destinations

You need to configure connectivity from your SAP BTP Cloud Foundry subaccount to SAP S/4HANA to allow SAP BTP applications to securely access remote services that run on the Internet or on-premise.

> **i** Note
>
> Depending on your bot, you need a `<path>` to be added to the URL property of the destination. For the SAP S/4HANA template chatbot, use <path> =`/sap/opu/odata/sap`.

S/4HANA On-Premise

Pre-requisite

SAP Cloud Connector is configured for your subaccount. For more information, see Principal Propagation SSO Authentication for HTTP.

Specify the following credentials:

Property	Value
`Name`	Specify a name for the destination Example - **`CAI_<system><client>_PP`**
`Type`	*HTTP*
`Description`	Enter a description
`URL`	`http://<virtual host in Cloud Connector>/<path>`
`ProxyType`	*OnPremise* (for communication via Cloud Connector)
`Authentication`	*PrincipalPropagation*

S/4HANA Cloud

Create and configure a **SAML Assertion** destination for the application in the Cloud Foundry environment. For more information, see SAML Assertion Authentication.

Specify the following credentials:

Property	Value
`Name`	Specify a name for the destination Example - **`CAI_<system><client>`**
`Type`	*HTTP*
`Description`	Enter a description.
`URL`	`https://<S/4HANA Cloud tenant host>.s4hana.ondemand.com/<path>`
`ProxyType`	*Internet*
`Authentication`	*SAMLAssertion*
`Audience`	`https://<S/4HANA Cloud tenant host).s4hana.ondemand.com`
`AuthnContextClassRef`	`urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession`
`nameIdFormat` (additional property)	`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

3.3 Configure SAP Conversational AI Web Client and FLP Plugin

Configure SAP Conversational AI Web Client

You need to first configure SAP Conversational AI Web Client which is a conversational user interface for connecting to SAP Conversational AI chatbots via the SAP Conversational AI Web Client channel. For more information, see Configuration Guide for SAP Conversational AI Web Client.

Configure SAP Fiori Launchpad Plugin

To display SAP Conversational AI Web Client in the SAP Fiori Launchpad, you need to add the plugin in the FLP.

SAP S/4HANA On-Premise

For SAP S/4HANA version 1809 or higher, the recommended way to add the plugin is using the ABAP FLP configuration.

1. Please follow the instructions as described in section *Activating Plug-Ins in Customizing* under Activating Plug-Ins on the ABAP Platform.
2. Make the following entries:

Field	Default Value
UI5 Component ID	`sap.cai.webclient`
URL	`<subscription_path>/resources/public/webclient/fiori`

SAP S/4HANA Cloud

The FLP plugin is automatically configured once you create a communication arrangement between the system and SAP Conversational AI.

For more information, see Connect SAP BTP Subaccount to SAP S/4HANA ABAP System [page 21].

3.4 Maintain Custom Content Security Policy

Maintain a custom content security policy to enable loading the plugin script as cross-origin resource.

1. Open Manage Content Security Policy app, click *Trusted Sites* and navigate to details for Resources Scripts.
2. Click *New* in *Managed by Customer* section.
3. Enter the URL of you SAP Conversational AI tenant under *Trusted Content* and choose *Save*.

3.5 Allowlisting the FLP Domain

To allowlist the hosting domain, you must follow the steps as per your landscape.

Custom FLP Domain (SAP S/4HANA On-Premise Only)

Context

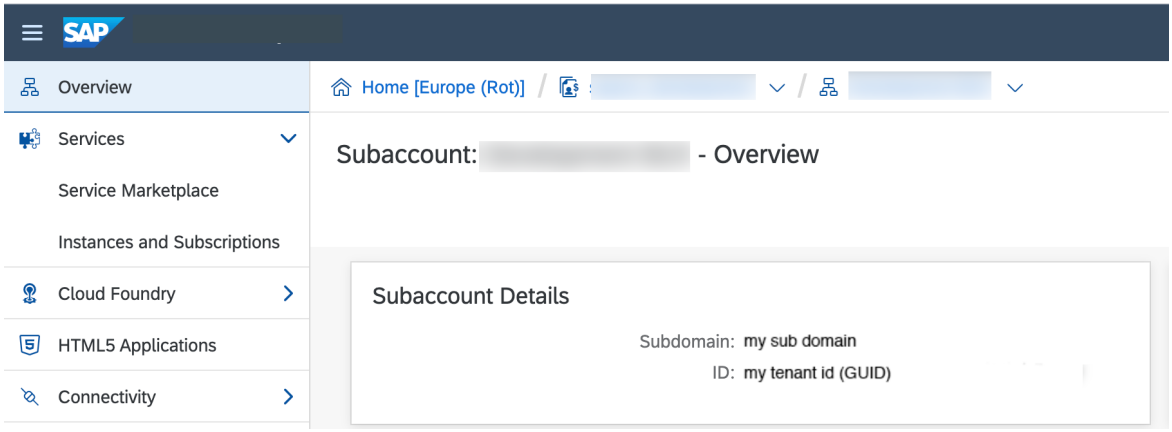
If you need to get a custom domain allowlisted, you can do this by raising a ticket (with medium priority) titled as *SAP Conversational AI - Service Request – Allow-listing* for the component `CA-ML-CAI-USM`. Mention the

domain to be allowlisted and specify if only the standard HTTPS port (443) needs to be allowlisted or all the ports are to be allowlisted. For more details, see Configuration Guide for SAP Conversational AI Web Client.

XSUAA Service (SAP S/4HANA Cloud and On-Premise)

Prerequisites

- You need basic knowledge of how to use a REST API client. You can use command line clients like curl or applications like Postman (which you can download from getpostman.com).
- You need to have access to the XSUAA configuration API, which relies on retrieving an OAuth token. For further information, refer to SAP Note 2760424.
- You need to know the technical tenant ID (GUID) of your Cloud Foundry subaccount. You can find this in the *Overview* section of your subaccount:



Context

The SAP Conversational AI Web Client runs inside an iFrame element to offer complete isolation from the hosting page. For security reasons, the Cloud Foundry authentication service (XSUAA) prevents the logon page from being embedded in an `iframe` element unless the origin domains are allowlisted . This cannot currently be done from the SAP Business Technology Platform, but only via REST API calls.

Procedure

1. Obtain an OAuth token for the XSUAA REST API services, as described in SAP Note 2760424. You can use curl, as described in this SAP Note, but can also use any other REST client you are comfortable with. When using Postman, it is recommended that you enable the Postman Interceptor, which automatically carries over browser cookies into your REST requests.
2. Execute the following request:

`GET "https://api.authentication.<landscape>.hana.ondemand.com/sap/rest/authorization/v2/tenants/<tenant ID>/settings "`

with the following header:

Header Name	Value
Authorization	Bearer `<OAuth token>`

Explanation of Variables

Variable Name	Explanation
landscape	The landscape domain of the Cloud Foundry region you connect to. This can also be seen on the *Overview* page of your subaccount, under *Cloud Foundry* > *API Endpoint*. It will be the same regional domain component.
tenant ID	The tenant GUID obtained as explained under *Prerequisites* above
OAuth token	The OAuth token obtained in Step 1 above

The GET request will return the current tenant-specific XSUAA settings as a JSON object. This object contains one key, `iframeDomains`, which is a space-separated string of all allowlisted domains (including wildcards) for which XSUAA login will be allowed from within an `iframe` element.

3. Change the `iframeDomains` setting. You need to allowlist all host names or domains (with wildcards) of the SAP Fiori launchpads that the SAP Conversational AI Web Client is to be integrated with. It is important that you enter the host names and domains as they will appear in the browser. For example, if you have a reverse proxy in your landscape, and the browser connects to the proxy instead of directly to the ABAP front-end server, you need to allowlist the reverse proxy here.

   To update the `iframeDomains` setting, execute a PATCH (HTTP method PATCH) request:

   `PATCH "https://api.authentication.<landscape>.hana.ondemand.com/sap/rest/authorization/v2/tenants/<tenant ID>/settings"`

   with the following headers and body format:

Header Name	Value
Authorization	Bearer `<OAuth Token>`
Content-Type	application/json

```
{
 "iframeDomains": "https://my.full.hostname.com https://*.my.subdomain.com
https://*.my.subdomain-with-specific-port.com:8000 "
}
```

The placeholders used in the body format should be replaced with your hostnames and/or subdomains.

You can also use the following Postman Collection, which describes three sample requests. You need to replace the variables in the sample code with the information given above.

Sample Code

```
{
    "info": {
        "_postman_id": "d5eefb0a-d67b-48c9-a808-6ce4ad197175",
        "name": "IframeDomain setup",
        "schema": "https://schema.getpostman.com/json/collection/v2.1.0/
collection.json"
    },
    "item": [
        {
            "name": "GetClientToken",
            "event": [
                {
                    "listen": "test",
                    "script": {
                        "id": "d4d0c7d9-9c93-4cab-8cad-4f91f3f722ab",
                        "exec": [
                            "pm.test(\"Status code is 200\", function ()
{",
                            "    pm.response.to.have.status(200);",
                            "});",
                            "var jsonData = pm.response.json();",
                            "pm.environment.set(\"tenant_token\",
jsonData.access_token);",
                            ""
                        ],
                        "type": "text/javascript"
                    }
                }
            ],
            "request": {
                "auth": {
                    "type": "basic",
                    "basic": [
                        {
                            "key": "password",
                            "value": "{{clientsecret}}",
                            "type": "string"
                        },
                        {
                            "key": "username",
                            "value": "{{clientid}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "POST",
                "header": [
                    {
                        "key": "Accept",
                        "type": "text",
                        "value": "application/json"
                    },
                    {
                        "key": "Content-Type",
                        "name": "Content-Type",
                        "value": "application/x-www-form-urlencoded",
```

```
                        "type": "text"
                    }
                ],
                "body": {
                    "mode": "urlencoded",
                    "urlencoded": [
                        {
                            "key": "grant_type",
                            "value": "client_credentials",
                            "type": "text"
                        }
                    ]
                },
                "url": {
                    "raw": "{{protocol}}{{subaccount}}.{{uaadomain}}/oauth/
token",
                    "host": [
                        "{{protocol}}{{subaccount}}",
                        "{{uaadomain}}"
                    ],
                    "path": [
                        "oauth",
                        "token"
                    ]
                }
            },
            "response": []
        },
        {
            "name": "Get Settings",
            "request": {
                "auth": {
                    "type": "bearer",
                    "bearer": [
                        {
                            "key": "token",
                            "value": "{{tenant_token}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "GET",
                "header": [],
                "url": {
                    "raw": "https://api.{{uaadomain}}/sap/rest/
authorization/v2/tenants/{{tenant_id}}/settings",
                    "protocol": "https",
                    "host": [
                        "api",
                        "{{uaadomain}}"
                    ],
                    "path": [
                        "sap",
                        "rest",
                        "authorization",
                        "v2",
                        "tenants",
                        "{{tenant_id}}",
                        "settings"
                    ]
                }
            },
            "response": []
        },
        {
```

```
            "name": "Patch Settings",
            "request": {
                "auth": {
                    "type": "bearer",
                    "bearer": [
                        {
                            "key": "token",
                            "value": "{{tenant_token}}",
                            "type": "string"
                        }
                    ]
                },
                "method": "PATCH",
                "header": [
                    {
                        "key": "Content-Type",
                        "name": "Content-Type",
                        "value": "application/json",
                        "type": "text"
                    }
                ],
                "body": {
                    "mode": "raw",
                    "raw": "{\n    \"iframeDomains\": \"{{iframeDomains}}
\"\n}"
                },
                "url": {
                    "raw": "https://api.{{uaadomain}}/sap/rest/
authorization/v2/tenants/{{tenant_id}}/settings",
                    "protocol": "https",
                    "host": [
                        "api",
                        "{{uaadomain}}"
                    ],
                    "path": [
                        "sap",
                        "rest",
                        "authorization",
                        "v2",
                        "tenants",
                        "{{tenant_id}}",
                        "settings"
                    ]
                }
            },
            "response": []
        }
    ]
}
```

3.6 Verify SAP Conversational AI Web Client Plugin

Log in to SAP Fiori Launchpad as an S/4HANA business user. Check if the SAP Conversational AI Web Client icon is visible in the FLP shell header.

3.7 Access OData Services From A Chatbot

Access the OData services from a chatbot.

SAP S/4HANA On-Premise

1. Activate the corresponding SAP S/4HANA OData services to allow querying and updating data by SAP Conversational AI.
   For more information, see Activating OData Services.
2. Assign authorization to business user.
   For example, provide authorization to SAP Fiori apps by configuring roles for tile catalogs and assigning the roles to users. For more information, see Configuring Roles for Tile Catalogs and Groups.
3. Adapt OData resource access control for SAP S/4HANA OP in SAP Cloud Connector.
   For more information, see Configure Access Control.

SAP S/4HANA Cloud

In SAP S/4HANA Cloud, OData services are used in Fiori apps and as APIs.

- Assign authorizations to business users for Fiori apps and their corresponding OData services via business catalogs and business roles.
  For more information, see How to Maintain Business Users.
- When using API OData services, listed in SAP Business Accelerator Hub, you need to first configure communication management apps to integrate your system with other systems and enable data exchange.
  For more imformation, see Communication Management.
- You can define custom OData services to enable external consumption.
  For more information, see External API: Exposing a Custom CDS View as OData API.

4 Designtime Set Up

4.1 Assign Roles in SAP Conversational AI

To allow the user to access the existing bots or create a new one, you need to assign the *cai_developer* role in SAP Business Technology Platform.

For more information, see Assign Roles.

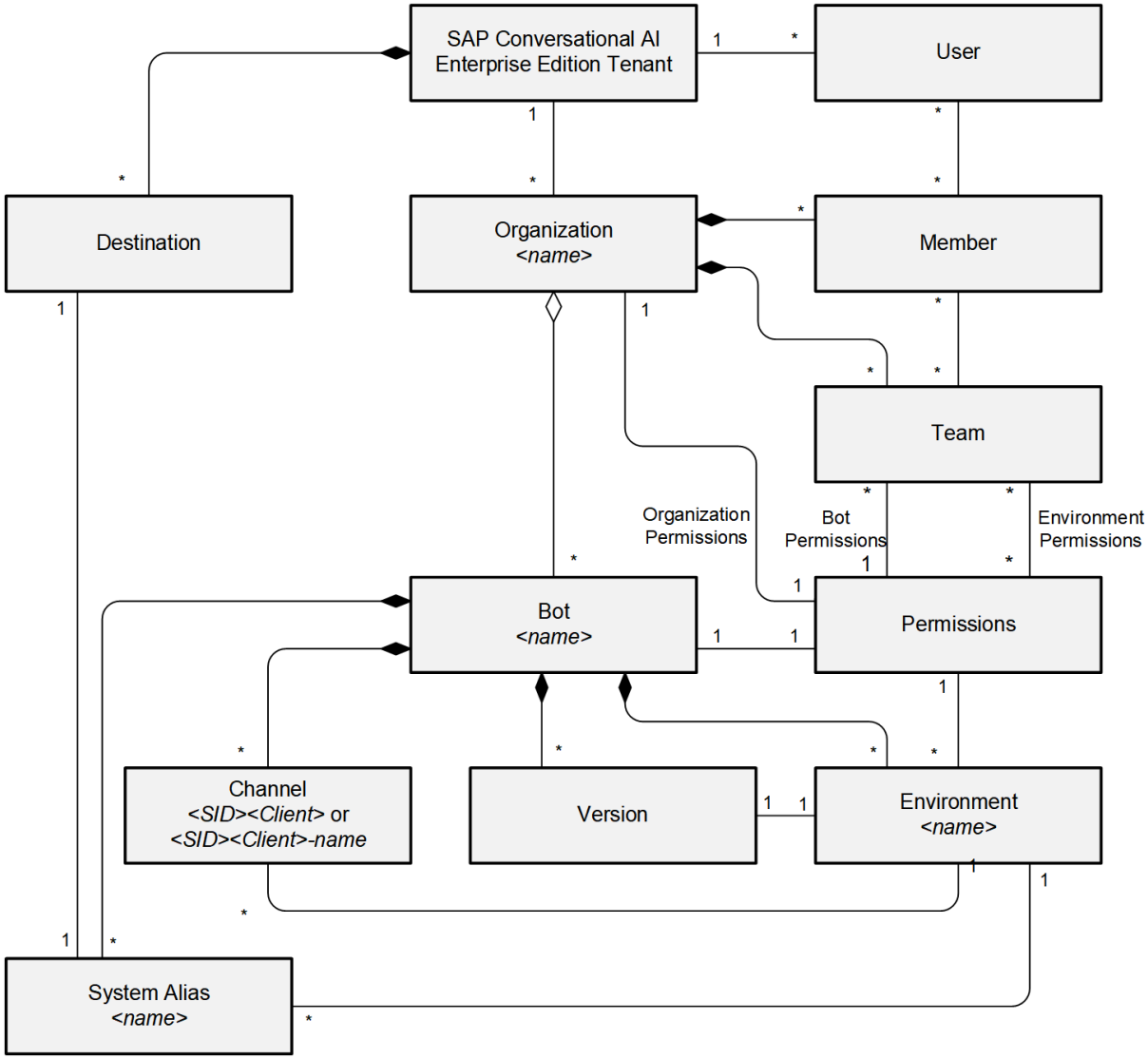
4.2 Create Organizations and Teams

Create organizations and teams to allow multiple users to collaborate on the bots in your SAP Conversational AI tenant.

1. Create organizations and teams in your SAP Conversational AI application (enterprise tenant). For more information, see Organizations.
2. Add members to the organizations and teams.

   > → Remember
   >
   > The user must have the *cai_developer* role assigned in SAP BTP and should have logged on to the SAP Conversational AI tenant at least once before being added as a member in the organization or team.

3. Assign appropriate premissions to the members based on your business need. For more information, see Permissions at Organization Level.



4.3 Import SAP S/4HANA Template Chatbot in SAP Conversational AI Enterprise Tenant

Download the SAP S/4HANA template chatbot and import it into your SAP Conversational AI tenant.

Download SAP S/4HANA Template Chatbot

In order to use the bot, you need to download the zip archive from the SCN repository and import it into the SAP Conversational AI enterprise tenant. After importing the bot, ownership may be transferred to an existing organization. For more information, see Guide for Operational Purchaser Chatbot for SAP S/4HANA.

Import SAP S/4HANA Template Chatbot in SAP Conversational AI Tenant

The template bot is downloaded in the form of content package (zip file). Save the file to your local folder and carry out the following steps:

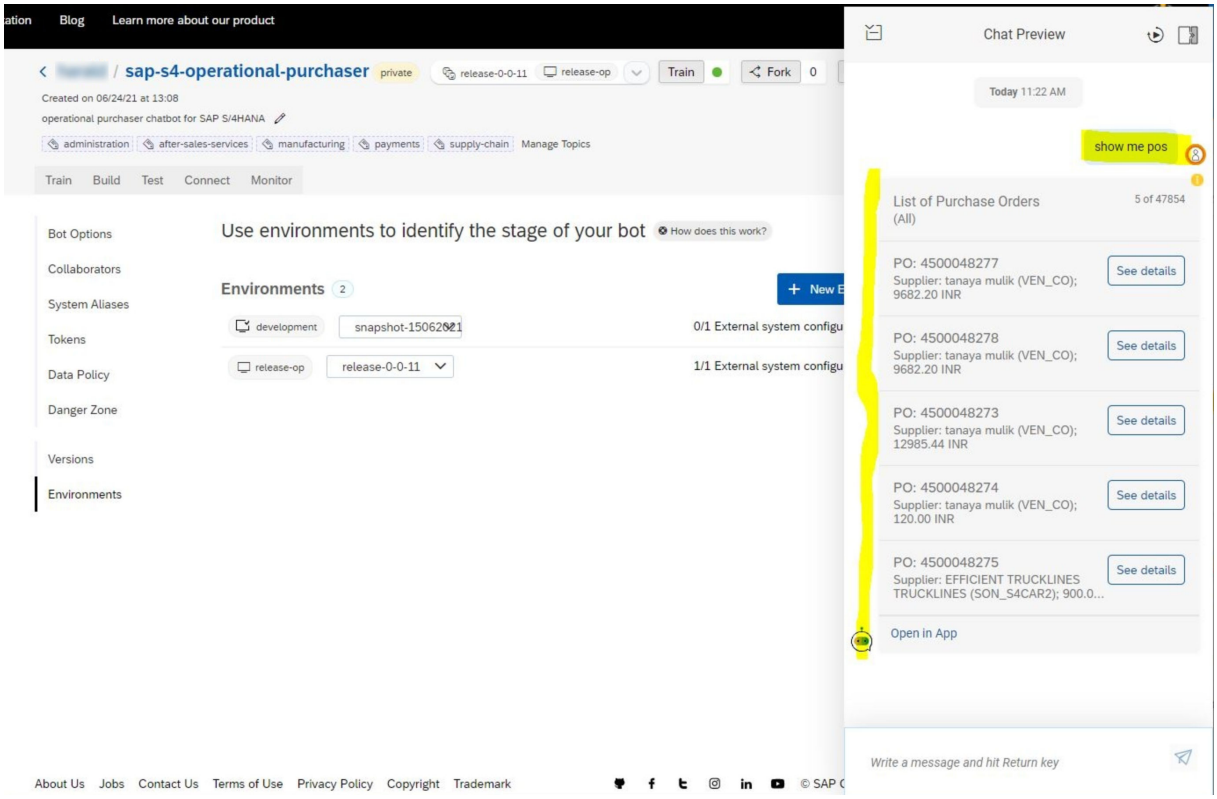
1. Login to your SAP Conversational AI enterprise tenant.
2. Import the zip file into your SAP Conversational AI enterprise tenant. For more information, see Export and Import your Bots across Tenants.

   The bot version is visible under your bot *Settings* *Versions*.
3. Assign an environment to the bot version under *Settings* *Environments*.
4. In the assigned environment, map the system alias to use the destination to connect to the SAP S/4HANA system. For more information, see Configure Destinations [page 22] and System Alias Configuration.

Test the Imported Bot Version

To test the bot version, go to your bot *Settings* and select the imported version.

Open *Chat Preview* and chat with the bot to ensure that it responds with the appropriate information.



4.4 Connect Chatbot to Web Client

Connect your chatbot to SAP Conversational AI Web Client using an application ID.

Prerequisites

To use the application ID method, the SAP Conversational AI Web Client needs to be integrated into the application shell of the SAP Fiori launchpad of the SAP S/4HANA system. For information on requirements and the integration process, see the Configuration Guide for SAP Conversational AI.

Procedure

- Provide two mandatory parameters and one optional channel title:

  Configuration

Field	Description	Example
Name	The technical name of the channel	`my-new-channel`
Application ID	For SAP S/4HANA systems with SAP Fiori launchpad as the front end, the application ID is `<SID><CLIENT>`	`ABC123`
Channel Title	A title that will be displayed in the channel selection menu when more than one channel is mapped to a given application ID.	`My Channel Title`

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP