Implementation Guide

CUSTOMER

SAP Fiori Cloud

Document Version: February 16, 2017 – 2017-02-16

SAP Fiori Cloud for SAP Business Suite - Implementation Quick Guide

SAP Fiori Cloud for SAP Business Suite

Content

1 Quick Guide for Implementation: External Access Point

The following procedure guides you through the process of setting up SAP Fiori Cloud in an external access point scenario.

> **Note**
>
> For HTML output only: To display more detailed information about the respective implementation step, click on the step title.

This implementation quick guide contains the basic information required for the respective steps with links to more detailed information, such as the underlying concepts in the landscape configuration guide or more detailed step-by-step procedures in the respective product documentation. We recommend that you right-click on these links and choose *Open Link in New Tab* (Google Chrome) or *Open in New Tab* (Internet Explorer). Otherwise, going back to this guide may be cumbersome and you easily loose track where you are.

The following figures depict the system landcsape for the external access point scenario with two different deployment options: The OData provisioning option and the SAP Gateway option.

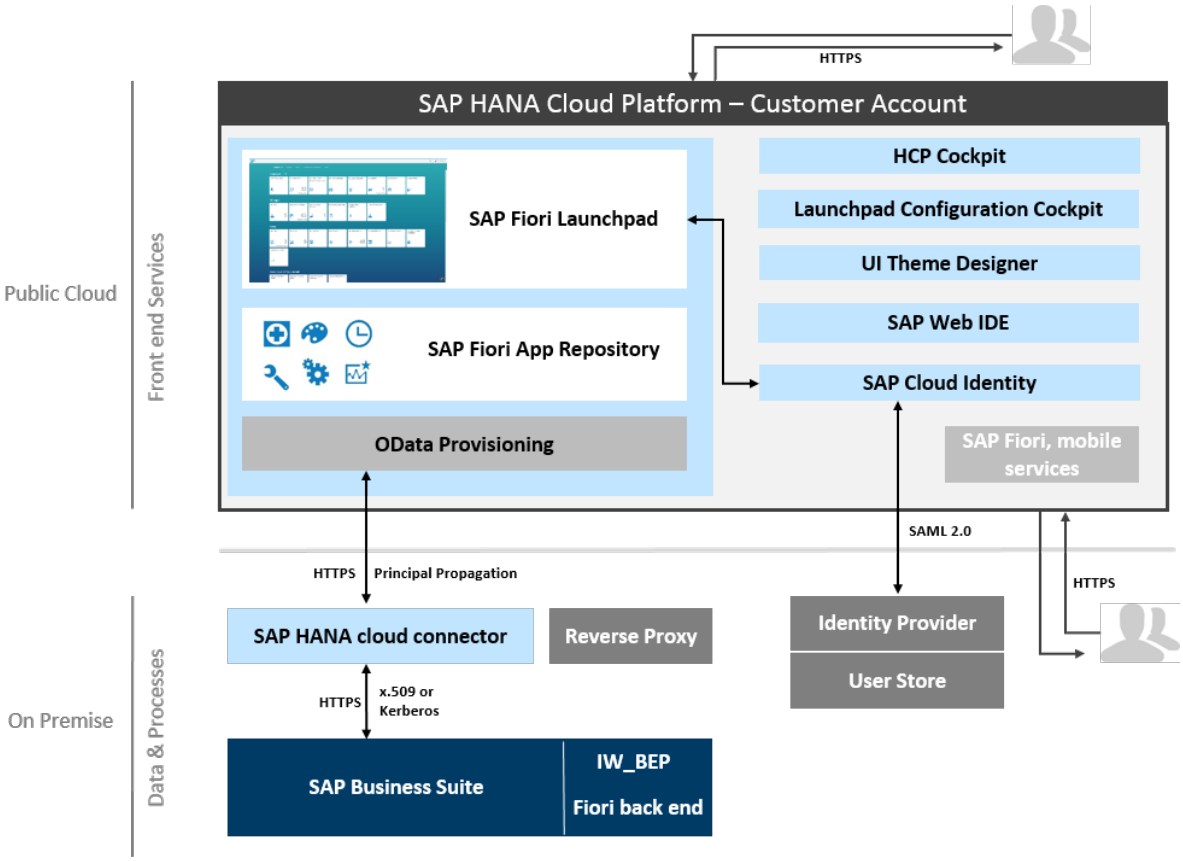

Figure 1: External Access Point Landscape with OData Provisioning

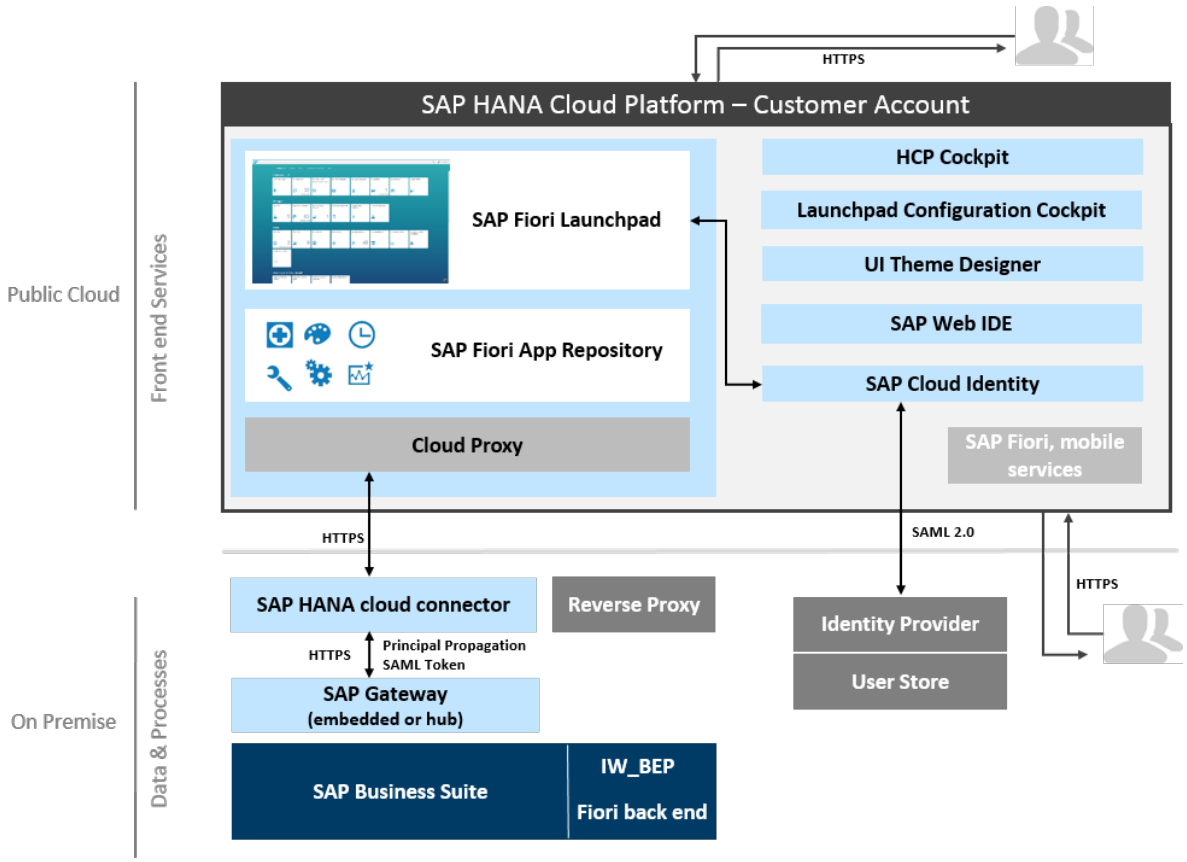

Figure 2: External Access Point Landscape with SAP Gateway

Prerequisites

When you log on to SAP HANA Cloud Platform for the first time after subscribing to SAP Fiori Cloud, you are subscribed to the portal service, but no other subscriptions or content is available.

To activate the subscriptions for your account, open the *Services* panel in your SAP HANA Cloud Platform account, choose *Portal Service* > *Go to Service*. A cloud portal site directory opens where you create a new launchpad site. The SAP Fiori launchpad configuration cockpit (FCC) opens and a popup is displayed. In the popup, select *SAP Fiori Cloud for SAP Business Suite* and choose *Add Content*. If you skip the popup, you can access it back by choosing *Add Content to Launchpad* from the user menu in the upper right corner.

Once you have selected the content, the popup no longer appears when you open the FCC and the entry in the user menu disappears. Your content and subscriptions will then be available in your account and you can start with the implementation.

Your choice is account-specific: If you create a new account on SAP HANA Cloud Platform, the dialog appears again when you log on to FCC the first time.

Step 1: Select the SAP Fiori Apps for SAP Fiori Cloud

Currently, SAP Fiori Cloud provides an extract of the available SAP Fiori apps. Whereas the front end components for the SAP Fiori apps for SAP Fiori Cloud are provided by the SAP HANA Cloud Platform, you have to make sure that the required back end components are available in your back end system.

The SAP Fiori apps reference library contains information about the product features as well as information about the required back end components, versions, and support packages for each app and enables you to decide about the apps you want to implement.

To access the SAP Fiori apps reference library and to send the information about the back end requirements to the system administrator, proceed as follows:

1. Open the SAP Fiori apps reference library under http://www.sap.com/fiori-apps-library and select the *Available via SAP Fiori Cloud* category on the left hand side.
2. From the list of available apps, select the apps that you want to implement:
   - To create a holistic view of the required implementation and configuration steps, choose *Aggregate*.
   - To share this information with the system administrator who has to make sure that all required back end requirements are met, choose *Share*.

   The system administrator needs this information later in the process for setting up the back end and the connection to HCP.

More Information

Access to the SAP Fiori App Reference Library: http://www.sap.com/fiori-apps-library

Step 2: Set Up Your SAP HANA Cloud Platform Account

Your account on SAP HANA Cloud Platform is your single point of access to all services for configuring the cloud-side of SAP Fiori Cloud. When you sign up for SAP Fiori Cloud, your account on the SAP HANA Cloud Platform is provided to you, fully provisioned with the required services. The account information that you need for initial logon is provided in the e-mail you receive after you have signed up for SAP Fiori Cloud.

Log on to SAP HANA Cloud Platform. On the overview page, you can do the following:

- Create additional accounts for your organization.
- Manage the quota.
- Create integration tokens.

When you open your *Account*, all services you require for setting up and configuring SAP Fiori Cloud as described in the following steps are available in the panel on the left hand side.

More Information

Managing the account: Managing Accounts and Quota in the SAP HANA Cloud Platform documentation

For setting up additional accounts, see *Lifecycle Management*.

Step 3: Assign SAP HANA Cloud Platform Member Roles

Members can access accounts and use the SAP HANA Cloud Platform cockpit based on their assigned roles. The roles define the scope of the available functionality the user can access.

When you subscribe to SAP Fiori Cloud, the initial account information is part of the sales order and contains the HCP access data for the *Administrator* member role. We recommend to create at least two more administrators immediately after you receive the initial account information. This avoids roadblocks in the implementation due to an unavailability of the HCP access data. Alternatively, if you do not have access to the initial account information, open a ticket to get another user with *Administrator* role added.

Prerequisites:

- You have a user with *Administrator* role for your HCP account.
- The members you want to add have a SAP user ID. The user IDs can be requested on SAP Service Marketplace under http://service.sap.com/request-user. These users are automatically registered with the SAP ID service, which controls user access to SAP HANA Cloud Platform.

To add account members and assign roles, open the *Members* panel in the SAP HANA Cloud Platform cockpit and choose *Add Members*. Enter the user IDs and select the respective roles.

More Information

About account member roles: Account Member Roles in the SAP HANA Cloud Platform documentation

About adding members: Managing Members in the SAP HANA Cloud Platform documentation

Step 4: Install, Configure, and Activate SAP Gateway (On-Premise Installation Only)

You use the SAP Gateway to set up and activate the OData services which retrieve the business data for the SAP Fiori apps from your back end system.

> **Note**
>
> This step is only required if you use the SAP Gateway on-premise in either the hub or embedded deployment option, see *System Landscape and Architecture*.

Prerequisites:

If no SAP Gateway is installed yet, choose one of the deployment options for SAP Gateway and install the SAP Gateway components accordingly. For more information, see the SAP Gateway Installation Guide under SAP Gateway Installation Guide.

The following steps only give a rough overview about the mandatory and optional configuration tasks. For configuring and activating the SAP Gateway, use the SAP Gateway Configuration Guide.

1. Make the general configuration settings (mandatory).
2. Configure the OData channels (mandatory).
3. Configure the settings for content scenarios (optional).

More Information

SAP Gateway documentation: SAP Gateway

How to configure SAP Gateway: SAP Gateway Configuration Guide

Step 5: Install Back End OData Components

Based on the aggregated information from the SAP Fiori apps reference library, the system administrator installs all required back end components and applies the required notes.

The steps below describe the general process that we recommend. For a detailed step-by-step description, see the chapter *Maintenance Planner-Based SAP Fiori Installation* in the Maintenance Planner User Guide.

You can also download the required files directly from the SAP Software Download Center and deploy them manually. This allows you to deploy only single product versions. For more information, see Downloading and Installing Product Versions in the SAP Fiori documentation.

Proceed as follows:

1. To plan the additions to your on-premise system and to download the corresponding software components, use the Maintenance Planner. You can choose *Prepare apps for planning with Maintenance Planner* in the SAP Fiori apps reference library, however, we strongly recommend to call the Maintenance Planner directly.

   > **Note**
   >
   > The Maintenance Planner includes the SAP Fiori front end UI add-ons in the `stack.xml` and archives in your download basket. However, they are not required for SAP Fiori Cloud. They are deployed in your SAP Gateway system and are available to connect on-premise SAP Fiori apps which are not available for SAP Fiori Cloud.

2. Use the Software Provisioning Manager for the installation of new components or the Software Update Manager for updates of the existing components for the installation in your on-premise system.
   Both tools are available on the SAP Service Marketplace as part of the Software Logistics Toolset.

   > **Note**
   >
   > For information about Software Update Manager (SUM) and the Support Package Manager (SAINT), the two options for updating the system, see SAP note 1803986.

3. In addition to the components, it may be necessary to install SAP notes. The required notes are mentioned in the SAP Fiori apps reference library, however, we recommend that you perform a search in SAP notes.

Post-Installation Tasks

After the installation of the back end components, open transaction `SU25` in your back end system and run the postprocesses 2A, 2B, and 2C. This may be necessary to update the existing user roles.

For testing, create a new user, for example `FIORIUSER`, and add the roles of the SAP Fiori apps to this user in transaction `PFCG`. Depending on the app, additional authorizations may be required, see the *Troubleshooting* section below.

Step 6: Set Up SAP HANA Cloud Connector

The SAP HANA cloud connector runs as an on-premise agent in a secured network and acts as a reverse invoke proxy between the on-premise network and SAP HANA Cloud Platform (HCP). Due to its reverse invoke support, you do not need to configure the on-premise firewall to allow external access from the cloud to the on-premise systems, the SAP HANA cloud connector builds a secure tunnel between the SAP HANA Cloud Platform and your on-premise system.

Prerequisites: See the prerequisites for using the SAP HANA cloud connector at Prerequisites in the SAP HANA cloud connector documentation.

To install and configure the SAP HANA cloud connector, proceed as follows:

1. Install the SAP HANA cloud connector.
   The SAP HANA cloud connector is free. You can download it from https://tools.hana.ondemand.com/#cloud. For the installation, follow the installation procedure in the SAP HANA cloud connector documentation under Installing the Cloud Connector.
2. Set up the cloud connector.
   To open the cloud connector, enter the following URL in your Browser: `https://<hostname>:<port>`. `<hostname>` refers to the machine on which you have installed the cloud connector in step 1 and `<port>` is the connector port you have specified in step 1 (default is `8443`).
   Follow the steps described in the SAP HANA cloud connector documentation under Initial Configuration.

   > **Note**
   >
   > Cloud connector has no function to restore a password or to request a new password. Make sure that you store the password in a secure location.
   >
   > You can also use LDAP (Lightweight Directory Access Protocol) to configure the cloud connector authentication, see Using LDAP for Authentication.

3. Choose *Connect* to establish and test the connections to the SAP HANA Cloud Platform and the back end system.

   > **Tip**
   >
   > You can only connect one cloud connector. If you get the green traffic light for the test, but the `CONNECT_FAILED` message, check if another cloud connector is already running.

More Information

SAP HANA Cloud Connector documentation: SAP HANA Cloud Connector

Step 7: Set Up Destinations to Back End System in SAP HANA Cloud Platform

> **Note**
>
> This step is relevant if you use the SAP Gateway on-premise for OData connection. If you use the OData provisioning service, continue with step 8, see Step8: Activate IW_BEP Services for OData Provisioning in the Back End System [page 9].

The SAP Fiori apps in your SAP Fiori Cloud subscriptions are preconfigured with the destination name `SAP_GATEWAY`. If you use this name for the destination, the apps are automatically assigned to the destination. If you use a different name, you have to assign this destination to each subscription manually.

1. Open *Destinations* from the *Connectivity* panel in the SAP HANA Cloud Platform cockpit and choose *New Destination*.
2. If you use the SAP Gateway for exposing your back end system to the Internet, enter the following information:
   - Name: `SAP_Gateway`
   - Type: `HTTP`
   - Description: <SAP Gateway System>
   - URL: `https://gateway:50001`
   - Proxy Type: `OnPremise`
   - Authentication: `PrincipalPropagation`
3. Save your entries.

More Information

About destinations: Configuring Destinations from the Cockpit

Step 8: Activate IW_BEP Services for OData Provisioning in the Back End System

> **Note**
>
> This step is relevant if you use the OData provisioning service.

Enable the back end access for the OData provisioning service in the back end system as follows:

1. In transaction `PFCG`, create a new custom role for your user with the authorization template `/IWBEP/RT_MGW_ADM`.
2. In transaction `SU01`, create the back end user and assign the custom role. You can also use an existing user with the required authorizations.
3. In transaction `SICF`, activate `SAP/IW_BEP`.

> **Note**
>
> To activate role assignments in the HCP, you need to refresh the session.

Step 9: Assign Authorization Roles to Users in the Back End System

Back end authorization roles are provided for the OData services. These roles need to be assigned to users. The role information is available in the aggregated information in the SAP Fiori app reference library under *Aggregated Configuration Information* > *Back-End Authorization Roles (PFCG)*.

To assign the roles to users, proceed as follows:

1. In transaction `PFCG`, enter the role name according to the information in the SAP Fiori app library.

   > **Note**
   >
   > Some roles provide an authorization template and not a role. In this case, create a custom role with the authorization template.

2. Open the *User* tab and enter the User IDs.
3. Save your entries.

> **Note**
>
> To activate role assignments in the HCP, you need to refresh the session.

Step 10: Set Up OData Provisioning Service on HCP

> **Note**
>
> This step is only relevant if you use the OData provisioning service for OData connection.

The OData provisioning service is available in the *Services* panel of the SAP HANA Cloud Platform cockpit and can be used to establish a connection to exchange business data between the back end system and the HCP via OData services.

To set up the OData provisioning, proceed as follows:

1. In the *Roles* panel of the *OData Provisioning Configuration*, assign the `GW_Admin` and `GW_User` role to your HCP account user.
2. Open the *Destinations* panel of the SAP HANA Cloud Platform cockpit and create the destination to the OData provisioning service.
   The SAP Fiori apps in your SAP Fiori Cloud subscriptions are preconfigured with the destination name `SAP_Gateway`. If you use this name for the destination, the apps are automatically assigned to the destination. If you use a different name, you have to assign this destination to each subscription manually.
   - Name: `SAP_Gateway`
   - Type: `HTTP`
   - Description: <optional>
   - URL: <Start the service and use the URL in the address bar of your browser>
   - Proxy Type: `Internet`
   - Authentication: `AppToAppSSO`
3. Open the *OData Provisioning* service from the *Services* panel of the HCP cockpit and choose *Configure OData Provisioning* > *Destinations*. Enter the destinations URL of the back end system where your OData service implementations are present.

> **Note**
>
> The on-premise URL of your back end systems must be whitelisted in the SAP HANA cloud connector. For this, enter the system and path in the *Connectivity* panel under *Access Control*. The URL path is `/sap/iwbep`.

- Name: `SAPERP`
- Type: `HTTP`
- Description: <Name of your back end system>
- URL: Enter the URL you created as destination to back end system in the SAP HANA cloud connector: `https://<virtualhost>/sap/iwbep?sap-client=<client>`.
- Proxy Type: `OnPremise`
- Authentication: `PrincipalPropagation`

> **Tip**
>
> For testing purposes, you can set the Authentication to `BasicAuthentication` and use a HTTP connection in the URL. In this case, you have to enter the user and password of the back end user you have created in step 8, see Step 8: Activate IW_BEP Services for OData Provisioning in the Back End System [page 9]. Make sure that you set the Authentication to `PrinicpalPropagation` and connection to HTTPS before you go live with the solution.

4. Choose *Go to Service*. The *OData provisioning Administration* opens. Select the OData service name and choose *Register*. Register the OData services for all SAP Fiori apps you want to use. You find the information in the aggregated documentation from the SAP Fiori apps reference library.
5. In the *Roles* panel of the *OData Provisioning Configuration*, assign the *GW_User* role to all users who access the SAP Fiori apps.

> **Note**
>
> To make this easier for large number of users, you can define groups and assign the role to the group. The users must then be assigned to the group in the *Trust* panel of the HCP Cockpit.

6. To check if the OData services are running, open the OData provisioning Administration and choose *Open Service Document*.

> **Note**
>
> By default, the OData provisioning service caches the OData metadata. When you change the OData service, refresh the metadata cache as follows: Open the OData provisioning menu and choose *Metadata* > *Metadata Cache Cleanup* > *Clear*.

> **Tip**
>
> In case of issues, check Troubleshooting [page 15] section below.

More Information

OData provisioning documentation in the SAP HANA Cloud Platform documentation: OData Provisioning: Administration

Step 11: Register OData Services in the SAP Gateway System

> **Note**
>
> This step is only required if you use SAP Gateway on premise for the OData connection.

You find the required OData service names in the *Aggregated Configuration Requirements* section of the aggregated app information from the SAP Fiori app reference library. Go to the *OData Services* section and note the OData services and versions you need.

> **Note**
>
> For activation of OData services when you use the OData provisioning service, see Step 8: Set Up Odata Provisioning Service [page 10].

To register the OData services in the SAP Gateway system, proceed as follows:

1. Assign OData service authorizations in SAP Gateway.
   In the SAP Gateway system, assign the OData service authorization to a new or existing role, such as a business role that has been adjusted according to your needs. Proceed as follows:
   1. In transaction `PFCG` create the role `Z_GW_USER` with the authorization profiles `/IWFND/RT_GW_USER` and `S_SERVICE`. Assign this role to your Fiori user and Fiori admin user.
   2. In transaction `PFCG` create the role `Z_GW_ADMIN` with the authorization profile `/IWFND/RT_ADMIN`. Assign this role to your Fiori admin user.
2. Open transaction `/IWFND/MAINT_SERVICE` and choose *Get Services* or filter for specific service.
3. Select the service and add the selected services.
4. On the *Activate and Maintain Services* page, double check that your services have been added to the list of services.
5. Select one of the OData services and choose *SAP Gateway Client* > *Execute*. Check the response and test one of the collections.

> **Note**
>
> Instead of activating OData services individually for each app, use a task list to activate the OData services for several apps at the same time.

More Information

For using task lists for the activation, see Activating OData Services for Several SAP Fiori Apps.

Step 12: Configure the SAP Fiori Apps in the Back End System

Check in the back end configuration section of the aggregated information from the SAP Fiori apps documentation if configuration in the back end system is required for the apps.

Step 13: Configure the SAP Fiori Apps in the SAP Fiori Configuration Cockpit

The SAP Fiori apps are now deployed to the SAP HANA Cloud Platform and you can start the configuration in the SAP Fiori launchpad configuration cockpit (FCC). You can access the FCC either from the SAP Fiori launchpad or from the *Services* panel of the SAP HANA Cloud Platform.

The required fields are preconfigured. You can adapt this configuration, if required.

More Information

About the SAP Fiori Launchpad Configuration Cockpit

SAP Fiori: Let's talk FCC - Part 1 - 3

Step 14: Set Up User Authentication and Principal Propagation in the SAP HANA Cloud Connector and on HCP

The user authentication establishes and verifies the identity of a user. This is a prerequisite for accessing the SAP Fiori apps. The apps are protected with a SAML 2.0 authentication method, authenticating the user against a trusted identity provider. This authentication method is used in combination with principal propagation through short-lived certificates to pass the user identity from the client.

> **Tip**
>
> To simplify the process, you can start with a basic authentication setup to check that your app is working and the back end user roles are set properly before you configure the principal propagation. For more information, see Troubleshooting [page 15].

Proceed as follows:

1. Configure trust in the SAP HANA Cloud Connector, see Configure Trust in the Cloud Connector.
2. Configure the settings for SAML 2.0 communication between HCP and the trusted identity provider in the *Trust* panel of the HCP cockpit, seeID Federation with the Corporate Identity Provider.
3. Establish trust between HCP and your corporate IdP.
4. Establish trust on the level of your corporate IdP to the service provider on HCP.
5. Establish user propagation by means of the *PrincipalPropagation* property in the *Destinations* panel of the HCP cockpit.
6. Connect to the user store. If you have an existing on-premise system with a populated user store, you can connect SAP HANA Cloud Platform to use this on-premise user store via the SAP Cloud Identity service. This connection is used to check credentials, search for users, retrieve user details, and retrieve information about the groups a user is a member of, which can then be used for authorization.

   > **Note**
   >
   > You can also use SAP Cloud Identity service to create the users in HCP. However, for the authentication with your back end system to work properly, these users have to correspond to the users in your back end system, meaning double maintenance of all users. This apporach is intended mainly for use in demo systems with a limited user base. For productive use with a larger number of users, we recommend to connect your back end user base to HCP.

Test the SAP Fiori Apps

You can now open the apps from the SAP Fiori launchpad and check if the back end connection works.

More Information

Principal Propagation Authentication

SAP Cloud Identity Service

Corporate User Store, section *Configure Connection to a Corporate User Store*

Step 15: Set Up Authorization Flow

You define the authorization flow by means of users, roles and user groups which you assign to application roles and catalogs.

Assigning Cloud Portal Roles to User Groups and Users

First, you assign SAP Fiori launchpad on cloud users to business roles and define groups. Open the Portal service in the HCP Cockpit and choose *Configure Portal Services Roles*. Here you can create new roles and groups and assign users to roles and groups.

The `TENANT_ADMIN` role is predefined to your user. Assign this role to other users who shall have administrative permissions over the launchpad, and access the SAP Fiori configuration cockpit (FCC). You can assign the role to single users or you can define a group for users with admin rights and assign the role to the group.

More information:

About Roles in the SAP HANA Cloud Portal documentation

Assign Content to Roles

1. Assign end users to a user group by means of SAML 2.0 assertions.
   SAML 2.0 assertions can be used to transfer user attributes from an identity provider (IdP) to a service provider. The attributes can be specified on IdP level and may also be used to transfer information about user groups. The IdP may have a custom configuration concerning which user groups are to be included into the target assertion. The way the attributes are transferred is standardizes and based on SAML 2.0 specification. On the service provider side, a user can be mapped automatically to user groups based on the attribute valies. The user groups must be created manually by the customer's administrator. For more information, see Corporate Identity Providers.
2. Define the application roles.
   Open the *Subscriptions* panel in the HCP cockpit and choose one of your subscribed apps. Open the *Roles* panel and create the required roles for the app. These roles should be associated with the target business scenarios that are available for your end users. For more information, see Managing Roles.
3. Assign user groups to the app roles.
   You can assign user groups to the app roles either in the *Roles* panel of the *Subscriptions* panel in the HCP cockpit, or on the *Authorizations* panel.
4. Include the app role in a catalog.
   You use catalogs for application role assignment. A content admin has to add the application toles to the correpsonding vatalogs. All users assigned to the application role via the user group can access the content of the catalogs that are also assigned to this application role. This means that all users assigned to a certain user group in a target IdP or LDAP system have access to all application roles in the corresponding catalog.

To assign the app role to catalogs, open the SAP Fiori configuration cockpit and select *Catalogs*.

> **Tip**
>
> In case of issues, see Troubleshooting [page 15].

Troubleshooting

The following sections provide troubleshooting information about some issues that have come up so far. For updates, also check out the Tips and Tricks for On-Boarding SAP Fiori Cloud blog.

User Cannot Access Data From an App - Missing User Roles (Step 14)

Some SAP Fiori apps require additional roles for accessing the data. If the roles are missing, the user gets an data access error when he wants to open the app. If you are not sure about the required roles, proceed as follows:

1. Add the `SAP_ALL` authorization template to your user.
2. Open transaction `ST01` and start a trace for authorization check. Set a filter for your user ID.
3. Call the SAP Fiori app with your user. The trace log shows a list of all authorization objects.
4. Add these authorization objects to your user, for example, by creating a custom role in transaction `PFCG`.
5. Remove the `SAP_ALL` authorization and try again.

OData Service Registration is Not Possible in OData Provisioning (Step 8)

If you try to register an OData service and you cannot see any services, check the SAP Cloud Connector log for the following entry:
sap.core.connectivity.protocol.http.handlers.HttpProtocolOutboundHandler#tunnelclient-5-1#0xd2e301e#Access denied to / for virtual host. If this log entry exists, check the following:

- Open transaction `SICF` in your back end system and make sure that `sap/iwbep` is activated.
- For accessing the `IW_BEP` component from the OData provisioning service, the `/IWBEP/RT_MGW_ADM` authorization template is needed. If your user does not have the required authorization, create a new role in transaction `PFCG` in the back end system, add the authorization template, and map the role to your user.
- Check if your `sap-client` is set in the URL in the destination configuration, e.g. `http://s2y:8000/sap/iwbep?`**`sap-client=300`**.
- For principal propagation, a trust to the OData provisioning service (gwaas) must be defined in the SAP Cloud Connector. Choose *Synchronize* to make sure that all services are displayed.

End-to-end Trust With Principal Propagation has Errors (Step 13)

Errors in your security settings may cause the following issues when you set up E2E trust with principal propagation:

- User is not able to log on to the SAP Fiori launchpad
  Possible error: Wrong SAML2 assertion
  The role that is defined for your user in your IdP may not match the group and role settings for your HCP service. To check the assertion, use a browser tool (SAML tracer).
- User gets an Authentication Required dialog when calling an SAP Fiori app
  Possible errors:

- Wrong principal is propagated: The user is not accepted by the back end. Use a SAML tracer: Enable SCC trace and set the log level to *Debug*. If the SCC log shows a similar entry, check your IdP settings: *#DEBUG'com.sap.scc.security#tunnelclient-5-1#0x26df8606#Generated X.509 certificate with subject CN=<wrong principal>*.
- Broken mutual SSL between SCC and ABAP: Analyze the ICM trace on ABAP.
- Broken trust SCC to ABAP: Analyze the SCC log and SMICM trace on ABAP.

Use Basic Authentication Instead of Principal Propagation for the First Setup (Step 13)

To make the implementation process easier, it may be helpful not to start with a full E2E security setup and use a basic authentication setup for your development environment instead. This enbles you to check if your app is working and the back end user roles are set properly before you set up the full security settings for principal propagation.

To set up basic authentication, change the following setup steps:

- Check in your backend (RZ10) that no icm/HTTP/redirect is set for the HTTP port
- In SCC create a HTTP connection to your backend with no principial type
- In the OData Provisioning setup create a destination with basic authentication. Use the credentials of your test user. Be sure that the oData service in OData Provisioning is registered by using this destination. When you later change the setup to prinicipal propagation you should delete and register the service again.

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

go.sap.com/registration/contact.html