Implementation Guide

CUSTOMER

SAP Fiori Cloud
Document Version: 3.0 – 2016-10-31

SAP Fiori Cloud for S/4HANA - Implementation Quick Guide

Content

1 Quick Guide for Implementation: Internal Access Point

The following procedure guides you through the process of setting up SAP Fiori Cloud in an internal 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 figure depicts the system landcsape for the internal access point scenario.

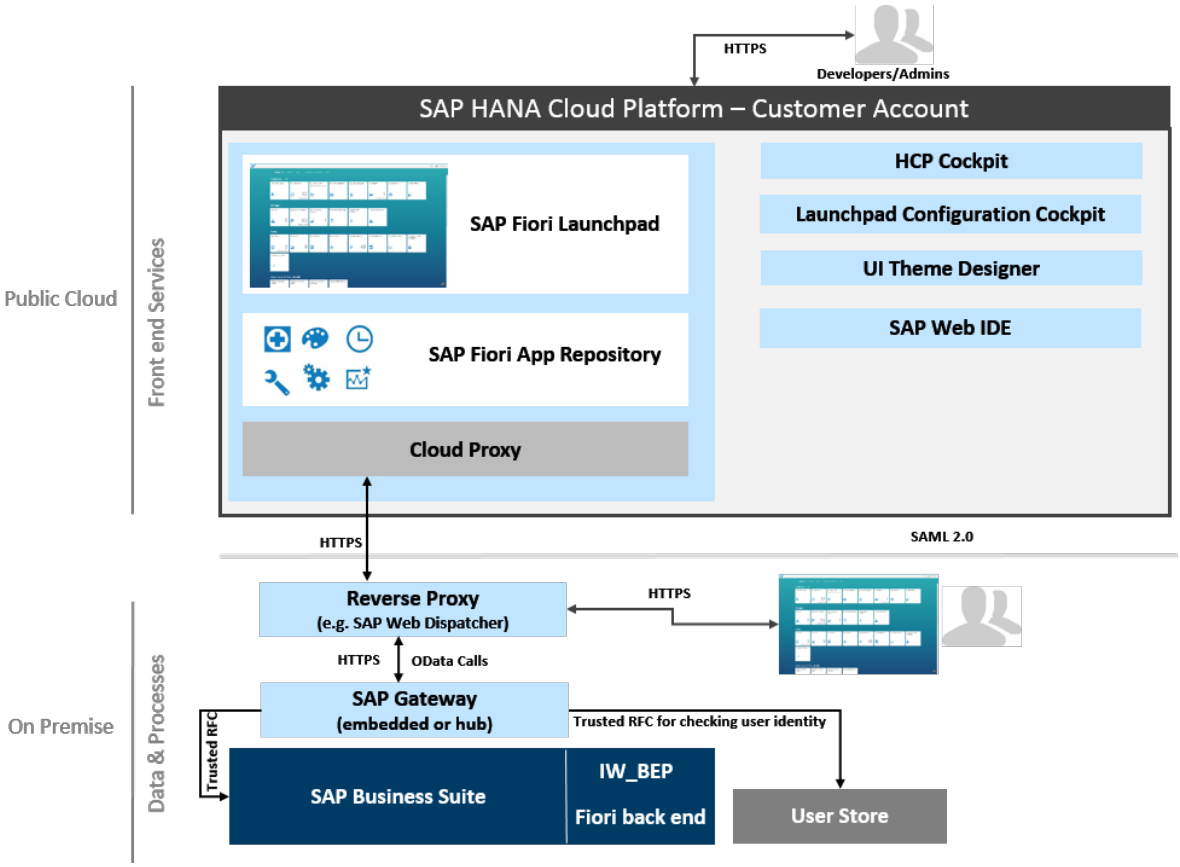


Figure 1: Internal Access Point Landscape

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 S/4HANA* 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 https://fioriappslibrary.hana.ondemand.com and select the *SAP Fiori Apps on SAP HCP* 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 system and the connection to the SAP HANA Cloud Platform.

More Information

Access to the SAP Fiori App Reference Library: http://www.sap.come/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* in the SAP Fiori Cloud Landscape Configuration Guide.

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.

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.

> **Note**
>
> 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.

Step 6: Assign Back End Authorization Roles

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. Open transaction `PFCG` in the back end system and enter the role name.

> **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.

Step 7: Register, Confirm, and Test OData

SAP Fiori uses OData as protocol for the communication with the back end system. OData is a RESTful protocol, leveraging HTTP GET/POST/PUT methods. The OData services are provided by the SAP Gateway server or the OData provisioning service on HCP.

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.

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 8: Configure the SAP Fiori Apps in the Back End

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

Step 9: Configure the SAP Fiori Apps in the SAP Fiori Launchpad 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 10: Set Up User Authentication and Principal Propagation

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.

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.

More Information

Principal Propagation Authentication

SAP Cloud Identity Service

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

Step 11: 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*.

Step 12: Set Up and Configure the Reverse Proxy

A reverse proxy loads the UI components from the SAP HANA Cloud Platform while the OData calls remain in the customer's network. The reverse proxy is installed and running in the on premise landscape. You can, for example, use the SAP Web Dispatcher as reverse proxy for SAP Fiori Cloud. For information about installing the SAP Web Dispatcher, see Importing the SAP Web Dispatcher. If you use a different reverse proxy, see the documentation of the respective reverse proxy.

The SAML2 identity provider is configured in HCP, see Set up Authorization Flow [page 9].

The SAML2 identity provider is configured in the same ABAP AS in which the SAP Gateway is running, see Using SAML 2.0.

> **Note**
>
> In the SAML2 IdP service provider configuration, all end points to the SAP Gateway should have the reverse proxy host name. For example, if the gateway host name is `my-sap-gateway.internal.corp` and the reverse proxy host name is `my-reverse-proxy.internal.corp`, for the assertion consumer service endpoint `https://my-sap-gateway.internal.corp/sap/saml2/sp/acs/000` should be replaced with `https://my-reverse-proxy.internal.corp/sap/saml2/sp/acs/000`.

> **Note**
>
> Blocking third-party cookies in your web browser can cause problems in the authentication flow between the SAP Fiori launchpad and the Gateway system. To avoid this, apply one of the following options:
>
> - Run the SAML2 IdP and the reverse proxy on the same domain.
> - Enable third-party cookies in the web browser.
> - If third-party cookies shall be disabled, add an exception for the SAML2 IdP domain; note that this option is not applicable in mobile devices.

Apply the SAP notes 1977537 and 2193513 to your SAP Gateway system if they do not already exist in your installed support package.

To set up SAP Fiori launchpad and SAP Gateway access for the internal internal access point scenario, you need to set up and configure the reverse proxy:

> **Note**
>
> The configuration examples in the following procedure are using the SAP Web Dispatcher as an example for reverse proxy configuration. However, you can use any standard reverse proxy as well. For information about the required configuration, see the documentation of the respective reverse proxy.

1. The reverse proxy accesses the SAP Fiori launchpad with a preconfigured custom domain.

   > **Note**
   >
   > Before you start with the configuration, you need to have a quota for domains configured for your account, see Purchasing a Customer Account. For further prerequisites for the configuration of the custom domain, see Configuring Custom Domains and Prerequisites.

   Proceed as follows:

   1. Install the SDK tool, see Installing the SDK.
   2. Follow the custom domain configuration as described under Configuring Custom Domains.

   > **Note**
   >
   > In the following steps, `mycustomdomain.com` is used as custom domain and `my-reverse-proxy.internal.corp` is used as reverse proxy domain.

2. Add the routes to SAP Fiori launchpad (FLP) on cloud and to the SAP Gateway system in the configuration file for reverse proxy properties.

   > **Note**
   >
   > The port for the SAP Fiori launchpad and SAP Gateway routes shall be the default SSL port – 443.

   - Route to FLP on cloud:
     The URL paths that start with the following paths should be routed to your SAP Fiori launchpad on custom domain (`mycustomdomain.com`) after each route: `/cloud/flp /sites /sap/fiori /sap/bc/lrep /saml2 /fiori /v1 /portal /flp /themedesigner /api /orion /resources/sap/dfa/help /sap/ui5/1/resources/sap/dfa/help /sap/ui5/1/innovation/resources/sap/dfa/help /sap/ui5/1/fcc/resources/sap/dfa/help /sap/dfa/help /sap/bc/ui2/app_index /sap/backend/`

     > **Example**
     >
     > **Example:** Routes from SAP Web Dispatcher to FLP on cloud:
     >
     > - `SID` = unique system ID, for example `FLP`
     > - `EXTSRV` = `mycustomdomain.com` (custom domain as defined in step 1)
     > - `SRCSRC` = `443` (default SSL port)
     > - `SRCURL` = `/cloud/flp;/sites;/sap/fiori;/sap/bc/lrep;/saml2;/fiori;/v1;/portal;/flp;/themedesigner;/api;/orion;/resources/sap/dfa/help;/sap/ui5/1/resources/sap/dfa/help;/sap/ui5/1/innovation/resources/sap/dfa/help;/sap/ui5/1/fcc/resources/sap/dfa/help;/sap/dfa/help;/sap/bc/ui2/app_index;/sap/backend`

- `PROXY` = Customer network proxy
- Additional settings: `STANDARD_COOKIE_FILTER = OFF`, `SSL_ENCRYPT = 2`

```
wdisp/system_8 = SID=FLP, EXTSRV=https://mycustomdomain.com:443, SCRSRV=*:
443, SRCURL=/cloud/flp;/sites;/sap/fiori;/sap/bc/lrep;/saml2;/fiori;/v1;/
portal;/flp;/themedesigner;/api;/orion;/resources/sap/dfa/help;/sap/ui5/1/
resources/sap/dfa/help;/sap/ui5/1/innovation/resources/sap/dfa/help;/sap/
ui5/1/fcc/resources/sap/dfa/help;/sap/dfa/help;/sap/bc/ui2/app_index;/sap/
backend, PROXY=<customer's proxy>, STANDARD_COOKIE_FILTER=OFF,
SSL_ENCRYPT=2
```

- Route to SAP Gateway system:
  The URL paths that start with the following paths should be routed to your SAP Gateway system (`my-sap-gateway.internal.corp`) after the routes: `/sap/opu/odata /sap/saml2`.

  ### Example

  Example: Routes to the SAP Gateway system:

  - `SID` = SAP system ID, for example `XYZ`
  - `NR` = SAP system number
  - `CLIENT` = SAP system client
  - `MSHOST` = Message server host
  - `MSPORT` = Message server port
  - `SRCSRV` = `443` (default SSL port)
  - `SRCURL` = SAP Gateway OData (`/sap/opu/odata`) and SAML2 paths (`/sap/saml2`)
  - Additional settings: `STANDARD_COOKIE_FILTER = OFF`

  ```
  wdisp/system_1 = SID=<SAP system ID>, NR=<nr>, CLIENT=<client number>,
  MSHOST=<MS host>, MSPORT=<MS port>, SCRSRV=*:443, SRCURL=/sap/opu/
  odata;/sap/saml2, STANDARD_COOKIE_FILTER=OFF
  ```

- Enable the port in the reverse proxy for SAP Fiori Cloud routes.

  ### Example

  For SAP Web Dispatcher, enable port 443:

  - `PROT` = Transfer protocol, `HTTPS`
  - `HOST` = SAP Web Dispatcher host name
  - `PORT` = Default SSL port
  - `EXTBIND` =

  ```
  icm/server_port_1 =
  PROT=HTTPS,HOST=mywebdispatcher.zdm.corp,PORT=443,EXTBIND=1
  ```

3. All routes that the reverse proxy forwards to the SAP Fiori launchpad (`mycustomdomain.com`) should be updated with the following headers:
   - `HOST`: Reverse proxy host (`my-reverse-proxy.internal.corp`)
   - `X-Custom-Host`: SAP Fiori launchpad custom domain (`mycustomdomain.com`)

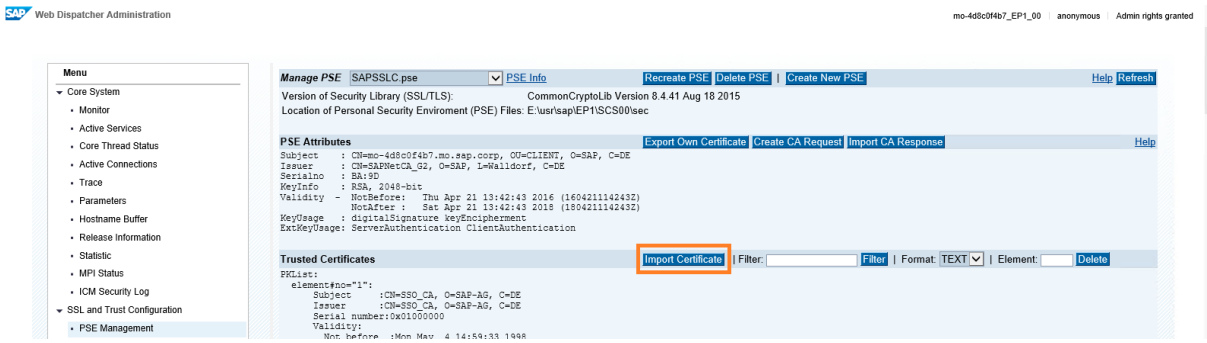
Example

In SAP Web Dispatcher configuration, add a condition for `SID=FLP` in the redirect configuration file and add the `X-Custom-Header` to the request to FLP specifying the custom FLP domain. In the response, the FLP subscription URL in the location header should be overridden with the SAP Web Dispatcher URL.

```
if %{SID} = FLP
begin
SetHeader X-Custom-Host mycustomdomain.com
SetHeader HOST mywebdispatcher.zdm.corp
NOP {break}
end
```

4. Upload the custom domain SSL certificate to the SAP Web Dispatcher (only required if you use SAP Web Dispatcher as reverse proxy).

   Open the web dispatcher administration console and choose *SSL and Trust Configuration* > *PSE Management*. Choose the PSE file for your client certificates from the dropdown list. Unter *Trusted Certificates* choose *Import Certificate* and copy and paste the certificate including `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`. Choose *Import*.



5. **Optional, only relevant for SAP Web Dispatcher** Configure the SAP Web Dispatcher to act as a global cache server.

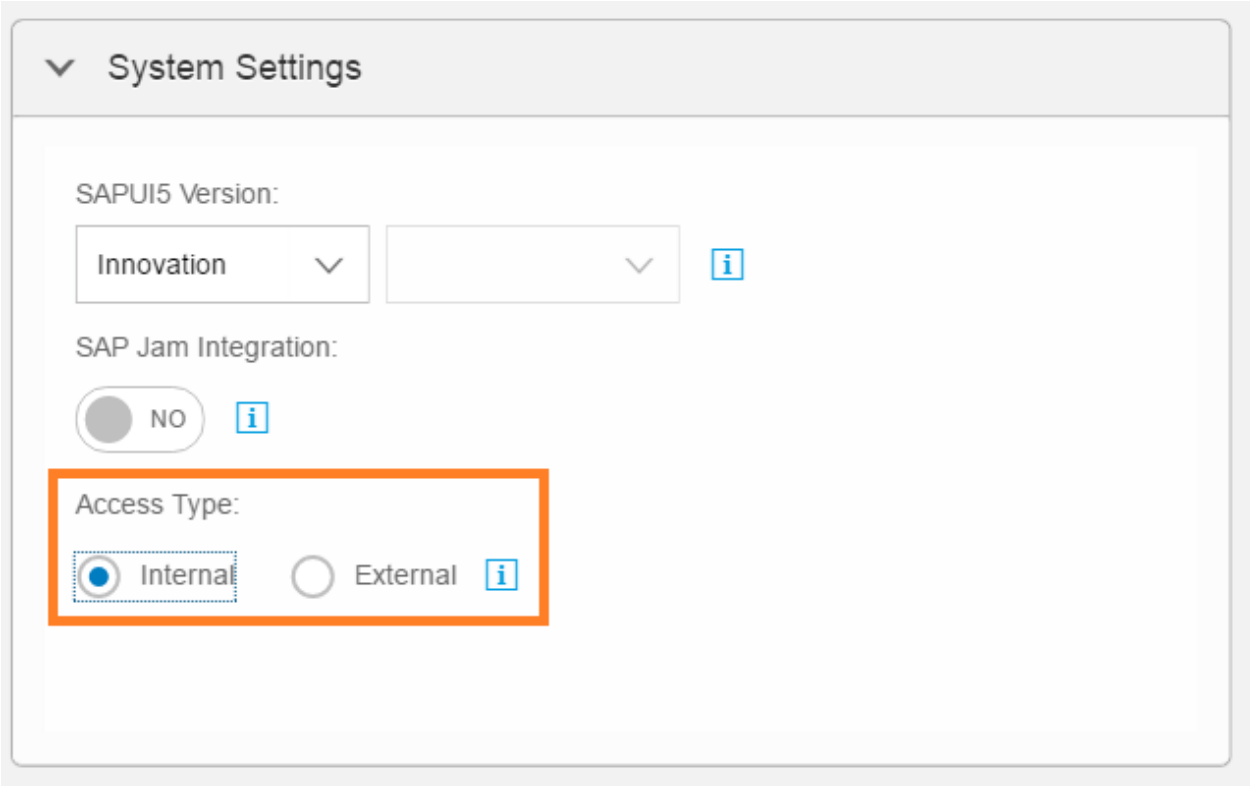
   This is an optional configuration that may help to improve the performance. To configure the global cache in the Web Dispatcher, add the following line to the Web Dispatcher's profile file:

   `icm/HTTP/server_cache_0 = PREFIX=/`

   For more information, see icm/HTTP/server_cache_<xx>. For information about other lines that can be added to customize the Web Dispatcher cache, see the *Internet Server Cache Parameters* section in Profile Parameters for the ICM and SAP Web Dispatcher.

Step 13: Activate the Internal Access Point Scenario in FCC

In the SAP Fiori launchpad configuration cockpit, under *Site Settings* > *Properties* and switch to *Edit*. Select *Internal* then save and publish.



Step 14: Assign OData Service Authorizations

Assign OData service authorizations for the SAP Fiori apps to your users in SAP Gateway and on the back end server.

You need the following information for each SAP Fiori app:

- OData service (version number)
- Delivered authorization role (PFCG role) in the back end server

> **Caution**
>
> Several authorization default values are connected to the OData service. To ensure that all these default values are assigned to a user, follow the instructions in the documentation links provided below.

1. 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.

2. 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.

   .

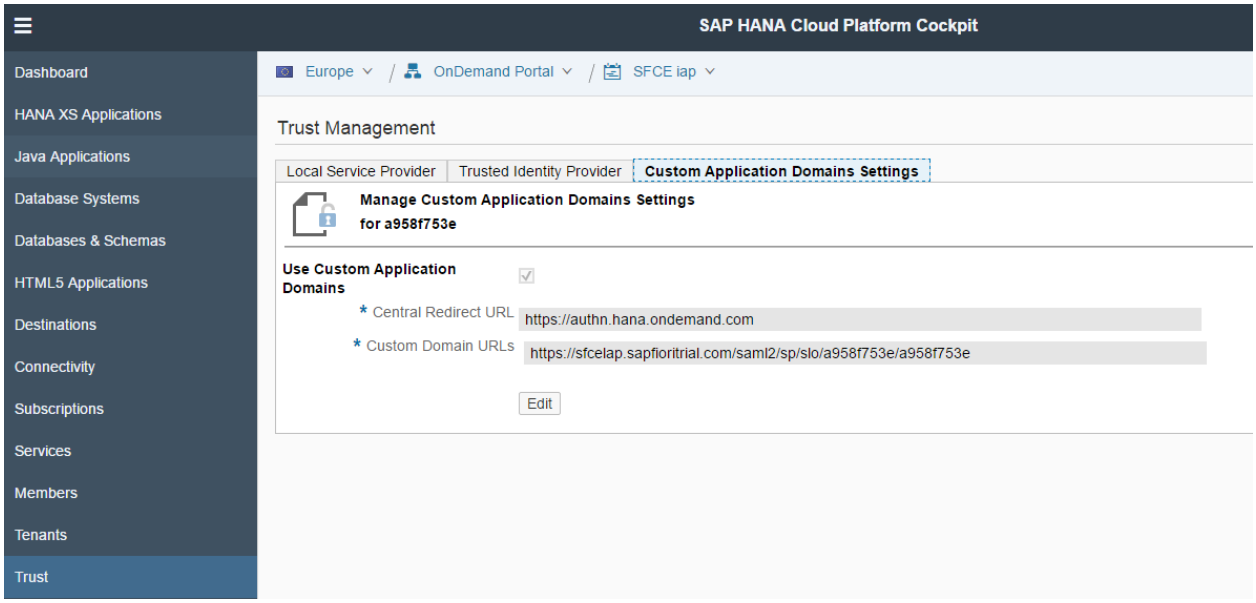
Step 15: Configure Single Log Out

To enable single logout, you need to configure the custom domain URLs for the SAML single sign-on flow in the HCP cockpit. Even if single sign-on works successfully with your application at the custom domain, you will need to follow the current procedure to enable single logout.

Proceed as follows:

1. In the *Trust Settings* in HCP cockpit, open the *Custom Application Domains* tab.
2. Enable *Use Custom Application Domains*. The *Central Redirect URL* field is preset.
3. Enter your custom domain in the *Custom Domain URLs* field.
4. Save your changes.

The system generates the respective single logout service endpoints. Test them in your Web browser and make sure they are accessible from there.



For more information, see Configuring Custom Domains > Configure Single Logout.

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 wilful 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