



IMPLEMENTATION GUIDE | CUSTOMER

SAP Fiori Cloud

Document Version: 1.0 – 2019-01-03

Implementation Quick Guide - External Access Point

SAP Fiori Cloud for SAP Business Suite

Content

1 Quick Guide: External Access Point. 3

1 Quick Guide: External Access Point

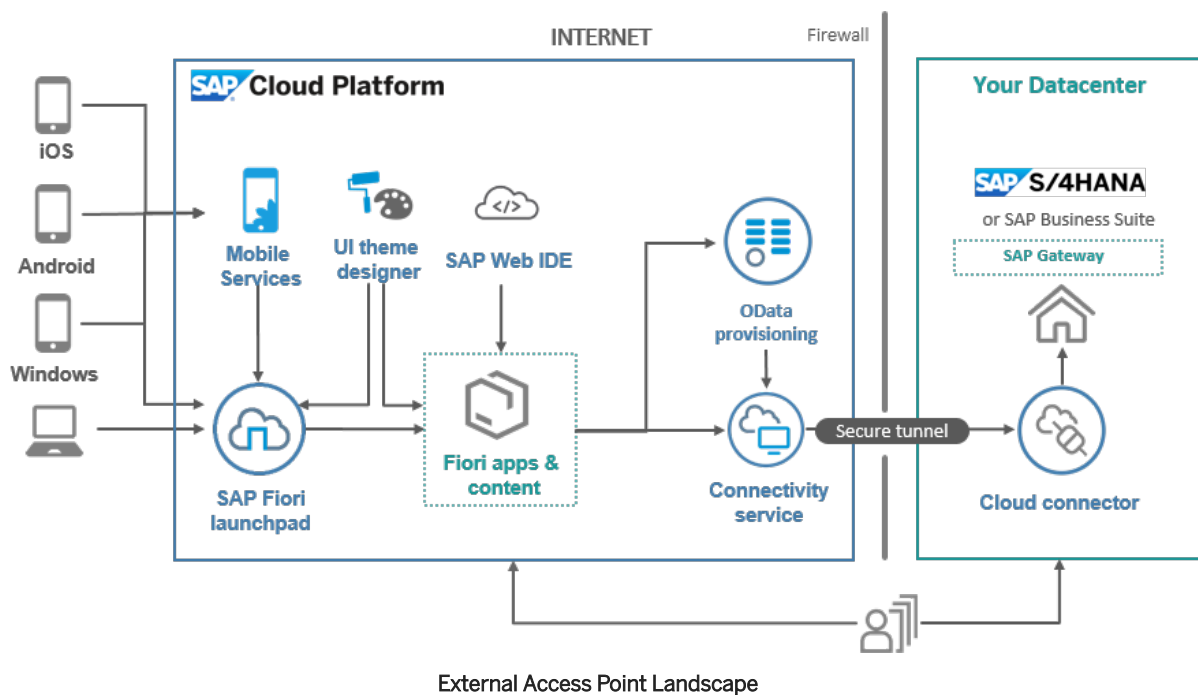
The following procedure guides you through the process of setting up SAP Fiori Cloud in an external access point scenario.

i 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 lose track where you are.

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



Prerequisites

Task	Where	More Information
You have installed, configured, and activated SAP Gateway (On-Premise Installation Only).	On Premise	For more information, see the Installation Guide and the Configuration Guide in SAP Gateway .
You have an account on the SAP Cloud Platform.	SAP Cloud Platform	
You have assigned to your user member roles on the SAP Cloud Platform.	SAP Cloud Platform	For more information, see Managing Member Authorizations and Managing Members on the Neo Environment .

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 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 [SAP Fiori Apps Reference 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](#).

i Note

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.

More Information

Access to the SAP Fiori App Reference Library: <https://fioriappslibrary.hana.ondemand.com/sap/fix/externalViewer/#/filters/FaaSEditions>

Step 2: 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.

i 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 Support Portal as part of the [Software Logistics Toolset \(SL Tools\)](#), under [System Maintenance](#) and [System Provisioning](#), respectively.

i 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 `FIORUSER`, 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 3: Activate IW_BEP Services for OData Provisioning in the Back End System

i Note

This step is relevant if you use the OData provisioning service. For information about the prerequisites for using OData provisioning see the Prerequisites section in [OData Provisioning: Administration](#).

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

1. In transaction `PFCG/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`.

i Note

To activate role assignments in the SAP Cloud Platform, you need to refresh the session.

Step 4: 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.

i 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.

i Note

To activate role assignments in the SAP Cloud Platform, you need to refresh the session.

Step 5: Register OData Services in the SAP Gateway System

i 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.

i Note

For activation of OData services when you use the OData provisioning service, see [Step 8: Set Up Odata Provisioning Service \[page 9\]](#).

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.

i 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 6: Set Up SAP Cloud Platform Cloud Connector

The SAP Cloud Platform 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 Cloud Platform. 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 Cloud Platform cloud connector builds a secure tunnel between the SAP Cloud Platform and your on-premise system.

Prerequisites: See the prerequisites for using the SAP Cloud Platform cloud connector at [Prerequisites](#).

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

1. Install the SAP Cloud Platform cloud connector.
The SAP Cloud Platform 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 Cloud Platform cloud connector documentation under [Installation](#).

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 Cloud Platform cloud connector documentation under [Initial Configuration](#).

i 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 [Use LDAP for Authentication](#).

3. Choose [Connect](#) to establish and test the connections to the SAP 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 Cloud Platform cloud connector documentation: [Cloud Connector](#)

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

i 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 3, see [Step 3: Activate IW_BEP Services for OData Provisioning in the Back End System \[page 6\]](#).

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 Cloud Platform cockpit 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: [Configure Destinations from the Cockpit](#)

Step 8: Set Up OData Provisioning Service on SAP Cloud Platform

i 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 Cloud Platform cockpit and can be used to establish a connection to exchange business data between the back end system and the SAP Cloud Platform 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 SAP Cloud Platform account user.
2. Open the [Destinations](#) panel of the SAP 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 SAP Cloud Platform cockpit and choose [Configure OData Provisioning](#) > [Destinations](#) . Enter the destinations URL of the back end system where your OData service implementations are present.

i Note

The on-premise URL of your back end systems must be whitelisted in the SAP Cloud Platform 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 Cloud Platform 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 3, see [Step 3: Activate IW_BEP Services for OData Provisioning in the Back End System \[page 6\]](#). Make sure that you set the Authentication to `PrincipalPropagation` 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.

i 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 SAP Cloud Platform cockpit.

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

i 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 \[page 14\]](#) section below.

More Information

OData provisioning documentation in the SAP Cloud Platform documentation: [OData Provisioning: Administration](#)

Step 9: Set Up User Authentication and Principal Propagation

You set up user authentication and principal propagation in the SAP Cloud Platform cloud connector and on SAP Cloud Platform. 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 \[page 14\]](#).

Proceed as follows:

1. Configure trust in the SAP Cloud Platform cloud connector, see [Set Up Trust](#).
2. Configure the settings for SAML 2.0 communication between SAP Cloud Platform and the trusted identity provider in the *Trust* panel of the SAP Cloud Platform cockpit, see [Application Identity Provider](#).
3. Connect to the user store. If you have an existing on-premise system with a populated user store, you can connect SAP 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.

i Note

You can also use SAP Cloud Identity service to create the users in SAP Cloud Platform. 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 approach 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 SAP Cloud Platform.

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 Platform Identity Authentication Service](#)

[Corporate User Store](#), section *Configure Connection to a Corporate User Store*

Step 10: Activate Content for SAP Fiori Cloud

The following options are available for acquiring SAP Fiori Cloud:

- A subscription-based commercial model, in which you are already subscribed to the SAP Fiori Cloud service
- A consumption-based commercial model that uses cloud credits, in which you have access to all services, including the SAP Fiori Cloud service

For more information about these models, and to find out which one suits your needs, see [SAP Cloud Platform Onboarding with the Consumption-Based Commercial Model](#).

Subscription-Based Model

To activate SAP Fiori Cloud content when using the subscription-based model:

1. In your SAP Cloud Platform subaccount, select *Services*.
2. Click the *Portal* service, and then choose *Configure Portal*.
3. Select *Roles*, and make sure your s-user is assigned to the TENANT_ADMIN role.

i Note

If your subaccount has trust to a non-default Identity Provider, then assign a user from this IdP to the TENANT_ADMIN role.

4. In the information bar at the top of the screen, click [Portal](#) and choose [Go to Service](#).
The SAP Fiori launchpad [Admin Space](#) opens.
5. Select the [Site Directory](#), and click [Edit](#) in the tile of the [Default](#) site. If there are no sites, click the large + (plus) icon to create a new SAP Fiori launchpad site.
The SAP Fiori launchpad configuration cockpit opens and a popup is displayed, in which you can select business content.
6. In the popup, select the desired business content and choose [Add Content](#).
The selected content is added to the [Content Packages](#) list.
The subscriptions to the HTML5 apps are available in your subaccount in the SAP Cloud Platform cockpit.
If you close the popup, you can access it again by choosing [Add Content](#) from the bottom of the [Content Packages](#) list.

Consumption-Based Model

To activate SAP Fiori Cloud content when using the consumption-based model:

1. In your SAP Cloud Platform subaccount, select [Services](#).
2. Search for the [SAP Fiori Cloud](#) service, and enable it.

⚠ Caution

If you disable the Portal service, the SAP Fiori Cloud service will be disabled automatically.

3. Click the [SAP Fiori Cloud](#) tile, and then choose [Configure SAP Fiori Cloud](#).
4. Select [Roles](#), and make sure your s-user is assigned to the TENANT_ADMIN role.

i Note

If your subaccount has trust to a non-default Identity Provider, then assign a user from this IdP to the TENANT_ADMIN role.

5. In the information bar at the top of the screen, click [SAP Fiori Cloud](#) and choose [Go to Service](#).
The SAP Fiori launchpad [Admin Space](#) opens.
6. Select the [Site Directory](#), and click [Edit](#) in the tile of the [Default](#) site. If there are no sites, click the large + (plus) icon to create a new SAP Fiori launchpad site.
The SAP Fiori launchpad configuration cockpit opens and a popup is displayed, in which you can select business content.
7. In the popup, select the desired business content and choose [Add Content](#).
The selected content is added to the [Content Packages](#) list.
The subscriptions to the HTML5 apps are available in your subaccount in the SAP Cloud Platform cockpit.
If you close the popup, you can access it again by choosing [Add Content](#) from the bottom of the [Content Packages](#) list.

Step 11: Configure the SAP Fiori Launchpad

In the SAP Fiori launchpad configuration cockpit, you need to activate the content package to work with, and configure the external access point landscape.

You access the launchpad configuration cockpit either from the SAP Fiori launchpad or from the [Services](#) panel of the SAP Cloud Platform cockpit.

In the launchpad configuration cockpit, proceed as follows:

1. Select [Settings](#), and under [System Settings](#), select the [External](#) access type. The following option becomes available: [Access Classic UIs](#), where you select how to handle external access to classic UIs, which include SAP GUI and Web Dynpro ABAP apps. Select [Yes, and show in launchpad](#). For more information about the access options, see [Setting Up an External Access Point Landscape](#).

More Information

[SAP Fiori Launchpad Sites](#)

Step 12: 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 SAP Cloud Platform 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 launchpad configuration cockpit. 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](#)

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 standardized 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 values. 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 SAP Cloud Platform 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 SAP Cloud Platform 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 roles to the corresponding catalogs. 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 launchpad configuration cockpit and select *Catalogs*.

→ Tip

In case of issues, see [Troubleshooting \[page 14\]](#).

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 9)

Some SAP Fiori apps require additional roles for accessing the data. If the roles are missing, the user gets an 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 `PF09`.
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 Platform 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 `/IWBEPP/RT_MGW_ADM` authorization template is needed. If your user does not have the required authorization, create a new role in transaction `PF09` 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 Platform cloud connector. Choose *Synchronize* to make sure that all services are displayed.

End-to-end Trust With Principal Propagation has Errors (Step 9)

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 SAP Cloud Platform 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 9)

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 enables 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 principal 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 principal propagation you should delete and register the service again.

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 a 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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

© 2018 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.