Security Guide | PUBLIC
Document Version: 7.2 SPS 17 – 2023-07-03

Security Guide for SAP Fiori Apps 1.0 for SAP Solution Manager 7.2

THE BEST RUN SAP

Content

1 Document History

> ⚠ Caution
>
> Before you start the implementation and configuration of SAP Solution Manager, make sure you have the latest version of this document. You can find the latest version at SAP Fiori For SAP Solution Manager (SAP Help Portal).

The following table provides an overview of the most important document changes.

Support Package Stacks (Version)	Date	Description
SP10 and 11	May 2020 and February 2021	No updates.
SP10	2019-12-02	**Solution Manager Administration Apps** Substituted System Monitoring catalogue and group with SAP Solution Manager Administration catalog and group.
SP09	2019-06-17	**SAP Fiori Apps Reference Library** Added information about the SAP Fiori Apps Reference Library to section *SAP Fiori Application Configuration*
SP08	2018-12-03	**New SAP Fiori Applications** Overview Pages Applications for *SAP Solution Manager Administration App*: • Early Watch Reports • Basic Configuration • User Management **SAP Fiori Apps Note** • For error corrections in roles and authorizations for SAP Fiori Apps front-end roles and authorizations, see SAP Note 2712850. • For error corrections in roles and authorizations in SAP Fiori Apps back-end roles and authorizatiosn, see SAP Note 2250709. **New Section: Personalize your FIORI Launchpad** You can adapt the SAP Fiori launchpad to your requirements.

Support Package Stacks (Version)	Date	Description
SP07	2018-05-14	**Composite Roles** As of SP07, composite roles in SAP Solution Manager are no longer supported. All business user definitions with accordingly assigned roles are available with their documentation in application Solution Manager User Administration (SMUA) and in transaction SOLMAN_SETUP. For more information on business users (Use Case IDs), see the according section in the *Authorization Concept Guide*. For more information on the application SMUA, see the *Secure Configuration Guide*. **New: Persona Based Business Roles for Fiori Launchpad** New persona based *Business Catalogue Roles* are available to be assigned to users, see new section on *Business Catalogue Roles*. **New SAP Fiori Applications** • CCM: Object Viewer Wanting to Create your Own Tiles, Groups, and Roles, see more information in section *SAP Fiori Application Configuration*.
SP06	2017-10-31	**New SAP Fiori Applications** • DVM: Reorganisation and Decompression • CCM: Managing Namespaces Wanting to Create your Own Tiles, Groups, and Roles, see more information in section *SAP Fiori Application Configuration*.

Support Package Stacks (Version)	Date	Description

SP05	2017-05-08	**General Information**
		With Support Package SP05, security - relevant information for SAP Fiori Applications are described in guide *SAP Fiori Application Authorization*.
		• As of Release 7.2, the security information is published within three separate guides:
		  • *SAP Solution Manager Authorization Concept*
		  This guide contains all information referring to the general concept of security and authorizations for the complete stack for SAP Solution Manager.
		  • *Secure Configuration Guide*
		  This guide contains all information referring to security aspects, users and authorizations used in transactions SOLMAN_SETUP and SMUA. In addition, users and authorization for the migration procedure for the process documentation are included.
		  • *Application Security Guide*
		  This guide contains all information referring to security aspects and authorizations for individual scenarios/applications.
		  i Note
		  All relevant changes for the individual applications/scenarios are documented in the document history of the individual sections.

2 Security Guide - SAP Fiori App Authorizations

Use

> ⚠ Caution
>
> For **Usage Rights for SAP Solution Manager**, check the following information in SAP Support Portal at: http://support.sap.com/solution-manager/usage-rights.html

This guide refers to application specific roles and authorizations. For general information on the authorization concept of Solution Manager or setup security, refer to the according complimentary guides on SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager.

For any issues with security, authorizations, roles, and user management for SAP Solution Manager use `SV-SMG-AUT`.

To get started

What is this guide about? SAP Solution Manager covers a wide range of divers scenarios you can use. As a customer, you might want to start with one scenario, and later on add another scenario in your landscape. Therefore, SAP delivers scenario-specific security guides per scenario which cover all relevant information for this specific scenario.

> ⚠ Caution
>
> Before you start using this scenario-specific guide, you must read the core information about security issues in SAP Solution Manager, and the *Landscape Setup Guide*, which refers to all security-relevant information during basic configuration of SAP Solution Manager. Without this information, we do not recommend to set up any specific scenario. This guide does also not replace the daily operations handbook that we recommend customers to create for their productive operations.

This guide covers the following topics:

- **Getting Started:** find out about target groups of this guide. Links for any additional components you can find in the Core Guide.
- **Prerequisites:** find out about the specific system landscape components such as `RFC` - destinations and technical users, and how they connect to each other.
- **Users and Authorizations:** find out, which users SAP recommends, and which user roles SAP delivers for them. This includes a detailed description of all users and the according roles which represent them. Here, you also find information on the relevant work center(s).
- **Scenario Integration:** according to the life-cycle approach the various scenarios integrate with each other. Here, you can find out about authorizations you need to assign to your users for these cases.

To enable your end-users to work with the application, you need to assign them authorizations in the Solution-Manager-system and in the managed systems.

When you are working in a project to implement new business processes or change existing ones, a number of project members with different tasks are involved. SAP delivers recommended user descriptions on which SAP delivered roles are modelled. These user descriptions and roles can only be regarded as templates for you. You need to first define which tasks the individual members in your company execute, and then adjust the according roles.

> ⚠ Caution
>
> The roles delivered by SAP can only be regarded as models for adjustment to your company's needs.

What is Your Opinion?

We are always interested in how we can improve our documentation to your needs. In the Support Portal, you can leave your feedback online, which is regularly checked by us.

Integration

Security topics are relevant for the following phases:

- Configuration
- Operations

> → Recommendation
>
> Use this guide during all phases. For a detailed overview of which documentation is relevant for each phase, see guides reference on SAP Support Portal at: https://help.sap.com/viewer/p/SAP_Solution_Manager.

More Information

For a complete list of the available SAP Security Guides, see SAP Support Portal: https://help.sap.com/viewer/p/SAP_Solution_Manager

3 General Security Information

SAP Fiori / SAP Gateway

General security - related topics are mitigated by the front-end security of your Central Hub system, such as URL redirection, administrator access, input validation, and so on.

Authentication

Authentication is managed by the SAP Fiori Framework. Access is only allowed to a known user. This user must have a password. The access is certificate based.

Authorization

Authorization for the user is shipped by Software Component `ST-UI` for SAP Solution Manager applications. In addition, for each individual application back-end authorization and RFC - communication autorization are required. Any error corrections can be found in SAP Note 2712850.

- The **Trusted RFC** between front-end and back-end is protected by authorization object `S_RFCACL`. For more information on the individual application, see the according section in this guide, for more information on `S_RFCACL` handling in general, see *Authorization Concept Guide*.
- The recommended **composite roles** can be restricted by removing roles: `SAP_SMWORK*`, `SAP_SM_FIORI_LP_EMBEDDED`, and all explicitely mentioned roles.
- **Authorization objects** can be restricted, and are explicitely mentioned.

Tile Accessibility

Tiles are grouped in SAP Fiori Groups. A SAP Fiori Group is assigned to a Catalogue. In the User Interface you find only those files which are assigned to a group of a catalogue as being visible. If you do not find a specific tile, you need to check in the catalogue for it and assign it.

In case you see a Tile, but cannot access its application, you are missing authorizations for it as end-user.

Session Handling

Sessions are handled by the front-end. Note, that the usage of SSO is recommended.

HTTP Protection

In the frond-end the Web Dispatcher is used. HTTPS is recommended.

Upload and Download of Documents

Uploading unchecked documents of any kind of external data such as office documents, images and binaries is considered insecure, unless they are scanned for malicious or suspicious content. Virus scans should be performed every time potentially polluted data is imported via input channels into the SAP system. Possible input channels are:

- File upload from frontend devices or the server file system
- File upload via Internet
- Document exchange via RFC, XML, PI, and so on

> → Recommendation
>
> We recommend deploying SAP virus scan profiles (VSI).

Other Sources

For more information, check the according security information for SAP Fiori and SAP Gateway in the SAP Help Portal: http://help.sap.com ▶ *Technology Platform* ▶.

4 SAP Fiori Application Configuration

SAP Fiori Launchpad is the generally advised User Interface by SAP. You can use SAP Fiori Launchpad with SAP Solution Manager either:

- **embedded** within SAP Solution Manager (any SAP Solution Manager application running within SAP Fiori Launchpad UI), or
- **on a separate server** in a Central Hub (specific applications for SAP Fiori Launchpad UI)

In the following sections, we explain which roles and authorizations are required to run SAP Solution Manager either way. Specific information regarding individual SAP Fiori Apps are given within the section for the according scenario. Since SAP Fiori for SAP Solution Manager is a separate product, the documentation of the apps shipped with that product are documented in the according help in the SAP Help Portal..

SAP Fiori Apps Reference Library

All SAP Solution Manager SAP Fiori Apps are contained in the SAP Fiori Apps Reference Library .

The SAP Fiori apps reference library contains only SAP Solution Manager apps release with software component ST-UI. Within the SAP Fiori Apps Reference Library, choose `All Apps` → `STUI`. This path leads you to chapter *Other SAP Fiori Apps*.

> **!** Restriction
>
> The SAP Fiori apps reference library does not contain all SAP Fiori Apps Reference Library available in SAP Solution Manager Launchpad. Some of the tiles which SAP delivers in the SAP Solution Manager are Web Dynpro applications, rather than Fiori apps, and can not be deployed with software component ST-UI on a central hub system. These applications are therefore not available in the Fiori Apps Reference Library. The applications on the SAP Solution Manager Fiori Launchpad that are not Fiori apps are well documented in the SAP Solution Manager application help. You can find the information on these applications in the documentation of the relevant process, e.g. Business Process Operations.

SAP Solution Manager Embedded SAP Fiori Launchpad

To successfully assign SAP Fiori Launchpad authorizations, you need to assign to the end-user:

- Role `SAP_SM_FIORI_LP_EMBEDDED`
  All SAP Solution Manager applications that run in the Work Centers can also be called using SAP Fiori Launchpad. Therefore, all users within SAP Solution Manager require single role `SAP_SM_FIORI_LP_EMBEDDED`, which contain relevant authorizations for the launchpad call. The role is automatically assigned to all users, which are created using transaction `SOLMAN_SETUP` and available in all relevant composite roles for users.
- Role `SAP_SMWORK*`

To be able to call the User Interface Tiles, you need navigation information assigned to the user. All Catalogue and Group (Tiles) information is delivered within the *Menu Tab* of the already existing Work Center Navigation roles `SAP_SMWORK*`.

- Authorization object `S_ESH*`
  Many applications called, require *Embedded Search* authorizations `S_ESH*`, which are delivered within the core authorization roles for each application.
- Authorization object `S_SERVICE`
  Due to the use of OData - Services, authorization for services is required. You find the specific OData - Services, and their according `S_SERVICE` authorization in the core roles for the scenario in question.

> **i Note**
>
> If your security requirements do not permit `S_SERVICE`, you can always set the object inactive or remove the service from the *Menu Tab*.

SAP Fiori Catalogue, Group, and Tile Assignments

For SAP Solution Manager, all available tiles are assigned to catalogues. They are not necessarily assigned to a pre-delivered group. For configuration tiles, they are all assigned directly to the catalogue.

Authorization Checks

Tiles receive data. Authorizations are checked by the OData service and the functions in the back-end system.

SAP Fiori App Running on a Central Hub with SAP Solution Manager Backend System

To successfully assign SAP Fiori Launchpad authorizations, you need to:

Configure Prerequisites

To be able to run the SAP Fiori App, you need to configure the following settings with a suitable *Configuration User*.

This Configuration User must have authorization object `S_RFCACL` assigned.

> **→ Recommendation**
>
> As authorization object `S_RFCACL` is a security-critical authorization object, we recommend to remove this authorization or disable the Configuration User after configuration of the application.

1. Configure the SAP Gateway correctly on the Central Hub.
2. Configure a Trusted RFC - Connection between Solution Manager and Central Hub.
3. Copy the OData - Service in the Front-end system.
   How to Copy the OData - Service
   1. In transaction `SPRO`, go to *SAP NetWeaver* > *UI Technologies* > *SAP Fiori* > *Initial Setup* > *Initial Launchpad Configuration* > *Service Maintenance of SAP Gateway* >.
   2. Call the transaction, and choose the button *Add Service*.
   3. In the new dialog, enter the System ID of your Back-end system in the field *System Alias* via F4 Help, in our case SAP Solution Manager system ID.

The system asks for your Trusted RFC - Connection to be able to call the OData - Service from the back-end.

4. Press the button *Get Services*.
   The system calls the OData - Services from the SAP Solution Manager into the Front-End system using the Trusted RFC - Connection.
5. Enter the specific OData - Service name (`IWSG`) which is given in the role description tab of the template role `SAP_STUI_<scenario description>_AUTH` into the field *Technical Service Name*.
6. Choose button *Add Selected Services*.
7. In the appearing dialog, the system displays the name of the service that is to be copied. Here, you can change the name space or leave it as *Z*.
8. Choose a transport package or use a local package `&TMP`.
9. Enter.
10. Go back to screen *Activate and Maintain Services*.
11. Check, if your copied service is available in the list, and double click on it.
12. Check, that the *ICF - Node* is displayed for the service, and activate the ICF - Node by choosing the button *ICF Node -> Activate*.
13. For the service to appear later on in the `PFCG` authorization fields, load the meta data by choosing the button *Load Meta Data*. Then, call the service once by using the button *Call Browser*.
14. Check, that the System Alias is also correct.
    You can now add the copied service to your role.

4. **Adding the OData Service to Your Role**
   1. Call transaction `PFCG`, and choose your role.
   2. Change into *edit* mode, and open tab *Menu*.
   3. Choose the button *transaction*, and here choose entry *Authorization Default*. The system displays a new dialog.
   4. In the dialog, via F4 help choose in the field *Authorization Default* entry **`TADIR Service`**, and in field *Obj Type* value **`SAP Gateway: Service Groups Metadata`**.
   5. Entere your copied OData service, and choose *Copy*.
   6. Go back and choose tab *Authorizations*.
   7. Check that authorization object `S_SERVICE` is filled, generate the profile, and go back.
   8. Execute the *User Comparison* on tab *User*.

For more information, see the SAP Solution Manager Configuration Guide. In addition, you can check the Implementation Guide in the system using transaction `SPRO`, go to *SAP NetWeaver* > *UI Technologies* > *SAP Fiori* > *Initial Setup*.

In the Backend System SAP Solution Manager

- Authorization object `S_ESH*`
  Each application called requires Embedded Search authorizations `S_ESH*`, which are delivered within the core authorization roles for each application.
- Authorization object `S_SERVICE`
  Each specific SAP Fiori application is called using an OData - Service (Gateway Service). The Gateway Service is delivered within *Menu Tab* of the core role for the application. The according authorization object `S_SERVICE` is delivered with status *active*.

> **i Note**
>
> If your security requirements do not permit `S_SERVICE` if not needed, you can always set the object inactive or remove the service from the *Menu Tab*.

- Authorization objects `S_RFC` and `S_RFCACL`
  The front-end components communicate by OData - Services through a Trusted RFC - Destination with the back end Solution Manager system. This requires the user in the back-end to have assigned Remote Function Call authorization `S_RFC` and Trusted RFC authorization `S_RFCACL`. Both authorization objects are delivered in role `SAP_SM_FIORI_FRONTEND` which needs to be assigned to the user.

> **→ Recommendation**
>
> Role `SAP_SM_FIORI_FRONTEND` is **not added** to the automatic user generation within transaction `SOLMAN_SETUP`. Due to the security critical objects, this role **needs to be assigned manually** only to users that are allowed to call the SAP Fiori App.
>
> We highly recommend to maintain authorization object `S_RFCACL` specifically for this use case (System ID, Client, and User ID).

In the Front-End System (Central Hub) SAP Fiori

You have to assign both types of roles to your user in the frontend-system.

Roles Delivered with SAP Solution Manager (Software Component ST-UI)

- Catalogue and Tiles
  To be able to call the User Interface Tiles, you need navigation information assigned to the user.
  All Catalogue and Group (Tiles) information is delivered within the *Menu Tab* of navigation roles `SAP_STUI_<scenario description>_TCR`.
- Authorization for `S_SERVICE` (OData - Service)
  Each specific SAP Fiori application is called using an OData - Service (Gateway Service). Within the SAP Fiori environment, you are required to copy this OData-Service into your name space, and then add the copied Service to the *Menu Tab* of the role. The information for the specific Gateway Service is delivered within the *Description Tab* of the role `SAP_STUI_<scenario description>_AUTH` for the application.
- Mandatory Additional SAP Fiori Relevant Services
  For SAP Fiori to operate correctly, you need also add in the authorizations role for your application the following Odata - Services or assign role `SAP_STUI_GENERAL_AUTH` (Please check the *Menu* tab in this role.):
  - Service `/UI2/INTEROP*` (Object Type: *IWSV*)
  - Service `/UI2/PAGE_BUILDER_PERS*` (Object Type: *IWSV*)

> **i Note**
>
> This authorization is required for any SAP Fiori Application, not only SAP Solution Manager. You also assign the according authorization roles shipped by SAP Fiori: `SAP_UI2_USER_700`.

Roles Delivered by SAP Fiori

- Users require additional access to services and according authorization objects delivered by SAP Fiori.
  Execute the according IMG activities under transaction `SPRO`: *SAP NetWeaver* > *UI Technologies* > *SAP Fiori* > *Initial Setup* > *Initial Launchpad Configuration* > *Assign Launchpad Authorization to Users*.

SAP Fiori Catalogues, Groups, and Tiles

Concept

For SAP Solution Manager, each "Work Center" relates to one catalogue. In this catalogue, all relevant applications of the specific Work Center are available as tiles. In addition, specific application tiles are included. Still, not all tiles are displayed by default in the SAP Fiori Launchpad. The system displays only those tiles which are included in a specific group which relates to the according catalogue. You can have a number of different groups referencing to one catalogue.

Catalogues and Groups

- Catalogues and Groups are delivered within the Solution Manager navigation roles `SAP_SMWORK*`. Due to this concept, the group associated to the relevant catalogue contains all required tiles that carry functionality which is also present in the Work Centers. If you require to have other groupings of tiles, you need to maintain them in the system (according to SAP Fiori Guidelines), and assign the group to a role manually.
- Tiles are displayed by SAP Fiori Launchpad UI, irrespective whether the user has received the according authorizations to run the application or not. If you want to hide specific Tiles, you need to maintain the catalogues and your roles accordingly. In case you do not see any KPI numbers in a tile, the user has not the authorization for the respective OData - Service and related authorizations.

Specific Groups for Applications

If specific groups are required for certain catalogues, these groups are added to the applicable authorization core roles. For instance, in Business Process Monitoring specific groups are required. They are added to the roles for Business Process Monitoring. In addition, the complete group for the work center is available in role `SAP_SMWORK_BPO`. If you are not working with the Work Center as your central User Interface, you can then remove the role `SAP_SMWORK_BPO` from your user as tile information is given in the usual authorization roles.

Additional Topics

Personalization

Tiles can be personalized. If you require just an additional tile in a personalized screen, you can add any tile from any catalogue without specific permissions to add the tile in your Launchpad.

Creating Your Own Tile Catalogs, Groups, and Roles

In case, you want ot configure your own Launchpad Tiles, Groups, and Catalogs, see more here: https://blogs.sap.com/2017/08/24/sap-fiori-launchpad-in-sap-solution-manager-creating-your-own-tile-catalogs-groups-and-roles/

.

Update Launchpad or SAP Fiori App (Cache Invalidation)

To be able to clear existing UI5 caches and reset the cached tiles for the Launchpad, run activity *Invalidate Caches* in transaction `SPRO` ▶ *SAP NetWeaver* ▶ *UI Technologies* ▶ *SAP Fiori* ▶ *Data Administration* ▶ *Invalidate Caches* ▶

Assignment of Catalogues and Groups to Reference Users

- If you are working with *Reference Users*, make sure that the Catalogue and Group roles `SAP_SMWORK_*` are assigned directly to the individual users. SAP Fiori Launchpad does not recognize the navigation menu if only assigned to the *Reference User*.
- When you use *Reference User* assignments make sure you invalidate the cache beforehand, and execute all activities mentioned in SAP Note 1947910. You can invalidate the cache by executing IMG activity *Invalide Caches* in transaction `SPRO`. Navigate to *SAP NetWeaver* > *UI Technologies* > *SAP Fiori* > *Data Administration* > *Invalidate Caches.*

Enterprise Search in SAP Fiori Launchpad

To be able to use the Embedded Enterprise Search, your user must have authorization object `S_ESH*` assigned. In general, these authorization objects are contained in the template user roles which are delivered as Standard roles by SAP.

Scan Profiles Used for Attachment Uploads of Documents to SAP Fiori Apps

Attachments uploaded pass through the SAP Virus Scan interface. If you wish to scan the contents of attachments, you must set up and configure the SAP Virus Scan interface. Configuration includes setting up a commercial third party virus scanning product, for more information see SAP Note 786179.

Once you have configured the SAP Virus Scan interface, you will need to enable the following virus scan profiles:

- `/SIHTTP/HTTP_UPLOAD` checks within Web Dynpro and CRM UI
- `/SCET/GUI_UPLOAD` checks within SAP GUI
- `/SCMS/KPRO_CREATE` checks when saving in all relevant cases

Calling an Application Independently - Standalone

In case, you want to call an application independently from Fiori Launchpad, you need to add the calling BSP application to your user menu, either in your favorites or in the menu of the user roles directly.

5 Personalize your Fiori Launchpad

With SAP Solution Manager 7.2, SAP made all major applications available as tiles in the SAP Fiori Launchpad. The tile groups and catalogs SAP delivers are only an example and superset. You may want to create own catalogs and groups and fill these group with tiles to tailor your end-user's workplace.

Access the *Launchpad Designer* from the Implementation Guide (IMG) using transaction `SPRO` → SAP Solution Manager Implementation Guide → SAP Customizing Implementation Guide → SAP NetWeaver → UI Technologies → SAP Fiori → Configuring Launchpad Content → Adding Apps to SAP Fiori Launchpad → Configure Target Mappings and Tiles → SAP Fiori Launchpad Designer, or use transaction `/UI2/FLPD_CONF` to personalize your SAP Fiori Launchpad.

1. Create your own *Catalog*.
2. Create your own *Group*.
3. Add tiles to your *Catalog*.
4. Add tiles from your *Catalog* to your *Group*.
5. Add your *Catalog* and *Group* to a `PFCG` navigation role.

   > → Tip
   >
   > You can add your new *Catalog* and *Group* to one of the SAP Solution Manager navigation roles `SAP_SMWORK_***`.

6. Assign your role to your end-user.

6 Data Volume Management

6.1 Determine the Size of Aging Data for HANA System

Memory requirements are very precious for HANA system. Therefore, data that are rarely used can be moved to low cost, slow data storage area, so that the system has more memory for running efficiently

With this SAP Fiori App, you can determine aging data to be able to optimize the memory usage of HANA systems by moving the not used (old history) data into less expensive storage.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description

1. End user logs on to the application, and displays a list of all relevant HANA systems and their size of aging data, according to the requirements of the user.
   Systems can be filtered from the back-end with authorization object `AI_LMDB_OB` which is included in role `SAP_SYSTEM_REPOSITORY_DIS`.
2. The logon user can see the list all required systems and per system the size of hot and cold data, the count of active aging objects.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In your SAP Solution Manager system, create template user `DVM_DIS_<SID>` via transaction `SOLMAN_SETUP`.

The relevant OData - Service is delivered per default in the individual core role.

> **→** Recommendation
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

→ Recommendation

Make sure to maintain authorization object S_RFCACL accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- SAP_STUI_DVM_AGING_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_DVM_AGING_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

6.2 SAP BW Housekeeping

IT Management wants to reduce costs for system operations. One of the possibilities is to clean the system from unnecessary data. When the system does not grow, the existing hardware can be used for a longer time. When planning a migration to SAP HANA, the system should be as small as possible in order to save migration time and costs for SAP HANA.

With this SAP Fiori App, you can identify the largest tables with temporary data in order to know where to start best with the technical housekeeping of the system.

i Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description

1. End user logs on to the application, and displays a list of all relevant BW systems with overview information about estimated saving potentials, according to the requirements of the user.
   Systems can be filtered from the back-end with authorization object AI_LMDB_OB which is incldued in role SAP_SYSTEM_REPOSITORY_DIS.

2. The logon user can see the list of all required systems and the size of not acccessed and read only data per system.
3. The logged in user can request the execution of the BW analysis job (requires authorization `S_BTCH_*` with user `SOLMAN_BTC`)

Authorizations in the Back-End SAP Solution Manager (ST Component)

In your SAP Solution Manager system

- create template user `DVM_DIS_<SID>`via transaction `SOLMAN_SETUP`.
- assign single role `SAP_SM_BATCH_RELE` to be able to request the execution of the BW analysis job or activate in role `SAP_DVM_DIS` authorization objects `S_BTCH_*`.

The relevant OData - Service is delivered per default in the individual core role.

> → Recommendation
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> → Recommendation
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_DVM_BWHK_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_DVM_BWHK_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

6.3 Determine Unused Info Provider and Near Line Storage Data in SAP BW Systems

IT management wants to reduce costs for system operations. One of the possibilities is to clean the system from unnecessary unused data. When the system does not grow, the existing hardware can be used for a longer time. When planning a migration to SAP HANA, the system should be as small as possible in order to save migration time and costs for SAP HANA.

With this SAP Fiori App, you can to identify the info providers with unused data in order to know where to start best with technical housekeeping of the system.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description

1. End user logs on to the application, and displays a list of all relevant systems with the size of unused data, according to the requirements of the user.
   Systems can be filtered from the back-end with authorization object `AI_LMDB_OB` which is incldued in role `SAP_SYSTEM_REPOSITORY_DIS`.
2. The logon user can see the list all required systems and with an overview of info objects where unused data exist, plus Near Line storage data.
3. Logged in user can request the execution of the BW analysis job (requires authorization `S_BTCH_*` with user `SOLMAN_BTC`)

Authorizations in the Back-End SAP Solution Manager (ST Component)

In your SAP Solution Manager system

- create template user `DVM_DIS_<SID>`via transaction `SOLMAN_SETUP`
- assign single role `SAP_SM_BATCH_RELE` to be able to request the execution of the BW analysis job or activate in role `SAP_DVM_DIS` authorization objects `S_BTCH_*`

The relevant OData - Service is delivered per default in the individual core role.

> **→** Recommendation
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role SAP_SM_FIORI_FRONTEND in the back end system. The role contains S_RFC and S_RFCACL authorization.

> → Recommendation
>
> Make sure to maintain authorization object S_RFCACL accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- SAP_STUI_DVM_BWNLS_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_DVM_BWNLS_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

6.4 Reoganisation and Compression

For systems used over a long period of time, data is cluttered in storage. Then, it can be useful to identify, how much storage space can be recovered by applying reorganization and compression techniques. This can be used to work economically on these systems to recover space. Else, it may be better to add more storage. This App helps you to determine the potential size savings by using reorganization and compression for your system landscape.

> → Recommendation
>
> Only managed systems using DB6 or Oracle database are supported.

> ℹ Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description

1. The system displays a list of SAP systems with reorganization and compression saving potential (requires authorization object `AI_LMDB_OB` which is included in role `SAP_SYSTEM_REPOSITORY_DISP`)
2. The users filter the system by entering the system ID in the search area.
3. Systems which meet the criteria are displayed for selection.
4. The end- user selects a single system for details.
5. The end - user can execute a batch job to trigger a new analysis (requires authorization objects `S_BTCH*` which are included in role `SAP_SM_BATCH_RELE`) and `SM_DVM_APP` with `ACTVT 01` (create).

Authorizations in the Back-End SAP Solution Manager (ST Component)

In your SAP Solution Manager system

- create template user `DVM_DIS_<SID>`via transaction `SOLMAN_SETUP`
- assign single role `SAP_SM_BATCH_RELE` to be able to schedule jobs or activate in role `SAP_DVM_DIS` authorization objects `S_BTCH_*`.
- authoriaztion object `SM_DVM_APP` with `ACTVT 01` (create) to trigger a new analysis and submit this analysis.

> → Recommendation
>
> You need to add this authorization value `ACTVT 01` manually. We recommend to copy single role `SAP_DVM_DIS` into your namespace, and assign this activity separately. This is only required, if you run the batch job analysis. If you do not allow the user to run the batch job analysis, this object is not required.

The relevant OData - Service is delivered per default in the individual core role.

> → Recommendation
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> → Recommendation
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- SAP_STUI_DVM_REORG_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_DVM_REORG_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

7 Quality Gate Management

7.1 Approve Q-Gates and Urgent Changes

This SAP Fiori application is for *Quality Manager* and *Quality Advisory Board* to be able to easily pass/not pass a Q-Gate or approve/reject an urgent change. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see *Authorization Concept Guide*.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description

Users can do the following:

1. End user logs on to the application.
2. The logon user can see the list of QGM scenarios to which he/she is assigned to as Quality Manager or Quality Advisory Board.
3. By selecting a QGM scenario in the list, the logged on user can see the list of Q-Gates and the list of urgent changes of the current active cycle of the selected QGM scenario in different tabs.
4. By clicking a Q-Gate in the Q-Gate list, the logon user can navigate to the *Q-Gate Detail Page*.
   - In the Q-Gate detail page, the logged on user can upload/download documents related to the Q-Gate.
   - In the Q-Gate detail page, the logged on user can input/see the comments related to the Q-Gate.
   - In the Q-Gate detail page, the logged on user can pass/not pass/reset the Q-Gate based on its current status.
5. By clicking an urgent change in the urgent change list, the logged on user can navigate to the urgent change detail page.
   - In the urgent change detail page, the logged on user can upload/download documents related to the urgent change.
   - In the urgent change detail page, the logged on user can input/see the comments related to the urgent change.
   - In the urgent change detail page, the logged on user can approve/reject the urgent change based on its current status.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In the back-end SAP Solution Manager system, assign the relevant roles:

(You can find a list of all required roles by using transaction `SOLMAN_SETUP`.

- for Quality Manager (use case ID `QGM_QM_<SID>`, specifically role `SAP_SM_QGM_STATUS_QM`)

- for Quality Advisory Board (use case ID `QGM_QAB_<SID>` specifically role `SAP_SM_QGM_STATUS_QAB`)

The relevant OData - Service is delivered per default in the individual core role.

> **→ Recommendation**
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> **→ Recommendation**
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_QGM_QGATE_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_QGM_QGATE_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

Additional Security Measures

Display of Transport Requests

In the application, end-users can display transport request information that are managed from QGM applications. The system displays this data whenever the end-user has functional authorization for QGM assigned: `SM_CM_FUNC` with `ACTVT` relating to `QAB`. This authorization object is assigned per default in the according back-end user role `SAP_SM_QGM_STATUS*`.

8 Incident Management

8.1 My Incidents

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see *Authorization Concept Guide*.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the Authorization Concept for Solution Manager.

Use Case: My Incidents

This application allows users to view and respond to their ITSM Incidents. Users can do the following:

- View the details of their Incidents: Details include short text, long texts (restricted by authorization object `CRM_TXT_ID` authorizations), status, priority, attachments, and so on.
- Send an answer back to the Incident processor. This implicitly changes the status of the Incident to *In Process*.
- Add attachments such as Word documents, screen shots, and so on.
- Confirm or withdraw the Incident.

Authorizations in the Back-End SAP Solution Manager (ST Component)

> **i** Note
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, create the template user `IM_CREAT_<SID>` via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for Key-Users for Incident Management `SAP_SUPPDESK_CREATE`.

Due to the nature of the application as a subset of the complete functionality of Incident Management for Key-Users, **not all authorizations for the key user in this role are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SUPPDESK_CREATE` role accordingly.

In this case, remove all roles relating to SAP Solution Manager work center usage as well as BW-related roles:

- `SAP_SMWORK_INCIDENT_MAN`
- `SAP_SM_FIORI_LP_EMBEDDED`

- SAP_SM_CRM_UIU*
- SAP_SM_BI_INCMAN_REPORTING (needs to be assigned separately)

To allow for a trusted RFC - destination, you need also assign role SAP_SM_FIORI_FRONTEND in the back end system. The role contains S_RFC and S_RFCACL authorization.

Authorizations in the Front-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general Gateway Service authorizations.
- SAP_STUI_ITSM_MYINC_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_ITSM_MYINC_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

8.2 Resolve and Dispatch Incidents

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see *Authorization Concept Guide*.

> **i Note**
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the Authorization Concept for Solution Manager.

Use Case: Resolve and Dispatch Incidents

This application allows a processor or a dispatcher to dispatch and respond to ITSM Incidents. Users can do the following:

- View the details of their Incidents: Details include short text, long texts (restricted by authorization object CRM_TXT_ID authorizations), status, priority, attachments, and so on.
- List incidents which are assigned to him/her.
- Dispatch incidents.

- Send incidents back to the reporter, Support Desk, or SAP.

Authorizations in the Back-End SAP Solution Manager (ST Component)

> **i** Note
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, create the template user `IM_DSPT_<SID>` via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for processors or dispatchers for Incident Management `SAP_SUPPDESK_DISPATCH`.

Due to the nature of the application as a subset of the complete functionality of Incident Management for processors or dispatchers, **not all authorizations for the processor or the dispatcher in this role are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SUPPDESK_DISPATCH` role accordingly. In this case, remove all roles relating to SAP Solution Manager work center usage as well as BW-related roles:

- `SAP_SMWORK_INCIDENT_MAN`
- `SAP_SM_FIORI_LP_EMBEDDED`
- `SAP_SM_CRM_UIU*`
- `SAP_SM_BI_INCMAN_REPORTING`

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

Authorizations in the Front-End (ST-UI Component)

The following three roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.
- `SAP_STUI_ITSM_DISPATCH_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_ITSM_DISPATCH_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

9 Requirement Management

9.1 My Requirements

Here you find specific information on the individually delivered applications that can be used on a Central Fiori Hub.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the security guide for the Authorization Concept for Solution Manager.

Use Case: My Requirements

This application allows users to create, edit, and display Business Requirements.

Authorizations in the Back-end SAP Solution Manager

The relevant Odata - Service is added to the core roles for the *Business Process Expert* (maintain and create) and *Business Manager* (determine priorities and decide realization) for Requirement Management .

In the back-end SAP Solution Manager system assign the relevant composite roles for these users. Due to the nature of the application, as a subset of the complete functionality of Requirement Management, not all authorizations in these roles are required. If your security does not allow this many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_RM*` role accordingly, remove all roles relating to CRM WebClient, as well as BW-related roles.

To allow a trusted RFC - destination, you need to assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> **i** Note
>
> As you can modify SAP Fiori Apps to your own purpose, we do not deliver any specifically predefined roles for them.

Authorizations in the Frond-end

The following three roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.
- `SAP_STUI_MYREQ_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_MYREQ_AUTH`

This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:

1. Copy the Odata service into your name space.
2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

10 System Recommendation

10.1 My System Recommendations

Here you find specific information on the individually delivered applications that can be used on a Central Fiori Hub.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the security guide for the *Authorization Concept for Solution Manager*.

Use Case: My System Recommendations

This application allows users to view SAP Notes. It completely substitutes the former Web-based application for System Recommendation.

Authorizations in the Back-end SAP Solution Manager

The relevant Odata - Service is added to the core roles for the System Recommendation application.

In the back-end SAP Solution Manager system, create the template user `SYR_DIS_<SID>` via transaction `SOLMAN_SETUP`.

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

Authorizations in the Frond-end

The following three roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.
- `SAP_STUI_SYSREC_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_SYSREC_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

11 System Monitoring

11.1 System Monitoring

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub.

> **i Note**
>
> General configuration and role information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the security guide for the *Authorization Concept for Solution Manager*.

Use Case: System Monitoring

System Monitoring proactively monitors the status of the systems, hosts, and databases in the SAP Solution Manager system landscape. The end user can analyze the status of various metrics, events, and alerts generated. Users can do the following:

- Get a status overview of all technical systems, including instances, databases, and hosts.
- Drill down from status overview information to single metrics and events.
- Display the details of metrics and events, including their thresholds and current rating or value
- Access landscape information.

Authorizations in the Back-end SAP Solution Manager

- The relevant Odata - Service is added to the core role `SAP_SM_SYM_LEVEL01` for System Monitoring.
- In the back-end SAP Solution Manager system create the template user `SM_L1_<SID>` via transaction `SOLMAN_SETUP`. Due to the nature of the application, as a subset of the complete functionality of System Monitoring, not all authorizations for the user in this role are required. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_SYM_LEVEL01` role accordingly. Remove in authorization object `SM_MOAL_TC ACTVT PO` (postpone).
- To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> **i Note**
>
> As you can modify SAP Fiori Apps to your own purpose, we do not deliver any specifically predefined roles for them.

Authorizations in the Frond-end

The following three roles are delivered for front-end usage for the application (Software Component ST-UI):

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.
- `SAP_STUI_APPOPS_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_APPOPS_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, do the following:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

12 Message Flow Monitoring

12.1 Message Flow Monitoring

Here, you find specific information on the individually delivered applications that can be used on a central SAP Fiori Hub.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central SAP Fiori Hub, you can find in the *Security Guide for the Authorization Concept* for Solution Manager.

Use Case: Message Flow Monitoring

Message Flow Monitoring is used to monitor the flow and view details of each flow instance. The App displays the statistical data of flow instances. Users can do the following:

- display the statistical data at various levels: flow group, flow type and flow instance (`SM_MFM_FG`)
- search for specific flow instances using various attributes
- save the searches for future use
- edit and delete searches
- cancel and restart PI messages

Authorizations in the Back-End SAP Solution Manager (ST Component)

> **i** Note
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, create the template user for Level 1 via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for Message Flow Monitoring `SAP_SM_MFM_LEVEL01`.

Due to the nature of the application as a subset of the complete functionality **not all authorizations for the Level 1 user in these roles are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_MFM_LEVEL01` role accordingly. In this case, remove the following authorization objects:

- `S_TCODE`
- `SM_WC_VIEW`

Modify authorization object `SM_MOAL_TC`: Remove `ACTVT 78` (Assign), `ACTVT PO` (Postpone), and `ACTVT 71` (Create analysis report)

To allow for a trusted RFC - destination, you need also assign role SAP_SM_FIORI_FRONTEND in the back end system. The role contains S_RFC and S_RFCACL authorization.

Authorizations in the Frond-End (ST-UI Component)

The following three roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general Gateway Service authorizations.
- SAP_STUI_MFMON_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_MFMON_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

13 End-User Experience Monitoring

13.1 User Experience Monitoring

Here, you find specific information on the individually delivered applications that can be used on a central SAP Fiori Hub.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central SAP Fiori Hub, you can find in the *Security Guide for the Authorization Concept* for Solution Manager.

Use Case: User Experience Monitoring

This application gives the possibility to list the User Experience (UX) Monitoring scripts with their last execution metrics, availability and performance. From the script list, users have the possibility to drill down to the list of robots running a particular script, then to the list of the last executions for the selected script on the selected robot, and finally to the steps of the selected execution. It also provides a robot oriented view to drill down through a robot perspective from the list of UX Monitoring robots down to the scripts steps.

Authorizations in the Back-End SAP Solution Manager (ST Component)

> **i** Note
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, create the template user for Level 1 via transaction `SOLMAN_SETUP`. The relevant Odata - Service is delivered per default in the core role for User Experience Monitoring `SAP_SM_EEM_LEVEL01`.

Due to the nature of the application as a subset of the complete functionality **not all authorizations for Level 1 user in these roles are required to run the application**. If your security does not allow these many authorizations for the SAP Fiori application in the back-end system, you need to maintain the `SAP_SM_EEM_LEVEL01` roles accordingly. In this case, remove the following authorization objects:

- `S_TCODE`
- `SM_WC_VIEW`

Modify authorization object `SM_MOAL_TC`: Remove `ACTVT 78` (Assign), `ACTVT PO` (Postpone), and `ACTVT 71` (Create analysis report)

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

Authorizations in the Frond-End (ST-UI Component)

The following three roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.
- `SAP_STUI_UXM_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_UXM_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

14 Early Watch Alert

14.1 Early Watch Alert Reports

Here, you find specific information on the individually delivered applications that can be used on a central Fiori Hub. For more information on the concept of SAP Fiori Launchpad and Central Hub Scenarios, see *Authorization Concept Guide*.

> **i Note**
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the Authorization Concept for Solution Manager.

Use Case: My EarlyWatch Alert Reports

This application allows users to view Early Watch Alert Reports. Users can do the following:

- view EWA reports
- filter report list
- mark report lists/chapters as favourites

Authorizations in the Back-End SAP Solution Manager (ST Component)

> **i Note**
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them.

In the back-end SAP Solution Manager system, assign the relevant single role `SAP_OP_DSWP_EWA` to the user. The relevant OData - Service is delivered per default in this role.

> **i Note**
>
> As this role allows for change authorization, you may want to reduce the authorizations for display purposes. In general, activity fields for all authorization objects should be restricted to view or display activities.

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

Authorizations in the Frond-End (ST-UI Component)

The following three roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general Gateway Service authorizations.

- `SAP_STUI_EWA_CHK_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_EWA_CHK_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

15 Custom Code Management App

15.1 Managing Namespace Settings

With this SAP Fiori App you can display SAP determined code origin (table storage: `AGSCCL_NSPACE`, `AGS_CC_OBJ_NSP`) and display and/or change customer code origin for custom namespaces (table storage: `AGSCCL_NSPACE`). It is possible to determine, whether a customer object, a partner object or a SAP object has been modified. You can enter a customer code origin to overrule the automatically determined code origin if required.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description Data Flow

1. The system provides information about the determined code origin of a namespace.
2. The end - user checks the code origins and is allowed to enter and save a Customer Code origin to overrule the automatically determined code origin.
3. The system checks these changes (requires authorization to change system settings for modification).
4. The end- user confirms the change.
5. The system updates the changed code origin.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In the back-end SAP Solution Manager system, create template user `CC_DIS_<SID>` via transaction `SOLMAN_SETUP`.

The relevant OData - Service is delivered per default in the individual core role.

> → Recommendation
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

→ Recommendation

Make sure to maintain authorization object S_RFCACL accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- SAP_STUI_GENERAL_AUTH
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- SAP_STUI_CCM_NAMESPACE_TCR
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- SAP_STUI_CCM_NAMESPACE_AUTH
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object S_SERVICE is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

15.2 Object Viewer

With this SAP Fiori App you can display all object of the Object Library, maintain attributes, change Owner, and change Contract. This application provides the inventory of custom code objects on customer landscape in a central location from all systems with important attributes of the objects. This provides transparency into the custom code and analyze further action to manage them.

i Note

General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description Data Flow

1. The system provides information about object searched for.
2. The end - user checks can change attributes, mainatin Owners, maintain Contracts.
3. The system updates the change of the object..

Authorizations in the Back-End SAP Solution Manager (ST Component)

The administrator for this application requires in the back-end SAP Solution Manager system:

- User ID for the display user for CCM, for simple display actions
- User ID for the end user in CCM with full authorization, to be able to change attributes, change Owner, change Contracts (Authorization object `SM_CCM_LIB`)

> **i Note**
>
> Make sure to assign the correct back - end role to your end-user with the correct maintenance of all `SM_CCM*` authorization objects.

The relevant OData - Service is delivered per default in the individual core roles.

> **→ Recommendation**
>
> As you can modify SAP Fiori Apps to your own purpose, SAP does not deliver any specifically predefined roles for them. The back-end composite roles contain single roles which are only relevant for use within SAP Solution Manager work centers, such as `SAP_SMWORK*` and `SAP_SM_FIORI_LP_EMBEDDED`. You can remove these roles in case the composite role is only relevant for SAP Fiori App usage. In addition, if your security department requires you to apply specific authorizations, you need to trace the back end user for required authorizations and authorization values.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> **→ Recommendation**
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following two roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_CCM_OBJECTVIEW_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_CCM_OBJECTVIEW_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.
  2. Add the copied service to your role *Menu*.
  3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
  4. Generate the profile.
  5. Assign the role to your user.

16 SAP Solution Manager Administration App

16.1 Overview Page (OVP) EWA

With this SAP Fiori App you can display Early Watch Alert Reports and user's favorite transactions.

> ℹ Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description Data Flow

1. The system provides information about the Early Watch Alert Reports.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In the back-end SAP Solution Manager system assign roles `SAP_DSWP_OP_EWA` and role `SAP_SYSTEM_REPOSITORY_DISP`.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> → Recommendation
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_OVP_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_OVP_EWA_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.

2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

16.2 Overview Page (OVP) Basic Configuration

With this SAP Fiori App you can display an overview on the percentage of activities in transaction SOLMAN_SETUP for the mandatory scenarios and access to the transaction.

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description Data Flow

1. The system provides information about the Early Watch Alert Reports.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In the back-end SAP Solution Manager system assign roles `SAP_STUI_OVP_BASIC`.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> **→** Recommendation
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_OVP_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_OVP_BASIC_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.

2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

16.3 Overview Page (OVP) User Management

With this SAP Fiori App you can display number of users depending on status and kind of system within Solution Manager User Administration (SMUA).

> **i** Note
>
> General information on the integration of Fiori Launchpad (Embedded Fiori) and the scenario of a Central Fiori Hub, you can find in the Security Guide for the *Authorization Concept for Solution Manager*.

Use Case Description Data Flow

1. The system provides information about the Early Watch Alert Reports.

Authorizations in the Back-End SAP Solution Manager (ST Component)

In the back-end SAP Solution Manager system assign roles `SAP_STUI_OVP_USER`.

Authorizations for Trusted RFC Connection

To allow for a trusted RFC - destination, you need also assign role `SAP_SM_FIORI_FRONTEND` in the back end system. The role contains `S_RFC` and `S_RFCACL` authorization.

> → Recommendation
>
> Make sure to maintain authorization object `S_RFCACL` accordingly. For specific information for this object, see the *Authorization Concept Security Guide*.

Authorizations in the Frond-End (ST-UI Component)

The following roles are delivered for front-end usage for the application:

- `SAP_STUI_GENERAL_AUTH`
  This role contains general authorizations which are required for the SAP Fiori Frontend.
- `SAP_STUI_OVP_TCR`
  This role contains Catalogue and Tiles for the application. This role should not be copied into your name space as it is a navigation role.
- `SAP_STUI_OVP_USER_AUTH`
  This role refers to the relevant Odata service in the *Description* tab of the role. Before you can assign the role to your end-user, you must configure the OData- Service:
  1. Copy the Odata service into your name space.

2. Add the copied service to your role *Menu*.
3. Check that authorization object `S_SERVICE` is entered into the *Authorization* tab.
4. Generate the profile.
5. Assign the role to your user.

17 Business Catalogue Roles

The Business Catalogue Roles underneath are assigned catalogue with according tiles only relevant for the type of user.

> **i Note**
>
> Any authorizations relevant for working with the assigned tiles need to be assigned to the relevant users, separately. For this information, see all roles relating to applications available in SAP Solution Manager in the *Application - Specific Security Guide*, for other applications than SAP Solution Manager, see the according Application and Security Guide.

Business Catalogue User Roles Assignment

User	User Definition	Business Catalogue Role
System Administrator	Attends to IT operations on a system or application level. Configures and monitors systems, processes incidents and service requests, and oversees patching and upgrade processes. Typically identified as a user with a highly-technical focus.	SAP_STUI_SYSADMIN_BR
Business Process Expert	Adds detailed business process knowledge to defining and operating specific business processes on an application level. Makes requests for changes, works with business-relevant background jobs, and monitors business process and data quality. May participate in testing. Typically identified as a key user representing business processes run by an IT solution.	SAP_STUI_BIZPROCEXPERT_BR
IT Manager	Monitors the big picture of an IT application. Accesses a variety of dashboards and analytics to get a quick overview of an IT solution's status. May take an interest in release management and general IT solution planning. Typically identified as a non-technical user responsible for the overall functioning of an IT solution.	SAP_STUI_ITMANAGER_BR
Quality Expert	Aims at upholding quality standards for an IT solution. Oversees or engages in testing activities. Influences change, release, and data quality processes. May seek up-to-date data on incidents and monitoring status. Typically identified as having competent awareness of technical issues.	SAP_STUI_QUALITYEXPERT_BR
End-User	Works with business-relevant IT applications. Creates and views both IT incidents and service requests, though rarely interacts directly with application management functions. Typically assumed to operate without any specific technical expertise.	SAP_STUI_COMMONUSER_BR

Important Disclaimers and Legal Information

Hyperlinks

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

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

Videos Hosted on External Platforms

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

Beta and Other Experimental Features

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

Example Code

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

Bias-Free Language

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

www.sap.com/contactsap

THE BEST RUN SAP