Installation Guide | PUBLIC
2019-09-20

Installation Guide

SAP Quotation and Underwriting for Insurance 1.1

THE BEST RUN SAP

Content

1 Introduction

1.1 About this Document

This document describes how to setup an SAP Quotation and Underwriting for Insurance solution. This includes the instructions for downloading, installing and configuring the FS-PRO, FS-QUO and FS-IPW components that comprise the Design Time and Runtime applications.

1.2 Audience

The information in this document is intended for application server administrators and database administrators (DBAs).

1.3 Overview

With this new release, the FS-PRO and FS-QUO installation procedure has been drastically simplified. Many of the manual steps from the past have been integrated into a script.

Basis admins will now have to spend more time in the beginning gathering information that will be entered into a single properties file. A single properties file is used to support both the FS-PRO and FS-QUO installation. That is, the properties file should be filled in with all of the information required to do a FS-PRO and a FS-QUO installation before you begin installing. The property `app_type` will determine which application is installed for a given execution of the script.

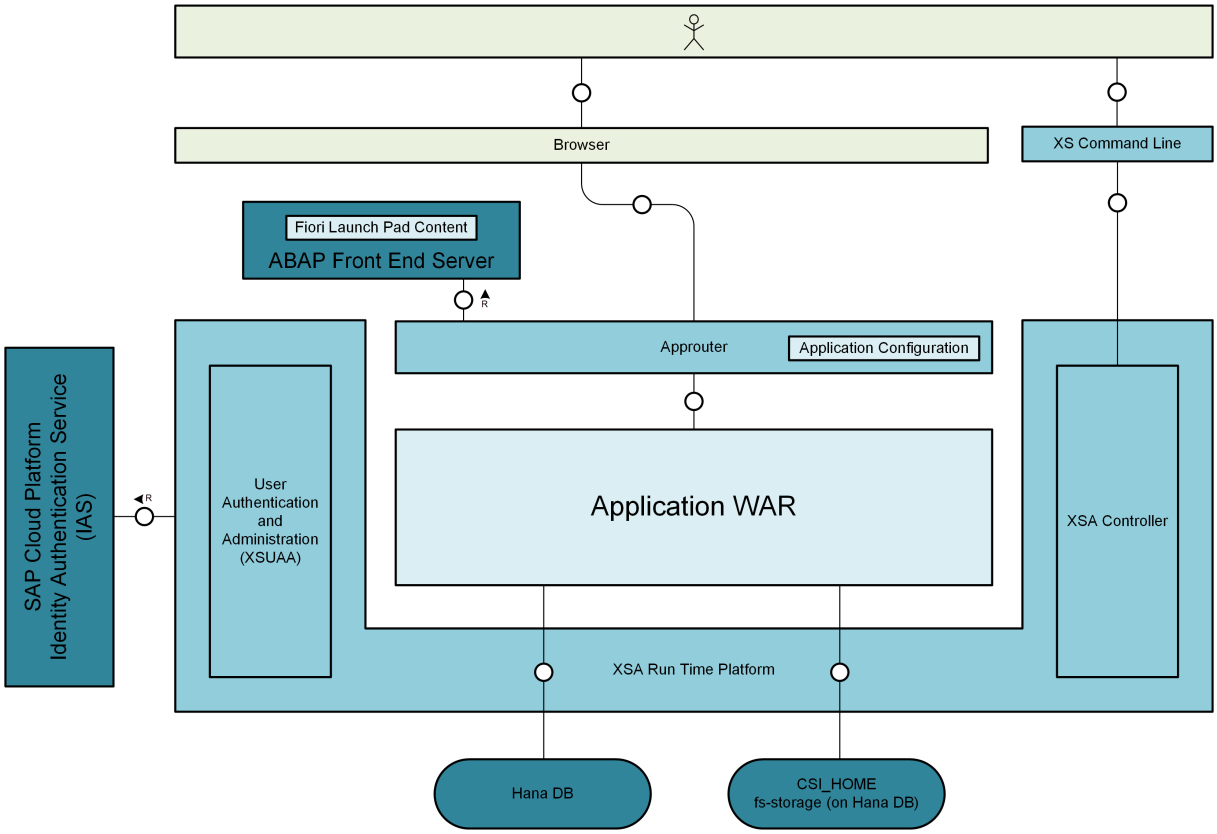
Information includes directory paths, user names, passwords, port numbers, etc. Once the properties file has been filled in the basis admin will execute a single script to complete the installation. The script must be executed twice: once for FS-PRO (`app_type=designtime`) and the second time for FS-QUO (`app_type=runtime`).

> ⚠ Caution
>
> FS-PRO must be installed first and it must be successful before you can proceed with installing FS-QUO.

The installation does not require any further user interaction after the passwords have been entered. The user only needs to check the log at the end to ensure that the installation completed successfully.

2 Prerequisites

2.1 System Landscape



SAP HANA XS Advanced Platform

Application Router (approuter)	The approuter handles HTTP request routing, URL-level authorization, and CSRF token handling. As part of application deployment and update, two application-specific files are installed with the approuter, `xs-app.json` and `xs-security.json`. For deployment, these files are packaged with the application WAR file into a Multi-Target Architecture (MTAR) file.
Runtime Platform Application Container	The platform's application container is based on Cloud Foundry's buildpack concept. Buildpacks provide framework and runtime support for apps. They examine your apps to determine what dependencies to download and how to configure the apps to communicate with bound services. When you push an app, the platform automatically

	detects an appropriate buildpack for it. This buildpack is used to compile or prepare your app for launch. This application has two components packaged into a single Multi-Target Architecture (MTAR) file. 1. The approuter is deployed with the `node.js` buildpack. 2. The core server application WAR file is deployed with the Apache TomEE buildpack.
User Authentication and Administration	XS User Authentication and Administration (XSUAA) is a service for user authentication and authorization.
Controller and Command Line Interface (CLI)	The platform has a command line interface for executing routine system administration tasks, including application installation and deployment.

Other Landscape Components

ABAP Front End Server (FES)	The FES hosts the landscape's Fiori Launchpad. As part of the installation process, application content (including the Fiori Launchpad tile configuration and Fiori application static content) is deployed to this server.
HANA Database	The application requires an SAP HANA database. Only SAP HANA is supported.
Audit Log Service	The application uses the platform's `auditlog` service to perform Data Protection and Privacy (DPP) logging. For more information about auditing, see the Change Logging and Read-Access Logging.
fs-storage Backing Service (CSI_HOME)	The application requires a file share. FS-PRO and FS-QUO use a backing service called `fs-storage`, which is located on the SAP HANA database server.
SAML Identity Provider (IdP)	This component must be setup and available before FS-QUO is installed. The Fiori launchpad (FLP) URL for FS-QUO has been programmed to go directly to the IdP login page. If it is not available then an error will occur and you will be presented with the XSA login page first. On that page you will see a link to the IdP login page.

Application Content

Application WAR file	Executable code for the application is deployed in the form of a WAR file. Along with the content for the approuter, this is packaged into an MTAR file.
Approuter Configuration	Two configuration files, the application descriptor (`xs-app.json`) and the security descriptor (`xs-security.json`), are deployed with the approuter. Along with the application WAR file, they are packaged into an MTAR file.
Database Content	Application database tables and sample content are included as part of the installation process.

CSI_HOME Content	Application shared file folders and content are included as part of the installation process.

2.2 Server System Requirements

Before you begin, ensure that all of the system requirements have been satisfied.

FS-PRO and FS-QUO require SAP HANA Platform Edition and the XS Advanced (XSA) Runtime component.

> ⚠ Restriction
>
> FS-PRO and FS-QUO only supports XSA port-based routing mode.

Refer to the specific server-side requirements below.

Supported Databases

FS-PRO and FS-QUO hosts their application database on SAP HANA exposed as a service instance in the XS Advanced Runtime environment. As such it requires SAP HANA Platform Edition.

The following version is supported:

- 2.0 SP04 - Revision 2.00.041.0

For more information and installation instructions, see the Installing an SAP HANA System topic in the *SAP HANA Server Installation and Update Guide*.

Also note the following requirements:

- For a database system that is configured in Multiple Container mode, the tenant container database must already be created. It is always recommended to have a separate tenant database container.
- Do not use the SYSTEMDB container to install the database.
- Increase the `plan_cache_size` config parameter from the default value of 2GB to 8GB. If you are using the SAP HANA Studio to make this change, you can find this under the *Configuration* tab in *indexserver.ini*.

Application Runtime Requirements

FS-PRO and FS-QUO require XS Advanced Runtime as the application runtime environment, which must be installed as an additional component on the SAP HANA system. The following versions are supported:

- 2.0 SP04 - Revision 2.00.041.0

For more information, see the Installing XS Advanced Runtime topic in the *SAP HANA Server Installation and Update Guide*.

Furthermore, the XS Advanced Runtime component must be updated to build 1.0.117.

Also note the following requirements:

- The logical database must be enabled and mapped to the XS Advanced organization used for FS-PRO and FS-QUO. For more information, see the Maintaining Database Instances in XS Advanced topic in the *SAP HANA Administration Guide*.
- A trusted server certificate is required to avoid security and connectivity issues. For more information, see the XS Advanced Certificate Management topic in the *SAP HANA Security Guide*.
- **Restriction**

  A single HANA tenant database is required. The silent installer only supports the installation of FS-PRO and FS-QUO in the same tenant.

Single Sign-On (SSO) Requirements

The FS-QUO Runtime application consists of a Fiori front-end component that is installed on an ABAP or S4/HANA On-Premise system, and a Java back-end component that is installed on a SAP HANA XS Advanced system. To ensure that the Fiori application can access the back-end OData services without separate authentication, SAML 2.0 must be enabled on both systems for single sign-on.

You may use any SAML 2.0 identity provider, including SAP-provided solutions such as SAP Cloud Platform Identity Authentication and SAP Single Sign-On. ABAP or S4/HANA On-Premise, as well as SAP HANA XS Advanced, will be configured as SAML 2.0 service providers.

For more information, see:

- Managing SAML Identity Providers in XS Advanced
- Single Sign-On with SAML 2.0 (See the *SAML 2.0 in AS ABAP* section)
- SAP Cloud Platform Identity Authentication Service

2.3 Client System Requirements

Client systems accessing the FS-QUO application require a supported web browser. As well, administrators require an SAP HANA client and the XS Advanced CLI client to perform the necessary administrative tasks during FS-QUO installation.

Note

Internet Explorer is the only web browser that is compatible with the Product Modeler and the URL must be added to the *Compatibility View Settings*.

2.4 Installer Requirements

Before you attempt an installation, ensure that all of the installer requirements have been satisfied.

The silent installer is only certified to run on the HANA server where XSA is installed. It is strongly recommended that the silent installer is executed using the HANA tenant DB OS user as this user will already have access to the HANA client tools.

The silent installer requires that the following server system requirements are compliant:

- A single HANA tenant database is required. The silent installer only supports the installation of FS-PRO and FS-QUO in the same tenant.
- HANA 2.0 SP04 (Revision 2.00.041.0) with XSA 1.0.117
- An XSA org and space have been created
- HANA Client installed (in particular, the command line tool hdbsql)
- JDK 1.8 (to be used by Apache Ant)

  > ⚠ Caution
  >
  > A message (`Unable to locate tools.jar. Expected to find it in <path>.`) will appear when the silent installer is executed if the JRE is set as the JAVA_HOME and/or in the PATH environment variable. To resolve the issue, set JAVA_HOME and/or PATH to a JDK.

- XS CLI client, version 1.0.117

  > ⓘ Note
  >
  > The absolute path for the silent installer path can't contain spaces.

You will also need to have the following software installed:

- cURL (Client URL), any version

Passwords

As the silent installer program runs, you will be asked to enter and confirm passwords to provide access to some of the application components affected by the installation process. You should possess the passwords for the following accounts before attempting an installation:

- Application Installer user.
- HANA tenant DB system user
- Technical users admin and system for Product Web Services (PWS). This user can be created at installation time.
- Technical user for FS-PM
- Technical user for SAP Business Partner for Financial Services (FS-BP)
- Technical user for CMS (if applicable)

Note that you will have three opportunities to correctly enter and confirm each password. After the third failed attempt, the installation process stops and you will have to start again from the beginning.

2.5 FS-PM Integration Requirements

When integrating FS-QUO with FS-PM, unicode must be enabled on FS-PM for successful integration.

For details on enabling unicode refer to the FS-PM documentation.

2.6 Substitution Variable Placeholders

The following table defines the substitution variables used in this guide. Gather the information listed prior to beginning.

Substitution Variable	Description
`<rel>`	The release version that you are installing.
`<sp>`	The support package version you are installing or upgrading.
`<pl>`	The patch level of you are installing or upgrading.
`<si_home>`	The location of the silent installer.
`<xsa_api_url>`	The SAP HANA XS Advanced API endpoint URL. Typically the URL is `https://<host>:3<instance>30`, where `<host>` is the host name of the SAP HANA XS Advanced system, and `<instance>` is the instance number.
`<org>`	The SAP HANA XS Advanced organization that was created during installation or upgrade of SAP HANA XS Advanced.
`<pro_designtime_space>`	The target space within SAP HANA XS Advanced organization. Application services for the FS-PRO Design Time application are installed in this space.
`<quo_runtime_space>`	The target space within SAP HANA XS Advanced organization. Application services for the FS-QUO Runtime application are installed in this space.
`<admin_user>`	The name of the administrative user for FS-PRO and FS-QUO.

Substitution Variable	Description
`<quo_runtime_uaa_app_name>`	The application name of the FS-QUO Runtime application as registered in the SAP HANA XS Advanced User Account and Authentication (UAA) service. When choosing this name for your FS-QUO deployment, the following restrictions apply: • The name must be unique within the organization where the FS-QUO application is deployed. Consequently, you must use different names for Design Time and Runtime • The name can be up to 100 characters, however you should minimize the length. • Only the following characters are allowed: a-z, A-Z, 0-9, _, - if you are deploying them to different spaces in the same organization. Generally, it is best practice to use the name `FS-QUO-designtime`.
`<quo_runtime_app_url>`	The URL to the FS-QUO Runtime approuter application.
`<flp_url>`	The HTTPs URL to your ABAP front-end server which hosts the FS-IPW component.

3 Preparation

3.1 Downloading the Assembly

You will need to download the assembly ZIP file for the FS-PRO, FS-QUO and FS-IPW components, which contain all of the files that will be used during the update process.

Context

The FS-QUO package will contain the silent installer and all of the necessary files to complete both the FS-PRO and FS-QUO installation. FS-IPW is a separate package, contained within the FS-QUO package, that will be installed onto a Netweaver 7.5 ABAP system.

The assembly ZIP file can be downloaded from the SAP Software Download Center.

Before you start, you must obtain the necessary authorization for the account that you are using to download SAP software. For assistance, contact your organization's administrator or account manager.

Procedure

1. Log in to SAP Software Downloads.
2. When prompted, log in using credentials with the appropriate download access.
3. Go to the *INSTALLATIONS & UPGRADES* tab.
4. Expand the *By Alphabetical Index (A-Z)* item and choose the letter *Q*.
5. In the category list, locate and choose the *QUO UNDERWRITING INS 1.1* Installation Product.
6. Go to *COMPRISED SOFTWARE COMPONENT VERSIONS* tab and choose *FS-QUO 510*.
7. In the *Items Available to Download* list, select the zip file entry named *FS-QUO 510* for download.

   You can either download it directly from the web browser, or add it to the download basket for download via the SAP Download Manager.

Results

You have downloaded the necessary assembly ZIP files, which will be used during the update.

3.2 SAP Notes

Before you attempt to install FS-QUO, you need to read the following SAP Notes:

- 2804822 UI5(1.60) Upgrade issues

3.3 Creating Spaces in XS Advanced for FS-PRO and FS-QUO

The FS-PRO Design Time and the FS-QUO Runtime applications must be installed in the same space, which must be created before the installation is attempted.

Context

The FS-PRO and FS-QUO applications are each packaged as a multi-target application (MTA). An MTA has an ID which must be unique at the space level. As both FS-PRO and FS-QUO have their own identifier, the silent installer will deploy both applications in the same space.

For more information, see:

- Organizations and Spaces
- Maintaining Organizations and Spaces in XS Advanced

Procedure

1. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

   > → Tip
   >
   > You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the `xsa-admin` entry.

2. When prompted, log in as an XSA administrative user.

   Use either `XSA_ADMIN` or an existing user with comparable access.

3. In the main page, click *Organization and Space Management*.
4. Select `<org>` on the organization list pane.
5. Select + *Create Space* on the organization detail pane.
   A pop-up dialog opens.
6. Enter `<space_name>` as the space name and then select *Create*.

7. Save your changes.

Results

The space `<space_name>` is now created for deployment of the FS-PRO Design Time and the FS-QUO Runtime applications.

3.4 Creating an Administrative User in SAP HANA XS Advanced

To streamline the FS-PRO and FS-QUO installation process, create and set up an administrative user with platform and application access in XS Advanced.

Context

The FS-PRO and FS-QUO installation processes involve various XS Advanced administrative tasks, such as creating spaces, deploying applications, and configuring user authorizations. For simplicity, a user must be created in XS Advanced and assigned the necessary authorizations to perform all such tasks. As outlined in the Role Collections for XS Advanced Administrators topic in the *SAP HANA Administration Guide*, a set of role collections must be assigned.

For more information, see:

- Setting Up Security Artifacts topic in the *SAP HANA Administration Guide*.

Follow the steps below to create a new user and assign the necessary role collections to the user.

Procedure

1. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

   > → Tip
   >
   > You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the `xsa-admin` entry.

2. When prompted, log in as an XSA administrative user.

   Use either `XSA_ADMIN` or an existing user with comparable access.

3. Choose *User Management* on the main page.
4. Choose *New*.

The *New User* pop-up dialog opens.

5. Enter the required information for the `<admin_user>` and select *Create*.
6. Select `<admin_user>` in the XSA business users list.
7. Select the *Roles* tab on the *User Details* page.
8. Choose *Add*.
   A pop-up dialog opens.
9. Select the checkbox next to the following role collections and select *OK*:
   - `XS_AUTHORIZATION_ADMIN`
   - `XS_CONTROLLER_ADMIN`

     > **Note**
     >
     > The `XS_CONTROLLER_ADMIN` role allows management of all organizations and spaces without explicitly assigning organization and space roles. If desired, you can assign the `XS_CONTROLLER_USER` role collection and the appropriate organization and space roles instead.

   - `XS_USER_ADMIN`
10. Save your changes.

3.5 Gathering the Information for the Properties File Settings

The silent installer relies on a properties file to determine the actions that will be executed during the installation. The values for the parameters in the properties file must be gathered prior to attempting an installation.

A checklist has been provided to help you keep track of the parameter values.

> **Note**
>
> The properties that are gathered now will cover both FS-PRO and FS-QUO installation. Even though FS-PRO is installed first, the installer script requires knowledge of FS-QUO during the installation. And vice versa.

3.5.1 Properties File Settings Checklist

The first step of your installation is to gather the necessary system information. You can print this checklist to record the information that you will need.

Environment Variables/Properties

✔	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`xs_server`	
	`org`	
	`space`	
	`system`	
	`xs_client_path`	
	`installer_user_id**`	

**Password is required

Deployment Parameters

✔	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`operation`	clean_install
	`app_type`	

Tenant Database Properties

✔	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`xs_tenant_db_main_user**`	
	`xs_tenant_db_host`	
	`xs_tenant_db_port`	
	`xs_tenant_db_instance`	

**Password is required

XS Platform Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`xs_api_endpoint`	
	`uaa_url`	
	`uaa_clientid`	
	`uaa_clientsecret`	
	`approuter_proxy_host`	
	`approuter_proxy_port`	
	`quo_flp_idp_name`	

Application-Specific Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`product_type`	
	`fs_pm_enabled`	
	`cms_enabled`	
	`xs_team_port_range`	
	`flp_url`	

> ### Note
>
> If the `cms_enabled` parameter is set to FALSE, you don't need to set the `cms_server_url` or `cms_server_user` parameters.

Application Port Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`dt_approuter_port`	
	`rt_approuter_port`	
	`dt_port`	
	`rt_port`	

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	dt_installer_port	
	rt_installer_port	

Design Time Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	dt_db_schema	
	dt_memory_size	
	pro_csihome	

Runtime Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	rt_db_schema	
	rt_memory_size	
	quo_flp_idp_name	
	quo_csihome	

FS-BP Integration Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	fs_bp_client	
	fs_bp_system_number	
	fs_bp_host	
	fs_bp_user_name**	

**Password is required

FS-PM Integration Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`fs_pm_client`	
	`fs_pm_system_number`	
	`fs_pm_host`	
	`fs_pm_user_name**`	
	`fs_pm_icm_app_id`	

**Password is required

CMS Properties

✓	Installation Properties File Parameter Name	Enter Your System's Value for the Properties File Parameter Here...
	`cms_server_url`	
	`cms_server_user**`	

**Password is required

> ### Note
>
> If the `cms_enabled` parameter is FALSE, you do not need to set the `cms_server_url` or `cms_server_user` parameters.

Related Information

3.5.2 Environment Variables/Properties

As part of the installation process, you will need to set values in a properties files. You will need to configure the following platform-specific settings:

`xs_server`

This setting specifies the fully qualified host name of the HANA XSA server.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`org`

This setting specifies the name of the XSA organization where the application will be deployed.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`space`

This setting specifies the name of the XSA space where the application will be deployed.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`system`

This setting specifies the name of the system/application you wish to deploy.

Format: Free-form text

This value can be any alpha-numeric text. It is recommended to keep this value short, as it will be used as 1/5 of the total deployed application name.

In conjunction with `org` and `space`, the deployed application name will follow this pattern:

`<org>-<space>-<system>-<dt:rt>-<blank:approuter:installer>`

where

- `<dt/rt>` - `<dt>` is Design Time and `<rt>` is Runtime
- `<app_function>` - blank is for the main web application; approuter is an application that handles all HTTP/HTTPS traffic for the main web application; installer is an application that will assist with installing the file system and database for the main application.

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`xs_client_path`

This setting specifies the path your local XS client.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`installer_user_id`

This setting specifies the XSA user that was mentioned in the *Creating an Administrative User in SAP HANA XS Advanced* topic.

Format: Free-form text

> ⚠ Caution
>
> This value is always upper-case even if you created the user using lower case and/or mixed case characters.

3.5.3 Deployment Parameters

As part of the installation process, you will need to set values in a properties file. You will need to configure the following settings to define actions taken during the installation:

`operation`

This setting specifies the type of operation to be performed by the silent installer.

This value must be set to `clean_install`.

`app_type`

This setting determines the type of system that will be installed.

The possible values are `designtime` or `runtime`.

If this value is incorrect, it will cause a Fatal Error during the installation process.

3.5.4 Tenant Database Properties

As part of the installation process, you will need to set values in a properties files. You will need to configure the following properties for the tenant database:

`xs_tenant_db_main_user`

This setting specifies the user name of the main user for the tenant database.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`xs_tenant_db_host`

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`xs_tenant_db_port`

This setting specifies the SQL port of the tenant database.

> → Tip
>
> To find this value, log into the tenant database using the following command:
>
> ```
> hdbsql -n <hostname> -i <instance_number> -d
> <tenant_db_name> -u system
> ```

Then execute this query:

```
SELECT SERVICE_NAME, PORT, SQL_PORT, (PORT + 2)
HTTP_PORT FROM SYS.M_SERVICES WHERE
((SERVICE_NAME='indexserver' and
COORDINATOR_TYPE= 'MASTER') or (SERVICE_NAME='xsengine'));
```

The SQL port for the indexserver is the required value.

Format: Integer

If this value is incorrect, it will cause a Fatal Error during the installation process.

`xs_tenant_db_instance`

This setting specifies the name of the tenant database instance.

Format: Integer

If this value is incorrect, it will cause a Fatal Error during the installation process.

3.5.5 XS Platform Properties

As part of the installation process, you will need to set values in a properties files. You will need to configure the following platform-specific settings:

`xs_api_endpoint`

This setting specifies the SAP HANA XS Advanced API endpoint URL.

Format: Free-form text

Typically the URL is `https://<host>:3<instance>30`, where `<host>` is the host name of the SAP HANA XS Advanced system, and `<instance>` is the instance number.

This value can also be looked up using the command `xs system-info`. Look for the `controller endpoint`.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`uaa_url`

This setting specifies the URL for the XSUAA security endpoint.

Format: Free-form text

Typically the URL is `https://${<xs_server>}:3${<xs_tenant_db_instance>}32/uaa-security`.

This value can be looked up by using either the `xs e xsa-admin` or `xs e xsa-cockpit` commands. The xsa-admin application is deployed in the SAP space of your org. Look for the URL under the *User-Provided* > *destinations* > *name* > *uaa* section.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`uaa_clientid`

This setting specifies the XSUAA client ID. This value can be looked up by using either the `xs e xsa-admin` or `xs e xsa-cockpit` commands. The xsa-admin

application is deployed in the SAP space of your org. Look for the clientid under the *VCAP_SERVICES* > *xsuaa* > *credentials* section.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`uaa_clientsecret`

This setting specifies the encrypted password for the XSUAA client ID. This value can be looked up by using either the `xs e xsa-admin` or `xs e xsa-cockpit` commands. The xsa-admin application is deployed in the SAP space of your org. Look for the clientsecret under the *VCAP_SERVICES* > *xsuaa* > *credentials* section.

Format: Free-form text

If this value is incorrect, it will cause a Fatal Error during the installation process.

`approuter_proxy_host`

This setting specifies the host name of the proxy server, if one is required for the network environment.

Format: Free-form text or BLANK

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`approuter_proxy_port`

This setting specifies the port number of the proxy server, if one is required for the network environment.

Format: Integer or BLANK

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`quo_flp_idp_name`

This setting specifies the SAML Identity Provider name that XSA is connected to for SSO.

The value can be obtained by going to *Security* > *Trust Configuration* > *SAML IdP* > *name* in the XSA Cockpit.

Format: Free-form text or BLANK

If the this value is incorrect, the installation will complete but the IdP login page will not initially appear. Instead you will be presented with the XSA login page first and on that page you will see a link to the IdP login page.

3.5.6 XSA Service Instances Properties

As part of the installation process, you will need to set values in a properties files.

The installation process does not require any changes to the XSA Service Instances properties. These properties will be set automatically by the silent installer to conform to a standard naming pattern. The properties are for use during updates only.

`dt_db`

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

dt_fs

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

dt_uaa

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

dt_auditlog

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

rt_db

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

rt_fs

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

rt_uaa

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

rt_auditlog

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the update process.

3.5.7 Application-Specific Properties

As part of the installation process, you will need to set values in a properties file. You will need to configure the following settings for FS-QUO:

product_type

This setting specifies which line of business and bootstrap products will be imported, built, published, and deployed.

This setting works in conjunction with the `app_type` parameter (`designtime` or `runtime` settings).

The possible values are:

base-pro	Use this value for a Design Time installation.
risk-based	Use this value for a Runtime installation that will feature risk-based products.
cov-based	Use this value for a Runtime installation that will feature coverage-based products.

The business unit will have to tell the basis admin which line of business the system will be used for.

If this value is incorrect, it will cause a Fatal Error during the installation process.

fs_pm_enabled

This setting indicates if FS-PM will be integrated with the system.

For Design Time systems, the Design Time IFBC Integration Settings must be provided.

For Runtime systems, the FS-BP Intergration Properties and FS-PM Integration Properties must be provided.

The possible values are:

true	The FS-PM integration is enabled.
false	The FS-PM integration is disabled.

The business unit will determine if integration with FS-PM is required.

If this value is incorrect, it will not cause a Fatal Error during the installation process.

cms_enabled

This setting indicates if a CMS (Content Management Server) will be integrated with the system.

CMS are for Runtime systems only.

If set to `true` then the Content Management System (CMS) Integration Properties must be provided.

The possible values are:

true	The CMS will be integrated with the system.
false	The CMS will not be integrated with the system.

The business unit will determine if integration with CMS is required.

If this value is incorrect, it will not cause a Fatal Error during the installation process.

xs_team_port_range

This setting can be used to manage port number usage.

In conjunction with the Application Ports properties, the property will assign a specific range of ports for each system - Design Time and Runtime. Each system require 3 ports. This mechanism will keep the port range of the 2 systems close to each other but not overlap.

Format: 3 digit integer that is >=100 and <=655.

If this value is incorrect, it will cause a Fatal Error during the installation process.

flp_url

The setting specifies the Fiori Launch Pad URL where FS-IPW is deployed and is valid for Runtime systems only. FS-IPW is the front-end UI for Runtime.

Format: `https://<FLP_host_name>:<port>`

If this value is incorrect, it will not cause a Fatal Error during the installation process.

3.5.8 Application Port Properties

As part of the installation process, you will need to set values in a properties file. You will need to configure the following settings to determine port information:

> **Note**
>
> Users are allowed to specify their own port numbers. In order to ensure that users do not need to update their saved URL's, you must look up the current application ports and overwrite the "`${xs_team_port_range}0n`" values in all of the Application Port Properties. The current application ports numbers can be seen with the `xs apps` command.

`dt_approuter_port`

This setting specifies the approuter port number for the Design Time instance.

This is the port number that should be used to access the Design Time application.

This property can be used in conjunction with the property `xs_team_port_range` to define a patterned port range. Or the user can override the pattern and enter an explicit value. It is strongly recommended that you do not change this value explicitly and allow the team port range pattern to take effect. This will allow for easier updates in the future.

Format: `${<xs_team_port_range>}01`

If this value is incorrect, it will cause a Fatal Error during the installation process.

`rt_approuter_port`

This setting specifies the approuter port number for the Runtime instance.

This is the port number that should be used to access the Runtime application.

This property can be used in conjunction with the property `xs_team_port_range` to define a patterned port range. Or the user can override the pattern and enter an explicit value. It is strongly recommended that you do not change this value explicitly and allow the team port range pattern to take effect. This will allow for easier updates in the future.

Format: `${<xs_team_port_range>}02`

If this value is incorrect, it will cause a Fatal Error during the installation process.

`dt_port`

This setting specifies the web application port number for the Design Time instance.

This property can be used in conjunction with the property `xs_team_port_range` to define a patterned port range. Or the user can override the pattern and enter an explicit value. It is strongly recommended that you do not change this value explicitly and allow the team port range pattern to take effect. This will allow for easier updates in the future.

Format: `${<xs_team_port_range>}05`

If this value is incorrect, it will cause a Fatal Error during the installation process.

`rt_port`

This setting specifies the web application port number for the Runtime instance.

This property can be used in conjunction with the property `xs_team_port_range` to define a patterned port range. Or the user can override the pattern and enter an explicit value. It is strongly recommended that you do not change this value explicitly and allow the team port range pattern to take effect. This will allow for easier updates in the future.

Format: `${<xs_team_port_range>}06`

If this value is incorrect, it will cause a Fatal Error during the installation process.

`dt_installer_port`

This parameter has been deprecated.

`rt_installer_port`

This setting specifies the installer utility port number for the Runtime instance.

This property can be used in conjunction with the property `xs_team_port_range` to define a patterned port range. Or the user can override the pattern and enter an explicit value. It is strongly recommended that you do not change this value explicitly and allow the team port range pattern to take effect. This will allow for easier updates in the future.

Format: `${<xs_team_port_range>}04`

If this value is incorrect, it will cause a Fatal Error during the installation process.

3.5.9 Design Time Properties

As part of the installation process, you will need to set values in a properties file. You will need to configure the following settings to determine information for the Design Time instance:

`dt_db_schema`

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`dt_memory_size`

This setting specifies the total heap memory size for the Design Time instance, expressed in megabytes.

This value can be adjusted over time as needed. The initial value is enough to start a project.

Default value: 2048M

Format: An "M" is required at the end of the value.

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`pro_csihome`

> **Note**
>
> Do not alter the default value for this parameter.

Default value: csihome

If this value is incorrect, it will not cause a Fatal Error during the installation process.

3.5.10 Runtime Properties

As part of the installation process, you will need to set values in a properties file. You will need to configure the following settings to determine information for the Runtime instance:

`rt_db_schema`

Do not change the default value. The default value allows the silent installer to use a pre-determined naming pattern that will allow for easier future updates to be applied.

If this value is incorrect, it will cause a Fatal Error during the installation process.

`rt_memory_size`

This setting specifies the total heap memory size for the Runtime instance, expressed in megabytes.

This value can be adjusted over time as needed. The initial value is enough to start a project.

Default value: 2048M

Format: An "M" is required at the end of the value.

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`quo_csihome`

This setting specifies the directory name of the CSI Home for the Runtime deployment. The name itself is not important as users will not see it.

Format: Free-form text

Default value: csihome

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`quo_flp_idp_name`

This is the name of the SAML Identity provider that is used for SSO.

This name is case sensitive.

Default value: QUO-FLP-IDP

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process. However, the application will not function properly as the proper login page will not be presented to the user.

3.5.11 FS-BP Integration Properties

As part of the installation process, you will need to set values in a properties file. If your solution includes an integration with FS-BP, you will need to configure the following settings:

`fs_bp_client`

This setting specifies the client number of the FS-BP system on the ABAP server.

Format: 3 digit integer

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`fs_bp_system_number`

This setting specifies the instance number of the ABAP server where FS-BP is installed.

Format: 2 digit integer

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`fs_bp_host`

This setting specifies the hostname of the ABAP server where FS-BP is installed.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`fs_bp_user_name`

This setting specifies the technical user that FS-QUO will use to connect to the FS-BP server.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process.

3.5.12 FS-PM Integration Properties

As part of the installation process, you will need to set values in a properties file. If your solution includes an integration with FS-PM, you will need to configure the following settings:

`fs_pm_client`

This setting specifies the client number of the FS-PM system on the ABAP server.

Format: 3 digit integer

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`fs_pm_system_number`

This setting specifies the instance number of the ABAP server where FS-PM is installed.

Format: 2 digit integer

If this value is incorrect, it will not cause a Fatal Error during the installation process.

`fs_pm_host`

This setting specifies the hostname of the ABAP server where FS-PM is installed.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process.

fs_pm_user_name

This setting specifies the technical user that FS-QUO will use to connect to the FS-BP server.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process.

fs_pm_icm_app_id

This setting specifies the ICM application ID used to retrieve participant role of a business partner from ICM via FS-PM.

The value is specific to the FS-PM instance.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process.

3.5.13 CMS Properties

As part of the installation process, you will need to set values in a properties files. If your solution includes an integration with a CMS, you will need to configure the following settings:

cms_server_url

This setting specifies the connection endpoint URL for the CMS.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process. The value can be corrected after the installation process has been completed.

cms_server_user

This setting specifies the user ID that FS-QUO will use to connect to the CMS.

Format: Free-form text

If this value is incorrect, it will not cause a Fatal Error during the installation process. The value can be corrected after the installation process has been completed.

4 Design Time Application

4.1 Installing the Design Time Application

FS-PRO is installed using a properties file that is read by a shell script.

Prerequisites

You have met the prerequisites in Chapter 2 (Prerequisites) and have gathered the values for the parameters in Chapter 3 (Preparation). The ZIP package has been uploaded to the HANA server and is owned by the HANA tenant OS user. For the remainder of the guide, we will call the location of the silent installer `<si_home>`.

Context

> ⚠ Caution
>
> A clean install will do a clean up before it begins the actual installation. That is, any file system service, DB service, and deployed applications that have the same names that are provided in the `environment.properties` file will be deleted and then recreated. All data will be lost.

The shell script will perform the following steps:

1. Check some parameters for validity.
2. Create the application installer user.
3. Prepare the file system service.
4. Prepare the database service.
5. Prepare the audit log service.
6. Install the 'installer' app that will assist with the rest of the installation.
7. Create the CSI home.
8. Create the FS-PRO database.
9. Deploy the FS-PRO MTAR.
10. Configure the FS-PRO application settings.
11. Insert users into the FS-PRO that will be used by Product Web Services.
12. Import the base products.

Procedure

1. Log onto the HANA server as the HANA tenant OS user.
2. Go to `<si_home>` and unzip the FS-QUO package.
3. Go to `<si_home>/tools` and unzip the Apache ANT package.
4. Ensure that the file `<si_home>/silent_installer.sh` is executable.

   If it is not, change it by executing `chmod 744 silent_installer.sh`
5. Edit the file `<si_home>/properties/environment.properties` and enter the values for the parameters from Chapter 3.3. Values that need to be changed in the environment.properties file will be in the format `###[A-Z]###`.

   For example, if the original value in the properties file:

   ```
   xs_server=###XS_SERVER###
   ```

   You would replace it as follows:

   ```
   xs_server=myhanaserver.com
   ```
6. Save your changes.
7. Prepare your system to run the silent installer.

   The silent installer runs as a shell script process. It can take anywhere from 30 minutes to 2.5+ hours to complete. One method to ensure the process is not interrupted due to session disconnects is to use the utility `screen`. The use of `screen` will also allow you to close your current session and return to it later. To prevent SSH session timeouts, it is recommended that you use a keep-alive option in your SSH application (e.g. putty -> Connection > Sending of null packets to keep session active) or include the SSH option `ServerAliveInterval` when you connect. It is recommended that you set the *Seconds between keepalives* value to 300.
8. Run the shell script file `<si_home>/silent_installer.sh`.

   As the shell script executes, you will be asked to enter and confirm passwords as required.

   You will have three opportunities to correctly enter and confirm each password. After the third failed attempt, the installation process will stop and you will have to start again from the beginning.

   > → Tip
   >
   > While the script is running, you will not see any output as it is being redirected to a log file.
   > You can open another session and tail the log to watch the process: `tail -f <si_home>/silent_installer_<date_time>.log`
9. When the command prompt returns, the script has finished executing. You must review the log, `<si_home>/logs_archive/silent_installer_<date_time>.log`, to determine if the installation was successful. If the installation is successful, you will see a message similar to this one at the end of the log: `BUILD SUCCESSFUL Total time: 11 minutes 45 seconds`

   > ⓘ Note
   >
   > The amount of time it takes will vary from system to system. The installation of a coverage-based FS-QUO system in the SAP lab took ~9 minutes to complete. You can expect your installation to take about the same amount of time with a range of +/- 3 minutes. Risk-based systems will generally take less time.

In the event of a failure, all of the logs can be found in `<si_home>/logs_archive`. The logs in the sub folders have been zipped up into the file `logs_<date_time>.zip`. If you need to contact support, you will need to provide the `logs_<date_time>.zip` and `silent_installer_<date_time>.log` files.

If you are able to determine the cause of the failure (for example, a typo in the `environment.properties` file such as an invalid org name) it is safe to rerun the silent installer without restoring the database backup. If you are unsure if the installation can be restarted, you should contact support.

Next Steps

After completing the installation, do not delete the directory and contents of the silent installer. These files may be required for applying future SAP Notes. Keep the silent installer safely stored somewhere safe.

Related Information

Installer Requirements [page 9]
Gathering the Information for the Properties File Settings [page 15]
Properties File Settings Checklist [page 15]

5 FS-QUO Front End

5.1 Installation

5.1.1 Overview of Apps for Insurance from SAP

The FS-IPW component contains a bundle of transactional apps for insurance services from SAP that run on the SAP Fiori Launchpad.

The following apps are available for Risk-based solutions:

- Create New Business
- Manage Accounts
- Manage Producers
- Manage Policies
- My Submission Worklist

The following apps are available for Coverage-based solutions:

- Create Insurance Quote
- My Insurance Worklist
- My Underwriting Worklist
- Create Group Insurance Quote
- Manage Issued Policies
- My Insurance Tasks
- Create Insurance Quote from Master
- Create Master Insurance Quote

Product Information

The system landscape consists of front-end components and back-end components. These apps for insurance from SAP are part of the front-end components.

Component	UI for SAP Workplaces for Insurance
Software Component Version	UIFSIPW 310
Support Package	SP00
Delivery Date	Q3/2019

Integration

Data is exchanged between the apps and the back-end components using OData services.

Setup of App Environment for Insurance Services from SAP

You can use transactional apps to access the SAP Fiori system landscape in an ABAP environment.

Before implementing an app, set up the system landscape to enable SAP Fiori.

An app requires front-end components (providing the user interface and the connection to the back end) and back-end components (providing the data). The front-end components and the back-end components are delivered in separate products and have to be installed in a system landscape that is enabled for SAP Fiori.

Client

To be able to run the insurance apps, the runtime environment (for example, the browser) of the client must support HTML5.

ABAP Front-End Server

The ABAP front-end server contains all the infrastructure components for an SAP Fiori app. The UI components and the gateway are based on SAP NetWeaver. Typically, both are deployed on the same server.

The central UI component is a framework that provides the common infrastructure for all SAP Fiori apps: SAP Fiori launchpad is the basis of all SAP Fiori UIs, and provides fundamental functions for SAP Fiori apps such as logon, surface sizing, navigation between apps, and role- based app catalogs. End-users access the SAP Fiori apps from the SAP Fiori launchpad.

The apps must be additionally installed on the front-end server.

Java Back-End server (Business Functionality Layer)

The Java back-end component FS-QUO is installed in the business functionality layer, providing the business logic and the back-end data, including roles and authorizations. The back-end server runs on SAP HANA XS Advanced.

5.1.2 Configuring the Front-End Server

You need to configure the front-end server for FS-QUO before installing the FS-IPW component.

Procedure

1. Verify that the correct version of the following component is in place on the front-end server.

Product Version	Details
Central UI component	Comprised component version: USER INTERFACE TECHNOLOGY 7.53 (SAP_UI 753) with SAPUI5 Client Runtime 1.00 UI5CLIENT65P_10-80000549.ZIP

2. Specify the settings for supported languages in the SAP Gateway system and ensure that support for English, Korean, Japanese, and Chinese Traditional have been configured. Ensure that you have configured settings for both default and logon languages.

   You must install the same language packages for SAP Fiori in the SAP Gateway system and the SAP Business Suite back-end system.

   Ensure that the default language of the SAP Gateway system is the same as the default language of the back-end system, for example, English. If this is not the case, ensure that the SAP Gateway system contains a subset of the languages of the back-end system.

   The logon language for the ABAP Application Server is set according to the following process:

   a. If the Mandatory Logon Data indicator has been activated for a service in transaction `SICF`, the system uses the language that was entered there.
   b. If this is not the case, but the HTTP request contains the language in the HTTP header (as a header or a form field), you log onto the system using this language.
   c. The browser settings of the calling client are then used. The system selects as the logon language the first language from the list that is maintained in the browser, and which is also installed in the SAP system. The language list is specified using the HTTP header field `accept-language`.

      > **Note**
      >
      > In Internet Explorer, you can set the required language by choosing *Tools* > *Internet Options* > *Languages*.

   d. If no language is defined by this process, the classic SAP system mechanisms are used. The logon language is based on the user settings (in transaction `SU01`) and if nothing is entered here, the default language of the SAP system is used automatically.

Next Steps

Next, you need to install the `UIFSIPW 310` front-end component.

5.1.3 Installing the FS-QUO Front-End Using SAINT

You can install product versions with `SAINT`.

Context

You do not need to download a separate assembly for FS-IPW. The FS-IPW package is located inside of the FS-QUO assembly.

> → Remember
>
> Ensure that you have downloaded the most recent patch version.

Procedure

1. Download the FS-IPW package from *Installations & Upgrades* > *Q* > *QUO Underwriting INS* > *QUO Underwriting INS 1.1* > *Installation and Upgrade* > *51054065 (QUO Underwriting INS 1.1)*.
2. Download the FS-IPW updates from *Support Packages* > *Q* > *QUO Underwriting INS 1.1* > *Comprised Software Component Versions* > *UIFSIPW 310*.
3. Login to your ABAP server.
4. Run transaction `SAINT`.
5. Upload all of the packages by selecting *Installation Package* > *Load packages* > *[SAR archives from Front-End | SAR archives from application server]* from the menu.

   > → Tip
   >
   > Do not unpack the SAR file using SAPCAR at the OS-level. If you do, you will get a WARNING message later (`Missing signed manifest file`). The warning can be ignored, but it's better to avoid it altogether.
6. Select the packages and install them.

5.2 Post-Installation

5.2.1 Creating Semantic Objects

As part of the `UIFSIPW 310` installation process, the following semantic objects must be manually created on the ABAP front-end server using the `/UI2/SEMOBJ` transaction:

Semantic Object	Semantic Object Name
`InsuranceQuote`	Insurance Quote
`UnderwritingCase`	Underwriting Case
`GroupInsuranceQuote`	Group Insurance Quote
`InsuranceTask`	Insurance Task
`MasterInsurancePolicy`	Master Insurance Policy
`MasterInsuranceQuote`	Master Insurance Quote
`GeneralInsurancePolicy`	General Insurance Policy
`InsuranceAccount`	Insurance Account
`InsuranceProducer`	Insurance Producer
`InsuraceQuoteOption`	Insurance Quote Option
`InsuranceTransaction`	Insurance Transaction
`BusinessPartner`[1]	Business Partner
InsurancePolicyForQuote	Manage Issued Policies

For details, refer to https://help.sap.com/saphelp_uiaddon10/helpdata/en/60/9c84bbacb04fd8a17bdb5da742815f/content.htm.

[1] Reused

5.2.2 Configuring the *Maintain Business Partner* Tile

We can configure a *Maintain Business Partner* tile to leverage SAP GP-FS functionality within FS-IPW.

Prerequisites

SSO between the SAP Gateway on the FS-IPW front-end server and SAP GP-FS must be enabled.

Procedure

1. Create an RFC destination named **SAP_FS_BP** in SM59 (Transaction Code) on the FS-IPW front-end server and then perform a quick ping test.
   a. Enter **H** in the *Connection Type* filed.
   b. Go to the *Technical Settings* tab.
   c. Enter the *Target Host* and *Service No.* to point to the SAP GP-FS system.

      > **Note**
      >
      > If the SAP GP-FS system isn't in the same domain as the FS-IPW front-end server, you will need to use the SAP Web Dispatcher to bypass the domain issue. For more information, see SAP Note 2389824.

   d. Go to the *Logon & Security* tab.
   e. Select *Do Not Use a User* .
   f. Leave the *Language* field empty if you want to use the language from the calling application (from Launchpad logon language).
   g. Select *Send Assertion Ticket for Dedicated Target Sys.* pointing to the SID and client of the back-end server (SAP GP-FS system).
   h. Select *Active* under SSL.
2. In the Fiori Launchpad Designer, configure the target mapping.
   a. Select the **Transaction** application type as the default configuration.
   b. Set the system alias as **SAP_FS_BP** (configured in SM59).
   c. Add the **BUS_JOEL_MAIN-CHANGE_NUMBER** parameter (Format: Table Name-Column Name) used for SAP GP-FS navigation with parameters in FS-IPW Fiori Apps.

Related Information

SAP Note 1257108
http://scn.sap.com/community/netweaver-business-client/blog/2015/06/01/configuring-remote-systems-in-sm59

5.2.3 Roles and Authorizations

Role and authorizations are configured on both the ABAP front-end server and the Java back-end server.

On ABAP front-end servers, installing `UIFSIPW310` provides some roles for FS-IPW Fiori app access. These roles must not be used as-is. They can be copied to the Z namespace for customization. For example, `Z_UI2_USER_700`. There are also other Fiori Launchpad-related roles that are required by the platform and are documented in the Fiori Launchpad setup guide.

The required ABAP roles are dependent on the bootstrap that you imported earlier.

SAP_IPW_BCR_INSUW_T	This role is applicable to the following coverage-based apps: • Create Insurance Quote • My Insurance Worklist • My Underwriting Worklist • Create Group Insurance Quote • Manage Issued Policies • My Insurance Tasks • Create Insurance Quote from Master • Create Master Insurance Quote
SAP_IPW_BCR_INSAGENT_T	This role is applicable to the following coverage-based apps: • Create Insurance Quote • My Insurance Worklist • Create Group Insurance Quote • Manage Issued Policies • My Insurance Tasks • Create Insurance Quote from Master • Create Master Insurance Quote
SAP_IPW_BCR_PASINSUW_T	This role is applicable to the following risk-based apps: • Create New Business • My Submission Worklist • Manage Policies • Manage Accounts • Manage Producers
SAP_IPW_BCR_PASINSUWASST_T	This role is applicable to the following risk-based apps: • Create New Business • My Submission Worklist • Manage Policies

> ⚠ Caution
>
> Assign only one role to each user.

6 Runtime Application

6.1 Installing the Runtime Application

FS-QUO is installed using a properties file that is read by a shell script.

Prerequisites

You have successfully installed the Design Time Application, FS-PRO.

Context

> ⚠ Caution
>
> A clean install will do a clean up before it begins the actual installation. That is, any file system service, DB service, and deployed applications that have the same names that are provided in the `environment.properties` file will be deleted and then recreated. All data will be lost.

The shell script will perform the following steps:

1. Check some parameters for validity.
2. Create the application installer user.
3. Prepare the file system service.
4. Prepare the database service.
5. Prepare the audit log service.
6. Install the 'installer' app that will assist with the rest of the installation.
7. Create the CSI home.
8. Create the FS-QUO database.
9. Deploy the FS-QUO MTAR.
10. Configure the FS-QUO application settings.
11. Insert users into the FS-QUO that will be used by Product Web Services.
12. Import insurance specific content into FS-PRO's file system and database.
13. Import insurance products into FS-PRO.
14. Update FS-PRO's product deployment list.
15. Build all of the product artifacts.
16. Publish and deploy the products from FS-PRO to FS-QUO.
17. Sync the process and product flowstore in FS-QUO.
18. Update the FS-QUO database with insurance content.

Procedure

1. Log onto the HANA server as the HANA tenant OS user.
2. Go to `<si_home>`.
3. Edit the file `<si_home>/properties/environment.properties` and change the parameter `APP_TYPE` to `runtime`.
4. Ensure that the file `<si_home>/silent_installer.sh` is executable.

   If it is not, change it by executing `chmod 744 silent_installer.sh`
5. Save your changes.
6. Prepare your system to run the silent installer.

   The silent installer runs as a shell script process. It can take anywhere from 30 minutes to 2.5+ hours to complete. One method to ensure the process is not interrupted due to session disconnects is to use the utility `screen`. The use of `screen` will also allow you to close your current session and return to it later. To prevent SSH session timeouts, it is recommended that you use a keep-alive option in your SSH application (e.g. putty -> Connection > Sending of null packets to keep session active) or include the SSH option `ServerAliveInterval` when you connect. It is recommended that you set the *Seconds between keepalives* value to 300.
7. Run the shell script file `<si_home>/silent_installer.sh`.

   As the shell script executes, you will be asked to enter and confirm passwords as required.

   You will have three opportunities to correctly enter and confirm each password. After the third failed attempt, the installation process will stop and you will have to start again from the beginning.

   > → Tip
   >
   > While the script is running, you will not see any output as it is being redirected to a log file. You can open another session and tail the log to watch the process: `tail -f <si_home>/silent_installer_<date_time>.log`
8. When the command prompt returns, the script has finished executing. You must review the log, `<si_home>/logs_archive/silent_installer_<date_time>.log`, to determine if the installation was successful. If the installation is successful, you will see a message similar to this one at the end of the log: `BUILD SUCCESSFUL Total time: 130 minutes 35 seconds`

   > ⓘ Note
   >
   > The amount of time it takes will vary from system to system. The installation of a coverage-based FS-QUO system in the SAP lab took ~130 minutes to complete. You can expect your installation to take about the same amount of time with a range of +/- 30 minutes. Risk-based systems will generally take less time.

   In the event of a failure, all of the logs can be found in `<si_home>/logs_archive`. The logs in the sub folders have been zipped up into the file `logs.zip`. If you need to contact support, you will need to provide the `logs.zip` and `silent_installer_<date_time>.log` files.

   If you are able to determine the cause of the failure (for example, a typo in the `environment.properties` file such as an invalid org name) it is safe to rerun the silent installer without restoring the database backup. If you are unsure if the installation can be restarted, you should contact support.

Next Steps

After completing the installation, do not delete the directory and contents of the silent installer. These files may be required for applying future SAP Notes. Keep the silent installer safely stored somewhere safe.

Related Information

Installer Requirements [page 9]
Gathering the Information for the Properties File Settings [page 15]
Properties File Settings Checklist [page 15]

7 FS-QUO Front End and Back End Application Integration

7.1 Trusting the SAPUI5 Content Delivery Network

This procedure adds the SAPUI5 official Content Delivery Network (CDN) site's CA certificate to the XSA Runtime's trusted certificates list.

Prerequisites

You have the root certificate of the certificate authority which signs the official CDN site's certificate in base64 encoded X.509 format.

Context

The main entry point of FS-QUO is the approuter component of the main application. It redirects client requests to the FS-QUO application as well as various resources. One of these resources is the SAPUI5 libraries which is provided by SAPUI5 official CDN and therefore resides outside of the SAP HANA XS Advanced runtime server. The approuter only redirects outbound requests to trusted resources. For the approuter to successfully retrieve SAPUI5 libraries from the official CDN, you need to add the official CDN site's CA certificates to the SAP HANA XS Advanced Runtime's trusted certificates. Ensure that you add all of the certificates that are in the certification path.

For more information, see:

- Variant for Bootstrapping from Content Delivery Network
- Maintaining Trust Certificates in XS Advanced (using xs command-line interface)

Procedure

1. Go to https://sapui5.hana.ondemand.com/ and download the site certificate.

   > ⚠ Caution
   >
   > Ensure that you have downloaded and saved all of the necessary site certificates (including all parent certificates for the CDN certificate).

2. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

> → Tip
>
> You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the xsa-admin entry.

3. When prompted, log in as `<admin_user>`.
4. Select the *Trusted Certificates* tile from the main page.
5. Choose *Add*.
   The *Add Trusted Certificate* dialog box opens.
6. Enter the following details:
   a. Enter the name for the certificate in the *Alias* field.
   b. Choose *Certificate*.
   c. Browse to the folder containing the certificate and select it.
   d. Select *HTTP* as the *Usage*.
   e. Choose *Add*.

   > ⚠ Caution
   >
   > Ensure that you add **all** of the certificates to XSA.
7. In a command prompt window, run the following commands to allow the FS-QUO approuter component to pick up the new trusted certificate:

```
xs restage FS-QUO-approuter
xs restart FS-QUO-approuter
```

7.2 Trusting the ABAP Server on the SAP HANA XS Advanced Runtime

This procedure adds the ABAP server's certificate to the SAP HANA XS Advanced Runtime's trusted certificates list.

Prerequisites

You have the root certificate of the certificate authority which signs your ABAP front-end server's certificate in base64 encoded X.509 format.

Context

The main entry point of FS-QUO is the approuter component of the main application. It redirects client requests to the FS-QUO application as well as various resources. One of these resources is the FS-QUO front-

end FS-IPW components which resides in the ABAP front-end server. The approuter only redirects outbound requests to trusted resources. For the approuter to successfully redirect the client requests to the ABAP front-end server, you need to add the ABAP server's CA certificate to the SAP HANA XS Advanced Runtime's trusted certificates.

For more information, see:

- Maintaining Trust Certificates in XS Advanced
- Manage Certificates

Procedure

1. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

   > → Tip
   >
   > You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the xsa-admin entry.

2. When prompted, log in as `<admin_user>`.
3. In the main page, select the *Trusted Certificates* tile.
4. Choose *Add*.
   The *Add Trusted Certificate* dialog box opens.
5. Enter the following details:
   a. Enter the name for the certificate authority's root certificate which signs your ABAP front end server's certificate in the *Allias* field.
   b. Choose *Certificate*.
   c. Browse to the folder containing the certificate and select it.
   d. Select *HTTP* as the *Usage*.
   e. Choose *Add*.
6. In a command prompt window, run the following commands to allow the FS-QUO approuter component to pick up the new trusted certificate:

   ```
   xs restage FS-QUO-approuter
   xs restart FS-QUO-approuter
   ```

7.3 Overwriting the HTTP Header Host Using the ABAP Server's Internet Communication Manager

This procedure rewrites the Host header of the HTTP request coming from FS-QUO's JAVA back-end application on the SAP HANA XS Advanced server to Fiori front end applications on ABAP front-end server.

Context

When the approuter component of FS-QUO's main application forwards HTTP requests to the FS-IPW applications to the ABAP front-end server, the approuter moves the original value of the HTTP header `Host`, which is the SAP HANA XS Advanced server's host name, to the HTTP header `x-forwarded-host`. It also assigns the ABAP front end server's host name to the HTTP header `Host`. To allow the FS-IPW applications to properly locate back-end OData services on the SAP HANA XS Advanced server, you need to revert the HTTP Header `Host`'s value to the SAP HANA XS Advanced server's host name. The procedure below is an example of how to overwrite the HTTP Header by setting up an action file in the ABAP server's Internet Communication Manager (ICM).

For more information, see:

- Administration of the ICM - SAP NetWeaver
- Modification of HTTP Requests

Procedure

1. In the ABAP server's ICM profile, add a new HTTP modification parameter to specify a path to an action file. The action file is a plain text file.

   The following example shows the HTTP modification parameter in the profile:

   ```
   icm/HTTP/mod_0 =
   PREFIX=/,FILE=<absolute_path_action_file>
   ```

2. Create a plain text file in the location shown in the previous step. Create a HTTP modification rule so that when HTTP request's header `Host` is the ABAP server's host and `x-forwarded-host` is the SAP HANA XS Advanced server's host, overwrite the header `Host` with the `x-forwarded-host`'s value.

   The following example shows the HTTP modification rule in the action file:

   ```
   if %{HTTP_HOST} regimatch <abap_fqdn_regex> [AND]
   if %{HEADER:x-forwarded-host} regimatch <xsa_fqdn_regex>
       SetHeader Host %{HEADER:x-forwarded-host}
   ```

3. Restart the ABAP system to allow the ICM profile change to take effect.

8 SAML 2.0 Configuration

To allow end users to log in and have access to both FS-QUO's Fiori front-end and Java back-end components, SAML 2.0 authentication should be enabled on the SAP HANA XSA Runtime and the ABAP front-end server. The SAP HANA XSA Runtime and the ABAP front-end server must be configured as SAML service providers and bridged to a SAML 2.0 identity provider.

On top of bridging the SAP HANA XSA Runtime and the ABAP front-end server to a SAML 2.0 identity provider, you need to apply the configurations in this chapter to complete Single Sign-On and Single Logout setup for FS-QUO.

> ⓘ Note
>
> Any SAML 2.0 identity provider can be used. SAP Cloud Platform Identity Authentication Service (SCP IAS) is used for demonstration purpose in this guide.

Prerequisites

The SAP HANA XSA Runtime where FS-QUO resides must be configured as a SAML service provider and bridged to the SAP Cloud Platform Identity Authentication Service (SCP IAS) tenant. You can log in to the SAP HANA XSA Runtime as a user authenticated by the SAP IAS tenant.

The ABAP front-end server where FS-IPW resides must be configured as a SAML service provider and bridged to the SCP IAS tenant. You can login to the ABAP front-end server as a user authenticated by the SAP IAS tenant.

For more information, see Configure SAML 2.0 Service Provider.

SAML Assertion Attributes

The following Assert Attributes are required.

User Attribute	Assertion Attribute
Groups	Groups
First Name	given_name
Last Name	family_name
Email address	email

> → Remember
>
> Assertion attribute names are case-sensitive.

For more information, see Configure the User Attributes Sent to the Application.

Subject Name Identifier

The Subject Name identifier in the SAML Assertion must be set to the user's *Login Name*.

Fore more information, see Configure the Subject Name Identifier Sent to the Application.

Default Name ID Format

The Default Name ID Format should be set to `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.

For more information, see (Optional) Configure the Default Name ID Format Sent to the Application.

Related Information

- Maintaining SAML Providers
- Configuring AS ABAP as a Service Provider

8.1 Removing the SLO Endpoint of the SAP HANA XS Advanced Runtime from the Identity Provider

You need to remove the default Single Logout endpoint of the SAP HANA XS Advanced Runtime from the SCP IAS tenant.

Procedure

1. Login to the Administrative Console of SCP IAS tenant as a tenant administrator.
2. Navigate to *Application & Resources* > *Applications*.
3. From the list of applications, select the item that represents the SAP HANA XS Advanced Runtime which hosts FS-QUO application.
4. Select *SAML 2.0 Configuration* tab from the right pane.
5. Navigate to *Single Logout Endpoint* and delete the endpoint URLs.
6. Save your changes.

8.2 Removing the SLO endpoint of the Identity Provider from XSA

You need to remove the default Single Logout endpoint of the SAP HANA XS Advanced Runtime from the SCP IAS tenant.

Procedure

1. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

   > → Tip
   >
   > You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the `xsa-admin` entry.

2. When prompted, log in as `<admin_user>`.
3. Choose the *SAML Identity Provider Configuration* tile.
4. Select the SCP IAS tenant from the *SAML Identity Provider List*.
5. Remove all the SingleLogoutService nodes from the *Metadata* field.
6. Save your changes.

8.3 Implementing a Logout Page

A custom logout page is required to log out of the back-end server during the Fiori Launchpad logout process.

For a general discussion of this issue, see Ensuring Complete Logout from Integrated Systems..

The following link provides a sample custom logout page invoking the logout URL from FS-QUO: Creating a Custom Logout Page

Note that this only works when the logout page is setup in Web Dispatcher, unless the full FS-QUO Java back-end URL is provided.

The high level-steps in this process are as follows:

1. Create a custom logout HTML page and upload it to the ABAP front-end server as a BSP application.
2. Configure an external alias for the ICF node `/sap/public/bc/icf/logoff` to redirect the logout to the custom logout page.

8.3.1 Configuration Steps for the Logout Page

Before you can create a custom logout page, you need to configure some settings for Single Sign-On (SSO).

Procedure

1. Log in as the Admin user to the Administrative Console for the SAP Cloud Platform IAS Tenant.
2. Navigate to the *Applications & Resources* > *Applications*.
3. Select the application name (your XSA server).
4. Select *SAML 2.0 Configuration*.
5. Navigate to *Single Logout Endpoint* and delete the endpoint URL.
6. Save your changes.

8.3.2 Creating a Custom Logout HTML Page and Upload It to the ABAP Front-end Server as a BSP Application

You need to create a custom logout HTML page and upload it to the ABAP front-end server as a BSP application.

Procedure

1. Add the logout rules to the SAP Web Dispatcher.

   Ensure the logout URLs to be used are routed to the correct system.

   ```
   wdisp/system_<rule_number> = SID=<gateway_system_ID>,
   EXTSRV=https://<external_system_server_host><external_system_server_port>,
   SRCSRV=*:<Fiori_Launchpad_port>,
   SRCURL=<data_services_roots
   example: /sap/opu/odata/,separated by ;>
   ```

   Or

   ```
   wdisp/system_<rule_number> =
   SID=<gateway_system_ID>,MSHOST=<message_server_host>,
   MSPORT=<message_server_port>,SRCSRV
   =*:<Fiori_Launchpad_port>,SRCURL=<data_services_roots
   example: /sap/opu/odata/,separated by ;>
   ```

2. Create the custom logout page. The URL of this logout page must use SAP Web Dispatcher as its origin.
   - For each system from which you want to log out, add a request Logout call with the proper logout URL.
     For a J2EE server, issue a GET request to logout servlet, for example `/csiroot/logout`.
     For ABAP systems, call the `/public/bc/icf/logoff` service on each server.

- Redirect to the actual logout page:
  `document.location = <custom logout page>`
  This redirects to the launchpad login page, instead of the front-end server's default `/public/bc/icf/logoff` node.
  The following is an example of a logout page:

```
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html;charset=UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta http-equiv="Cache-Control" content="no-cache, no-store, must-
revalidate" />
    <meta http-equiv="Pragma" content="no-cache" />
    <meta http-equiv="Expires" content="0" />
    <script src="<flp_url>/resources/sap/ui/thirdparty/jquery/
jquery-1.11.1.js"></script>
</head>
<body>
    <em id="message">Logout is in progress...</em>
    <script>
    (function () {
        "use strict";
        /*global document, jQuery*/
        var iPending = 0;
        function requestLogout(sUrl) {
            document.location = sUrl;
        }
        // FS-QUO logout URL (accessible only via Web Dispatcher unless
using
        // full URL to the Java back-end server)
        requestLogout("<quo_runtime_app_url>/do/logout");
    }());
    </script>
</body>
</html>
```

3. Upload the custom logout page as a UI5 BSP Node, using Transaction Code `SE38` and report `/UI5/UI5_REPOSITORY_LOAD`.

   > **Note**
   > - The custom logout page can be accessed as a BSP node.
   > - The custom logout page should be publically accessible, but the UI5 BSP node requires user authorization. A public node reference to the custom logout page must be created.

4. To create a custom logout page node, perform the following steps:
   a. Run transaction `SICF`.
   b. Select the Public Service Node's namespace `/sap/public/bsp/sap`.
   c. Open the Create Service Wizard icon.
   d. Accept the *Warning and Hints* messages.
   e. Select the *Internal Alias* radio button.
   f. Enter the *Name* and *Description* for the public custom logout page node.
   g. Choose the newly-created UI5 BSP Node and choose *Continue*.
5. Finally, redirect /sap/public/bc/icf/logoff to the custom logout page as follows:
   a. Run Transaction Code `SCIF`.
   b. Use the public custom logout page node's page as the `/sap/public/bc/icf/logoff` node's logout page.

8.3.3 Configuring an External Alias for the ICF Node to Redirect Logout to Custom Logout Page

You need to configure an external alias for the ICF node to redirect logout to custom logout page.

Procedure

1. Login to the ABAP front-end system and execute the `SICF` transaction.
2. Go to the `/sap/public/bc/icf/logoff` node.
3. Once the service loads, go to *Error Pages* > *Logoff Page* > *Redirect to URL*.
4. Choose the pencil icon and enter the redirection URL as **`/sap/bc/ui5_ui5/ui2/ushell/shells/abap/Fiorilaunchpad.html`**.
5. Save your changes.
   a. If the wizard prompts you for credentials, the password entry needs to be made here to complete the implementation.
   b. Go to the *Logon Data* tab and clear the *User* and *Password* fields and choose *Save* again.

8.4 Creating a Sample Underwriter User for Single Sign-On

You can create a sample underwriter user and assign the necessary role collections to the user.

Prerequisites

The SAP HANA XS Advanced Runtime where FS-QUO resides must be configured as SAML service providers and bridged to the SAP Cloud Platform Identity Authentication Service (SCP IAS) tenant. You can log in to the SAP HANA XS Advanced runtime as a user authenticated by the SAP IAS tenant.

The ABAP front-end server where FS-IPW resides must be configured as SAML service providers and bridged to the SCP IAS tenant. You can login to the ABAP front-end server as a user authenticated by the SAP IAS tenant.

A user has been created on the ABAP front-end server and assigned to an ABAP role. This user can be manually created beforehand or automatically created during the SAML 2.0 login process.

A user has been created in the SCP IAS tenant with the *Login Name* `<uw_user>` and assigned to the `<uw_user_group>` user group. For detailed instructions, refer to Create a New User and Create a New User Group in the *SAP Cloud Platform Identity Authentication Service Guide*.

> → Tip
>
> You can define `<uw_user>` the same as the user on the ABAP front-end server, so that the *Login Name* is the federated identity for SAML 2.0 authentication.

For more information, see:

- Maintaining SAML Providers
- Configuring AS ABAP as a Service Provider
- Identity Federation in AS ABAP

Context

The landscape with an FS-QUO Runtime on SAP HANA XS Advanced and the insurance apps on an ABAP front-end server hosting a Fiori Launchpad requires Single Sign-On using SAML 2.0 authentication. The SAML identity provider recommended for this solution is SCP IAS. End users of FS-QUO, such as agents and underwriters, must be managed in the SAML identity provider and SAP HANA XS Advanced and assigned to the appropriate roles.

For more information, see:

- Security Guide
- SAP Cloud Platform Identity Authentication
- User Administration and Authentication in SAP HANA XS Advanced

Procedure

1. In a web browser, go to the URL of the XS Advanced Administration and Monitoring tools.

   > → Tip
   >
   > You can find the URL by going to `<xsa_api_url>/v2/info` in a web browser and obtaining the value/URL of the `xsa-admin` entry.

2. When prompted, log in as `<admin_user>`.
3. In the main page, select the *Application Role Builder*.
4. Select *Role Collection* in the left menu.
5. Select the + icon at the bottom of the role collections list.
   A pop-up dialog opens.
6. Enter the name `<quo_runtime_uw_rc>` and a description, then select *Create*.

   For example, enter **`QUO Runtime Underwriter Role Collection`** as the description.
7. Choose the newly created role collection in the role collections list.
8. Select the *Roles* tab in the editor pane.
9. Select *+ Add Application Role*.
   A pop-up dialog opens.
10. In the resulting dialog, perform the following actions and select *OK*:
    a. Choose `<quo_runtime_uaa_app_name><uaa_app_name_suffix>` from the *Application Name* dropdown list, where `<uaa_app_name_suffix>` is a generated suffix added by XSUAA based on the plan used for the service instance.

b. Choose *UW_User_RT* from the *Template Name* dropdown list.

   This role provides access to underwriting apps.

c. Choose *UW_User_RT* from the *Application Role* dropdown list.

   This is the same as the template name.

11. Save your changes.
12. Return to the main page of XS Advanced Administration and Monitoring tools.
13. Choose the *SAML Identity Provider Configuration* tile.
14. Choose the *SAP IAS* tenant on the left pane.
15. Click *Role Collections* tab on the right pane.
16. Click *+ Add* to add a new row to the bottom of the Assertion Based Role Collections table.
    a. Enter `<quo_runtime_uw_rc>` in the *Role Collection* field.
    b. Enter `<uw_user_group>` in the *Value* field.
    c. Save your changes.
17. Return to the main page of XS Advanced Administration and Monitoring tools .
18. Select *User Management* on the main page.
19. Select *New*.
    A pop-up dialog opens.
20. Create a user `<uw_user>` and select *Create*.
    The pop-up dialog closes and the user is created.
21. Select `<uw_user>` in the SAP HANA XS Advanced business users list.
22. Choose the *Role Collections* tab on the user details page.
23. Select *Add*.
24. Select the checkbox next to `<quo_runtime_uw_rc>` and select *OK*.
25. Save your changes.

Results

You have created a sample underwriter user and assigned appropriate roles for Single Sign-On access to the insurance apps.

8.5 Validating Single Sign-On and Single Logout

After creating a sample underwriter user, you can validate Single Sign-on access to insurance apps on the ABAP front-end server and the FS-QUO application on SAP HANA XS Advanced.

Prerequisites

You have created a sample underwriter user.

Procedure

1. Launch a web browser and go to `<quo_runtime_app_url>/sap/bc/ui2/flp`.
2. When prompted with the SAP HANA XS Advanced login page, select the link of SCP IAS tenant below the login form.
3. Log in to the Fiori Launchpad as <uw_user>.
   The insurance app tiles appear in the Fiori Launchpad.
4. Select the *Create Insurance Quote* tile if coverage-based products were deployed or the *Create New Business* tile if risk-based products were deployed.
5. Verify that the app launched successfully.

   Failure to successfully access these applications is an indication of an issue with either the user setup or the application deployment.
6. Log out from the Fiori Launchpad.

Results

You have verified that the both the front-end server and back-end server of the FS-QUO application are successfully installed and SAML 2.0 Single-Sign On between the components is correctly configured.

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