Security Guide | PUBLIC
2019-09-20

Security Guide

SAP Quotation and Underwriting for Insurance 1.1

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Before You Start

This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

Fundamental Security Guides

FS-QUO is be deployed in an SAP HANA XS Advanced environment. For more detailed information on security issues relevant to such deployments, see the following documentation: SAP HANA Security Guide

Consult the Help Portal to view Security Guides and other documentaiton for SAP products and applications.

Configuration

You can find the configuration steps for implementing security for FS-QUO in the *SAP Quotation and Underwriting for Insurance Administration Guide*.

Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

Content	Quick Link
SAP Help Portal	https://help.sap.com/viewer/index
Security	http://scn.sap.com/community/security
Related SAP Notes	https://support.sap.com/en/my-support/knowledge-base.html
Released platforms	https://support.sap.com/en/release-upgrade-maintenance.html#section_1969201630
SAP Solution Manager	https://support.sap.com/en/solution-manager.html

2 Introduction

> ⚠ Caution
>
> This guide doesn't replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document isn't included as part of the *Installation Guides*, *Configuration Guides*, *Technical Operation Manuals*, or *Upgrade Guides*. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

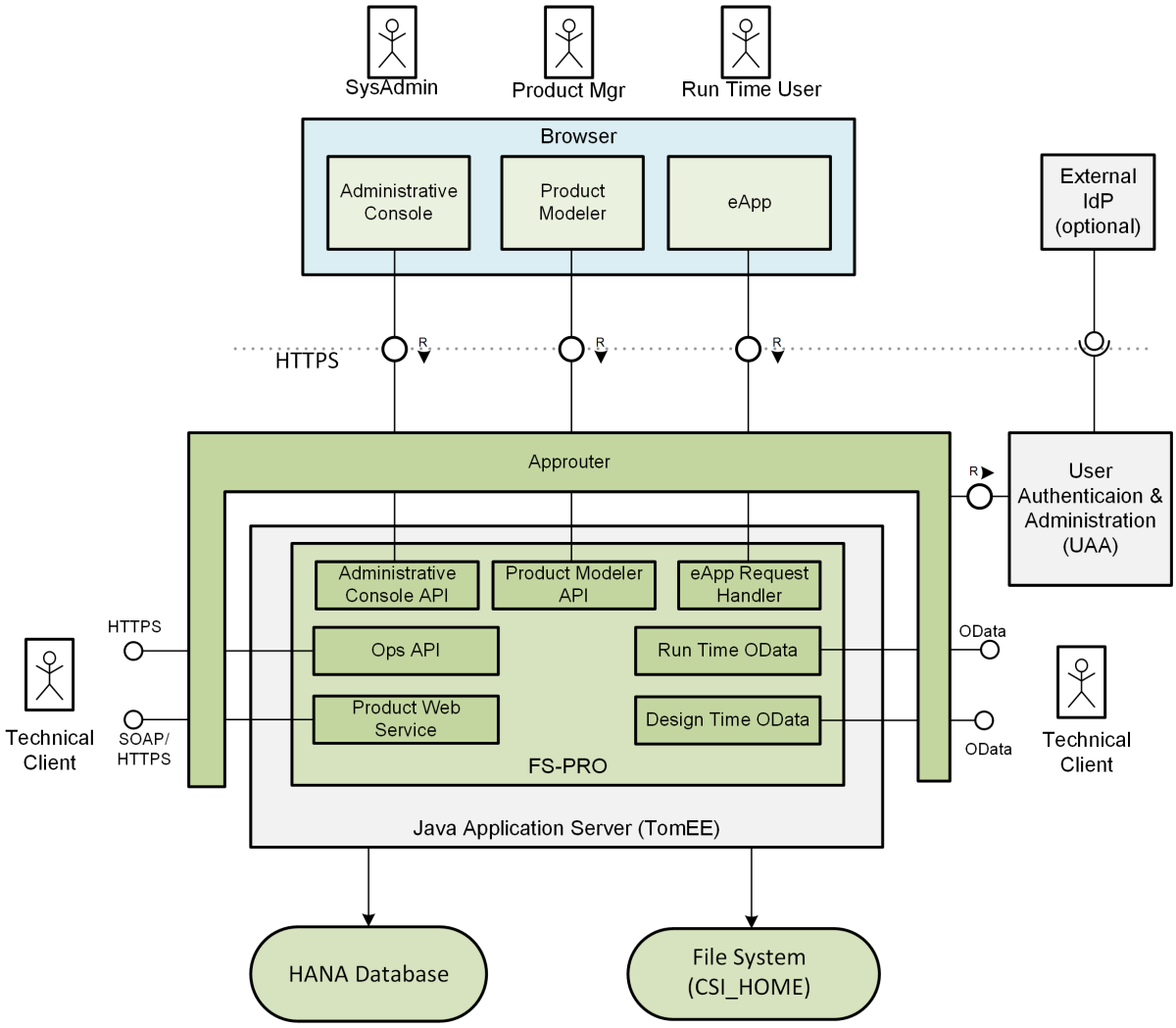
With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system shouldn't result in loss of information or processing time. These demands on security apply likewise to FS-QUO. Data protection is important for FS-QUO due to the sensitive nature of the data that is collected and stored to create insurance quotes or issue insurance policies. Legal regulations also require you to have certain security measures in place. To assist you in securing FS-QUO, we provide this *Security Guide*.

About this Document

The *Security Guide* provides an overview of the security-relevant information that applies to the FS-QUO.

3 SAP HANA XS Advanced Security LandscapeWeb

3.1 Design Time Server (FS-PRO)



Web Applications: Administrative Console, Product Modeler and eApp

The Administrative Console and the Product Modeler are web applications. Administrative Console is intended for system administrators, with a restricted set of users granted authorization to access it. Product Modeler

is an application for product managers and product designers to configure new and maintain existing product definitions. Typically, a small set of power users is granted authorization to access Product Modeler.

Service interfaces: Ops API, Product Web Services, Runtime OData and Design Time OData

These service APIs are intended for use by other applications via technical accounts. The Ops API is used by external process automation tools to manage FS-PRO server configuration. Due to the extensive access to server configuration, technical accounts with authorization to use this API should be carefully restricted. The Design Time OData service has similar access to the Product Modeler application. Product Web Services and Runtime OData both have similar access to eApp applications.

FS-PRO Server

FS-PRO is hosted on Apache TomEE. Approuter is hosted on `node.js`.

For information regarding securing application servers, see the Security for SAP HANA Extended Application Services, Advanced Model topic in the *SAP HANA Security Guide*.

HANA Database

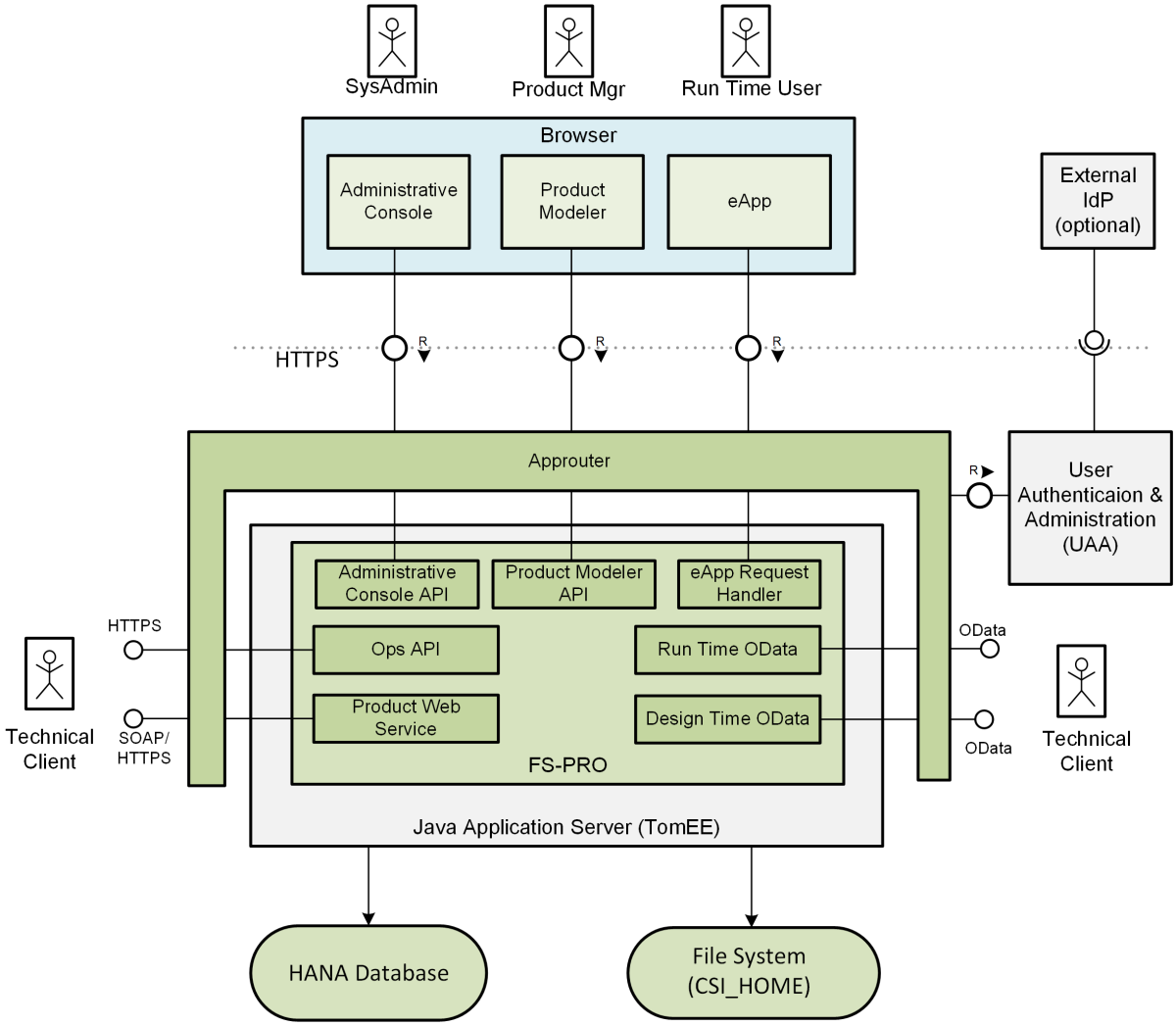
FS-PRO servers use SAP HANA as a database for Design Time product structure and design data.

Information on securing the SAP HANA database is covered in platform documentation.

CSI_HOME File System

FS-PRO servers use a shared file system to store files such as log files, product configuration JAR files, and application configuration files. In SAP HANA XS Advanced, the shared file system is a backing service called `fs-storage`. In SAP HANA XS Advanced, `fs-storage` is implemented as a shared folder on the SAP HANA database server. Access to `fs-storage` is handled by the platform, so secure access to the underling file system is ensured by the platform.

3.2 Runtime Server (FS-QUO)



Web Applications: Fiori Applications,Administrative Console

FS-QUO has several Fiori applications, which are hosted on an ABAP front-end server and communicate with the back-end FS-QUO server over HTTPS. These applications are the primary web applications accessed by regular users.

Administrative Console is intended for system administrators, with a restricted set of users granted authorization to access it.

Service interfaces: Ops API, Product Web Services, Runtime OData, FS-IPW OData and UW OData

These service APIs are intended for use by other applications via technical accounts. The Ops API is used by external process automation tools to manage FS-QUO server configuration. Due to the extensive access to server configuration, technical accounts with authorization to use this API should be carefully restricted. Product Web Services and Application-to-Application (A2A) interfaces are intended to be accessed by technical account with basic authentication. FS-IPW and UW OData interfaces are used by Fiori applications, so regular users are authorized to access these APIs.

FS-QUO Server

On SAP HANA XSA, FS-QUO is hosted on Apache TomEE. Approuter is hosted on `node.js`.

For information regarding securing application servers, see the Security for SAP HANA Extended Application Services, Advanced Model topic in the *SAP HANA Security Guide*.

HANA Database

FS-QUO servers use SAP HANA as a database for Runtime data.

Information on securing the SAP HANA database is covered in platform documentation.

CSI_HOME File System

FS-QUO servers use a shared file system to store files such as log files, product configuration JAR files, and application configuration files. The shared file system is a backing service called `fs-storage`. In SAP HANA XS Advanced, `fs-storage` is implemented as a shared folder on the SAP HANA database server.

Access to `fs-storage` is handled by the platform, so secure access to the underling file system is ensured by the platform.

4 Authentication

4.1 Supported Protocols

Web Clients

The FS-PRO and FS-QUO web clients follow the standard Cloud Foundry security architecture on the SAP HANA XSA platform. HTTP requests from the browser to the FS-QUO server are routed through an intermediary called the Approuter. The Approuter, in turn, redirects any requests without a valid session token to the platform's User Authentication and Administration (UAA) service, which acts as an OAuth 2.0 Authorization Server. UAA in turn can optionally be configured to route login requests to an external identity provider (IdP). The selection of IdP is configured in the platform. On SAP HANA XSA, the IdP is by default SAP HANA, but can be configured to use an external IdP such as SAP Cloud Platform Identiaty Authentication Service (IAS), or Microsoft Active Directory.

As specified by Cloud Foundry security architecture, in addition to authenticating the user, UAA also determines the user's roles and other attributes, including all permissions granted via those roles, and includes that information in an OAuth assertion token in the form of a JSON Web Token (JWT). The JWT is returned in the HTTPS response to the Approuter.

The Approuter then forwards the original request along with the JWT in the HTTPS request header to the back-end server.

The back-end server validates the JWT, parses it, extracts the user ID and permissions, and creates the user session on the server.

The JWT is only attached to HTTPS requests between the Approuter and the application server. It is never exposed to the web client. The Approuter maintains a table of sessions and their associated JWT tokens.

Service APIs (Ops, Design Time OData, Runtime OData)

HTTPS requests for services (OData, Ops API) are usually be routed through the Approuter, and authentication is handled by XSUAA, typically using basic authentication. The full set of available authentication methods depends on the configured IdP. Basic authentication (credentials in the form of userID and password encoded in Base64) is supported on SAP HANA XSA.

Alternatively, an external caller can use OAuth 2.0 to request a JWT token directly from the UAA server. In this case, the HTTPS requests should be sent along with the JWT directly to the Runtime server, bypassing the Approuter.

Product Web Services SOAP requests (URL: `csiroot/psruntime`) are allowed to pass through the Approuter unauthenticated, because for these URLs, FS-QUO enforces `WS-Security UsernameToken` authentication: user ID and password must be specified in the SOAP header in the HTTP request body.

- The username supplied in the `UsernameToken` section must be managed via the *User* > *Edit users* menu option in the Runtime Administrative Console. The password for the username account is managed there as well.

For more information on managing authentication on SAP HANA XSA, see the User Authentication topic in the *SAP HANA Security Guide*.

Web Client APIs (FS-IPW and UW OData)

HTTPS requests for web client APIs (FS-IPW and UW OData) are routed through the Approuter, and authentication is handled by XSUAA, typically using form-based authentication. The full set of available authentication methods depends on the configured IdP.

For more information on managing authentication on SAP HANA XSA, see the User Authentication topic in the *SAP HANA Security Guide*.

5 Authorization

For information on managing user authorizations in SAP HANA XSA, see the Authorization Management Tools topic in the *SAP HANA Security Guide*.

5.1 Resource URL Authorization

Authorization for users to access specific URLs which are related to specific functionalities is managed by the platform authorization tools.

FS-QUO and FS-PRO are shipped with a set of standard Role Templates and associated scopes, described in the table below. These Role Templates can be assigned to Role Collections, and Role Collections assigned to Users and Groups, using the platform authorization management tools.

Authorizations are checked on every HTTP request. The table lists the URL patterns that are authorized by each Role Template.

After authorization checks on the HTTP request URL, additional authorization checks on specific actions are performed in the business service layer inside the application server.

> **Note**
>
> If you create your own role collections, remember to add it to the user. You will also need to assign the appropriate authorizations for the FS-IPW apps. For example, you will need to assign UW_User_RC to a user in order for them view submissions in the Underwriting Worklist. If you will be creating Underwriting Groups, then the groups created in the UW groups component will need a role collection defined.

Insufficient scopes for a user will result in their browser displaying a `403 Forbidden` error.

> **Note**
>
> URL patterns that begin with `/A2A/` are intended for application-to-application usage, and have basic authentication. The URL patterns `/csiroot/productCatalog/` and `/csiroot/assembledComponentValueRow/` are also intended for A2A use and have basic authentication. All other URL patterns have UAA authentication, which includes OAuth, SAML, X.509 and form-based authentication.

> **Note**
>
> All authenticated users are authorized to access the URL pattern `/sap/`, which is the URL for the Fiori Launch pad. ABAP authorization checks are then applied to determine which tiles are visible to the user.

5.1.1 FS-QUO and FS-IPW OData API Role Templates

Role Template Name: UW_User_RT

Scope & Permissions Granted	AccessQuo AccessEApp AccessUW uwSubmissionListQuery uwCaseMassReassign uwSimulate UWFullAccess AccessCustomServlet assignSubmission
Typical Usage	Access to apps
Applicable Instance	Runtime

URL Patterns	`/csiroot/eapp-runtime/`
	`/A2A/csiroot/ipw/quo/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/quoteSummary/odata.svc/`
	`/A2A/csiroot/ipw/uw/odata.svc/`
	`/A2A/csiroot/ipw/eApp/odata.svc/`
	`/csiroot/ipw/`

Role Template Name: DPP_Officer_RT

Scope & Permissions Granted	ManageDataPrivacy AccessEApp AccessQuo AccessUW AccessCustomServlet
Typical Usage	Access to DPP-related apps.
Applicable Instance	Runtime

URL Patterns	`/csiroot/dpp/`
	`/csiroot/eapp-runtime/`
	`/A2A/csiroot/ipw/quo/odata.svc/`

	`/A2A/csiroot/ipw/quo/web/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/quoteSummary/odata.svc/`
	`/A2A/csiroot/ipw/uw/odata.svc/`
	`/A2A/csiroot/ipw/eApp/odata.svc/`
	`/csiroot/ipw/`

Role Template Name: QUO_User_RT

Scope & Permissions Granted	AccessQuo AccessEApp AccessCustomServlet
Typical Usage	Access to apps, but no underwriting access.
Applicable Instance	Runtime

URL Patterns	`/csiroot/eapp-runtime/`
	`/A2A/csiroot/ipw/quo/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/quoteSummary/odata.svc/`
	`/A2A/csiroot/ipw/uw/odata.svc/`
	`/A2A/csiroot/ipw/eApp/odata.svc/`
	`/csiroot/ipw/`

5.1.2 Administration Role Templates

Role Template Name: Administrator_RT

Scope & Permissions Granted	ManageSystemConfigure	Manage system configuration
	ManageWebService	Manage Product Web Services (deploy Product Web Services, upload product)
	ManageGeneratedRuntimeContent	Manage generated Runtime content (synchronize flowstores, load cache)
	ADMINISTRATOR	Full access to all Administrative Console functionality
Typical Usage	Application super administrators	

Applicable Instance	Design Time Runtime

URL Patterns	`/csiroot/admin*`
	`/csiroot/psruntime/ws/`
	`/csiroot/ii/pc/jsp/enu/componentchooser/`

Role Template Name: Content_Admin_RT

Scope & Permissions Granted	ManageGeneratedRuntimeContent	Synchronized the deployed the product content to the Runtime application
Typical Usage	Product content administrators	
Applicable Instance	Design Time Runtime	
URL Patterns	`/csiroot/admin*` `/csiroot/ii/pc/jsp/enu/componentchooser/`	

Role Template Name: Webservice_Admin_RT

Scope & Permissions Granted	ManageWebService	Manage Product Web Services, upload and deploy product JAR files to SOAP web services
Typical Usage	Product Web Services administrators	
Applicable Instance	Runtime	
URL Patterns	`/csiroot/admin*` `/csiroot/psruntime/ws/`	

Role Template Name: System_Admin_RT

Scope & Permissions Granted	ManageSystemConfigure	Manage FS-QUO Design Time or Runtime system configuration
Typical Usage	System configuration administrators	
Applicable Instance	Design Time Runtime	

URL Patterns	`/csiroot/admin*`

Role Template Name: Product_Deployer_RT

Scope & Permissions Granted	ViewProduct	View, but not modify, product content
	DeployProduct	Remotely deploy products from Design Time to Runtime applications
	PRODUCT_DEPLOY_ROLE	Can access product deploy to Runtime transaction
Typical Usage	Users that need permission to deploy products to the Runtime application	
Applicable Instance	Runtime	

URL Patterns	`/csiroot/ii/pc/*`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`
	`/csiroot/service/`
	`/csiroot/servlet/(.*)-service`
	`/csiroot/productCatalog/`
	`/csiroot/assembledComponentValueRow/`	

5.1.3 eApp Role Templates

Role Template Name: EApp_User_RT

Scope & Permissions Granted	AccessEApp	Access to the eApp runtime application
	AccessCustomServlet	Access to the custom servlet
Typical Usage	eApp users	
Applicable Instance	Runtime	

URL Patterns	`/A2A/csiroot/ipw/quo/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/odata.svc/`
	`/A2A/csiroot/ipw/quo/web/quoteSummary/odata.svc/`
	`/A2A/csiroot/ipw/uw/odata.svc/`
	`/A2A/csiroot/ipw/eApp/odata.svc/`
	`/csiroot/ipw/`	

5.1.4 Product Modeling Role Templates

Role Template Name: Product_Modeler_Admin_RT

Scope & Permissions Granted	ViewProduct	View, but not modify, product content
	ModifyProduct	Modify product content
	PublishProduct	Publish products
	DeployProduct	Deploy products
	ModifyProductTemplate	Modify product content (including product templates)
	SE_ADMIN_ROLE	Viewing objects, viewing and changing permissions other than Execute and reassigning the ownership of an object
Typical Usage	Product modelers	
Applicable Instance	Design Time	

URL Patterns	`/csiroot/ii/pc/`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`
	`/csiroot/servlet/(.*)-service`
	`/csiroot/service/`
	`/csiroot/productCatalog/`
	`/csiroot/assembledComponentValueRow/`	

Role Template Name: Product_Modeler_Author_RT

Scope & Permissions Granted	ViewProduct	View, but not modify, product content
	ModifyProduct	Modify product content (not including product templates)
	PublishProduct	Publish products
	DeployProduct	Deploy products
	SE_AUTHOR_ROLE	Creating and maintaining objects
Typical Usage	Product modelers managing only marketable products (not product templates)	

> **Note**
>
> Users with this permission can access the product repository but not the System repository

Applicable Instance	Design Time

URL Patterns	`/csiroot/ii/pc/`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`
	`/csiroot/servlet/(.*)-service`
	`/csiroot/service/`
	`/csiroot/productCatalog/`
	`/csiroot/assembledComponentValueRow/`

Role Template Name: Product_Viewer_RT

Scope & Permissions Granted	ViewProduct	View, but not modify, product content
Typical Usage	Read-only access to product configuration	
Applicable Instance	Design Time	

URL Patterns	`/csiroot/ii/pc/`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`
	`/csiroot/servlet/(.*)-service`
	`/csiroot/productCatalog/`
	`/csiroot/assembledComponentValueRow/`	

Role Template Name: Product_Custom_View_Creator_RT

Scope & Permissions Granted	ViewProduct	View, but not modify, product content
	CUSTOM_VIEW_CREATOR_ROLE	Customize view to generate product report
Typical Usage	Product managers	
Applicable Instance	Design Time	

URL Patterns	`/csiroot/ii/pc/`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`	

```
/csiroot/servlet/(.*)-service
/csiroot/productCatalog/
/csiroot/assembledComponentValueRow/
```

5.1.5 Operations APIs Role Templates

Role Template Name: Ops_User_RT

Scope & Permissions Granted	UpdateCSIHome	Update CSI_HOME files
	ImportObject	Import objects
	ExportObject	Export objects
	BuildObject	Build objects
	SyncObject	Synchronize objects
	PublishProduct	Publish products
	DeployProduct	Deploy products
	OPS_API_EXECUTION_ROLE	Access to all Operations APIs
	SE_ADMIN_ROLE	In FS-PRO, this role permits the following actions: • viewing objects • viewing and changing permissions other than Execute • re-assigning the ownership of an object
Typical Usage	Technical clients calling Ops API	
Applicable Instance	Design Time Runtime	

URL Patterns	`/csiroot/ii/pc/`
	`/csiroot/pa/pc/`
	`/csiroot/pcportal/`
	`/csiroot/servlet/(.*)-service`
	`/csiroot/service/`
	`/csiroot/productCatalog/`	

5.1.6 FS-PRO OData API Role Templates

These scopes are relevant for Technical clients calling FS-PRO OData services. All Role Templates in this section have permissions specified in `permissions_config.xml` in CSIHome.

Role Template Name: Product_OData_Deploy_RT

Scope & Permissions Granted	PRODUCT_ODATA_DEPLOY_ROLE	FS-PRO OData service: deploy activity-related transactions
Typical Usage	Managing scheduled activities Managing scheduled activities	
Applicable Instance	Design Time	
URL Patterns	`/csiroot/productCatalog/` `/csiroot/assembledComponentValueRow/`	

Role Template Name: Product_OData_ReadWrite_RT

Scope & Permissions Granted	PRODUCT_ODATA_READONLY_ROLE	FS-PRO OData service: read-only access to product or component data value rows
	PRODUCT_ODATA_READWRITE_ROLE	FS-PRO OData service: product or component data value row read and write actions
Typical Usage	Ability to create, update and delete data value rows Read-only access	
Applicable Instance	Design Time	
URL Patterns	`/csiroot/productCatalog/` `/csiroot/assembledComponentValueRow/`	

Role Template Name: Product_OData_ReadOnly_RT

Scope & Permissions Granted	PRODUCT_ODATA_READONLY_ROLE	FS-PRO OData service: Object-level read-only access rights for specified objects (individual products or components) that are defined

		in the Product Modeler. It includes `Read` permission. It will allow a user to read a data value row by conjunction with Product OData permissions. It should work in conjunction with other non-object level Product_OData_xxx permissions.
Typical Usage	Read-only access to product lists, data rows, and scheduled activities. Allows data searches	
Applicable Instance	Design Time	
URL Patterns	`/csiroot/productCatalog/` `/csiroot/assembledComponentValueRow/`	

Role Template Name: Product_OData_Object_FullAccess_RT

Scope & Permissions Granted	PRODUCT_OBJECT_LEVEL_FULLACCESS_ROLE	FS-PRO OData service: Object-level full access rights for specified objects (individual products or components) that are defined in the Product Modeler. It includes `Read`, `Write` and `Full Control` which has permission to grant rights to other FS-PRO roles through the Product modeler UI. It will allow a user to modify a data value row by conjunction with Product OData permissions. It should work in conjunction with other non-object level Product_OData_xxx permissions.
Typical Usage	Bypasses the object-level permission defined in the Product Modeler permission settings. Allows full permission (read, write, full) to the object (products, components, etc).	
Applicable Instance	Design Time	
URL Patterns	Not applicable	

Role Template Name: Product_OData_Object_WriteAccess_RT

Scope & Permissions Granted	PRODUCT_OBJECT_LEVEL_WRITEACCESS_ROLE	FS-PRO OData service: Object-level write and read access rights for specified objects (individual products or components) that are defined in the Product Modeler. It includes `Write` and `Read` permission. It will allow a user to modify a data value row by conjunction with Product OData permissions. It should work in conjunction with other non-object level Product_OData_xxx permissions.
Typical Usage	Bypasses the object-level permission defined in the Product Modeler permission settings. Allows write permission to objects (products, components, etc)	
Applicable Instance	Design Time	
URL Patterns	Not applicable	

Role Template Name: Product_Runtime_OData_RT

Scope & Permissions Granted	ExecuteProductRuntimeOData	FS-PRO Runtime OData service: execution
Typical Usage	Executes the Runtime OData services.	
Applicable Instance	Runtime	
URL Patterns	`/csiroot/productRuntime/` `/A2A/csiroot/productRuntime/`	

5.1.7 Product Web Services Runtime Role Templates

Role Template Name: Product_Web_Service_Runtime_RT

Scope & Permissions Granted	AccessProductWebServiceRuntime
Typical Usage	Access to Product Web Services in the Runtime application.

Applicable Instance	Runtime
URL Patterns	Not applicable

5.1.8 Data Visibility

User groups and role collections can also be used to control data visibility of submissions and tasks in the Quotation and Task worklists.

In the current implementation of data visibility, submissions and tasks are visible to their creator, as well as creator's peers. That is, anyone who is part of any of the user groups that the creator belongs to will see creator's submissions and tasks.

Example: Example user configuration:

There are two teams reporting to a manager. The agents within each team should see each other's submissions and tasks but should not see submissions and tasks of the other team. A manager of the two teams wants to see everyone's submissions. To achieve this data visibility the following user setup should be implemented:

	Role Collection	Users
Team A	TEAM_A_RC	Uw_A1, Uw_A2, Uw_A3,...
Team B	TEAM_B_RC	Uw_B1, Uw_B2, Uw_B3,...
Manager	TEAM_A_RC, TEAM_B_RC	Uw_Mgr1

> **Note**
>
> Be aware that if there is a Role Collection which is assigned to all users then everyone will see everyone's submissions and tasks.

For more information about the current implementation of data visibility, see Understanding the Data Visibility Framework and Data Visibility Configuration.

5.2 Object-Level Authorization

FS-PRO provides a facility to manage access to objects in Product Modeler.

The set of roles that can be used for object-level authorization, and the permissions assigned to each role, are managed in the following XML file: `<CSI_HOME>/ppms/app/pa/custom/integration/permission/permission_config.xml`

This file can be edited using the Design Time Administrative Console web application.

For more information on assigning object-level permissions to objects and roles, see Understanding Permissions and FS-PRO.

PermissionSets are collections of permissions, grouped together for convenience. PermissionSets are similar to the RoleTemplates used for URL-level authorizations, described in the previous section.

Permissions and PermissionSets are assigned to Roles in permission_config.xml. Administrators can assign Roles to users using the platform authorization management tools. Permissions can be assigned directly to users in in permission_config.xml.

Changes to `Permission.XML` take effect after a restart of the Design Time application.

Node Name		Description	Comments
<PermissionConfig>		Master node	Only one per XML file All other nodes must be child nodes of this
<AllUsersPermissions>		Default permissions for all users	Child of PermissionConfig
	<Permission>	Name of permission	Child of AllUsersPermission
<PermissionSets>		Parent node for permission set	Child of PermissionConfig
	<ParentPermission>	Name of permission set	Child of PermissionSets Only one per PermissionSets
	<ChildPermission>	Name of permission	Child of PermissionSets One or more per PermissionSets
<RolePermissions>		Parent node for role	Child of PermissionConfig
	<Role>	Name of role	Child of RolePermissions Only one per RolePermissions
	<Permission>	Name of permission	Child of RolePermissions One or more per RolePermissions
<UserPermissions>		Parent node for user permissions	Child of PermissionConfig
	<UserLoginName>	Login name (ID) of user	Child of UserPermissions Only one per UserPermissions

Node Name		Description	Comments
	<Permission>	Name of permission	Child of UserPermissions One or more per UserPermissions

6 Logging

FS-QUO Application Log Files

Application log files are by default located in the shared folder `{$CSIHOME}/env/logs`.

Log Setting	Default Value	Application Configuration Variable	Comment
FS-QUO system log folder	`${CSI.home}/env/log`	Path: *System* > *Log* > *System Logs* Configuration Variable: `RuntimeLogPath`	Includes application log files, config change log files
Product Modeler folder	`${CSI.home}/env/log`		
Product Modeler audit log	`YES` (enabled)	Path: *System* > *Env* > *Debugging Setting* Configuration Variable: `EnableChangeLog`	Enable audit log of updates to product models
Administrative Console audit log	`ENABLED`	Path: *System* > *Env* > *Logger Config Setting* Configuration Variable: `AdminAuditTrailMode`	
Ops API long-running process log folder	`${CSI.home}/env/log/lrp/`	Path: *System* > *Env* > *Logger Config Setting* Configuration Variable: `LRPLogPath`	
Log4J configuration file	(None)	Path: *Application* > *ProductAuthority* > *Env* > *Application Environment* Configuration Variable: `Log4JXML`	

SAP HANA XSA Security Audit Log Files

For more information on SAP HANA XSA security log files, see the Security-Relevant Logging and Tracing section in the SAP Hana Security Guide.

Note on Log File Clean-up

FS-QUO is configured by default to roll over log files. Log files that reach a configurable size (*System* > *Env* > *Config* > *MaxRolloverFileSize*) will roll over to a numbered backup log file. Backup log files cycle through a configurable number of files (*System* > *Env* > *Config* > *MaxRolloverFileNumber*). These configuration settings are managed in the Administrative Console.

With this configurability, system administrators can control the maximum amount of disk space occupied by application log files.

This applies to both the Design Time (Product Modeler) and the Runtime application servers.

Note on User Names in Log Files

In certain circumstances, user first names, last names and login IDs may appear in messages in log files. These can be found using file text search utilities. Log files that are deemed to be lo longer required can be deleted using standard file deletion commands and utilities.

7 Understanding Data Protection and Privacy (DPP)

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulation, it is necessary to consider compliance with industry-specific legislation in different countries. SAP provides specific features and functions to support compliance with regards to relevant legal requirements, including data protection. SAP does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information does not give any advice or recommendation in regards to additional features that would be required in particular IT environments; decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

> ⓘ Note
>
> In the majority of cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion or de-personalization of personal data. SAP does not provide legal advice in any form. Definitions and other terms used in this document are not taken from any given legal source.

7.1 Glossary of DPP Related Terms

Person or Data Subject	The individual whose data is being stored in FS-QUO.
Person Id	An identifier used in the system that uniquely identifies a person, and is visible in the user interface.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health, or sex life or sexual orientation • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses

- Personal data concerning insurances and bank or credit card accounts

Private data	Information that is either personal or personal sensitive data.
Privacy context	A grouping of tables and fields within the persisted data model of FS-QUO representing private data directly related to the data subject or individual whose data is being stored. Located within the Product Modeler as configurable components within the `Extended Underwriting Application Configuration` reference object.
Data Privacy Officer	A user defined within FS-QUO who is has been assigned to a role with the role template `DPP_Officer_RT`, and by virtue of that someone who has rights related to DPP operations. The Data Privacy Officer can run a report to retrieve all private data stored in FS-QUO for a data subject. The Data Privacy Officer can also run a process to de-personalize all data associated with a data subject.
Persisted data model	A data model, which exactly represents data as stored in the database.
Database	The physical collection of information represented by the persisted data model of FS-QUO.
Data exposure point	A point at which private data is exposed by the application and logging of private data should occur.

7.2 User Consent for Collection of Personal Data

Since the data model for the system, specifically including the capture and usage of personal data, is configured by customers, there is no standard capability for capturing user consent for collecting such data.

The user interface extensions to obtain such consent can be added by customization. The result of the request for consent can be stored in the system data model through extensions to the standard data model.

7.3 Understanding FS-QUO Support for DPP Compliance

FS-QUO provides logging, reporting, and de-personalization support for DPP compliance.

Logging

Private data is logged so it is traceable to a person or system that has access to that data. Private data leaving FS-QUO through any channel is logged as well.

Reporting

FS-QUO provides a reporting tool for a Privacy Data Officer to be able to view private data belonging to a person.

De-personalization

FS-QUO supports data protection-relevant functions, such as the removal of private data stored in FS-QUO upon request. Removal can be the deletion or de-personalization of private data. Out-of-the-box, FS-QUO provides the ability to de-personalize private data.

7.3.1 Adding Additional Fields to Existing Privacy Tables

Context

If you have extended an existing table in the database with new fields containing private data, add additional fields to existing privacy tables as follows:

Procedure

1. Launch Internet Explorer and log in to the Product Modeler at the following URL: `https://<pro_designtime_app_url>/csiroot/ii/pc/`
2. Within the *Search* panel located in the lower left corner, enter **`Extended Underwriting Application Configuration`** and choose *Search*

   The `Extended Underwriting Application Configuration` reference object is displayed within the *Search Result* panel.
3. Open the `Extended Underwriting Application Configuration` reference object.
4. Expand the *Data Privacy* > *Privacy Contexts* folder on the Product Tree.
5. Find the existing privacy context that contains the table you wish to add additional fields to and expand it by double-clicking.

   The table hierarchy is shown beneath the privacy context you have chosen.
6. Find and select the table you wish to add fields to and select the *Values* tab.
7. Right-click the far left column of the last row of data and choose *Add*
8. Enter the following information as applicable:

Field Enter the name of the new field within the table.

> **Note**
>
> Ensure that the name of the field matches exactly with the actual field name within the physical table of the database.

Privacy Level Choose one of the following (if applicable):

`[0] - Personal`	If the data within the *Field* attribute is personal.
`[1] - Sensitive`	If the data within the *Field* attribute is sensitive personal.

Identifier Choose one of the following (if applicable):

`[ID] - Person ID`	If the data within the *Field* attribute is the person ID.
`[LINK] - Foreign Key`	If the data within the *Field* attribute is a foreign key for the table defined in the *Table* attribute.
`[CHILD] - Child Table`	If the data within the *Field* attribute is a primary key for the child table defined in the *Table* attribute.

Table If the *Identifier* attribute contains the value `[LINK] - Foreign Key` then enter the table name within the database that has a foreign key relationship with the current table in context.

If the *Identifier* attribute contains the value `[CHILD] - Child Table` then enter the table name within the database that is a child table of the current table in context.

> **Note**
>
> Ensure that the name of the table matches exactly with the actual table name within the physical table of the database.

Search Criteria Enter the field name of the current table in context that is used as the primary search key during logging and reporting.

Search Type Choose one of the following (only applicable if *Search Criteria* is populated):

`[DATE] - Date`	If the *Search Criteria* attribute value is a date type field.
`[NUMERIC] - Numeric`	If the *Search Criteria* attribute value is a numeric type field.
`[TEXT] - Text`	If the *Search Criteria* attribute value is a text type field.

> **Note**
>
> The configuration allows for table nesting in which case the *Identifier* and *Table* fields identify the appropriate relationships.

7.4 Understanding DPP in the Product Modeler

Private data must be identifiable within FS-QUO.

Configuration for DPP is required within the Product Modeler to do the following at runtime:

- Determine which fields are private data.
- Provide a means to be able to search and de-personalize private data.
- Provide de-personalization validation configuration to determine if private data can be de-personalized or not.
- Configure the de-personalization format.

7.4.1 Understanding Privacy Contexts

A privacy context is a grouping of tables and fields within the database representing private data.

Privacy contexts are represented in the Product Modeler as configurable components and are located within the `Extended Underwriting Application Configuration` configuration object under *Extended Underwriting Application Configuration* > *Data Privacy* > *Privacy Contexts*

Each privacy context component identifies the table structure that the context is composed of as well as a special validation query used during de-personalization. The privacy context component has the following configured attributes defined within the *Attributes* tab:

Table	The table name in the database belonging to the current privacy context. **Note** The table name must match exactly with what is defined in the data model.
Validation Query	The SQL query used to find all policy quote options that are tied to private data defined in the privacy tables within the given privacy context. The policy quote options found are then checked to determine if related private data can be de-personalized or not since only inactive policies and quote options can be de-personalized. This check is done as part of the validation during the de-personalization process.
Effective Date	This field is currently not being used
Expiration Date	This field is currently not being used

Related Information

Adding New Privacy Contexts [page 33]

7.4.2 Adding New Privacy Contexts

You can configure additional privacy contexts in the Product Modeler.

Context

If you have extended the database of FS-QUO with new tables containing private data, you will:

- Create a new standalone privacy context at the system level.
- Assemble the new standalone privacy context within the `Extended Underwriting Application Configuration` reference object.

Procedure

1. Launch Internet Explorer and log in to the Product Modeler at the following URL: `https://<pro_designtime_app_url>/csiroot/ii/pc/`
2. Create a new standalone privacy context at the system level as follows:
   a. Go to *System Repository* > *Base Library* > *Components* > *Reference* > *Contexts* in the *Studio Tree*.
   b. Select the *New Object* icon  .

      The *New Object* dialog appears.
   c. Populate the *Name* field with an appropriate name for your privacy context following the existing convention of **`<table name> Context`**.
   d. Leave all of the other fields with their default values and select *OK*.
   e. Double-click the newly created component, which opens the component in a new tab.
   f. Select the *Attributes* tab.
   g. Right-click the leftmost column and choose *Insert Column* > *As Child*
   h. Enter the following values:

Attribute Name	**`Table`**
Data Type	Select **`TEXT`**
Length	**`50`**
Required	Enable this by selecting the checkbox.

      Leave all other fields with their default values.
   i. Right click the leftmost column and choose *Insert Column* > *As Child*
   j. Enter the following values:

Attribute Name	**`Validation Query`**
Data Type	Select **`CLOB`**

      Leave all other fields with their default values.

k. Save your changes.

3. Assemble the new standalone privacy context within the `Extended Underwriting Application Configuration` reference object as follows:
   a. Within the *Search* panel located in the lower left corner, enter **`Extended Underwriting Application Configuration`** and press *Search*
      The `Extended Underwriting Application Configuration` reference object is displayed within the *Search Result* panel.
   b. Open the `Extended Underwriting Application Configuration` reference object.
   c. Right-click the *Data Privacy* > *Privacy Contexts* folder on the Product Tree and select *Add*.
      The *Object Picker* dialog displays.
   d. Search for the privacy context object you created in the previous steps.
      Your privacy context is displayed within the *Object Search Result* panel
   e. Select your privacy context and choose *Select*.
      Your privacy context is now assembled under the following location: *Data Privacy* > *Privacy Contexts* > `<Your Privacy Context>` folder.
4. Populate the required values for the attributes
   a. Select the *Values* tab.
   b. Select the field under *Table* and enter the name of your new table.
   c. Select the field under *Validation Query* and enter the query that maps the **`POLICY_QUOTE`** table with your new table.

> → Tip
>
> See the validation queries configured out-of-the-box for the other privacy contexts as examples.

7.4.3 Understanding Privacy Tables

Nested within each individual privacy context are components that represent tables that contain private data.

Each table component has the following configured attributes defined within the *Attributes* tab:

Field	The field name within the table containing personal or sensitive data.
Privacy Level	A data list selector containing the following possible values: **(blank)** — Blank field. **[0] - Personal** — Indicates that the field contains personal data. **[1] - Sensitive** — Indicates that the field contains sensitive personal data.
Identifier	A data list selector containing the following possible values:

> ⚠ Restriction
>
> A field cannot have a value in both the *Privacy Level* and *Identifier* attributes.

[ID] - Person Id	Indicates that the field is the person ID.
[LINK] - Foreign Key	Indicates that the field is a foreign key for the table defined in the *Table* attribute (if applicable).
[CHILD] - Child Table	Indicates that the field is a primary key for the child table defined in the *Table* attribute (if applicable).

Table

If the *Identifier* attribute contains the value `[LINK] - Foreign Key` then the *Table* attribute value is the table name within the database that has a foreign key relationship with the current table in context.

If the *Identifier* attribute contains the value `[CHILD] - Child Table` then the *Table* attribute value is the table name within the database that is a child table of the current table in context.

Search Criteria

The field name of the current table in context that is used as the primary search key during logging and reporting.

> **Note**
>
> *Search Criteria* can apply to more than one field. If more than one field is marked as *Search Criteria* then all such fields must match in a search.

Search Type

A data list selector containing the following possible values (only applicable if *Search Criteria* is populated):

[DATE] - Date	If the *Search Criteria* attribute is a date type field.
[NUMERIC] - Numeric	If the *Search Criteria* attribute is a numeric type field.
[TEXT] - Text	If the *Search Criteria* attribute is a text type field.

> **Note**
>
> The configuration allows for table nesting in which case the *Identifier* and *Table* fields identify the appropriate relationships.

Related Information

Adding Additional Fields to Existing Privacy Tables [page 30]
Adding New Privacy Tables [page 36]

7.4.4 Adding New Privacy Tables

You can configure additional privacy tables in the Product Modeler.

Prerequisites

- There is an existing privacy context to which your table can be added to.

Context

If you have extended the database with new tables containing private data, you will:

- Create a new standalone privacy table at the system level.
- Assemble the new standalone privacy table within the appropriate privacy context in the `Extended Underwriting Application Configuration` reference object.

Perform the following steps:

Procedure

1. Launch Internet Explorer and log in to the Product Modeler at the following URL: `https://<pro_designtime_app_url>/csiroot/ii/pc/`
   The Product Modeler will open after a short delay.
2. Create a new standalone privacy table at the system level with the following steps:
   a. Within the *Studio Tree*, go to *System Repository* > *Base Library* > *Components* > *Reference* > *Tables* >.
   b. Select the *New Object* icon  .
      The *New Object* dialog appears.
   c. Populate the *Name* field with an appropriate name for your table following the convention of **`<table name> Table`**.
   d. Leave all of the other fields with their default values and select *OK*.
   e. Double-click the newly created component, which opens the component in a new tab.
   f. Select the *Attributes* tab.
   g. Right click the leftmost column and choose *Insert Column* > *As Child* >
   h. Enter the following values for each attribute:

Field	Attribute Name	**`Field`**
	Data Type	Select **`TEXT`**

	Length	**50**
	Required	Make the attribute a required field by selecting the checkbox.
Privacy Level	Attribute Name	**Privacy Level**
	Data Type	Select **DATA_LIST**
	Length	**250**
	Data List Source	Selecting this field brings up a *Data Source Picker* dialog box. Enter **getPrivacyLevel** as the *Search Term* field and choose *Search*. The search results returns an entry for *getPrivacyLevel*, which you can select. Choose *Select* to populate the *Data List Source* field.
	Required	Make the attribute a required field by selecting the checkbox.
Identifier	Attribute Name	**Identifier**
	Data Type	Select **DATA_LIST**
	Length	**250**
	Data List Source	Selecting this field brings up a *Data Source Picker* dialog box. Enter **getDPPIdentifiers** as the *Search Term* field and choose *Search*. The search results returns an entry for *getDPPIdentifiers*, which you can select. Choose *Select* to populate the *Data List Source* field.
	Required	Make the attribute a required field by selecting the checkbox.
Table	Attribute Name	**Table**
	Data Type	Select **TEXT**
	Length	**50**
Search Criteria	Attribute Name	**Search Criteria**
	Data Type	Select **TEXT**
	Length	**50**
Search Type	Attribute Name	**Search Type**
	Data Type	Select **DATA_LIST**
	Length	**250**
	Data List Source	Selecting this field brings up a *Data Source Picker* dialog box. Enter **getSearchType** as the *Search Term* field and choose *Search*. The search results returns an entry for *getSearchType*, which you can select. Choose *Select* to populate the *Data List Source* field.

Leave all other fields with their default values.

i. Save your changes.

3. Assemble the new standalone privacy table within the `Extended Underwriting Application Configuration` reference object with the following steps:
   a. Within the *Search* panel located in the lower left corner, enter **`Extended Underwriting Application Configuration`** and choose *Search*
   The `Extended Underwriting Application Configuration` reference object is displayed within the *Search Result* panel.
   b. Open the `Extended Underwriting Application Configuration` reference object.
   c. Expand the *Data Privacy* > *Privacy Contexts* folder on the *Product Tree*.
   All of the assembled privacy contexts are shown.
   d. Expand the privacy context your table belongs under.
   e. If you are adding your table as a top-level table (assembled directly under the privacy context component) then right-click the privacy context component you wish to add your table to and select *Add*. If you are adding your table under an existing table either with a parent-child or foreign key relationship, then keep expanding the tables under the existing privacy context until you find the appropriate table. Right-click the table and select *Add*.

   The *Object Picker* dialog displays.
   f. Search for the privacy table object you created in the previous steps.
   Your privacy table is displayed within the *Object Search Result* panel.
   g. Select your privacy table and choose *Select*.

Results

Your privacy table is now assembled.

7.4.5 Understanding De-personalization Validation

The *Anonymization Validation* component defines a validation rule that decides if private data for a given person can be de-personalized.

Out-of-the-box in FS-QUO, any private data belonging to a person that is associated with an active policy or quote option cannot be de-personalized.

The *Anonymization Validation* component is located in the Product Modeler within the `Extended Underwriting Application Configuration` configuration object under *Extended Underwriting Application Configuration* > *Data Privacy* > *Validation* > *Anonymization Validation*.

The *Anonymization Validation* component has the following configured attributes defined within the *Attributes* tab:

Validation Rule Name	The name of the validation rule.
Validation Rule	The validation rule that contains the validation business logic.

Description	Description of the validation rule.
SYSATTR_TABLE_NAME	The table name within the database where the validation rule performs necessary lookups.

> **Note**
>
> The validation rule provided out-of-the-box is an orchestration rule. An orchestration rule can call additional rules. As such, you can add more rules which are called by the orchestration rule.

For an example of how orchestration rules work in general, see Orchestrating Underwriting Rules.

For further details on validation rules see Working with Validations and Clearance Rules.

Related Information

Understanding De-personalization and Deletion of Private Data [page 52]

7.4.6 Understanding De-personalization Format Configuration

The `Anonymization Config` component defines the formatting applied to a private data field when it is de-personalized.

The *Anonymization Config* component is found under *Extended Underwriting Application Configuration* > *Data Privacy* > *Configuration* > *Anonymization Config* and has the following configured attributes defined within the *Attributes* tab:

Configuration	The name of the configuration that describes the type. For example, the value *Anonymization String* defines the formatting for all private data fields that are strings.
Value	The de-personalization format.

The de-personalization formatting is as follows:

Anonymization Business Partner ID	All instances of a Business Partner ID are set to the value defined in this field. Default value is **`0`**. This value can be the Business Partner ID of an Anonymous User within SAP GP-FS. As such, you can first create a new Business Partner record within SAP GP-FS that represents the Anonymous User. You then populate this field with the Business Partner ID created for that new record.
Anonymization String	All strings are set to the value defined in this field. Default value is **`*`**.
Anonymization Number	All numbers are set to the value defined in this field. Default value is **`0`**.
Anonymization Date	All dates are set to the value defined in this field. Default value is **`01/01/00`**.

Related Information

Understanding De-personalization and Deletion of Private Data [page 52]
Modifying the De-personalization Format [page 40]

7.4.7 Modifying the De-personalization Format

Context

If you would like to change the existing de-personalization format for the four defined field types, perform the following steps:

Procedure

1. Launch Internet Explorer and log in to the Product Modeler at the following URL: `https://<pro_designtime_app_url>/csiroot/ii/pc/`
2. Within the *Search* panel located in the lower left corner, enter **`Extended Underwriting Application Configuration`** and choose *Search*

   The `Extended Underwriting Application Configuration` reference object is displayed within the *Search Result* panel.
3. Open the `Extended Underwriting Application Configuration` reference object.
4. Expand the *Data Privacy* > *Configuration* folder on the *Product Tree*.
5. Select the *Anonymization Config* and select the *Values* tab.
6. Select the value pertaining to the configuration type you wish to change.

   The value field becomes an editable text field.
7. Change the value of the configuration type to your custom value.

   ⚠ Restriction

   - The *Anonymization Date* value must be in a proper date format.
   - The *Anonymization String* value, if set too long, may result in a database overflow error that can show up at a later time in runtime. The recommendation is to not go beyond a length of one character. When de-personalizing fields, it may be the case that the field is expected to have a fixed set of values. As such, a change to the value of the field may cause errors at runtime. When you configure your own fields to be personal or private, check to ensure that the values aren't expected to be fixed. You can check this in the FS-QUO Toolkit. Note that the sample *Privacy Context* configurations provided out-of-the-box does not have any fields that would cause such an error.

8. Save your changes.

7.4.8 Understanding Custom Configuration

The custom configuration component defines additional configuration for special cases such as evidence.

The custom configuration component is located in the Product Modeler within the `Extended Underwriting Application Configuration` configuration object under *Extended Underwriting Application Configuration* > *Data Privacy* > *Configuration* > *Custom Config*

Each row within the `Custom Config` component identifies the type of custom configuration, a search query for reporting and a validation query used during de-personalization. The `Custom Config` component has the following configured attributes defined within the *Attributes* tab:

Name	The name of the custom configuration entry. Out-of-the-box, there is an entry for **`Evidence`** which the DPP framework uses to identify the custom configuration entry dealing with evidence.
Search Query	The SQL query used to locate specific entries within the database. Out-of-the-box, the *Search Query* finds all entries for evidence that belong to a specific policy holder identified by the Business Partner ID.
Search Criteria	The search field used to map with the search key used within the *Search Query* value.
Validation Query	The SQL query used during validation to find all policy quote options tied to private data. The policy quote options found are then checked to determine if related private data can be de-personalized or not.
Effective Date	This field is currently not being used
Expiration Date	This field is currently not being used

7.5 Understanding Read and Change Access Logging

Any data exposure point must log all relevant operations on private data.

Read access logging (RAL) is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy. These common questions might be of interest for an application that uses RAL:

- Who accessed the data of a given business entity, for example a bank account?
- Who accessed personal data, for example of a business partner?
- Which employee accessed personal information, for example religion?
- Which accounts or business partners were accessed by which users?

These questions can be answered using information about who accessed particular data within a specified time frame. Technically, this means that all remote API and UI infostructures (that access the data) must be enabled for logging.

Every instance of read or update access to private data is recorded so it is traceable to a person or system that has access to that data.

Private data, which has left FS-QUO is recorded as well. For example, data, which has been transferred for print or quote letter.

The following outlines all of the data exposure points:

- FS-IPW Fiori-based static screens and eApps
- RFC calls
- Quote letter read and generation
- Uploading or downloading evidence
- Script rules

The FS-QUO logging framework is configured to log to the SAP HANA XS Advanced security log.

> ⓘ Note
>
> There are instances within FS-QUO where fields are over-logged. For example, imagine you open an eApp, which is longer than the visible page in the browser. You have to scroll down to see additional text. If there is sensitive personal data on that lower section, that data is logged as viewed whether you actually scrolled down or not. This is because the application doesn't necessarily know what is visible to the user. It only knows what is requested programmatically. There are similar cases in logging updates. eApps do not track individual data that is changed, it updates everything. As such, all those writes are logged as changes, even if the values have not been modified. A Data Privacy Officer can however, sort the logs, and look at the log entries of a particular field to see if the value has actually changed over time.

7.5.1 Enabling DPP Logging Through the Administrative Console

Enabling or disabling DPP logging is done through the Administrative Console.

Context

Out-of-the-box, DPP logging is disabled. To enable or disable DPP logging perform the following steps:

Procedure

1. Launch Internet Explorer and log in to the Runtime Administrative Console at the following location: `<pro_runtime_app_url>/csiroot/admin/`.
2. Choose *System* > *Edit Configuration Settings* > *Configuration* > *System* > *Log* > *System Logs* from the menu bar.
3. Locate the row with the *Name* value of *DPPLogEnabled*.

Within the *Override* field, select:	`Yes` to enable DPP logging. `No` or blank to disable DPP logging.

4. Choose *System* > *Reload Configuration Settings* from the menu bar.
   The reload options display.
5. Choose *Reload All Config*.

7.5.2 About Rules for Logging Changes and Access to Private Data

Logging of private data in FS-QUO is done differently for personal data and sensitive personal data.

The rules for logging private data are as follows:

Personal Data	For personal data that is read-only, no logging is performed. For personal data that is changed, all operations that change personal data as well as the changed values are logged.
Sensitive Personal Data	For sensitive personal data that is read-only, all operations that read sensitive personal data as well as the fields that are read are logged, not the values. For sensitive personal data that is changed, all operations that change sensitive personal data as well as the fields that are changed are logged, not the values.

Related Information

Logging Private Data for Static Screens, eApps, and RFC Calls [page 43]
Logging Private Data Within Script Rules [page 45]
Logging Private Data for Quote Letters [page 47]
Logging Private Data for Evidence [page 48]
Logging with Globalization [page 49]
Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.3 Logging Private Data for Static Screens, eApps, and RFC Calls

The log shows details about private data that has been read or changed.

For each data set subject to logging, a date and time stamped log entry is created containing the following information:

Private Data Type	The private data type being logged.

	The possible values are `Personal Data` or `Sensitive Data`.
Action	The action being performed. The possible values are `change` or `read`
User	The user identified by logon ID making the change.
Privacy Context	The privacy context in which the data resides.
Person ID	The person ID of the person.
Column	The column or field name within the privacy table containing the private data.
Table	The privacy table name containing the private data.
Identifying Key	An internal identifier such as PK_ID for the privacy table to allow for traceability.
Value	The new value set in the column or field. **Note** The value is populated only when logging personal data.
Channel	The means in which the personal data is read or changed. The possible values are `IPW, RFC, eApp, QUO`

See the following log entry examples:

Example

```
Personal data change by <Underwriter1> in context <Account> for person <209291>
on column <FIRST_NM> of table <ACCOUNT> with PK_ID <3011>, value set to <Grace>
in channel <RFC>.
```

Example

```
Sensitive data change by <Underwriter1> in context <Account> for person <209291>
on column <GENDER> of table <ACCOUNT> with PK_ID <3011> in channel <IPW>.
```

Example

```
Sensitive data read by <3SUW1> in context <Policyholder_Context>> for person
<8267> on column <GENDER_CD> of table <ABDAPOLHLDR> with PK_ID <8267> in channel
<eApp>.
```

Related Information

Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.4 Logging Private Data Within Script Rules

Logging can also be done within script rules.

Private data that is read or updated within a script rule is logged through a stem.

DPP Logging Stem

FS-QUO provides a logging stem, which can log both a read or change of private data that occurs within a script rule. The private data you decide to log is based on your privacy context configuration. You choose the individual fields you would like logged.

The logging stem has the following functions and parameters:

Stem Name	DPPLoggingStem	
Stem Functions	**`logChange(serviceCommand, dataObject, columnName, channel)`**	Checks if the column changed from the provided data object contains personal or sensitive personal data and if so, logs a message. This function takes four parameters.
	`logChange(serviceCommand, columnName, channel)`	Checks if the column changed from the current data object contains personal or sensitive personal data and if so, logs a message. This function takes three parameters.
	`logRead(serviceCommand, dataObject, columnName, channel)`	Checks if the column read from the provided data object contains sensitive personal data and if so, logs a message. This function takes four parameters
	`logRead(serviceCommand, columnName, channel)`	Checks if the column read from the current data object contains sensitive personal data and if so, logs a message. This function takes three parameters.

The various parameters are defined as follows:

`serviceCommand`	A standard object argument containing different objects required by the rule.
`dataObject`	The current data object containing the private data column.
`columnName`	The private data column name.
`channel`	The means in which the personal data is read or changed. The possible values are: • `CHANNEL_IPW` • `CHANNEL_QUO`

- `CHANNEL_RFC`
- `CHANNEL_EAPP`
- `CHANNEL_QUOTE_LETTER`
- `CHANNEL_ANONYMIZATION`

Example in FS-QUO

Out-of-the-box, FS-QUO provides an example of a call to the logging stem for an update operation within the `Life Capital 2009 92H0000S0002` sample product. The stem is called within the *populateGroupMemberPolicyDataFromSpreadsheetRow* service rule for a `logChange`, which is the rule that populates group member policy data from a spreadsheet. The service rule can be found at the following location: *Life Capital 2009 92H0000S0002* > *Configuration* > *Product Services* > *Service API*.

The following example shows a call to the DPPLoggingStem within the *populateGroupMemberPolicyDataFromSpreadsheetRow* service rule:

> ### Example
>
> ```
> CALL logChange IN LIBRARY DPPLoggingStem WITH serviceCommand,
> policyData:ABDAPOLHLDR, "ABDAPOLHLDR.BIRTH_DT","CHANNEL_IPW"
> ```
>
> In this example, the `logChange(serviceCommand, dataObject, columnName, channel)` function of the DPPLoggingStem is called to log a change operation on the `BIRTH_DT` column, which is part of the `ABDAPOLHLDR` table. Out of the box, the `BIRTH_DT` column within the `ABDAPOLHLDR` table is marked as a *Personal* field and therefore is logged during a change operation.

Log Output

The log output from the DPPLoggingStem has the following format:

Private Data Type	The private data type being logged. The possible values are `Personal Data` or `Sensitive Data`.
Action	The action being performed. The possible values are `change` or `read`
User	The user identified by logon ID making the change.
Privacy Context	The privacy context in which the data resides.
Person ID	The person ID of the person.
Column	The column or field name within the privacy table containing the private data.
Table	The privacy table name containing the private data.
Identifying Key	An internal identifier such as PK_ID for the privacy table to allow for traceability.
Value	The new value set in the column or field.

> **Note**
>
> The value is populated only when logging personal data.

Channel	The means in which the personal data is read or changed. The possible values are `IPW, RFC, eApp, QUO, Quote Letter`

The following is a log entry example:

> **Example**
>
> ```
> Personal data change by <Underwriter1> in context <Account> for person <209291>
> on column <FIRST_NM> of table <ACCOUNT> with PK_ID <3011>, value set to <Grace>
> in channel <IPW>..
> ```

For further details on stems see the following topics:

- Using Stems (Coverage-based products)
- Using Stems (Risk-based products)
- Extending Stem Implementation Classes and Stem Classes (Coverage-based products)
- Extending Stem Implementation Classes and Stem Classes (Risk-based products)

Related Information

Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.5 Logging Private Data for Quote Letters

The log reflects when a quote letter is being read or generated.

A log entry is created containing the following information:

Private Data Type	The private data type being logged. Value is `Sensitive Data`.
Artifact	Value is: `Quote Letter`
Artifact Name	The filename prefix of the quote letter.
Action	The action being performed. The possible values are `generated` or `read`.
User	The user identified by logon ID making the change.
Location	The location where the generated quote letter resides.
Channel	The means in which the personal data is read or changed. Value is `Quote Letter`.

See the following log entry examples:

> **Example**
>
> `Sensitive data in Quote Letter <QuoteLetter_103_1500324691888> read by <3SUW1> in location <D:/apps02/csihome/S02/env/quoteletter/> in channel <Quote Letter>.`

> **Example**
>
> `Sensitive data in Quote Letter <QuoteLetter_103_1500324691888> generated by <3SUW1> to location <D:/apps02/csihome/S02/env/quoteletter/> in channel <Quote Letter>.`

For further information on quote letters, see Configuring Quote Letter Generation

Related Information

Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.6 Logging Private Data for Evidence

The log also reflects when evidence is uploaded or downloaded.

Evidence is always assumed to contain sensitive personal data. A log entry is created containing the following information:

Evidence `<evidence_type>`	The evidence type. The possible values are: • `Consumer Reports` • `Credit Reports` • `Inspection Reports` • `Medical Questionnaire` • `Medical Reports` • `Photo of Property` • `Survey`
Evidence Name	The arbitrary name a user can assign to the evidence.
Action	The action being performed. The possible values are `uploaded` or `downloaded`.
User	The user identified by logon ID making the change.
Identifying Key	An internal identifier such as `PK_ID` for the `Evidence` table to allow for traceability.

Channel	The means in which the sensitive personal data is read or changed. Value is `IPW`.

See the following log entry examples:

> ### Example
>
> ```
> Evidence <Survey> <Evidence.msg> downloaded by <3SUW1> for <316> in channel
> <IPW>.
> ```

> ### Example
>
> ```
> Evidence <Medical Reports> <scheduler.properties> downloaded by <3SUW1> for <276>
> in channel <IPW>.
> ```

For information on evidence, see Managing Evidences.

Related Information

Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.7 Logging with Globalization

DPP logging has multilanguage support.

Currently, the following languages are supported:

- English
- Korean
- Chinese (Traditional)

You can enable multilanguage support by choosing the correct locale in your chosen browser.

Related Information

Viewing Security Logs in SAP HANA XS Advanced [page 49]

7.5.8 Viewing Security Logs in SAP HANA XS Advanced

DPP-relevant log messages can be viewed in the SAP HANA XS Advanced audit log.

For more information, see Viewing Audit Logs in XS Advanced.

7.6 Understanding DPP Reporting

A Data Privacy Officer can run a report displaying all private data stored in the system for a specified data subject.

FS-QUO provides a reporting tool (DPP report) that allows for a Data Privacy Officer to enter sufficient search criteria to uniquely identify a person. The search fields used for unique identification are configurable and defined within the Product Modeler. The search field attributes are *Search Criteria* and *Search Type* found under *Extended Underwriting Application Configuration* > *Data Privacy* > *Privacy Contexts* > `<Privacy table>` *Context*.

All static text and search criteria fields are displayed in the language and format based on your locale.

The DPP report is located at the following URL: `<quo_app_url>/csiroot/dpp/index.html`

7.6.1 About DPP Report Authorization

A Data Privacy Officer must be assigned to a role with the role template `DPP_Officer_RT` in order to be able to log in to the DPP report, search, and de-personalize private data. Assign all users who are Data Privacy Officers to this role through XSUAA and SAP Cloud Platform Identity Authentication Service (SCP IAS).

7.6.2 About DPP Search Fields

The DPP report contains search fields that are used to search private data within Sencha-based or Fiori-based applications.

Search fields are configured within each privacy table in the Product Modeler located within the `Extended Underwriting Application Configuration` configuration object under *Extended Underwriting Application Configuration* > *Data Privacy* > *Privacy Contexts*

The following search fields make up the full set of search criteria for both application types:

> **Note**
>
> If you have configured multiple fields within *Search Criteria* for a given privacy table, then populate all of those fields.
>
> > **Example**
> >
> > You have an *Account Context*, which has an *Account Table* privacy table. Your *Search Criteria* that you have configured are the fields *ACCOUNT_NM* (*Account Name*), *PHONE_NO* (*Phone Number*) and *BIRTH_TS* (*Birthday*). Populate all three search fields since the report searches all three fields together.

The following search fields apply to Fiori-based applications:

Business Partner Name	A search tool that allows you to search for a Business Partner ID given a name. Selecting this field brings up a *Select Business Partner* search dialog allowing you to enter a name or ID. This search option searches the SAP GP-FS system if it is available.
Business Partner ID	The Business Partner ID of the person.

The following search fields apply to Sencha-based applications:

First Name	The first name of the person.
Last Name	The last name of the person.
Date of Birth	The date of birth of the person. Selecting this field brings up a date selector dialog allowing you to choose the appropriate date.
Account Name	The name of the person associated with the account.
Phone Number	The phone number of the person.
Producer Name	The name of the Producer.
Producer Code	The Producer code.
Alternative Name 1	The alternate name of the person.
Alternative Name 2	The second alternate name of the person.

> **Note**
>
> To clear the data you entered in all of the search fields, press *Clear*.

Related Information

Understanding De-personalization and Deletion of Private Data [page 52]
Searching, Downloading, and De-personalizing Private Data [page 53]

7.6.3 About Search Results Output

The DPP report search results output is a union of all of the query results for all privacy contexts configured for the person being searched.

The report contains the following data:

Table	The database table name that contains the private data of the person identified by *Person ID* value.
Key	The unique key within the database identifiying the current data record.
Person ID	The ID that identifies the person within the *Table*.
Attribute	The field name within the *Table* that has been identified by configuration to contain private data.

Value The private data value belonging to the person.

> ### Example
>
> If the same account holder appears on 3 policies the same data will appear 3 times on the search screen.

Related Information

Understanding De-personalization and Deletion of Private Data [page 52]
Searching, Downloading, and De-personalizing Private Data [page 53]

7.7 Understanding De-personalization and Deletion of Private Data

Deletion or De-personalization of Personal Data

The handling of personal data is subject to applicable laws related to the deletion of such data at the end of purpose (EoP). If there is no longer a legitimate purpose that requires the use of personal data, it must be deleted or de-personalized. When deleting or de-personalizing data in a data set, all referenced objects related to that data set must be deleted or de-personalized as well. It is also necessary to consider industry-specific legislation in different countries in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted or de-personalized.

The DPP report within FS-QUO allows you to de-personalize any private data for a given person. The format in which data is de-personalized is configured through Product Configurator. The de-personalization process first goes through a validation as configured within the `Anonymization Validation` component which determines whether de-personalization can occur or not. The DPP report also allows you to download any private data generated to a file in CSV format. The fields within the output file are the same fields shown in the search results output.

> ### Note
>
> For evidence, the generated document is physically deleted from the filesystem through the DPP report. In all other cases, private data is de-personalized.

Limitations for De-personalization

Business Partner Search Within Different Sample Products

The data model of the sample products provided out-of-the-box in FS-QUO are closely modeled after those defined within FS-PM. As such, some sample products have different field names for the same table. For

example, the sample product `Life Capital 2009 92H0000S0002` contains the field `PARTNER_ID` within the table `COV_ABDASUBJCT` that represents the business partner ID. The sample product `Sample Household Product` however, contains the field `PARTN_ID` within the same table `COV_ABDASUBJCT` that also represents the business partner ID. Because the business partner ID maps to 2 different fields for the same table in the database, the DPP framework can only search and de-personalize private data for one product, not both.

> **Note**
>
> This limitation only applies if you have multiple products that have the business partner ID map to two different fields for the same table. Note also that logging is unaffected by this limitation.

For more information on integrating with FS-PM, see the Integration Guide for Coverage-based Insurance Solutions.

7.7.1 Searching, Downloading, and De-personalizing Private Data

Prerequisites

You have the correct role permissions as a Data Privacy Officer to search for and de-personalize private data for any given person.

Context

The search fields used for unique identification are configurable and defined within the Product Modeler. The search field attributes are *Search Criteria* and *Search Type* found under *Extended Underwriting Application Configuration* > *Data Privacy* > *Privacy Contexts* > `<privacy_table>` *Context*.

Procedure

1. To search for private data for a person, perform the following steps:
   a. Log in to the DPP report at the following URL: :`<quo_app_url>/csiroot/dpp/index.html`

      A logon screen appears.
   b. Enter your user name in the *User* field and your password in the *Password* field. Choose *Log On*.

      The *Personal Data Search* report is displayed.
   c. Enter the appropriate information within the search criteria fields that have been configured within Product Configurator.

> ### Example
>
> To search for a person within FS-IPW through Business Partner ID, enter the ID in the *Business Partner ID* search field or enter the name in the *Business Partner Name* field.

> ### Note
>
> All of the search input fields within the report are statically defined and contain all possible search input fields that uniquely identify a person. If you wish to add more search criteria fields, they must be configured within the Product Modeler and also added to the report UI through the FS-QUO toolkit.

d. At this point, verify that the data shown belongs to the user you searched for.

> ### Caution
>
> De-personalization is not reversible. If you cannot guarantee that the individual you are searching for is what is displayed, do not perform the next steps.

2. To download the report to a CSV file, perform the following steps:
   a. Choose the *Download* icon.

      A confirmation dialog is displayed asking you where to save the CSV file.
   b. All data from the report is captured in the CSV file.
3. To de-personalize all private data displayed in the report, perform the following steps:
   a. Choose *Delete Personal Data*.

      A confirmation dialog is displayed asking you to confirm deletion

> ### Note
>
> If validation fails, a message is logged indicating that de-personalization could not be performed. The following examples show possible error log messages:

> ### Example
>
> The following example shows an error log generated from a failed SQL update:
>
> ```
> Anonymization by <3SUW1> in context <Account Context> for person <23364>
> of table/dependent table <ACCOUNT> failed due to error <error message from
> server> in channel <IPW>
> ```

> ### Example
>
> The following log example shows an error log generated from a failed validation rule:
>
> ```
> Anonymization by <3SUW1> in context <Account Context> for person <064655>
> of table/dependent table <Account> did not occur due to the following
> validation results (<Validation Table Name:Validation Table ID:Validation
> Message>): POLICY_QUOTE:0122:”Effective date is within 365 days of current
> date”, POLICY_QUOTE:2215: ”Effective date is within 365 days of current
> date”, in channel <Anonymization>.
> ```

   b. To ensure that all data has successfully been de-personalized, perform the same search as in step 1 and verify that no data is returned.

7.7.2 About De-personalization Logging

During the de-personalization process, log messages are generated to show details of the following:

- What has been de-personalized.
- What the new values are based on de-personalization configuration.
- Who performed the de-personalization.
- The person whose private data has been de-personalized.

The following are a few examples:

> ### Example
>
> ```
> Personal data anonymized by <3SUW1> in context <Account Context> for person
> <2531> on column <ACCOUNT_NM> of table/dependent table <ACCOUNT>, value set to
> <*> in channel <Anonymization>.
> ```

> ### Example
>
> ```
> Sensitive data anonymized by <3SUW1> in context <Account Context> for person
> <12531> on column <ACCOUNT_NM> of table/dependent table <ACCOUNT>, value set to
> <*> in channel <Anonymization>.
> ```

7.7.3 Source Code Locations for DPP

The following outlines key source code locations relevant to DPP:

> ### Note
>
> To extend the DPP framework or add additional logging, use the toolkit that is provided with FS-QUO. For further details about the FS-QUO toolkit, see the Development Toolkit Guide. Note also that any classes within `camilionlib` cannot be modified directly.

Logging API (`camilionlib`)

Interface and Implementation	`com.sap.fs.pro.dpp.DataAccessLoggingService` `com.sap.fs.pro.dpp.impl.DataAccessLoggingServiceImpl`
Logging Stem for Rules	`com.sap.fs.pro.dpp.stem.DPPLoggingStem`

Configuration, Reporting, and De-personalization API (`camilionlib`)

Interface and Implementation	`com.sap.fs.pro.dpp.PersonCentricity` `com.sap.fs.pro.dpp.PersonCentricityImpl`

FS-IPW Fiori-based Logging Points

The following outlines the various code locations within FS-QUO for Fiori-based applications where DPP-specific logging occurs:

Static Screens, EApps	`com.sap.fs.quo.service.impl.SubmissionDataServiceImpl` `com.sap.fs.ps.eapp.screen.controller.JSONScreenController` (`camilionlib`)

RFC	`com.sap.fs.quo.core.stem.impl.DisplayIllustrationServiceImpl`
	`com.sap.fs.quo.service.impl.FSPMIntegrationServiceBase`
	`com.sap.fs.quo.service.impl.FSPMNativeBookingServiceImpl`
	`com.sap.fs.ps.transformation.service.impl.RfcOutboundTransformationBase` (`camilionlib`)

Quote Letter	`com.sap.fs.quo.service.impl.QuoteOptionDataServiceImpl` (`camilionlib`)
Evidence	`com.sap.fs.uw.odata.processor.PolicyEvidenceProcessor` `com.sap.fs.uw.cms.service.CMSDownloadProcessor`

DPP Report UI

The following outlines the various code locations within FS-QUO for the DPP report UI.:

DPP Report Web Project Module	`DPPWeb`

8 Services for Security Lifecycle Management

This section provides an overview of services provided by Active Global Support that are available to assist you in maintaining security in your SAP systems on an ongoing basis.

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.
  In this case, analyze and implement the identified SAP Notes if possible. If you can't implement the SAP Notes, the report should be able to help you decide on how to handle the individual cases.
- Whether an accumulation of critical basis authorizations has been identified.
  In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.
- Whether standard users with default passwords have been identified on your system.
  In this case, change the corresponding passwords to non-default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security-relevant configuration parameters
- Critical users
- Missing security patches

This service is available as a self-service within SAP Solution Manager, as a remote service, or as an on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation for a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance with predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers

configuration parameters, but it also covers critical security properties like the existence of a non-trivial Gateway configuration or making sure standard users don't have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in a secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more information about these services, see:

- EarlyWatch Alert: https://support.sap.com/en/offerings-programs/support-services/earlywatch-alert.html
- RunSAP Roadmap, including the Security and the Secure Operations Standard: https://support.sap.com/en/offerings-programs/methodologies/implement.html (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.

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

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP