PUBLIC

2025-02-17

SAP Signavio Process Manager Security Guide

THE BEST RUN SAP

Content

1 SAP Signavio Process Manager Security Guide

In this guide, you can find information about security topics relating to SAP Signavio Process Manager. The guide outlines the security measures in place as well as any security-related steps that you must take as an administrator.

SAP Signavio Process Manager uses an Amazon Web Services (AWS) environment for its back end. For more information about security on AWS, see the AWS documentation .

For information on certification and accreditation, see the SAP Trust Center.

2 User Administration, Authentication, and Authorization

SAP Signavio Process Manager has its own user management.

Manage Users and Groups

User accounts are created by invitation: You invite users to your workspace by email, provide them with a license and access rights, and manage their accounts.

In addition, SAP Signavio Process Manager users can invite internal and external process stakeholders to review and comment on diagrams. Internal users already have a SAP Signavio account. Externals need to create an account to log in.

> ⓘ Note
>
> If invited users can't access SAP Signavio, check the IP filtering settings of the workspace. Read more in section Set up IP address filtering [page 24].

With groups, you can effectively manage a large number of users and their access rights by creating a group for each organizational role and setting up a group hierarchy. This simplifies assigning access rights and feature sets to users.

To open the user management, click *Settings* in the sidebar of SAP Signavio Process Collaboration Hub and open the *User management* tab.

> ⓘ Note
>
> The email address you use to sign up cannot contain the German umlauts (such as ä, ö, ü) as special characters.

Users Invited for Feedback

Internal users

When users who already have an account and a license for this workspace are invited to review and comment on diagrams, they use their existing email address and password combination to log in.

Internal users are managed with the user management.

External Users

When external users are invited to comment on diagrams, they must create an account using the link in the invitation email. They can then sign in to SAP Signavio Process Collaboration Hub and view the diagram, for which they have received an invitation. Instead of a paid license, they are assigned a commenting license so that they can view and add comments.

The user accounts created in this way are like those created with the user management, but the following restrictions apply:

- Users can't see any other diagram then the one they were invited to.
- Users aren't assigned to any user group, not even the default groups.
- Users can't access any other SAP Signavio component.

To revoke access, remove the account from the user management. When you just remove the licenses, external users can still sign in to SAP Signavio Process Collaboration Hub. They no longer see any diagram, instead they are informed that their trial has expired.

If needed, you can keep the account and manage it like any other account, for example assign more licenses and provide more access rights.

Users Invited to a Workspace

In the user management, you invite new users to your workspace. You also select the license type and the user groups you want to assign to the new user.

The license for a new user is bound to the email address to which you send an invitation. The new user has to register with the same email address to use the license.

New users are automatically added to the user management once they have accepted the invitation and logged in to the workspace. You can then manage their access rights.

If users are not members of any group initially, they are able to read, write, delete or publish in all folders and models in the *Shared documents* folder.

If you want users to manage the workspace, you add them to the *Administrators* group.

Create Accounts

> ⓘ Note
>
> If you want to set up auto-provisioning for your workspace so that user accounts are created automatically on login, read more in section Single Sign-on Using SAML.

You have the following options to add users to your workspace:

- Create accounts with bulk invites. The accounts are created when users log in for the first time. Only then can you change users' access rights.

- Create user accounts instantly. With this option, you can change users' access rights immediately after you've created the accounts.

Every user you invite to your workspace has the following default permissions. Note that you can change these permissions by adding users to user groups.

- Viewing and editing diagrams in the folder *Shared documents*
- Viewing and editing dictionary entries

You can change users' permission in *Setup > Manage access rights* in the explorer of SAP Signavio Process Manager.

Create Accounts with Bulk Invites

> ⓘ Note
>
> Note that you can change users' access rights only after they have logged in for the first time.

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Invites*.
3. Paste the email addresses to the field. Email addresses must be separated by a whitespace.
4. Select one or more licenses from the drop-down list. Each user you invite will receive the selected licenses.
5. Optionally, you can assign each user to a user group from the drop-down list. When you create users groups, you can assign licenses that will be applied to each user of the group.
6. Choose *Send invites*.
   Email invitations with a link to the registration page are sent.

Create Multiple Accounts Instantly

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and click the *User management* tab.
   The user management opens.
2. In the sidebar, click *Invites*.
3. Paste the email addresses to the field. Email addresses must be separated by a whitespace.
4. Select one or more licenses from the drop-down list. Each user you invite will receive the selected licenses.
5. Optionally, you can assign each user to a user group from the drop-down list. When you create users groups, you can select licenses that will be applied to each user of the group.
6. Decide whether to send emails or not:
   - To send no invitation email to the users when you create their accounts, select *Do not send invitation email*. Users then only receive an email asking them to change their password.

- To send no email at all, select *Do not send change password email*.
  If service provider initiated authentication is enabled for the workspace, users are redirected to the identity provider, log in there, and enter the workspace. A SAP Signavio-specific password is not required.
  When SP-initiated authentication isn't enabled, users must reset their password by using the *I've forgotten my password* link on the login page.
  Read more in Single Sign-on Using SAML.

7. Choose *Create users*.
   User accounts are created instantly. To change the users' permission, go to the *Users* tab.

Delete pending email invitation

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Invites*.
3. Choose the user's email address.
4. On the right side, click *Cancel*. The link in the email invitation becomes invalid.

Resend email invitation

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Invites*.
3. Choose the user's email address.
4. On the right side, click *Resend*. An email invitation is sent again.

Delete a User Account

To remove a user from a workspace, you delete their account.

When you delete an account, all content in the *My Documents* folder is deleted as well. The content the user created in the *Shared documents* folder, their comments and changes, and the dictionary entries they created remain.

To remove a user, follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Users*.
3. Choose the user you want to remove from the workspace.
4. On the right panel, click *Delete*. The user's account is deleted and the user can no longer log in.

You can set how long personal data of deleted users is kept in the security settings, see section Editing the Security Configuration [page 24] for details.

Change User Settings

You can assign licenses to a user, assign users to groups, and reset the user's password. To do so, follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Users*.
3. Choose the user whose settings you want to change.
4. On the right panel, you have the following options to change user's settings:
   - *Licenses*: Assign a license by selecting a license form the drop-down list.
   - *Groups*: Assign user to a group by selecting a group from the drop-down list.
   - *Reset password*: Send a password reset email.
   - *Remove user*: Delete user account, see *Delete account*.

2.1 User Groups and Workspace Administrators

To manage access rights for multiple users and content, create user groups in SAP Signavio Process Transformation Suite. Learn how to add or delete user groups, customize their settings, and create workspace administrators to manage workspace settings and user access.

Managing access rights for individual users becomes hard to manage with a large number of users and a lot of content. We recommend that you create user groups to manage access rights and access to features. With user groups, you can manage the permissions of multiple users at once.

At the moment, no templates for creating user groups are available.

Add user groups

To add a group, follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Groups*.
3. On the right panel, enter the group name and click *Add a new group*. The new group is added.

For group settings, see User Group Settings [page 9].

Delete user groups

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Groups*.
3. Choose the group you want to delete.

4. In the right panel, click *Delete*.
5. Confirm with *Yes, delete this group*. The group is deleted. Users that are members of this group are not deleted.

User Group Settings

Follow these steps:

1. In SAP Signavio Process Collaboration Hub, click *Settings* in the sidebar and open the *User management* tab.
   The user management opens.
2. In the sidebar, click *Groups*.
3. Choose the group which settings you want to change.

You have the following options to change the group's settings:

- *Name*: Edit the name of the group.
- *Add new users to this group automatically*: Decide whether to define this group as the default group.
- *Select a group as member*: Create a group hierarchy by adding another group.
- *Users*: Remove users from the group by clicking *X*.
- *Select a user to add as a member*: Select a user from the drop-down list to add to group.

Default User Groups

When customizing user groups, you can set one or more groups as default groups. For example, you can use a default group to provide new users with a basic set of access rights.

To define a group as a default group, activate the option *Add new users to this group automatically* in the group settings.

Each user invited through the user management is assigned to all default groups by default.

To assign the user you want to invite to another group, you can assign user-specific user groups in the user management dialog when you set up the invitation.

Users created with SAML or CSV API are also assigned to the default groups, unless you specify other user groups by configuration.

Creating Workspace Administrators

In SAP Signavio Process Manager, administrators have extensive permissions to manage workspace settings and user access. The only thing they can't access or manage is the content in a modelers *My documents* folders.

ⓘ Note

- Administrators can make far-reaching changes to your workspace. For this reason, we recommend enabling people with tool-specific knowledge and experiences in business process management and process modeling.
- Users need a license for SAP Signavio Process Manager to become administrators.

To create an administrator account, follow these steps:

1. Create a user account.
2. In the explorer, go to *Setup* › *Manage access rights*. The user management dialog opens.
3. Open the *User groups* tab.
4. Select the group *Administrators*.
5. In the section *Add user/group*, select the user from the drop-down list.
6. Confirm with *Add*. The user now has administrative rights for your workspace.

- To revoke administrative rights, remove the user from the *Administrators* group.

2.2 Manage Access Rights

ⓘ Note

You need an administrator account to use this function.

This section describes how to define access rights to folders, diagrams, the dictionary, and dictionary categories. For information how to activate specific feature sets, see section Activating Feature Sets.

You can assign access rights for users and user groups.

Access rights are additive. Once users have access by being in a user group with access, the access rights cannot be taken away by adding the users to an additional group with less access or by setting user-specific access rights.

Folder Structure

If users are not members of any group initially, they are able to read, write, delete or publish in all folders and models in the *Shared documents* folder.

If you grant users access to a diagram and they don't have access to the folder containing the diagram, they can only view the diagram and the diagram path. They don't have access to any other diagrams in this folder. To restrict access rights based on organizational roles, we recommend setting up a folder structure that reflects the different access rights variations.

User Groups

We recommend to create user groups with access rights that match your organizational requirements. See section User groups [page 8].

Set Access Rights for Folders and Diagrams

If you give users access rights to a folder, they also have access to all subfolders and diagrams in that folder. By default, users can access the complete dictionary. You can limit access to specific dictionary categories and subcategories.

To define access rights, follow these steps:

1. In the explorer, go to *Setup* > *Manage access rights*. The user management dialog opens.
2. Open the *Access rights* tab. The tree structure shows all content of the > *Shared documents* folder.
3. Select the element for which you want to define access rights.
4. From the drop-down lists, select the users or user groups and the access right types. You find detailed descriptions of the access rights below.
5. Confirm with *Add*. The added users and their access rights are added to the list.

Limit access to specific folder content

> ⓘ Note
>
> Journey models and uploaded files always inherit the access rights of the folder in which they are stored. This means you can't limit access rights to specific journey models or uploaded files in a folder.

When you grant access to a folder, users have access to the complete folder. You can limit the access to specific folder content.

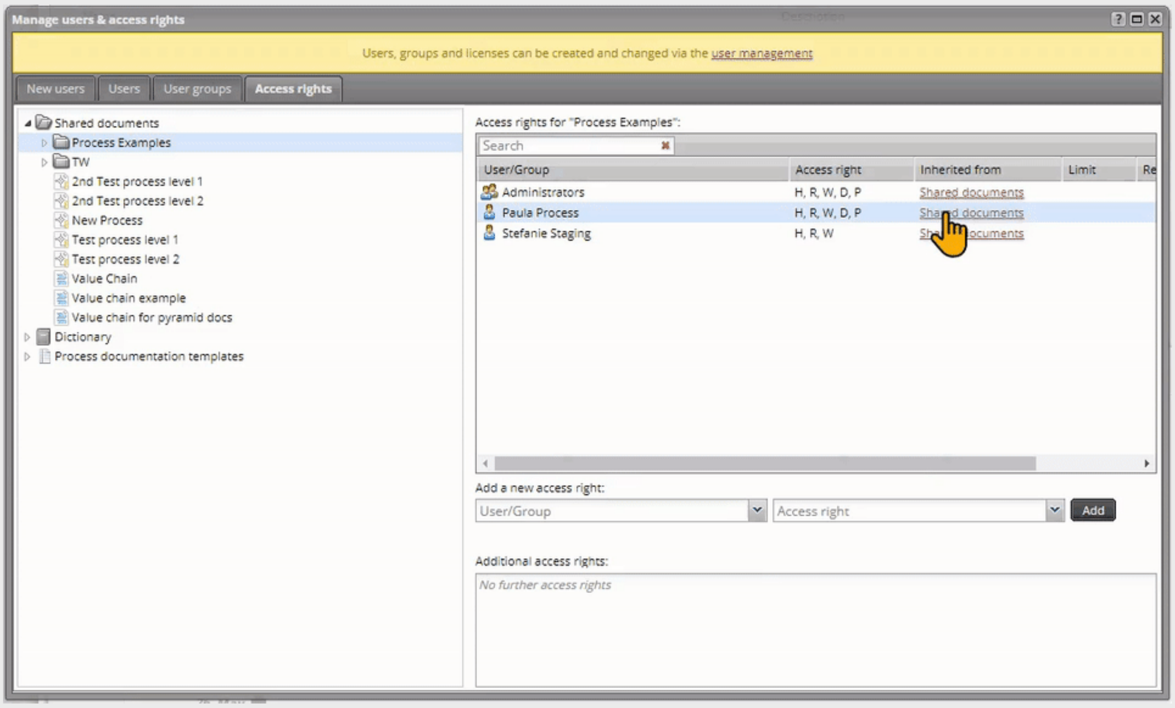
If you grant users access to a diagram and they don't have access to the folder containing the diagram, they can only view the diagram and the diagram path. They don't have access to any other diagrams in this folder.

Follow these steps:

1. Select users or user groups that have access rights.
2. Choose *limit*.
3. Select the content to which users should keep access.
4. Save with *Confirm*.

Example

Example:



Users, groups and licenses can be created and changed via the user management

Access rights for "Process Examples":

User/Group	Access right	Inherited from	Limit	Re
Administrators	H, R, W, D, P	Shared documents		
Paula Process	H, R, W, D, P	Shared documents		
Stefanie Staging	H, R, W	Shared documents		

Add a new access right:

Additional access rights:

No further access rights

Available Access Rights for Diagrams and Folders

Note

To effectively use approval workflows, you should restrict permission to publish diagrams in the SAP Signavio Process Collaboration Hub.

Access right	Details
Hub (H)	View published content in SAP Signavio Process Collaboration Hub
Read (R)	View unpublished content in the simulation tool, the revision comparison tool, the commenting view, and in SAP Signavio Process Collaboration Hub
Write (W)	Edit and save content in the editor
Delete (D)	Delete and move content To delete and move content between folders, users need write access for both folders and delete access for the folder from which the content is removed.

Access right	Details
Publish (P)	To publish content and move published content • To publish diagrams in SAP Signavio Process Collaboration Hub • To move published elements such as diagrams and folders • To embed a diagram on an external website

Access rights for SAP Signavio Process Collaboration Hub features

The commenting feature in SAP Signavio Process Collaboration Hub is a read access, since users who have been invited with the function *Invite anyone for feedback* can add comments to a diagram, but aren't able to edit it.

Set Access Rights for the Dictionary

You can manage dictionary access permissions through user groups based on your organizational needs. We recommend using user groups instead of assigning permissions to regular users.

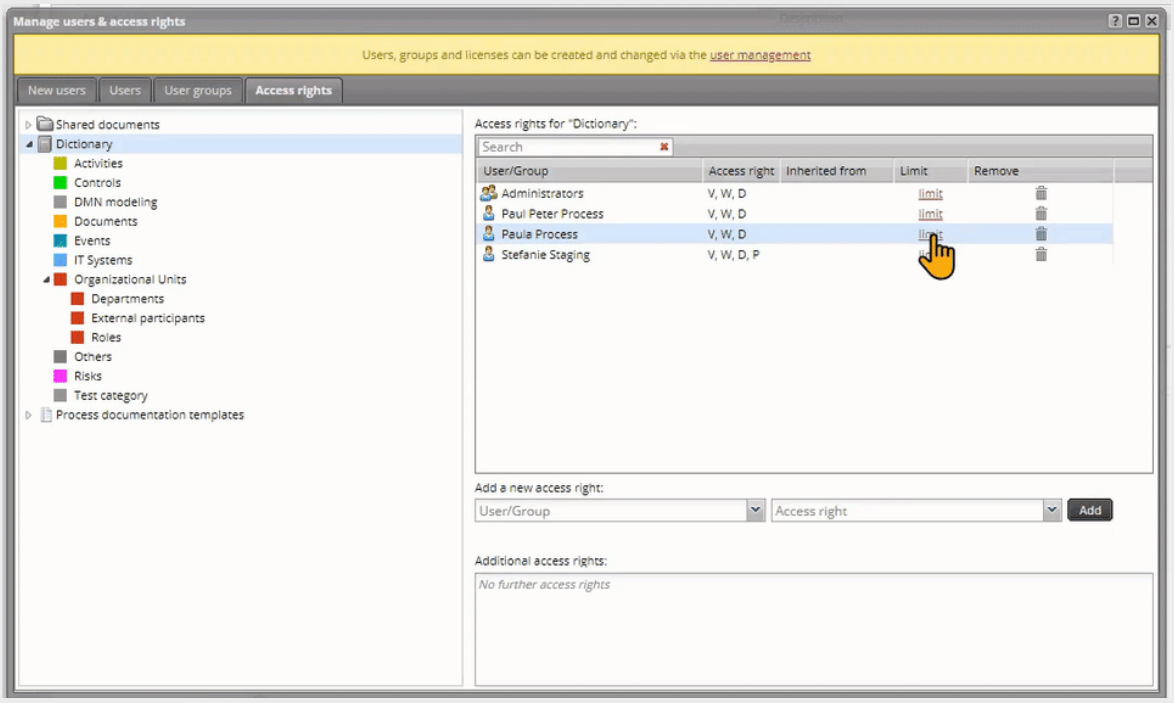
1. In the top-right corner of the explorer, go to ▶ *Setup* ▶ *Manage users & access rights* ▶.
2. Open the *Access rights* tab.
3. Select the dictionary folder.
4. From the drop-down lists, select the users or user groups and the access rights. You find detailed descriptions of the access rights below. The user management dialog opens.
5. Choose *Add*. The access rights you set are listed.

To limit access rights for the dictionary to specific categories, follow these steps:

1. In the *Access rights* tab, select the folder *Dictionary*.
2. Select users or user groups that have access rights set.
3. Choose *limit*.
4. Select the dictionary categories to which users should keep access.
5. Confirm in the dialog.

Example

Example:



Users, groups and licenses can be created and changed via the user management

Access rights for "Dictionary":

User/Group	Access right	Inherited from	Limit	Remove
Administrators	V, W, D		limit	
Paul Peter Process	V, W, D		limit	
Paula Process	V, W, D		limit	
Stefanie Staging	V, W, D, P			

Add a new access right:

User/Group

Access right

Additional access rights:

No further access rights

When you remove access to a dictionary category, entries from this category are no longer listed for the users, are not included in their search results, and can't be used by them when creating diagrams.

Note

Users can always view dictionary entries in the diagrams where they are used, even without having access to the dictionary category.

When users have limited access to the dictionary, they are no longer listed when you select the dictionary folder.

Access Rights for the Dictionary

Access rights can be set for the complete dictionary or dictionary categories.

Access right	Function
View (V)	View dictionary entries in the editor and in SAP Signavio Process Collaboration Hub . In the editor, the dictionary entries can be used during modeling.
Write (W)	Edit and save dictionary entries.

Access right	Function
Delete (D)	Delete and move content To delete and move dictionary entries between categories, users need write access for both categories and delete access for the category from which the entry is removed.
Publish (P)	Publish dictionary entries in SAP Signavio Process Collaboration Hub.

The access rights for dictionary categories only affect dictionary entries in these categories.

Set Access Rights for Variant Management

By default, users don't have access to all the available Variant Management feature sets. You can give or limit access to specific actions, as needed.

To do that, follow these steps:

1. In the top-right corner of the explorer, go to ▶ *Setup* ▶ *Manage users & access rights* ▶.
2. Open the *User groups* tab.
3. In the *Groups* field, select a user group to which you want to adjust permissions.
4. If needed, add more users or other groups to the selected user group.
5. In the *Feature sets* box, select or deselect the actions related to Variant Management that you want your user group to accesss.
6. Select *Save feature sets*.

> ⓘ Note
>
> See the list of all feature sets in Overview of Feature Sets.

Example of best practices when assigning feature sets to user groups

User	Permissions
Administrator	• Configures user groups. • Sets access to feature sets. • Has full access rights to all feature sets.
Process Architect	• Manages and structures the process repository, dictionary updates, and publishing. • Manages and configures dimensions and values.
Global Process Owner	• Monitors process adoption and operationl KPIs. • Communicates changes. • Manages and configures templates, their dimensions and values.

User	Permissions
Process Modeler or Local Process Owner (LPO)	• Creates and updates process models, collects feedback from domain experts. • Manages and configures variants, and their dimensions and values.

Change Access Rights

To edit access rights, you use the process for adding access rights.

To remove limitations to specific content, you need to grant full access to a folder or the dictionary first.

Remove Access Rights

To remove access rights, follow these steps:

1. In the explorer, go to *Setup* > *Manage access rights*. The user management dialog opens.
2. Open the *Access rights* tab. The tree structure shows all content of the *Shared documents* folder and of the dictionary.
3. Select the element for which you want to remove access rights. Users and their access rights are listed.
4. Choose *Remove*. If the *Remove* button isn't visible, click the parent folder in the *Inherited from* column, and remove the access right there.
5. Confirm with *Yes*.

Related Information

Manage Users and Groups

2.3 Single Sign-on Using SAML

> ⓘ Note
>
> You need an administrator account to use this function.

> ⓘ Note
>
> With SAP Signavio Process Manager version 14.6, administrators don't need SAP Signavio support anymore to configure single sign-on.

If you had already set up SSO with SAML for older versions, you must update both the IdP and the SP configuration for security reasons.

To update your configuration, follow the steps in section *Configure your IdP*.

Single sign-on (SSO) is an authentication method. When SSO is set up, users can access different applications by logging in with only one account. SAP Signavio

SAML is a standard to exchange authentication and authorization data between a service provider (SP) and an identity provider (IdP). SAP Signavio supports IdP-initiated authentication and SP initiated authentication.

SAP Signavio acts as an SP and agrees to trust an IdP to authenticate users. When a user wants to access SAP Signavio, SAP Signavio sends an authentication request to the IdP. The identity provider validates the user and generates an authentication assertion that allows the user to log in to the workspace with their credentials.

For more information, see *Enable SSO authentication using SAML*.

Just-in-Time Provisioning

When SSO using SAML is enabled, you can specify that users automatically get an account when they access SAP Signavio for the first time. This is called just-in-time (JIT) provisioning and allows users not to have to register with SAP Signavio themselves.

For JIT provisioning to work, the following conditions must be met:

- A user must be authenticated successfully with the IdP.
- The response from the IdP contains the mandatory attributes. Read more in section *Configure your IdP*.
- At least 1 unassigned license for SAP Signavio Process Collaboration Hub is available.

With JIT provisioning enabled, the following happens:

- When a user logs in for the first time, a new account is automatically created.
- When a user logs in who already has a SAP Signavio account and an IdP name ID, any IdP change on their first name, last name, and email address will be automatically updated in the SAP Signavio user management.

applies:

- A user receives a license that is specified in the IdP response, given that such a license is available in the workspace.
- A user is assigned to all groups that are specified in the IdP response, given that these user groups exist. User groups that don't exist are ignored.
- If a user is assigned to a user group that isn't included in the IdP response, the user is removed from this group.

When JIT provisioning is disabled, only users with an existing account can access the workspace. Other users will receive an error message. Read more on user management in section Manage Users and Groups.

Set up SSO using SAML

To set up SSO using SAML, you must configure the IdP and enable SSO for your workspace. Then, you can invite users.

All steps are described in detail in the following sections.

Configure your IdP

You can configure all third-party IdPs that support SAML 2.0, for example:

- ADFS 2.0/3.0
- Okta
- OneLogin

For the configuration, the SP and the IdP must exchange metadata files.

> ⓘ Note
>
> We recommend to use an IdP with multi-factor authentication enabled, particularly for administrator accounts.

Follow these steps:

1. In the explorer, click **Setup > Manage SAP Signavio Process Collaboration Hub authentication**.
   The configuration dialog opens.
2. Select *SAML 2.0 based authentication* from the drop-down list.
   The configuration dialog opens.
3. Download the IdP metadata file. To do so, click the link *Download the SAML service provider metadata* in the lower dialog area.
4. Upload this file to your IdP or configure your IdP manually with the information from the file.

In your IdP configuration, set the SAML response attributes as follows:

Attribute	Mandatory	Description
Name ID	yes	It's the primary identifier, must be unique, and doesn't change. For example, use the internal employee ID.
email	yes	Email address of a user
first_name	yes	First name of a user
last_name	yes	Last name of a user

Attribute	Mandatory	Description
signavio_licenses_v1	no	The name of the license that you want to assign to a user, for example "Enterprise Plus Edition", "Enterprise Edition" "Classic Edition", "Collaboration Hub", or "Workflow". ⓘ Note You can also assign SAP Signavio Journey Modeler licenses through SAMI. Use "Journey Modeling Standard" or "Journey Modeling Advanced". When you assign more than one license, add an `<AttributeValue>` element for each license name. Example: `<Attribute Name="signavio_licenses_v1"><AttributeValue>Enterprise Plus Edition</AttributeValue><AttributeValue>Workflow</AttributeValue></Attribute>`

Attribute	Mandatory	Description

signavio_groups_v1	no	The names of the groups that you want to assign to a user.
		Note
		The following 5 characters can't be used in group names:
		`"<>'&`
		When you assign more than one group, add an `<AttributeValue>` element for each group name. Example:
		`<Attribute Name="signavio_groups_v1"><AttributeValue>Employees</AttributeValue><AttributeValue>Sales</AttributeValue><AttributeValue>Process owners</AttributeValue></Attribute>`

If your IdP is Azure, you need to use the following attributes for licenses and groups:		
signavio_licenses_v1_azure	no	The name of the license that you want to assign to a user, for example "Enterprise Plus Edition", "Enterprise Edition" "Classic Edition", "Collaboration Hub", or "Workflow". When you assign more than one license, use a comma separated list. Example: "Enterprise Plus Edition,Workflow" Ensure that there is no space between license names. Spaces within license names are valid.

Attribute	Mandatory	Description
signavio_groups_v1_azure	no	The names of the groups that you want to assign to a user. ⓘ Note The following 5 characters can't be used in group names: **"<>'&** When you assign more than one group, use a comma separated list. Example: "modeling users,admins" Ensure that there is no space between group names. Spaces within group names are valid.

IdP configuration is complete. You can continue with enabling SSO for your workspace. Read more in the next section *Enable SSO using SAML*.

Example

Example section from a valid IdP response

```
<Subject>
                    <NameID>ID12345</NameID>
                    <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <SubjectConfirmationData
InResponseTo="ONELOGIN_6f26b11b-b290-4d2c-b79d-c46010fe686c"
NotOnOrAfter="2020-10-23T11:49:29.291Z" Recipient="https://
editor.signavio.com/api/v2/saml/v2/tenant/a41f284f4e8841b2c7f5e2af78663c0f/
login"/>
                    </SubjectConfirmation>
                    </Subject>
                    <Conditions NotBefore="2019-10-23T11:44:29.258Z"
NotOnOrAfter="2019-10-23T12:44:29.258Z">
                    <AudienceRestriction>
                    <Audience>https://editor.signavio.com/api/v2/saml/v2/
tenant/a41f284f4e8841b2c7f5e2af78663c0f/metadata</Audience>
                    </AudienceRestriction>
                    </Conditions>
                    <AttributeStatement>
                    <Attribute Name="signavio_licenses_v1">
                    <AttributeValue>Enterprise Plus Edition</AttributeValue>
                    <AttributeValue>Workflow</AttributeValue>
                    </Attribute>
                    <Attribute Name="email">
                    <AttributeValue>john.doe@signavio.com</AttributeValue>
                    </Attribute>
                    <Attribute Name="first_name">
                    <AttributeValue>John</AttributeValue>
                    </Attribute>
                    <Attribute Name="last_name">
                    <AttributeValue>Doe</AttributeValue>
                    </Attribute>
                    <Attribute Name="signavio_groups_v1">
                    <AttributeValue>Employees</AttributeValue>
```

```
                     <AttributeValue>Sales</AttributeValue>
                     <AttributeValue>Process owners</AttributeValue>
                     </Attribute>
                     </AttributeStatement>
```

Enable SSO using SAML

Before you start, you need the configuration metadata from your IdP. Read more in the previous section *Configure your IdP*.

Follow these steps:

1. In the explorer, click **Setup > Manage SAP Signavio Process Collaboration Hub authentication**.
   The configuration dialog opens.
2. Select *SAML 2.0 based authentication* from the drop-down list.
   The configuration dialog opens.
3. To enable IdP-initiated authentication, select *Enable SAML 2.0 authentication.*
   IdP-initiated authentication means that a user who logs in to the IdP must select SAP Signavio, and is then redirected to your workspace and logged in.
4. With SP-initiated authentication, a user who is logged out from SAP Signavio and tries to access your workspace, is redirected to the IdP, must log in to the IdP, and is then directed back to SAP Signavio and logged in.
   To additionally enable SP-initiated authentication, select *Allow service provider initiated authentication*.
5. For SP-initiated authentication, the initial request sent by the SP to the IdP can be signed with a certificate. If the authentication request is signed, the IdP has additional means to verify that the request was sent by the SP.
   To enable signing the authentication request, select *Sign authentication request*.
6. To enable just-in-time provisioning using SAML, select *Create new user accounts automatically*.
7. Paste the configuration metadata provided by your IdP to the field *XML Metadata*.

   > ⓘ Note
   >
   > - For certificate renewal, the federation XML file changes. For example, if the IdP certificate is renewed or updated, the metadata changes.
   > - Copy the latest federation XML into SAP Signavio when the certificate is renewed.

8. Confirm with *Save settings* and close the dialog.

Hint on links in invitation emails

SAP Signavio Process Manager users can send invitations emails to internal and external stakeholders.

If single sign-on is enabled but not enforced in your workspace, these invitations emails contain 2 web links:

- *Access using single sign-on (requires a company email account)*
  The following applies:
  - Users who are logged in to their company system are directly directed to SAP Signavio Process Collaboration Hub.
  - Logged out users need to enter their company credentials to log in.
  - New users need to register with their company email and get a SAP Signavio account.

- *Access as a guest (you will be asked to register with your name and email address)*
  The following applies:
  - Users with a guest account log in with their guest account credentials.
  - New users need to register.

Read more on the invitation features of SAP Signavio Process Manager in section Inviting Stakeholders to Comment on a Diagram.

Invite New Users by Email

If SP-initiated authentication and JIT provisioning is enabled, you can invite users to your workspace by sending them an email.

Follow these steps:

1. Get the workspace link:
   - Share a link to any content within your workspace, for example by copying the URL from your browser address bar.
   - Create a link to the workspace by adding the workspace ID as an URL parameter, for example **`https://editor.signavio.com/p/hub?t=<WORKSPACE_ID>`**
2. Paste the link to an email and send it to the users you want to log in with SSO using SAML.

Enforce SSO to Disable Login with Credentials

When SSO is enforced for your workspace, users can't log in using their SAP Signavio credentials. All users have to log in through the IdP.

If SP-initiated authentication is enabled, users are logged in when clicking a link to any content within your workspace, for example a published diagram in SAP Signavio Process Collaboration Hub, or a link that includes the workspace ID as an URL parameter.

When SSO is configured but not enforced for your workspace, the following applies:

- Users can log in through the IdP.
- Users can also log in by entering their email and password on the SAP Signavio login page.
- If SP-initiated authentication is enabled, a logged out user is always redirected to the IdP when clicking a link to content in your workspace.

> ⓘ Note
>
> When you've set up enforced SSO, make sure SSO is working before logging out from your workspace. Otherwise all users, including you, won't be able to access the workspace. To test the SSO configuration, log out and log in again with another user account.
>
> In case of problems, please contact our SAP Signavio service experts from the SAP for Me portal so they can disable this option for you.

To enforce SSO, follow these steps:

1. In the explorer, click *Setup > Edit security configuration*.
   The configuration dialog opens.
2. In the *Password policies* section, enable *Enforce SSO login*.
3. Confirm with *Save*.

2.4 Editing the Security Configuration

Here you can manage the security settings for your workspace.

To enhance IT security, you can limit the access to your workspace by filtering IP addresses. In addition, you can define password policies to enforce strong passwords.

The security settings apply to every user currently in the workspace and also to all future users.

Data Protection and Privacy

Here, you set how long personal information is kept after a user was removed from this workspace.

> ⓘ Note
>
> - For workspaces created after July 18, 2022, this setting is enabled and set to a default data retention period of 70 days.
> - For older workspaces, this setting is not automatically enabled.

You can set how long data is saved. The minimum time is seven days.

After the set time has passed, the user's personal information is irreversibly deleted from the workspace. Content the user created is not deleted. Comments, notifications, and related feed entries no longer show the user's name or email, they show **deleted user**.

While this setting is not enabled, deleted users aren't anonymized.

Set Up IP Address Filtering

> ⚠ Caution
>
> Users of the on premises edition cannot set up IP address filters.

The IP address filter allows you to define a list of trusted IP addresses that can access SAP Signavio Process Manager and SAP Signavio Process Collaboration Hub. Devices with unlisted IP addresses can't access the workspace even with a valid username/password combination. This setting can be useful, for example, if you want to restrict access to your workspace or SAP Signavio Process Collaboration Hub to one or more specific companies.

For specifying IP addresses, the following rules apply:

- The IP address filter is based on IPv4, so IPv6 addresses cannot be added to the list of trusted IP addresses.
- Only Internet IP addresses are accepted. Local area network (LAN) IP addresses can't be listed because they depend on the local network configuration.
- You must specify IP addresses in classless inter-domain routing (CIDR) notation. With the CIDR suffix, you specify whether to filter for an exact IP address or a range of IP addresses. The smaller the number after the slash, the greater the range of IP addresses.

> Example
>
> 99.123.134.246/8 –> range from 99.0.0.0 to 99.255.255.255
>
> 99.123.134.246/16 –> range from 99.123.0.0 to 99.123.255.255
>
> 99.123.134.246/24 –> range from 99.123.134.0 to 99.123.43.255
>
> 99.123.134.246/32 –> exactly 99.123.134.246

The operating administrator's IP address is added automatically, so if you are setting up the list of trusted IP addresses and are using a static IP address, you get access from your current device automatically.

To filter for IP addresses, follow these steps:

1. In the explorer, choose *Setup* > *Edit security configuration*.
2. Check Activate IP Filtering.
3. Enter a CIDR IP address and choose *Add*.
4. The IP address is added to the list of trusted addresses.
5. Save your changes.
   The IP address filter is active.

To remove an IP address from the list of trusted addresses, select the IP address and choose *Remove*.

To deactivate the IP address filtering completely, disable the option *Activate IP Filtering*.

Trusted Domains

> ⓘ Note
>
> SAP Signavio Process Collaboration Hub can only be embedded in third-party systems via iframes if trusted domains are used. If a domain not included in the trusted domains is used, web browsers don't load the page, and instead show a security violation page to the users.

To embed SAP Signavio products in an iframe using trusted domains, you have the following options:

- Use one of the public trusted domains
- Add workspace-specific trusted domains

Use Public Trusted Domains

Some common third-party tools use domains that are public trusted domains.

When you embed SAP Signavio Process Collaboration Hub in the following domains, no further action is required on your side:

- *.atlassian.net
- *.sharepoint.com
- *.force.com

Add Workspace-Specific Trusted Domains

> ⓘ Note
>
> When embedding SAP Signavio Process Collaboration Hub inside an iframe, you have to use HTTPS and cannot use any custom ports.

When you want to embed SAP Signavio Process Collaboration Hub in other third-party tools, you have to add the domains to the security configuration and adapt the URLs.

Follow these steps:

1. In the Explorer, open *Setup*> *Edit security configuration*.
2. In the section *Domain policies*, add the trusted domains.
3. Add the parameters **`<model ID>`** and **`?t=<workspace_id>`** to the URLs used for embedding.
4. To enable fullscreen mode for embedded pages, add the "fullscreen" value to the allow attribute in the iframe element.

Define a Password Policy

To enforce the use of secure passwords, you can implement a password policy. This allows you to prevent access security issues even if many users have access to your workspace.

Password policy applies whenever users set a password.

To define a password policy, follow these steps:

1. In the explorer, click *Setup > Edit security configuration*.
2. In the section *Password policies*, select the requirements that passwords have to fulfill (see list *Configuration options for password policy*).
3. Save your changes.
   The password policy is active and users need to choose a password that fulfills the password policy.

Configuration Options for the Password Policy

- *Enforce SSO login*
  Define whether users can log in using their email and password on the login page or whether to enforce SSO using SAML. Read more in section Single Sign-on Using SAML.
- *Complexity requirements*
  A password is accepted when it contains at least three of the following requirements:
  - at least one capital letter (A to Z)
  - at least one lower case letter (a to z)
  - at least one number (0-9)
  - at least one special character (!,§,$,%,&,?,#)

- *Consider user name*
  Users can't use their first or last name in a password, no matter if written in upper or lower case.
- *Consider user name (strict)*
  Users can't use three or more letters in the same order as in the user's first or last name in a password, no matter if written in upper or lower case.
- *Minimum password age*
  Users can't change a password, unless the specified number of days since the last change has passed.
- *Maximum password age*
  Users are prompted to change their password after the specified number of days has passed
  We recommend to set a maximum password age.
- *Minimum password length*
  Define the minimum length of a password. Usually, longer passwords are more secure than shorter ones.
- *Maximum password length*
  Define the maximum length of a password.
- *Password history*
  Users can't reuse passwords immediately. For example, if the number is set to 5, the last 5 used passwords can't be set as a new password.

Locked User Accounts

User accounts get locked after 10 failed log-in attempts with an incorrect password.

To unlock an account, you need to contact SAP Signavio support on the SAP for Me portal.

> ⓘ Note
>
> Accounts are only locked when using a log-in with email address and password, not when Single Sign-On (SSO) authentication is used.

Related Information

SAP for Me Service and Support

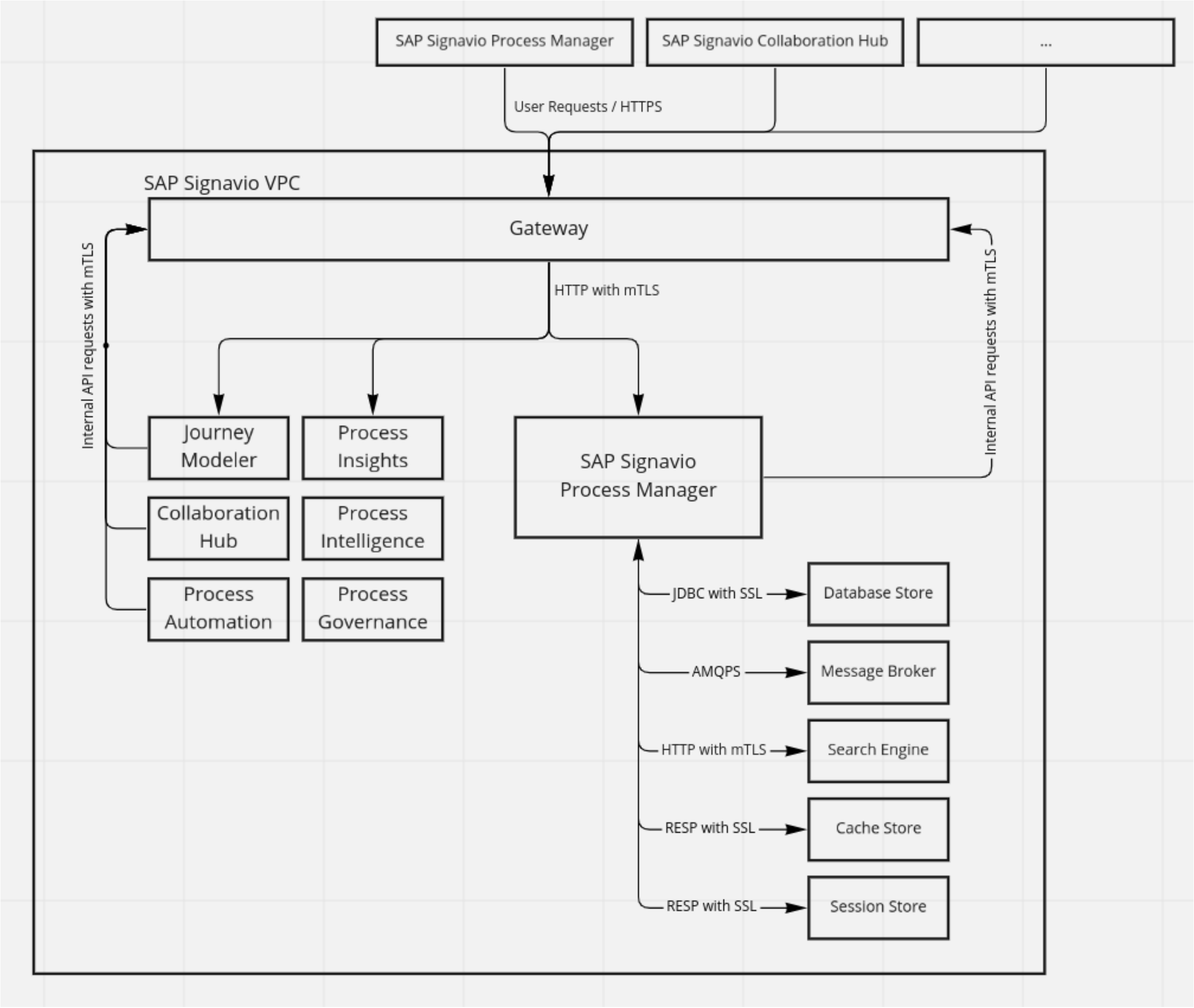
3 Session Security Protection

The session ID is unique and random, with high entropy (>64bits), preventing attackers from guessing or predicting the ID. The meaning of the session ID is stored on the server side inside the session management repository, and cannot be decoded on the client side. The session ID is stored in a cookie with the attributes `Secure` and `HttpOnly`.

`Secure` prevents the cookie transfer over unencrypted connections and prevents the stealing of the session ID through XSS attacks.

The Domain attribute `HttpOnly` instructs the web browser to only send the cookie to the origin server. Additionally, HTTP Strict Transport Security (HSTS) is used. This means the browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

4 Network and Communication Security



5 Audit log

SAP Signavio Process Manager keeps a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Audits and logs are essential for monitoring the security of your system and to track events in case of problems.

You can use the *Security Audit Log* to record changes to user data records or user removal. This log is designed for auditors who need to take a detailed look at what occurs in SAP Signavio Process Manager. You can then access this information for evaluation in the form of an audit analysis report.

The Security Audit Log provides for long-term data access. Currently there is no direct access to logs, it needs to be requested through Customer Support.

Please contact our SAP Signavio service experts from the SAP for Me portal.

You can find the following information in the Security Audit Log:

- Changes of user personal data: first and last name, telephone number and country
- Addition and removal of user from a workspace
- Addition and removal of user from a group

6 Data Storage Security

SAP Signavio Process Manager runs in a multitenant environment, with a tenant for each customer.

Customer data is therefore stored in separate tenants.

SAP Signavio Process Manager stores sensitive data such as passwords in encrypted form. Data saved in this area is encrypted using a secret key that is created explicitly for the application.

All data stored in the SAP Signavio Process Manager system is encrypted via database encryption at a disk level.

> ⓘ Note
>
> The database used by SAP Signavio Process Manager isn't accessible to you as a customer. As a result, you can't connect it to other services and any configuration can't be changed by you since this configuration is internal to the SAP Signavio Process Manager cloud application.

Data at Rest Encryption

Data stored at rest in the underlying storage is encrypted, so as are its automated backups, read replicas, and snapshots.

SAP Signavio Process Manager uses an Amazon Web Services (AWS) environment for its back end. For more information about security on AWS, see the AWS documentation .

7 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data protection and privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries.

SAP provides specific features and functions to support compliance with regard 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 should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements.

For more information regarding the use of personal data, see GDPR compliance.

7.1 GDPR Compliance

Data Subject Requests

In certain circumstances, individuals may have the following rights in relation to personal data:

- Right to access personal data.
- Right to rectify inaccurate personal data.
- Right to erase personal data.
- Right to restrict processing of personal data.
- Right to data portability.
- Right to object to processing of personal data.
- Right to withdraw consent to the processing of personal data.

If an end user of SAP Signavio products wishes to exercise rights in relation to personal data that may have been collected via, or stored within, SAP Signavio products, the end user should contact the party that is subject to the license agreement with SAP Signavio (which may be the end user's employer). If that contracting party requires additional assistance, it may contact SAP Signavio service experts from the SAP for Me portal.

> ⚠ Caution
>
> This process only catches records that are clearly connected to dedicated fields for personal data. This means, for example, if an email was typed into a text entry process documentation field, this documentation will not be considered by the data subject request since the documentation is not associated with a personal data field.

If an individual wishes to exercise rights in relation to data for which SAP Signavio acts as data controller, they should contact privacy@sap.com.

8 Security Recommendations

These recommendations help you evaluate the security of the configuration of SAP Signavio Process Manager.

> → Remember
>
> As part of the cloud shared responsibility model (restricted access), you're responsible for determining if any of these recommendations are relevant for your environment and to what extent.
>
> The security recommendations are provided as a courtesy, without a warranty, and can be subject to change. For more information, see the disclaimer.

Recommendations

Priority	Secure Operations Map	Service	Topic	Default Setting or Behavior	Recommendation	More Information	Last Updated	Index
Recommended	Authentication and Single Sign-On	Identity Authentication	Password Policy	Default authentication method to gain access to the application is username and password. Default password policies are applied if policies aren't defined for buyers or suppliers.	We recommend defining a strong password policy.	Manage Security Settings	2023-11-29	SIG-SPM-0000
Recommended	Authentication and Single Sign-On	Identity Authentication	Enforce SSO	When SSO is activated, a user still can log in using their credentials.	Enforce SSO to deactivate login with credentials. With that users can't log in using their SAP Signavio credentials. All users have to log in through the identity provider.	Single Sign-on Using SAML	2023-11-29	SIG-SPM-0001

8.1 Explanation of Table Headings

Get help understanding the table headings of the recommendations provided.

Explanation of Table Headings

Priority	Secure Operations Map	Service	Topic	Default Setting or Behavior	Recommendation	More Information	Last Updated	Index
Defines the criticality of the recommendation. For an explanation of the priority levels, see the following *Explanation of Priority* table.	The Secure Operations Map is a reference model to structure the broad area of security for content, discussions, and as a basis for a 360° view on security. For more information about the Secure Operations Map, see Security Overview as part of the *SAP Security Optimization Services Portfolio*.	Indicates the security service to which the recommendation applies.	Indicates the product area, topic, or feature to which the recommendation applies.	Describes the usage of the security setting, including any context, or default setting behavior (if available).	Defines our recommendation for this configuration.	A link to documentation that explains how you can achieve the recommendation.	The date of the last significant change.	A stable unique reference to identify the recommendation.

Explanation of Priority

Priority	Description
Critical	Exposes the system to significant risk or threatens system reliability.
Recommended	Improves the security of the landscape and significantly reduces the attack surface.
Advanced	Extends the recommendation to a higher standard. The recommendation either extends the security standards to higher level of protection or to additional areas, such as your organization-specific requirements.

9 Document History

This section provides an overview of the changes made in this SAP Signavio Process Manager security guide since March 2023.

Date	Comment
2023-03-25	Added an explanation of the table headings for the security recommendations: Explanation of Table Headings [page 35]
	Added a document history that lists changes to this guide as well as their date.

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