SAP Signavio Process Governance Security Guide

3.208

PUBLIC

Contents

1 SAP Signavio Process Governance Security Guide

In this guide, you can find information about security topics relating to SAP Signavio Process Governance. 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 Governance 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

In this section, you can find the access control user guide, information about organization settings (roles, access, groups), and authentication.

2.1 Next steps

Access control
Organization settings
Sign up and log in with SAP Signavio Process Governance

2.2 Access control

You can use access control in SAP Signavio Process Governance to restrict who can access a process, edit cases, or access specific tasks within a process. Processes and tasks default to public accessibility, which means that all users in the organization have access. When you configure access controls, you restrict access to specific users or groups.

2.2.1 Restrict access to processes

- Changes to the access rights for the process and for report creation are applied immediately.
- Changes to the access rights for cases take effect when a process is published and are not applied to existing cases. When you publish an access-restricted version of a process, all cases started before the publication stay accessible.

To apply process restrictions, follow these steps:

1. Open a process and select **Details**.
2. On the **Process details** page, open the **Options** tab, it has an **Access rights** section.
3. Click **Make this process private** to configure access control.
4. Grant permissions to users and groups.

When you make a process private, you can grant six different permissions to users and groups.

Edit process	Make changes to a process and publish new versions.
Start process	Start new cases for the process.
See process	See the process in the list of processes.
Edit cases	Work on the process' cases, by editing or completing tasks.
View cases	View the cases for the process.
Create reports	Create reports of the process.

For example, use the permission:

- **Edit process**, granted to a group, to restrict process editing to experienced process modelers
- **View process**, granted only to your own user, to hide incomplete or draft processes from other people while you create a first version
- **Start process**, granted only to your own user, so that people with **View process** and **Edit process** permission can collaborate on process modeling but cannot start cases until you publish it
- **Edit cases**, assigned to one group but not another, to allow one group to work on cases, while the other group can view their work.
- **View cases**, assigned to a group, to restrict access to cases that contain sensitive information,
- **Create reports**, granted to a business user group to allow them to analyze process metrics.

To remove all access restrictions on the process, click **Make this process public**.

2.2.2 Restrict access to user tasks

You can also restrict access to individual user tasks in a process. By default, user tasks have the access rights set for the process.
To apply user task restrictions, follow these steps:

1. Open a process and select the user task.
2. In the user task configuration panel, open the **Access Rights** tab.
3. Click **Define specific access** to configure access control.
4. Grant permissions to users and user groups:
    - **View task** - review the task and participate in discussion by adding comments
    - **Edit task** - change the task's title, assignment and due date, and create subtasks.

2.2.2.1 Example

Suppose you have a process that includes an approval, where someone from a **Managers** group must approve or reject a request from someone in the **Employees** group. You need to use the **Edit task** permission to restrict access to the approval user task, so that only managers can provide the approval.

2.3 Organization settings

> You need an administrator account to use this function.

You find the **Organization settings** in the user menu in the top right corner.
In SAP Signavio Process Governance, an organization represents a collection of users - typically a company - together with all their data. People outside your organization cannot see your organization's data. After you log in, you see all data inside one particular organization. If you belong to multiple organizations, you can switch between organizations by selecting a different organization in the user menu.

2.3.1 Edit the organization name

You can directly edit the displayed name, edits are visible after you reload the page.

2.3.2 Members

> If you use central user management in SAP Signavio Process Manager, the **Members** settings in the **Organization settings** are inactive.

Here you find the following functions:

- Adding and removing users
- Giving and revoking administrator privileges
- Adding and removing user groups
- Adding users to groups
- Inviting new users to your organization

2.3.2.1 Users

> When an organization is created with the first user, this user gets an organization administrator role by default.

The **Users** tab shows all users in your organization. You can view their email address, license type, and membership type - collaborator or administrator.
To export a CSV file with all users, click **Export all users**. For each user, the CSV files contains the following:

- User ID
- Full name
- Email address
- Admin status (true/false)

2.3.2.2 Change membership type

There are two types of users in SAP Signavio Process Governance, collaborators and administrators.
Administrators can give collaborators the administrator role.

- In the users table, click the icon  next to the user type. The user type changes.

2.3.2.3 Delete users

Administrators can delete users.
Follow these steps:

1. In the users table, click  **Remove**.
2. In the dialog, select a replacement user or activate **Select a replacement later**.
3. Confirm the removal.

Deleted users with task assignments that weren't replaced are listed in the **User off-boarding** section. Administrators are reminded weekly to specify a replacement.

2.3.2.4 User off-boarding - replace users

In this section, you see all deleted users without a replacement. You also see the open items linked to the deleted account.
When you remove users from your organization, there still could be unfinished tasks for their accounts, or the users were owners of workflows and reports. You can specify replacement users to take over. Replacement users have all necessary permissions to complete open tasks and cases, but don't inherit group memberships of the deleted users. Assignment for closed tasks is not changed for audit reasons.
To replace users, follow these steps:

1. Click **Select replacement**.
2. Select a replacement user.
3. Confirm in the dialog and click **Replace**.

Users are replaced

- in workflows: owner, assignments, candidates, default values for form fields, transition conditions, JavaScript test values, permissions
- in reports: owner, permissions
- in open tasks: assignments, candidates, permissions
- in cases: replacement users gets access to cases started *after* the replacement and implicit view on cases where the replaced users were assigned a task or were candidates for a task

Users aren't replaced

- in conditions: in custom rules in form fields and groups, in transitions (e.g. in automatic gateways), in reports
- in cases: the replacement users don't get access to cases started *before* the replacement

> Deleted users are removed from all groups. You need to manually assign replacement users to groups.

2.3.2.5 Deleting the user for SAP Signavio Process Manager integration

When you delete the user for the SAP Signavio Process Manager integration, you need to do the following:

- Set a replacement user
- Ensure that the replacement user has access to SAP Signavio Process Manager.
- Ensure that the replacement user has the same access rights to the dictionary.

Otherwise the dictionary integration no longer works.
Read more about how to set up the integration in section **Activating the Dictionary integration**.

2.3.3 Groups

The groups list shows the user groups in your organization. You can use groups to define candidates for tasks while creating the process, or to manage access rights for workflows and cases.
To create a new group, enter a group name in the text field above the group list and click **Create**.
Click a group's name to see a list of members and to add or remove members.

2.3.4 Invite a colleague

The invitations list shows pending invitations for SAP Signavio Process Governance.

1. Select a license type.
2. Enter the email address.
3. Click **Invite**.

Invited users receive an email with a link to the registration page, where they can create a SAP Signavio Process Governance user that will become a member of the organization.

2.3.5 Billing

The **Billing** tab shows your **Contract terms**:

- the number of remaining user licenses - how many more people you can add to the organization
- the license expiry date, after which you must renew your licenses to continue using SAP Signavio Process Governance.

You see a summary of your current license type.

2.3.6 Single Sign-On

Single sign-on (SSO) makes it possible to access SAP Signavio Process Governance using an existing corporate user account, so you do not have to log in to SAP Signavio Process Governance separately.

For more information, please contact our SAP Signavio service experts on the **SAP ONE Support Launchpad**.

> Users who are members of more than one organization are forced to log in using the identity provider when they are switching from an organization without SSO.

2.3.7 Workspace

2.3.7.1 Preferences

Preferences include settings that apply to the organization in general.
Time zone affects which time zone SAP Signavio Process Governance uses.
Email signature replaces the default SAP Signavio Process Governance team signature in notification emails .

2.3.7.2 Restrict process creation

Activate **Restrict process creation** to restrict the right to create processes to one user group.
Only users of the selected group have the permission to do the following:

- create new processes
- copy processes
- import processes

Users who are not members of the group but have editing rights for specific processes are still able to modify these processes.

> The transfer of processes between SAP Signavio Process Manager and SAP Signavio Process Governance is not affected by this restriction. Any modeler can transfer a process from SAP Signavio Process Manager to SAP Signavio Process Governance.

2.3.7.3 Labels

For a better overview of all processes in your organization, you can use labels to categorize processes, for example by department or status.

In the **Labels** section, you start with a set of default labels.
To add a new label, enter a new label name and click **Create label**.
Change the label color by clicking the color.

To change the label name, click .

To delete a label, click  next to the label and confirm by clicking  .

2.4 Sign up and log in with SAP Signavio Process Governance

SAP Signavio Process Governance is part of the SAP Signavio Process Transformation Suite. When you're signing up with SAP Signavio Process Governance, you are signing up with the Business Transformation Suite.

1. Go to the **SAP Signavio Process Governance login page**.
2. Click **Register a new account**.
3. Follow the steps on the screen to create your account.
4. Go to the Business Transformation Suite login page:
    - **Login page** (hosted in EU)
    - **Login page** (hosted in Australia)
    - **Login page** (hosted in US)
5. Use your account email and password to log in to the Business Transformation Suite. The launchpad opens, see section **Your launchpad** for details.

3 Session security protection

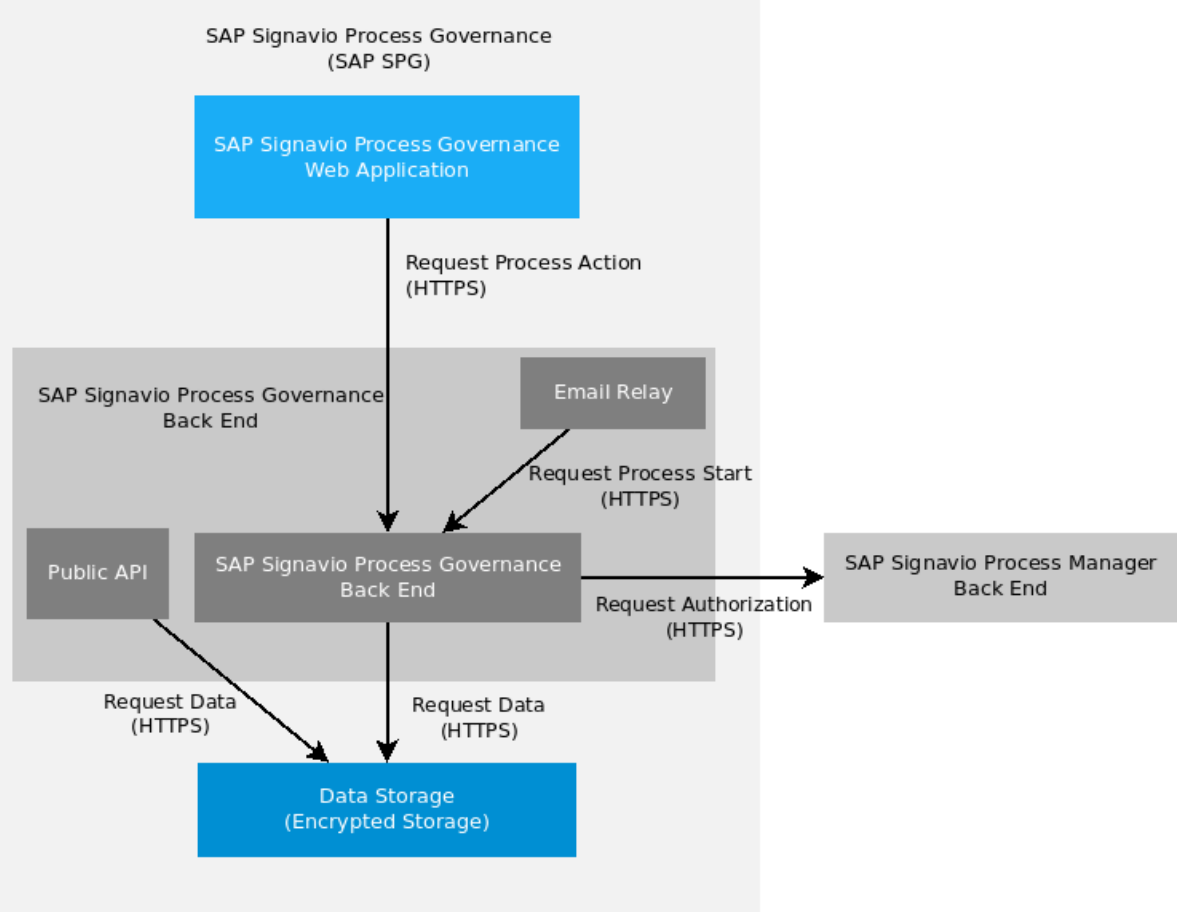
To protect network communications in which security-relevant cookies are transferred, all traffic in SAP Signavio Process Governance is served through HTTPS. The Content Security Policy is set to a strict level, this prevents JavaScript access to security session cookies.

Reference to SAP Signavio Process Manager SSO security guideline:

Single sign-on using SAML

4 Network and communication security

All data transmitted to and from components of SAP Signavio Process Governance is protected.



As shown in the figure above, all communication between the following channels uses the HTTPS protocol:

- SAP Signavio Process Governance backend and SAP Signavio Process Manager
- Email relay and SAP Signavio Process Governance backend
- Public API and SAP Signavio Process Governance backend
- SAP Signavio Process Governance backend and NoSQL Storage
- SAP Signavio Process Governance web application and SAP Signavio Process Governance backend

For information about data storage security, see section Data storage security.

5 Audit log

SAP Signavio Process Governance 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 Governance. 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 on the SAP ONE Support Launchpad.

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 an organization
- Addition and removal of user from a group

6 Data storage security

SAP Signavio Process Governance runs in a multitenant environment with a tenant for each customer. This means customer data is stored in separate tenants. SAP Signavio Process Governance can store 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 Governance system is encrypted in a NoSQL database at a disk level.

> The database used by SAP Signavio Process Governance isn't accessible to our customers. As a result, customers cannot connect it to other services and the configuration cannot be changed by our customers since this configuration is internal to the SAP Signavio Process Governance cloud application.

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.

You find details about the use of personal date here:

https://www.signavio.com/privacy/