PUBLIC
Document Version: 2026.18 – 2026-08-25

Security Guide

Content

1 SAP Datasphere Security Guide

Users with an administrator role are required to ensure the security of their SAP Datasphere tenant.

Security has always been an important element for the complete product life cycle of all SAP products, including product development, planning, and quality assurance. Like the other SAP products, SAP Datasphere was designed to fulfill the highest security standards which guarantee the safety of your data both from web attacks and from attacks in the cloud.

SAP provides capabilities to support you in implementing your requirements and concepts of security and data protection within the SAP Datasphere system landscape. On your side, you need to make sure to:

- Create and assign appropriate roles to your users. See Managing Roles and Privileges.
- Set up a secure data integration to the systems to which you connect to access data. See Integrating Data via Connections.

1.1 Cloud Network and Communication Security

SAP Datasphere supports encrypted communication for network communication channels.

We recommend using encrypted channels in all cases where your network isn't protected by other security measures against attacks such as eavesdropping, for example, when your network is accessed from public networks.

The following network communication channels are used by SAP Datasphere:

- Secure communication with SAP HANA using a client supporting JDBC/ODBC.
  This is limited to one use case: full access to an open SQL schema of the space.
  Separate users are available in *Space Management* for every open SQL schema. These users are considered "technical users". There is exactly one user for every open SQL schema.
  Basic authentication is supported for these technical users. Unencrypted connections to the database are not accepted.
- A channel used for modeling and administration via the SAP Datasphere web UI. This channel is used by business users and administrators who authenticate against an identity provider.
- Secure communication between SAP Datasphere and its command line interface, `datasphere`.
  The command line interface, `datasphere`, communicates with the SAP Datasphere tenant through https. Connections are protected using TLS/SSL and the recommendation is to use OAuth clients which don't require a passcode for each command issued via `datasphere`.

1.2 Identity Provider Settings

One identity provider for both SAP Datasphere and SAP Analytics Cloud.

SAP Datasphere and SAP Analytics Cloud share the same authentication mechanism. In your tenant, choose *My Products* , go to *Analytics* and then change the identity provider settings there. Once changed, you can use that identity provider to logon to SAP Datasphere as well.

> **Note**
>
> Any tasks (for instance, remote table replication or view persistency tasks) scheduled before you change the IdP configuration might fail to start. For more information about the issue and how to solve it, refer to the SAP Note 3089828

For more information on the identity provider settings, please see Enabling a Custom SAML Identity Provider in the SAP Analytics Cloud Help documentation.

For further information on using your SAP Cloud Platform Identity Authentication service tenant as an identity provider or a proxy to your own identity provider to host your business users take a look at Manually Establish Trust and Federation Between UAA and SAP Cloud Platform Identity Authentication Service in the SAP Cloud Platform documentation.

1.3 Password Policy

The passwords of database users are subject to certain rules. These rules are defined in the password policy.

Required role to configure the password policy: DW Administrator.

The password policy is configured in the *Configuration* page under *Security* and applied to your database user by either editing an exiting user or when creating a new user.

Database Password Policy

Configuration Parameter	Additional Information
Password Expiration	The number of days for which the initial password or any password set by a user administrator for a user is valid. To see how to configure the expiration date for database users take a look at Set a Password Policy for Database Users.

1.4 User Management

It is often necessary to specify different security policies for different types of users.

In SAP Datasphere, we differentiate between an application users that can access the SAP Datasphere web user interface (UI) and database users that can access the underlying SAP HANA database.

- Application Users [page 5]
- Database Users [page 5]
- SAP BW Bridge Users [page 8]

1.4.1 Application Users

The application user represents an actual user in SAP Datasphere and can be assigned as a member to a space.

User Type	Description	Additional Information
Application User	Role required to create the user: DW Administrator Role required to assign the user to a space: DW Space Administrator Created through the user interface under *Security* → *Users*. The user is added as a member within a space. Each user can be assigned with pre-defined roles or assigned to custom roles.	• Managing SAP Datasphere Users • Managing Roles and Privileges

1.4.2 Database Users

The database user is a technical user in SAP Datasphere that can access the underlying SAP HANA database.

SAP Datasphere provides two different database user types.

Database User on Space-Level

User Type	Description	Additional Information
Database User	Required role to create: DW Space Administrator Created and edited through the user interface under *Space Management* → <Space Name> → *Database Access* → *Database Users*. Different privileges can be assigned and combined when creating this user: • **Write on Open SQL schema** Creates an open SQL schema and the user is granted the `public` role. The database user is the owner and has read and write privileges on this schema. Possible use-case: Connects external tools and pulls data The credentials of this user are shown in the UI when creating the schema and are not stored in SAP Datasphere. Resetting the password is possible by using the UI to edit the database user. • **Read on space schema** Database users can only read data from the views stored in the space which have the property *Expose for Consumption* enabled (see Exposing Data For Consumption). They cannot read data from tables and views that are not exposed for consumption. Also, database users can read only from the Open SQL schema, the space schema (if the option "Enable Read Access (SQL)" has been selected when creating the database user) and some technical spaces (such as SYS or SYS_BI). > **Note** > However, when a space is defined as a monitoring space (see Configure Monitoring), database users have extended read capabilities on all schemas and tables. Possible use-case: Connects external tools and pushes data An option is provided to allow this user to additionally grant the `select` privilege to other users. Connects to an HDI container (ingesting or exposing to an HDI container).	• For more information on the public role, see Predefined Database (Catalog) Roles. • Create a Database User • Exchanging Data with SAP HANA for SQL Data Warehousing HDI Containers

Database User on Tenant-Level (Extended Capabillities)

User Type	Description	Additional Information
Database Analysis User Read access on the underlying SAP HANA database	Required role to create: DW Administrator Created and edited through the user interface under *Configuration*→ *Database Access* → *Database Analysis User*. Connects to the SAP HANA Cloud database to analyze, diagnose and solve database issues. Can be set to expire automatically making the user inactive. Can read all space data, SAP HANA monitoring views, traces, reproduce issues and use `explain plan`. **Note** You should only create a database analysis user to resolve a specific database issue and then delete it immediately after the issue is resolved (see Create a Database Analysis User to Debug Database Issues). This user can access all SAP HANA Cloud monitoring views and all SAP Datasphere data in all spaces, including any sensitive data stored there. **Note** All actions of the database analysis user are logged in the `ANALYSIS_AUDIT_LOG` view, which is stored in the space that has been assigned to store audit logs (see Logging Read and Change Actions for Audit). Audit logs can consume a large quantity of GB of disk in your SAP Datasphere tenant database. The audit log entries for database analysis users are kept for 180 days, after which they are automatically deleted. You can also manually delete the audit logs to free up disk space (see Monitor Read and Change Actions with Audit Logs). Also, a database analysis user can be automatically deactivated due to a large amount of disk storage consumed by audit logs (see Create a Database Analysis User to Debug Database Issues).	Create a Database Analysis User to Debug Database Issues

User Type	Description	Additional Information
Database User Group Administrator Read and write access on the underlying SAP HANA database	Required role to create: DW Administrator Created and edited through the user interface under *Configuration*→ *Database Access* → *Database User Group*. Isolated environments that offer additional capabilities to work on the SAP HANA Cloud database without compromising on security. The administrator of the group is automatically generated when creating the user group. Creates SQL users, creates schemas, performs DDL, DML and uses SQL with additional capabilities. Can be launched via SAP HANA database explorer.	Creating a Database User Group

1.4.3 SAP BW Bridge Users

For SAP BW bridge, application users for SAP BW bridge and for SAP Datasphere.

User Type	Description	Additional Information
SAP Datasphere Application User	Role required to create the user: DW Administrator Role required to assign the user to a space: DW Space Administrator Created through the user interface under *Security* → *Users*. The user is added as a member within a space. Each user can be assigned with pre-defined roles or assigned to custom roles.	• Managing SAP Datasphere Users • Managing Roles and Privileges
SAP BW bridge Application User	Role required to create the user: SAP_BR_ADMINISTRATOR_DWC Created in the SAP BW Bridge Cockpit	Creating Users

1.5 Authorizations and Roles

SAP Datasphere uses the space concept to ensure data governance.

Authorizations on Data-Level

Authorization is managed through the space concept meaning artifacts such as tables, views or stories as well as data in a particular space are only visible for users assigned to that space. On the other side, users assigned to a particular space have access to all artifacts and data of that space.

Spaces partition data into areas of responsibility and authority. This combined nature of data residence and data responsibility needs to be taken into account when creating an authorization concept.

Authorizations and Roles on Application-Level

Application-level authorizations for business users and administrators are maintained in *Security* > *Roles* and assigned to users in *Security* > *Users*. The roles determine which parts of the UI the assigned users are allowed to access and what the users are allowed to do in SAP Datasphere.

Related Information

Managing SAP Datasphere Users
Managing Roles and Privileges

1.5.1 Data Access Control

Data access controls allow you to apply row-level security to your objects. When a data access control is applied to a data layer view or a business layer object, the rows of data contained in the object are filtered based on the specified criteria.

Your criteria are defined in a table or view that lists SAP Datasphere user IDs (in the form required by your identity provider) and assigns them to one or more criteria.

For more information on creating and applying Data Access Controls see Securing Data with Data Access Controls.

1.6 Audit Logging

Audit logs are records of read or change actions performed in the database. They allow you to see who performed which action at which point in time.

Space Administrators can enable audit logs for read or change actions in their space. For more information, see Logging Read and Change Actions for Audit.

Administrators can then get an overview of space audit logs and delete them if needed (for example to free up disk space). You analyze audit logs by assigning the audit views to a space and then work with them in a view in the Data Builder. For more information, see Monitor Read and Change Actions with Audit Logs.

1.7 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.

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

> ⚠ Caution
>
> The extent to which data protection is supported by technical means depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Personal Data in SAP BDC Data Products

The personal data tags are displayed in the following editors where the object is either a data product entity or an object consuming data from a data product entity:

- Remote tables - See Review and Edit Imported Table Properties.
- Local tables - See Creating a Local Table.
- Graphical views - See Creating a Graphical View.
- SQL views - See Creating an SQL View.

> **Note**
>
> Personal data tracing is not supported for SQL views with language *SQLScript (Table Function)*.

- Task Chain - See Creating a Task Chain.

For more information, see Modeling with Personal Data.

Data Protection and Privacy when Using Data Marketplace

Currently, Data Marketplace does not provide the technical features to compliantly include personal data into your data products. For the moment, SAP requires you to not use personal data in your products or to anonymize personal data before transferring it to third parties.

Personal data covers 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. Natural persons can be identified directly based on, for example, names, phone numbers, e-mail addresses, postal addresses, user IDs, tax and social insurance numbers or indirectly through a combination of any other information.

Use of Customer Specific Encryption Keys (CSEK) - Data stored in SAP Datasphere is encrypted with CSEK. Be aware that if consumers download your data products into their own SAP Datasphere tenant, they will use the data that is replicated and encrypted with the consumers' own CSEK.

1.7.1 Glossary

The following terms are general to SAP products. Not all terms may be relevant for this SAP product.

Term	Definition
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Business purpose	The legal, contractual, or in other form justified reason for the processing of personal data to complete an end-to-end business process. The personal data used to complete the process is predefined in a purpose, which is defined by the data controller. The process must be defined before the personal data required to fulfill the purpose can be determined.

Term	Definition
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Data subject	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.
Deletion	Deletion of **personal data** so that the data is no longer available.
End of business	Defines the end of active business and the start of residence time and retention period.
End of purpose (EoP)	The point in time when the processing of a set of personal data is no longer required for the primary business purpose, for example, when a contract is fulfilled. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorizations (for example, tax auditors).
End of purpose (EoP) check	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization, for example, tax auditors.
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.
Purpose	The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.

Term	Definition
Residence period	The period of time between the end of business and the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Retention period	The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.
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, trade union membership, 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
Technical and organizational measures (TOM)	Some basic requirements that support data protection and privacy are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and privacy and require appropriate TOMs, for example: • **Access control:** Authentication features • **Authorizations:** Authorization concept • **Read access logging** • **Transmission control / Communication security** • **Input control / Change logging** • **Availability control** • **Separation by purpose:** Is subject to the organizational model implemented and must be applied as part of the authorization concept.

1.7.2 Personal Data Record

Data subjects have the right to receive information regarding their personal data undergoing processing.

There are different kinds of data which might contain personal information about a dedicated person or user.

- Transactional- and masterdata as such can contain personal data.
  To provide a personal data record, an understanding of the data model and corresponding semantics is required. As the owner of the data model, the customer is responsible to implement this feature. This can be done by defining suitable views collecting the personal data of the respective data subjects. These views can be used as a basis for information reports built with an analytics frontend, such as SAP Analytics Cloud.
- During creation of data models in SAP Datasphere, the name of the user is persisted (person responsible for the creation or modification). This personal data can be retrieved from the SAP Datasphere *Repository Explorer*.

1.7.3 Deletion 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.

If there is no longer a legitimate purpose that requires the use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted 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.

> **Note**
>
> Note that reporting on an aggregated layer can ease the handling of personal data with respect to deletion. Aggregated storage of historical data without any references to persons allows you to more easily delete data in upstream layers.

Being a data warehouse, SAP Datasphere is a secondary persistence receiving data from a leading system. Consequently, all deletions done for data protection and privacy reasons are also done in the source system and the deletion can be propagated to SAP Datasphere using a delete-and-reload pattern: First do the required deletion in the source system, then delete all data in the corresponding SAP Datasphere tables and replicate from the source system again.

To delete, see Creating a Table.

1.7.4 Cookies

Cookies management

When log on to SAP Datasphere, session cookies are stored for authentication purpose and are deleted when the session is closed. Additional persistent cookies might be used to store the most recent choices for content language and user interface language.

1.8 Sensitive Data

Sensitive data must be protected against unwanted disclosure.

The technical names that you create for SAP Datasphere objects can be displayed within SAP Datasphere as well as in other SAP products that integrate with SAP Datasphere. We recommend that you do not include any sensitive business or personal data in technical names.

For information on rules and restrictions that apply to the technical names of objects, see Rules for Technical Names.

1.9 Data Encryption at Rest

When using SAP Datasphere, customers' data, metadata, logs and backups are all encrypted at rest.

Your data are encrypted using customer-specific encryption keys. Each of these databases storing customers' data is encrypted with one single customer-specific encryption key:

- SAP Datasphere database (for runtime)
- SAP HANA Cloud, Data Lake (data lake relational engine and data lake files in the object store). See SAP HANA Cloud, Data Lake Welcome Guide.
- SAP BW bridge

All customers' metadata and configuration information are stored in a shared database instance which is managed by SAP. Each of these components is encrypted with one single encryption key:

- SAP Datasphere repository (such as design-time artifacts of modeled objects, users, list of favorite files and catalog metadata)
- Tenant configuration parameters
- Runtime artifact metadata (data flow metadata)
- Schedules of recurring tasks
- Users, roles and activities
- Data Marketplace (data product descriptions and other metadata, published samples and logos)

Controlling Access to Your SAP Datasphere Database and the Object Store with a Customer-Managed Keys (CMK)

If you need to control the access to your SAP Datasphere database or the object store, you can create a Customer-Managed Key (CMK) using SAP Key Management Service (KMS) and ask SAP to encrypt the database or the object store with the new key.

> ⚠ Caution
>
> Your database or object store can be encrypted either by an SAP generated key (using a customer-specific encryption key) or by a customer-managed key (using a CMK). Once you've decided to use a CMK to

control your database or object store, you cannot go back to using a customer-specific encryption key. Also, once you've created a CMK, you cannot change its key ID.

First, check the key requirements and the region availability of the SAP Key Management Service (see SAP HANA Database Key Management System in the *SAP HANA Cloud Administration Guide*). Once you've created the encryption key, an S-user must ask SAP to enable the key for the SAP Datasphere tenant by creating a ticket, as described in SAP Note 3368616.

You'll be able to enable, disable (temporarily) or delete (permanently) the key. If you disable the key, the SAP HANA Cloud database is stopped and unavailable to users. When users log into SAP Datasphere, they can see this message in the top banner: "The run-time database is overloaded or unavailable and certain features are disabled. If the connection isn't automatically restored shortly, open a support ticket."

1.10 System Backup and Recovery

SAP Datasphere's backup and recovery uses the SAP HANA Cloud service resiliency layer in the case of a disaster caused by factors within SAP's control. SAP is not responsible for recovery of customer data lost as a result of the customer's actions, including accidental deletion of a space or data resulting from inattentiveness or a failure to follow instructions to safeguard their data.

SAP Datasphere has safeguards in place to guard against the accidental deletion of data, including pop-ups and windows to confirm the customer's instructions to delete data. We encourage the customer to train their administrators accordingly and to ensure other good practices to prevent the accidental or inadvertent deletion of data.

> ⓘ Note
>
> You can reuse the objects (but not the data) that have previously been exported to another SAP Datasphere tenant (see Transporting Content Between Tenants and Importing and Exporting Objects in CSN/JSON Files).

SAP Datasphere is ISO 27001 certified, see SAP Trust Center.

For information about SAP Datasphere Service Level Agreement, see SAP Trust Center.

For information about SAP data centers, see SAP HANA Cloud data centers.

For information about SAP Datasphere regional data center availability, click the *Pricing* tab in the SAP Discovery Center.

1.11 Compliance Standards

Compliance standards for SAP Datasphere.

SAP Datasphere is compliant with:

- ISO/IEC 27001 Security Management System

- ISO/IEC 22301 Business Continuity Management System
- SOC 1 Type 2
- SOC 2 Type 2
- STAR Certification: ISO/IEC 27001:2013
- CSA STAR, CCM version 3.0.1
- EU Cloud CoC European Data Protection Code of Conduct for Cloud Service Providers ('EU Cloud CoC') in its version 2.11 ('v2.11')

For more information, see the SAP Trust Center.

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