PUBLIC
Document Version: 2021.22 – 2021-10-19

Security Guide

THE BEST RUN SAP

Content

1 SAP Data Warehouse Cloud Security Guide

The SAP Data Warehouse Cloud Security Guide is the entry point for all information relating to the secure operation and configuration of SAP Data Warehouse Cloud.

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 Data Warehouse Cloud 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.

Some of the most important security focus areas are listed in the following interactive image:

- Authorizations and Roles [page 9]
- User Management [page 5]
- Data Protection and Privacy [page 11]
- Identity Provider Settings [page 4]
- Cloud Network and Communication Security [page 4]

SAP provides capabilities to support you in implementing your requirements and concepts of security and data protection within the SAP Data Warehouse Cloud 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 Connecting to Sources.

1.1 Cloud Network and Communication Security

SAP Data Warehouse Cloud 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 Data Warehouse Cloud:

- 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 Data Warehouse Cloud web UI as well as for doing analytics using SAP Analytics Cloud (for SAP Data Warehouse Cloud tenants that were initially provisioned prior to version 2021.03). This channel is used by business users and administrators who authenticate against an identity provider.
- Secure communication between SAP Data Warehouse Cloud and its command line interface, `dwc`.
  The command line interface, `dwc`, communicates with the SAP Data Warehouse Cloud tenant through https. Connections are protected using TLS/SSL and the user must supply a single-use passcode for each command issued via `dwc`.

1.2 Identity Provider Settings

One identity provider for both SAP Data Warehouse Cloud and SAP Analytics Cloud.

SAP Data Warehouse Cloud 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 Data Warehouse Cloud as well.

> **i 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 Configuring Password Policies.

1.4 User Management

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

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

- Application Users [page 6]
- Database Users [page 6]

1.4.1 Application Users

The application user represents an actual user in SAP Data Warehouse Cloud 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 Data Warehouse Cloud Users • Managing Roles and Privileges

1.4.2 Database Users

The database user is a technical user in SAP Data Warehouse Cloud that can access the underlying SAP HANA database.

SAP Data Warehouse Cloud 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 Data Warehouse Cloud. Resetting the password is possible by using the UI to edit the database user.
	• **Read on space schema**
	The user can read the data that has been exposed.
	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.
		• Database Access
		  ○ Creating a Database User
		  ○ SAP HANA Cloud Deployment Infrastructure (HDI) Container

Database User on Tentant-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`.	• Analyzing and Diagnosing Database Errors • Database Analysis User
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 Database User Groups

1.5 Authorizations and Roles

SAP Data Warehouse Cloud 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 Data Warehouse Cloud.

Related Information

Managing SAP Data Warehouse Cloud 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 Data Warehouse Cloud 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 Data Access Controls.

1.6 Audit Logging

Auditing allows you to monitor and record selected actions performed in SAP Data Warehouse Cloud, providing you with visibility on who did what (or tried to do what) and when.

Logging of changes and logging of read access can be configured independently of each other. Both logs are implemented using the same mechanism, so the following section applies to logging of changes as well as the logging of read access.

Audit Logging of Customer-Owned Data within Spaces

1. You can enable auditing of SAP Data Warehouse Cloud objects for read and change operations on space-level in *Space Management* > *<Your Space>* > *Edit Space* > *Auditing*. You can set the retention time in days. The default and minimum retention time is 7 days and the maximum retention time is 10 000 days. If auditing has been enabled, entries of all SAP Data Warehouse Cloud related objects are saved in an SAP HANA audit log. These logs don't include the objects of the database access schemas, like open SQL schemas, for example.

   > **i Note**
   >
   > If you choose to enable audit logs, be aware that they can consume a large amount of storage in your SAP Data Warehouse Cloud tenant database, especially when combined with long retention periods.

2. For individual database schemas, you can enable auditing for read and change operations in *Space Management* > *<Your Space>* > *Edit Space* > *Data Access* > *Database User* > *Edit*. The retention time can be defined per schema.

   > **i Note**
   >
   > **Data Lake**
   >
   > Please note, that the statements issued via the execute-procedure for data lake are currently not audited in SAP Data Warehouse Cloud.

As a result, SAP HANA policies are created for the schemas of the space.

The policy names of the SAP Data Warehouse Cloud administered objects are:

- DWC_DPP_<space name>_READ
- DWC_DPP_<space name>_CHANGE

Viewing Auditing Logs

1. Choose a space that will contain the logs:

   Go to → > *Configuration*. Here you can enable to save and later display the audit logs directly in a certain space. Choose a space from the drop-down list. To configure this setting, you need the audit configuration

authorization. We recommend to create a dedicated space for audit logs, as you might not want all users to view sensitive data.

2. Reading audit logs:
   The audit logs are saved as external data, for example, as a view. You can select these audit logs in the *Data Builder*.
   - The data is located in the `AUDIT_LOG` view of the `DWC_AUDIT_READER` schema.
   - The audit logs of the database analysis user are saved separately in the `ANALYSIS_AUDIT_LOG` view.
   - To view the audit policies and the number of audit log entries, you can use the view `AUDIT_LOG_OVERVIEW` in the schema `DWC_AUDIT_READER`.

Logs of Changes to Design-Time Object and Settings

Changes of modeling objects (spaces, tables) as well as changes to system configurations are logged in *Security* > *Activities*.

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.

> **i** 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.

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.
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.

Term	Definition
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.
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

Term	Definition
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 Data Warehouse Cloud, the name of the user is persisted (person responsible for the creation or modification). This personal data can be retrieved from the SAP Data Warehouse Cloud *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.

> **i 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 Data Warehouse Cloud 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 Data Warehouse Cloud using a delete-and-reload pattern: First do the required deletion in the source system, then delete all data in the corresponding SAP Data Warehouse Cloud tables and replicate from the source system again.

Deleting data is explained in the SAP Data Warehouse Cloud Modeling Guide at Creating a Table (step 10).

1.8 Compliance Standards

Compliance standards for SAP Data Warehouse Cloud.

SAP Data Warehouse Cloud is compliant with:

- ISO/IEC 27001 Security Management System
  For more information, see Information Security Management System.
- ISO/IEC 22301 Business Continuity Management System
  For more information, see Business Continuity Management System.
- SOC 1 Type 2
  For more information, see SAP Business Technology Platform SOC 1 (ISAE3402) Audit Report 2021 H1.
- SOC 2 Type 2
  For more information, see SAP Business Technology Platform SOC 2 Audit Report 2021 H1.
- STAR Certification: ISO/IEC 27001:2013
  For more information, see STAR Registry Listing for SAP Business Technology Platform .
- CSA STAR, CCM version 3.0.1
  For more information, see SAP Business Technology Platform CSA STAR Certificate.
- 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 SAP Business Technology Platform EU Cloud CoC.

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 a 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