PUBLIC
Document Version: 2026.11 – 2026-05-20

SAP Datasphere Security Recommendations

Content

1 SAP Datasphere Security Recommendations. 3

1 SAP Datasphere Security Recommendations

These recommendations help you evaluate the security of the configuration of SAP Datasphere services in your landscape.

> → 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 may be subject to change. For more information, see the disclaimer.

See Explanation of Table Headings in the *SAP Business Technology Platform (SAP BTP)* documentation.

Security Recommendations

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
SAP Datasphere	Recommended	Security Monitoring and Forensics	Audit Data	The default and minimum retention time for audit log entries is 7 days, and the maximum retention time is 10 000 days. Furthermore, be aware that when you delete a space, all audit logs entries generated for the space, including audit log entries related to any Open SQL schema or HDI container associated with the space, will be permanently deleted.	Export audit log entries before they are deleted. Likewise, before deleting your space, you may want to export the audit log entries generated for your space.	Logging Read and Change Actions for Audit	2023-07-26	DS-0001

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
SAP Datasphere	Critical	Audit and Fraud Management	Audit Data	By default, audit logs are not enabled for spaces as they can consume a large amount of storage in your SAP Datasphere tenant. If users with the DW Space Administrator role have enabled audit logs to be created for their space, read and change actions (policies) are recorded. Users with the DW Administrator role can then get an overview of all audit logs and analyze who did what and when in the database. The default and minimum retention time of audit logs is 7 days and the maximum retention time is 10000 days. To enable audit logs via the command line: enter the audit logging policy for read and change operations and the number of days that the logs are retained. you can retain logs for any period between 7 and 10000 days. Default values: false, 30, false, 30	If you handle personal data in your tenant, we recommend that you enable audit logs to help comply with General Data Protection Regulation (GDPR). Users with the DW Space Administrator role can enable audit logs for their space in the space details page. You can also enable audit logs via the command line. Users with the DW Administrator role can then monitor the read and change actions performed in the database with audit logs, and see who did what and when.	Logging Read and Change Actions for Audit Monitor Database Operations with Audit Logs The Space Definition File Format	2023-07-26	DS-0002
SAP Datasphere	Critical	User and Identity Management	Authentication	The password policy applies only to database users where the *Enable Password Policy* property is selected.	Users with the DW Administrator role should set a password policy to cause database user passwords to expire after a specified number of days. The recommended maximum validity for non-privileged users is 90 days.	Set a Password Policy for Database Users	2023-07-26	DS-0003
SAP Datasphere	Recommended	User and Identity Management	Authentication	You can reset a database user password via the command line.	For security reasons, specify to receive the new password in an output file.	Manage Spaces and Space Access via the Command Line	2023-07-26	DS-0004

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
SAP Datasphere	Critical	Network Security	Encryption	SAP Datasphere supports encrypted communication for network communication channels. To enable a secure SSL/TLS-based connection for a connection type that supports remote tables but doesn't use a Data Provisioning Agent, you need to upload a server certificate to SAP Datasphere.	Use 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. Upload server certificates to enable secure SSL/TLS-based connections to certain sources.	Cloud Network and Communication Security Manage Certificates for Connections	2023-07-26	DS-0005
SAP Datasphere	Critical	Roles and Authorization	Authorization	For security reasons, all external connections to your SAP Datasphere instance are blocked by default.	Control the range of external public IPv4 addresses that get access to the database of your SAP Datasphere by adding them to an allowlist.	Manage IP Allowlist	2023-07-26	DS-0006
SAP Datasphere	Advanced	Data Privacy and Protection	Data Privacy	By default, SAP Datasphere keeps track of objects you've accessed, so that you can quickly locate those objects or files again	Keep the object tracking on. Clicking the *Manage Settings* button opens the *Settings* dialog for your account where you can enable or disable tracking and optionally clear previously tracked data. In addition, you can always click your user icon in the shell bar, select *Settings*, and then select the *Privacy* setting option to change profile settings.	Changing SAP Datasphere Settings	2023-07-26	DS-0007
SAP Datasphere	Recommended	Security Hardening	Session Management	By default, the session timeout is set to 3600 seconds (1 hour). The minimum value is 300 seconds, and the maximum value is 43200 seconds.	Set the amount of time before a user session expires if the user doesn't interact with the system. The recommended time frame is 3600 seconds (1 hour).	Administration Apps and Tools	2023-07-26	DS-0008
SAP Datasphere	Recommended	Security Monitoring and Forensics	Authorization	You can import analysis authorizations defined in SAP BW and SAP BW/4HANA systems into SAP Datasphere to provide row-level protection for data imported from these systems.	The report generating the permissions table in SAP BW/4HANA should run at least once a day and the remote table in SAP Datasphere is kept in remote (federated) access to ensure that it is always up-to-date. If you decide to replicate the permissions table, you should schedule at minimum a daily refresh.	Import SAP BW and SAP BW/4HANA Analysis Authorizations	2023-07-26	DS-0009

> **Note**
>
> In the *Configuration & Security Analysis* app of SAP Cloud ALM, you can view the following security settings: index DS-0001, DS-0002, DS-0003, and DS-0008. For each security setting index, you can view the value

used and, specifically for DS-0003 and DS-0008, whether the value matches the recommended value. See Configuration & Security Analysis in the *SAP Cloud ALM - Application Help* and Configuration & Security Analysis – Content on the *SAP Cloud ALM for Operations Expert Portal*.

For more information on SAP Datasphere security, see SAP Datasphere Security Guide.

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