PUBLIC
SAP BW/4HANA 2023 SPS06
2025-09-01

Security Guide SAP BW/4HANA

THE BEST RUN SAP

Content

1 Security Guide SAP BW/4HANA

Use

> ⚠ Caution
>
> This guide does not replace the administration or operation guides provided for productive operations.

Target Group

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. These guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why is Security Important?

With the increasing use of distributed systems and the Internet for managing business data, security requirements are also becoming more prominent. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. It is very important that user errors, negligence, or attempted manipulation do not result in loss of information or affect processing time. These security requirements also apply to SAP BW/4HANA. We have provided this security guide to help you to make SAP BW/4HANA more secure.

SAP Business Warehouse integrates, transforms, and consolidates data from all areas of an enterprise so that it can then provide this information for analysis, interpretation and distribution. This includes confidential corporate data, such as personal data from personnel administration. This data forms the basis of decisions and target-oriented actions in all enterprise areas. Secure data access and data integrity are therefore of paramount importance.

The following examples illustrate some of the threats that the SAP BW/4HANA system can be exposed to:

- Attacks from the Internet or intranet when using Web services
- Infringement of data protection guidelines as a result of unauthorized access to personal data

About This Document

This security guide provides an overview of all security-relevant information for SAP BW/4HANA.

Important Security Information

SAP BW/4HANA is based on the Application Server for ABAP. See http://help.sap.com/nw75 in the *Security Guide*. The security guide for SAP BW/4HANA describes additional security information or information that differs from the ABAP application server.

More Information

Content	Link
List of available SAP Security Guides	Services & Support
Community	http://scn.sap.com/community/security
Relevant SAP Notes	http://service.sap.com/securitynotes
Released platforms	http://service.sap.com/pam
SAP Solution Manager	http://service.sap.com/solutionmanager

2 User Administration and Authentication

Use

SAP BW/4HANA uses the user administration and authentication mechanisms from the Application Server for ABAP. The security recommendations and guidelines for user administration and authentication described in the Security Guide for Application Server ABAP therefore also apply to SAP BW/4HANA. In addition to these guidelines, we have included information about user administration and authentication that specifically applies to SAP BW/4HANA.

2.1 User Management

User Management for SAP BW/4HANA uses the mechanisms - such as tools and user types - contained in the ABAP.

For more information, see the *User Management* section in the Security Guide for SAP NetWeaver.

Users

Standard users that are created when the system is installed

More information: Protecting Special Users.

> ⚠ Caution
>
> Change initial passwords after installation to prevent misuse of standard users.

Users in SAP BW/4HANA

The following table provides an overview of additional users required in SAP BW/4HANA: These users do not form part of the standard delivery and do not have default passwords.

System	Users	Type	Description
SAP BW/4HANA	Database Users	Database Users	You can find information about database users in the Security Guide for SAP HANA.

SAP BW/4HANA	Background users in SAP BW/4HANA	Technical User	The background user in SAP BW/4HANA is used for communication with the SAP BW/4HANA source systems, for the extraction of data, and for background processes in SAP BW/4HANA. You create the background user in Customizing in SAP BW and assign the user a password (under *Automated Processes* > *Create User for Background Processes*). The system prompts the user to enter a background user password when connecting to the source system. The authorization profile for the background user is S_BI-WHM_RFC (see Authorization Profiles for Background Users).

SAP Source System	Extraction Users in the SAP Source System	Technical User	The background user in the SAP source system is used for communication with SAP BW/4HANA and for data extraction. If you connect an SAP source system to SAP BW/4HANA, the background user is created in the source system. You can create the user directly in the source system in user maintenance. In Customizing, you can enter a name in the Implementation Guide to use as the default name for the background user when connecting a new source system (under *Connections to Other Systems* > *Connections Between SAP Systems and BW Systems* > *Maintain Proposal for Users in the Source System (ALE Communication)*). If you are using a BW system as the source system, SAP recommends creating the background user for BW and the background user for the (BW) source system separately. The authorization profile for the background user in the source system is S_BI-WX_RFC (see Authorization Profiles for Background Users).

SAP BW/4HANA	Administrator	Individual User	The administrator in SAP BW/4HANA is responsible for connection to source systems, loading metadata and for the implementation of BW statistics. S/he develops the data model and plans and monitors the processes in SAP BW/4HANA (such as the loading process). **See also:** Authorization Profiles for Working with the Data Warehousing Workbench
SAP BW/4HANA	Authors and Analysts	Individual User	Authors and analysts require advanced analysis functionality and the ability to perform special data analysis. To perform their tasks, they need useful, manageable reporting and analysis tools.
SAP BW/4HANA	Executives and Knowledge Workers	Individual User	Executives and knowledge workers require personalized, context-related information provided in an intuitive user interface. They generally work with pre-defined navigation paths, but sometimes need to perform deeper data analyses. **See also:** Analysis Authorizations
SAP BW/4HANA	Information Consumers	Individual User	Information consumers require specific information (snapshot of a specific data set) to be able to perform their operative tasks. **See also:** Analysis Authorizations

2.2 Authentication and Single Sign-On

The authentication process makes it possible to check a user's identity before granting them access to SAP BW/4HANA or to data in SAP BW/4HANA. The application server supports various authentication mechanisms.

SAP BW/4HANA uses the authentication and single-sign-on mechanisms provided by SAP NetWeaver. The security recommendations and guidelines for user administration and authentication (described in the SAP NetWeaver Security Guide) therefore also apply to SAP BW/4HANA.

For more information, see the section about *user authentication* and *single-sign-on* in the SAP NetWeaver Security Guide, see OpenID Connect for the ABAP Platform and Using OpenID Connect.

Authentication and Single-Sign-On Mechanisms for SAP BW/4HANA

User ID and Password

SAP BW/4HANA uses a user ID and a password for logon.

For more information, see Logon and Password Protection in SAP Systems.

Secure Network Communications (SNC)

SAP BW/4HANA supports Secure Network Communications (SNC).

For more information, see Secure Network Communications (SNC).

SAP Logon Tickets

SAP BW/4HANA supports SAP login tickets. To make Single Sign-On available for several systems, users can obtain an SAP logon ticket after logging on to the SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication but can access the system directly after the system has checked the logon ticket.

For more information, see SAP Logon Tickets.

Client Certificates

As an alternative to user authentication with user ID and passwords, users with Internet applications via the Internet Transaction Server (ITS) can provide X.509 client certificates. User authentication then takes place on the Web Server using the Secure Sockets Layer Protocol (SSL Protocol). No passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

More information: X509 Client Certificates.

3 Authorizations

To ensure that SAP BW/4HANA represents the structure of your company and meets your company's requirements, you have to define who has access to what data and who can perform which actions in SAP BW/4HANA. There are two different authorization concepts for this, depending on the role and tasks of the user:

- **Standard Authorizations**
  You use these authorizations to determine who can do what when working with SAP BW/4HANA tools. The authorization concept for standard authorizations is based on the Application Server for ABAP authorization concept.
- **Analysis Authorizations**
  You use these authorizations to provide access to transaction data belonging to authorization-relevant characteristics, to sales data for example. Authorizations of this type are not based on the Application Server for ABAP authorization concept. They use their own concept based on the needs of BW reporting and analysis with SAP BW/4HANA instead.

Critical Authorizations

Critical Analysis Authorizations

Authorization	Description
0BI_ALL (authorization for all values of all authorization-relevant characteristics)	Every user with this authorization can access all the data at any time. Every user who has a profile containing authorization object S_RS_AUTH and who has entered 0BI_ALL (or has included it using an asterisk (*) for example), has complete access to all data. For more information, see the documentation for analysis authorizations, under Assigning Authorizations to Users.

Critical Authorization Templates

If you use authorization templates, note that some of these have wide-ranging authorizations:

Authorization Template	Description
S_RS_RDEAD (BW Role: Administrator (Development System))	These authorization templates contain wide-ranging authorizations on authorization object S_RFC.
S_RS_ROPAD (BW Role: Administrator (Production System))	

Authorization Template	Description
S_RS_TREQD (BW: Load Data (ALE, IDocs, RFC, Batch, Monitoring))	
S_RS_RDEMO (BW Role: Modeler (Development System))	These authorization templates contain authorizations for all InfoProviders on authorization object S_RS_COMP.
S_RS_TREPU (BW: Reporting User)	

More Information

Authorizations in the Documentation for SAP BW/4HANA

Authorization Log for Analysis Authorizations [page 12]

Checking Analysis Authorizations as Another User [page 12]

3.1 Authorization Log for Analysis Authorizations

A tool is available for analysis authorizations, which enables you to analyze authorization checks. It provides detailed information on authorization-relevant data access instances. This check can be switched on or off permanently, or as and when required - depending on the users involved. Access to this analysis tool should be protected using transaction RSECPROT and authorization object S_RSEC. Only authorized users should have access to the tool.

More Information

Error Log

3.2 Checking Analysis Authorizations as Another User

On the analysis authorization management screen, you can call specific transactions as another user by choosing *Execute as...* on the *Analysis* tab page. All checks for analysis authorizations (and only these authorizations) are run for the specified user. This makes it possible for a user to gain access to more authorizations than s/he would normally have. This transaction should therefore be specially protected using authorization object S_RSEC.

More Information

Management of Analysis Authorizations

OverviewAuthorization Objects

3.3 SAP HANA Authorizations for Mixed Modeling and Other Functions

For certain functions in SAP BW/4HANA, you also need authorizations in Authorizations for SAP HANA Analysis Processes (see Authorizations for SAP HANA Analysis Processes).

Authorizations for Generating SAP HANA Views

When creating objects in SAP BW/4HANA, you can generate SAP HANA views with the same structures during activation. This supports you in scenarios where data modeled in SAP BW/4HANA is merged with data modeled in SAP HANA with SAP HANA tools (mixed scenarios).

To be able to access SAP HANA views generated from SAP BW/4HANA, you need certain authorizations both in SAP HANA and in SAP BW/4HANA. Various authorizations are provided for the administration of these authorizations.

Authorizations for Searching with SAP HANA

To perform searches with SAP HANA, the technical user requires _SYS_REPO in SAP HANA certain authorizations. For security reasons, we recommend giving authorizations only for the tables that are actually required, not for the entire schema. To do this, use the following command:

```
GRANT SELECT ON sap<sid>.<table> TO _ sys_repo WITH GRANT OPTION;
```

- With <sid> = system ID of the SAP BW/4HANA system
- With <table> =

Table Name
RSBOHDEST
RSBOHDESTT
RSDAREA
RSDAREAT
RSDBCHATRXXL

Table Name
RSDCHA
RSDCHABAS
RSDFDMOD
RSDFDMOD_LOCAL
RSDFDMODT
RSDHAMAP
RSDHAMAPT
RSDIOBC
RSDIOBCIOBJ
RSDIOBJ
RSDIOBJCMP
RSDIOBJT
RSDKYF
RSDS
RSDST
RSDTIM
RSDUNI
RSFBP
RSFBPFIELD
RSFBPSEMANTICS
RSFBPT
RSKSFIELDNEW
RSKSNEW
RSKSNEWT
RSLTIP
RSLTIPT
RSLTIPXREF
RSOADSO
RSOADSOLOC
RSOADSOT
RSOHCPR
RSOHCPRT
RSOOBJXREF
RSOSEGR

Table Name
RSOSEGRLOC
RSOSEGRT
RSPLS_ALVL
RSPLS_ALVLT
RSRREPDIR
RSTRAN
RSTRANT
RSWSPLREF
RSZCOMPIC
RSZCOMPDIR
RSZELTDIR
RSZELTTXT
RSZELTXREF
RSZGLOBV
RSZRANGE
RSZWOBJTXT
RSZWVIEW
TADIR

See also SAP Note 2362807.

Authorizations for SAP HANA Analysis Processes

To be able to work with SAP HANA analysis processes, you need certain authorizations in SAP HANA and in SAP BW/4HANA.

Authorizations for SAP HANA Smart Data Access

Near-Line Storage with SAP IQ

For near-line storage with SAP IQ, you need the following authorization in SAP HANA:

- System Privilege: CREATE REMOTE SOURCE

If the remote source is not created with the SAP<SID> user but with a different database user instead, then this database user must assign the corresponding object authorizations to the SAP<SID> user:

- Object privilege: CREATE VIRTUAL TABLE on VIRTUAL_TABLES (SYS)

- Object privilege: DROP on VIRTUAL_TABLES (SYS)

Accessing the data from the system

If you use SAP HANA Smart Data Access, the remote data is accessed from the system with the database user used to connect the system to the SAP HANA database. When creating a remote source in SAP HANA, you specified a user for the connection to the source database. SAP HANA passes the SQL statements on to this user. Make sure that this user has sufficient authorizations in the relevant schemas and tables in the source database.

Related Information

Database Authorizations
Authorizations for Generated SAP HANA Views
Checking Object Authorizations
Analytic Privileges
SAP HANA Smart Data Access

4 Network and Communication Security

Your network infrastructure is extremely important for your system security. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at operating system level and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. In addition, if users are not able to connect to the server LAN (local area network), they cannot exploit known bugs and security gaps in network services on the servers.

The network topology for SAP BW/4HANA is based on the topology used by the Application Server for ABAP. The security guidelines and recommendations described in the SAP NetWeaver Security Guide therefore also apply to SAP BW/4HANA.

> ⓘ Note
>
> More information: SAP NetWeaver Security Guide.

Details that specifically apply to SAP BW/4HANA are described in the following topics.

4.1 Communication Channel Security

SAP BW/4HANA uses the following communication paths and protocols:

- RFC is used as the protocol for the following communication paths:
  - Front end and application server
  - Application server to application server
  - SAProuter and application server
  - Connection to database

  For more information on the secure usage of RFC for communication between systems, seeRFC/ICF Security Guide.
- HTTP, HTTPS, SOAP is used as the communication path between Web browser and application server.

RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol. SOAP connections are protected with Web services security.

> → Recommendation
>
> We strongly recommend using secure protocols (SSL, SNC) whenever possible.

For more information, see *Transport Layer Security* and *Web Services Security* in the Security Guide for SAP NetWeaver.

4.2 Communication Destinations

Connection destinations are required in SAP BW/4HANA in the following areas:

- Connecting data sources to the BW system
  These destinations are not usually shipped with the software. Instead, they are created on the customer's system.
  If you want to connect SAP systems and non-SAP data sources (as source systems) to SAP BW/4HANA, you usually need RFC destinations.
  The destination to the Myself SAP BW/4HANA is created automatically by the system the first time you open Data Warehousing Workbench.
  Communication between SAP BW/4HANA and source systems is the responsibility of SAP BW/4HANA background users and the background users in the source system (in the case of SAP source systems). The SAP BW/4HANA background user requires authorization profile S_BI-WHM_RFC. The background user in the SAP source system requires authorization profile S_BI-WX_RFC. For more information, see Authorization Profiles for Background Users.
- Starting a SAP Data Hub graph in SAP Data Hub 2.x using a SAP BW/4HANA process type.

4.3 Network Security

When using the SAP BW/4HANA, note the information under *Network and Communication Security* in the SAP NetWeaver security guidelines.

We recommend using firewalls to control the network traffic in your system landscape. A firewall comprises hardware and software components that specify which connections are permitted between communication partners. The firewall only allows the specified connections to be used. All others are blocked by the firewall. For more information, see *Using Firewall Systems for Access Control* in the SAP NetWeaver security guidelines.

To secure RFC connections or connections with Internet protocols, we recommend using Secure Network Communications (SNC) or Secure Sockets Layer (SSL).

4.4 Web Services and ICF Services

Various different Web services and ICF services are delivered with SAP BW/4HANA.

ICF Services

ICF services are based on the Internet Communication Framework (ICF) of the Application Server for ABAP. ICF services are HTTP services that are used to execute HTTP request handlers. The SAP BW/4HANA HTTP services allow you to display or exchange data from SAP BW/4HANA using a URL. Some of these services are implemented as Web services.

Structure of the URL

The URL of an HTTP service delivered in a BW namespace has the following structure:

<Protocol>://<Server>:<Port>/sap/bw/<Service>

- URL Prefix
  The values used for the place holder in the specified URL schema depend on the installation. For <Protocol>, http and https can be selected. For <Server>, enter your message server.
  You can check which URL prefix your BW system has generated as follows:
  1. Call Function Builder (transaction `SE37`).
  2. Enter **`RSBB_URL_PREFIX_GET`** as the function module name.
  3. Choose  *Test/Execute*. The *Test Function Module* screen appears.
  4. As import parameter `I_HANDLERCLASS`, enter the name of the ICF handler (HTTP Request Handler) for the required service.

     > **Note**
     >
     > You can find out the name of the ICF handler in the service maintenance transaction (`SICF`): Navigate to the required service component in the HTTP services tree. Double-click to open the *Change/Create a Service* dialog box. The HTTP request handler for the service is displayed on the *Handler List* tab page.

  5. Choose *Execute*. Export parameter `E_URL_PREFIX` contains the generated URL prefix.
- Service:
  Enter the technical name of the required service here. The name is made up of all elements of the path in the HTTP services tree (transaction `SICF`).

Prerequisites for Using the Service

The required HTTP service must be active.

> **Note**
>
> To check this, navigate to the required service component in Service Maintenance (transaction `SICF`). If the service is active, you cannot select the *Activate Service* entry in the context menu.

Web Services Required for SAP BW/4HANA

Web Services for	Web Services	Automatic activation via task list `SAP_BW4_SETUP_SIMPLE` in the task manager for technical configuration (transaction `STC01`)?
Web Dynpro ABAP as Basis	/default_host/sap/public/bc/ur /default_host/sap/public/bc/icons /default_host/sap/public/bc/icons_rtl /default_host/sap/public/bc/webicons /default_host/sap/public/bc/pictograms	Yes
Start progra for Analysis	/default_host/sap/bw/analysis	Yes
Modeling Tools (REST Services)	/default_host/sap/bw/modeling	Yes
Workspace Designer	/default_host/sap/bc/webdynpro/sap/rsl_ui_*	Yes
Workspace Query Designer	/default_host/sap/bc/ui5_ui5/sap/rsl_wqd	Yes
SAP BW/4HANA Master Data Maintenance	/default_host/sap/bc/webdynpro/sap/RSDMDM_MD_MAINTENANCE_APP /default_host/sap/bc/webdynpro/sap/RSDMDM_MD_NEW_APP	Yes
SAP BW/4HANA Hierarchy Maintenance	/default_host/sap/bc/webdynpro/sap/RSSHWDY_HIERARCHY_MAINT_APP	Yes
UI Building-Blocks for Query Display	/default_host/sap/bc/webdynpro/sap/fpm_bics_ovp	Yes
REST-based reporting interface	/default_host/sap/bw/ina/*	No
XML for Analysis	/default_host/sap/bw/xml/soap/xmla	No
Web Dynpro-based metadata repository	/default_host/sap/bc/webdynpro/sap/rso_metadata_repository	No

For information about the ICF and OData services required in order to use the SAP BW/4HANA Cockpit, see Configuring the SAP BW/4HANA Cockpit.

5 Security for Data Storage

Data Storage

In SAP BW/4HANA, data is stored on the application server database.

If end users evaluate data using Microsoft EXCEL, they can also store data locally. The end user has to make sure that no unauthorized person can access the locally stored data.

You can protect data from being accessed by unauthorized end-users by assigning analysis authorizations. In the default setting, data is not protected. You can flag the InfoObjects and fields in SAP BW/4HANA as authorization-relevant however. Data can then only be accessed if the user has the required authorizations.

Data Protection

LOPD Access Logging in Reporting and Planning Applications

The Spanish data protection law **L**ey **O**rgánica de **P**rotección de **D**atos de Carácter Personal (LOPD) stipulates certain rules that companies have to observe when processing, saving and handling personal data. These rules involve logging all access to highly-sensitive personal data. SAP BW/4HANA provides a mechanism for LOPD logging of access to data in reporting and planning applications. For more information, see SAP Note 933441.

6 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements, including data privacy.

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 guide does not give any advice or recommendations in regards to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

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

> ⓘ Note
>
> - Due to the local nature of BW workspace data, which is owned by single users or user groups rather than centrally, we do not recommend the use of personal data in BW workspace objects.
> - Documents are not managed by the system, and there are no features that allow analysis of the content of documents. Documents therefore should not be used to store personal data.

6.1 Glossary

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.

Term	Definition
Purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	In SAP Business Suite or SAP S/4HANA, a method of restricting access to data for which the primary **business purpose** has ended.
Deletion	The irreversible destruction of **personal data**.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
End of purpose (EoP)	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**. In SAP Business Suite or SAP S/4HANA, after the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization (e.g. tax auditors).
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, or trade union membership and the processing of 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
Residence period	The period of time after 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. In SAP Business Suite or SAP S/4HANA, 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.

Term	Definition
Where-used check (WUC)	In SAP Business Suite or SAP S/4HANA, a process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented. In SAP BW/4HANA, the where-used list in master data editing allows you to view the usage of individual master data records in InfoProviders and in other master data.
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.

6.2 Read Access Logging

Read access logging is used to monitor and log read access to sensitive data. This data may be categorized as sensitive by law, by external company policy, or by internal company policy.

Logging of read access to sensitive data can be implemented in several ways. We recommend using Read Access Logging (RAL).

Related Information

Application Server for ABAP Read Access Logging in SAP BW/4HANA [page 24]
Solution Overview [page 26]

6.2.1 Application Server for ABAP Read Access Logging in SAP BW/4HANA

Read Access Logging is a general Application Server for ABAP solution that can be configured to log read access to channels such as:

- Remote Function Calls (sRFC, aRFC, tRFC, qRFC, bgFRC)

- Dynpro
- Web Dynpro
- Web services
- Gateway (for OData)
- Analytics

Read Access Logging logs who accessed particular data within a specified time frame. ABAP implementations define which communication channels are logged and which policy is applied. Read Access Logging is always based on a logging purpose that is freely defined according to the requirements of an organization (for example, data privacy). This logging purpose is then assigned to each log entry as an attribute, which allows the log data to be classified and organized according to the logging purpose.

For more information, see section *Related Information*.

SAP BW/4HANA-specific Considerations

- Read Access Logging can be used to log access of SAP BW/4HANA data via the Analytics channel. Read Access Logging supports query requests, query results or outputs, value help in monitoring, administration, and modeling, master data and hierarchy maintenance, and data preview of InfoProviders. It does not support native SAP HANA access (this includes the SAP BW/4HANA-generated views) or SQL-access from ABAP.
  To enable logging, the following prerequisites have to be met:
  - In the Read Access Logging manager there has to be an active configuration for the Analytics channel.
  - In SAP BW/4HANA, you have to define InfoObjects as logging-relevant by assigning a business area and a log domain to them. InfoProviders are considered logging-relevant if they contain at least one logging-relevant InfoObject.
- The Dynpro channel can be used to log read access to tables in general (SE16) or to InfoProviders (LISTCUBE).
- Read access via OData queries is supported by the Gateway channel of Read Access Logging.

Related Information

For more information about Read Access Logging, see:

- *System Security for SAP NetWeaver AS for ABAP Only* documentation at https://help.sap.com/viewer/p/SAP_NETWEAVER_750
- SAP Note 2182094 - *Read Access Logging in SAP Gateway*

For more information about assigning business areas and log domains to InfoObjects, see:

- Editing Various Settings
- Creating Key Figures

6.2.2 Solution Overview

Logging of read access to sensitive data can be implemented in several ways. Which solution to choose depends on the customer's specific needs. The table below gives an overview of the different possibilities.

	Read Access Logging	BW UI Logging	Audit Trail on Database Level	LOPD (Ley Orgánica de Protección de Datos de Carácter Personal)
Out-of-the-box solution	√	√	□	√
BW integrated	√	□	□	√
Mechanism	Generic ABAP-based logging framework	Logs communication betweenSAP BW/4HANA and consumption layer	Database built-in auditing feature	Authorization-based logging on InfoProvider level
Considerations	• Logs read access via queries independent of UI/communication layer • Supports Core Data Services (CDS) • Logs responses as well as requests (configurable) • Logs access to master data maintenance, value help, hierarchy maintenance • Supports tables in general (SE16) and InfoProviders (LISTCUBE) via the Dynpro channel.	• Logs responses as well as requests • For supported front ends see the *UI Logging* documentation in section *Related Information* below • Does not log access to master data maintenance	• Used database has to support auditing • Solution has to be implemented by the customer	• Independent of UI/communication layer • Does not log access to Core Data Services (CDS) or master data maintenance

We recommend using Read Access Logging (RAL) as the solution for read access logging of master and transaction data in SAP BW/4HANA and in consuming analytic UIs. In earlier SAP BW/4HANA versions that do not provide the RAL Analytics channel, we recommend using LOPD as the solution for read access logging of transaction data in SAP BW/4HANA.

Related Information

Read Access Logging (RAL)

System Security for SAP NetWeaver AS for ABAP Only documentation at https://help.sap.com/viewer/p/SAP_NETWEAVER_750

SAP Note 2182094 - *Read Access Logging in SAP Gateway*

BW UI Logging

UI Logging documentation at https://help.sap.com/viewer/p/UI_LOGGING

Logging of SAP NetWeaver BW Access documentation at https://help.sap.com/viewer/p/LOGGING_SAP_NETWEAVER_BW_ACCESS

Database Audit Trail

For information about auditing activity in the SAP HANA database and auditing activity in SAP HANA systems, see the *SAP HANA Administration Guide* and the *SAP HANA Security Guide* in the SAP HANA Platform 2.0 documentation at https://help.sap.com/viewer/product/SAP_HANA_PLATFORM/.

LOPD

SAP Note 933441

6.3 Information Report

Each person has the right to obtain confirmation as to whether or not personal data concerning him or her is being processed. In SAP BW/4HANA it is possible to display all information stored about a certain data subject.

SAP BW/4HANA provides functions that allow you to show all BW objects that store personal data about a data subject. In SAP BW/4HANA, personal data might be stored as master data in InfoObjects. In the master data maintenance, a where-used list shows all BW objects referencing the ID of a data subject. You can check all objects found by the where-used list in order to display the personal data information stored. This way, you can show relevant information on a customer, for example. You can show the attributes of the characteristic as well as dependent transaction data in DataStore objects (advanced).

Characteristics in SAP BW/4HANA

From the editing screen for your characteristic in the BW modeling tools, you can jump to the master data editing screen if the characteristic has master data and/or texts by choosing *Miscellaneous*. Here, you can select the relevant ID and use the where-used list to show the usages in dependent BW objects.

Depending on the type of the BW object found, you can use the following functions to show the detailed data of the dependent object:

- Transaction data: BW Reporting Preview for the InfoProvider in the BW modeling tools or SAP GUI transaction LISTCUBE

- Master data: Master data maintenance
- Hierarchy data: Hierarchy maintenance

Local Characteristics in BW Workspaces

From the *Local Data* tab in the *My Workspace* area of the *BW Workspace Designer*, you can select the relevant local characteristic and jump to the master data editing screen by choosing *Maintain Masterdata*. Here, you can select the relevant ID and use the where-used list to show the usages in dependent (local or central) BW objects.

Depending on the type of the BW object found, you can use the following functions to show the detailed data of the dependent object:

- Transaction data: You can display detailed data of the dependent object by choosing *Display Data* on the *Local Provider* tab in the *My Workspace* area of the *BW Workspace Designer*.
- Master data: You can display detailed data of the dependent (local or central) characteristic in the corresponding master data maintenance.

Related Information

For more information about the master data maintenance and the where-used list in the master data maintenance screen, see:

- Creating and Changing Master Data
- Running a Where-Used List

For more information about hierarchy maintenance, see Creating and Changing Hierarchies.

6.4 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.

Depending on how many InfoProviders and InfoObjects are affected, there might be different approaches for deleting personal data:

- Full deletion in SAP BW/4HANA and reload from source system
  You can fully delete data from all relevant InfoProviders from top to bottom in SAP BW/4HANA and then reload the data from the source system, SAP Business Suite or SAP S/4HANA, for example.

  > **Note**
  >
  > Note that data, once it has been blocked or deleted in the SAP source system (SAP Business Suite or SAP S/4HANA, for example), cannot be transferred to SAP BW/4HANA anymore, meaning that the history of the data is lost. When transferring data from the source system, SAP BW/4HANA only gets the operational data. A possible solution could be to use InfoProviders with aggregated data without any references to persons in SAP BW/4HANA.

- Selective deletion in SAP BW/4HANA
- Anonymize master data (clearing of master data)

To find the InfoProviders and InfoObjects that are relevant for deletion, use the following approaches:

- For a DataSource, which might contain personal data, explore the data flow in the BW Modeling Tools with the transient data flow. From the data flow you can navigate to the single objects.
- For an InfoObject, use the where-used list in the master data maintenance to identify all relevant objects.
- For replicated data, you can use the data protection workbench. For more information, see section *Handling Replicated Data* below,

If you use data tiering to assign data to various storage areas, you have to take archived data into account when deleting personal data.

Handling Replicated Data

To handle data that has been replicated from SAP S/4HANA or SAP Business Suite systems, you can generate notifications from Information Lifecycle Management (ILM) actions and extract them to the SAP BW/4HANA system. These notifications can then be processed using the data protection workbench. For more information, see *Data Protection for Replicated Data - Data Protection Workbench* in the SAP BW/4HANA documentation.

Related Information

- Deleting Transaction Data [page 30]
- Deleting Change Log Data [page 30]
- Removing Personal Data from Master Data [page 31]
- Using a Transient Data Flow for a Persistent Object
- Running a Where-Used List
- Deleting Archived Data [page 32]
- Data Protection Workbench for Replicated Data

6.4.1 Deleting Transaction Data

To delete transaction data in DataStore objects, use selective physical deletion of records from the active table.

> **Note**
>
> - If the DataStore object has a change log, which contains sensitive, personal data, make sure you clean up the change log regularly.
> - To delete personal data from Staging DataStore objects, you can clean up the DataStore object regularly.
> - BW Workspaces: Local providers don't support selective deletion. To delete personal data from local providers, re-create the local provider by uploading a suitable file.

To selectively delete records from the active table, from the editing screen for your DataStore object (advanced) in the BW modeling tools, choose *Manage the DataStore Object (advanced)*. Then, from the *Environment* menu of the Manage UI, you can choose *Selective Deletion*.

Related Information

Managing DataStore Objects
Deleting Change Log Data [page 30]
Cleaning Up Requests Using Process Chains

6.4.2 Deleting Change Log Data

For DataStore objects that record changes in a separate change log table, you can clean up data from the change log using process type *Cleaning Up old Requests from DataStore Objects (advanced)*.

With this process type, you can delete requests that are older than a specified number of days. This way, the process type can be used to delete the change log on a regular basis, every few weeks for example.

> **Note**
>
> You can also use this process type to periodically delete data from Staging DataStore objects.

Related Information

Cleaning Up Requests Using Process Chains

6.4.3 Removing Personal Data from Master Data

To remove personal data from master data, you can either clear or anonymize affected personal or sensitive attributes, or, if clearing attributes is not sufficient in your case, you can delete the whole master data record (master data key).

Clearing Attributes

Master data can be changed either by editing attributes in SAP BW/4HANA or by delta handling of master data changes in the source system, for example SAP Business Suite, and uploading the changes to SAP BW/4HANA. Depending on the data model, clearing the personal or sensitive attributes in one of these ways might be sufficient to depersonalize the data. The key of the record will persist, however, and all InfoProviders using the InfoObject will still contain the transaction data referring to the depersonalized master data record.

> ⓘ Note
>
> If there is no data that is generated in SAP BW/4HANA, all data in the relevant InfoProviders and InfoObjects can be deleted and then loaded from the source system again.

To clear attributes in SAP BW/4HANA, from the editing screen for your characteristic in the BW modeling tools, you jump to the master data editing screen by choosing *Miscellaneous*. In the master data editing screen, you select the relevant ID and change the record.

Removing Master Data Key

If clearing attributes is not sufficient and a master data key must be removed from the system, all usages of that key must be found and the respective records have to be deleted using selective physical deletion.

To remove master data keys in SAP BW/4HANA, proceed as described in the following steps:

1. From the editing screen for your characteristic in the BW modeling tools, you jump to the master data editing screen by choosing *Miscellaneous*. In the master data editing screen, you select the relevant ID and use the where-used list in the master data maintenance screen to find the references.
2. For each found reference, delete the reference:
   - For transaction data, use selective deletion.
   - For master data, use master data deletion.
3. From the editing screen for your characteristic in the BW modeling tools, you jump to the master data editing screen by choosing *Miscellaneous*. In the master data maintenance screen, you select the relevant ID and choose *Delete*.

BW Workspaces

When master data of BW InfoObjects is extended by local workspace data, these locally added values can also be cleared or deleted using the master data editing screen. From the *Local Data* tab in the *My Workspace* area

of the *BW Workspace Designer*, you can select the relevant local characteristic and jump to the master data maintenance screen by choosing *Maintain Masterdata*. Here, you can clear the attributes as described above, or you can delete the master data keys of your local master data. For this purpose select the relevant ID and use the where-used list to show the usages in dependent (local or central) BW objects. Then you can delete the references, and finally you can delete the master data keys of your local master data.

Related Information

Creating and Changing Master Data
Managing DataStore Objects
My Workspace

6.4.4 Deleting Archived Data

In order to delete personal data from archives (also known as Near-Line Storage or cold store) created by SAP BW/4HANA the following steps apply:

1. Identify the BW Near-Line Storage archiving request(s) or, when using SAP BW/4HANA Data Tiering Optimization, DataStore object partition(s) that contain the data records to be deleted.

   You can find an overview of archiving requests on the Manage-UI of a DataStore object by choosing  *Manage Archiving*.
   You can find an overview of DataStore object partitions in the *DTO Temperature Administration* by choosing *Maintain Temperatures* on the *Settings* tab in the BW modeling tools' DataStore object editor.
2. Reload the respective BW Near-Line Storage archiving request(s) or DataStore object partition(s) to your SAP BW/4HANA primary database.
3. Use selective deletion for the respective InfoProvider to delete the relevant personal data.
4. Archive the respective BW Near-Line Storage archiving request(s) or DataStore object partition(s) again.

Related Information

Data Tiering
Reloading Archived Data
Deleting Transaction Data [page 30]

6.4.5 Authorization Concept for Data Protection Workbench

There are different roles involved that require different authorizations when you need to delete replicated data with the data protection workbench in SAP BW/4HANA.

Roles defined for handling replicated data with the data protection workbench

Data Protection Modeler

The modeler is responsible for putting all the objects in place that are necessary to get notifications from the source systems into BW. The modeler is authorized to perform the following tasks:

1. Activate content objects for the data protection workbench (InfoArea 0BWTCT_DPP):
    - DataSources
    - DataStore objects (advanced)
    - Transformations
    - Data transfer processes
    - Process chains
2. For custom notifications, he creates the following:
    - DataSources
    - Transformations
    - InfoSources
    - Data transfer processes
    - Process chains

In addition, the modeler is responsible to maintain the ILM configuration of the source systems so that notifications are created.

The modeler does not have the authorization to actually load data into the DataStore objects 0DPPNOT_I, 0DPPNOT_R.

Data Protection Administrator

The data protection administrator makes sure that notifications are replicated to SAP BW/4HANA on a regular basis. The administrator schedules the process chains created by the data protection modeler and might do maintenance work like deleting red load requests in 0DPPNOT_I, 0DPPNOT_R etc.

The administrator is not allowed to create any transformation or data transfer process associated with the data protection workbench.

Data Protection Operator

The data protection operator is the person that ultimately processes the notifications and performs the deletions. The operator does the following:

- Create worklists
- Work on worklists (set status, perform actions, read logs)

- Delete data from BW objects (InfoObjects and InfoProviders)

The operator can only consume the notifications in 0DPPNOT_I, 0DPPNOT_R, he might not delete or change them.

Other BW Administrators or Modelers

Apart from the people responsible for the data protection workbench operations, other admins or modelers will be working on the system. These people should be able to create any kind of BW object but they should not be allowed to do anything that might alter data protection notifications.

We assume that such a person might be authorized to work on the Z*-namespace and a whitelist of 0*-namespace objects.

Overview of SAP BW/4HANA authorizations

The following table provides an overview of which SAP BW/4HANA authorizations are necessary for which role for specific actions:

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Load data, activate content, delete BW data	S_RS_ADSO	RSINFOAREA=0BWTCT_DPP RSOADSONM=0DPPNOT_I, DPPNOT_R RSOADSOPAR=definition ACTVT=03(display), 23 (maintain)	-	RSINFOAREA=Z*, whitelist of 0-objects w/o 0BWTCT_DPP RSOADSONM=Z*, whitelist of 0-objects w/o 0DPPNOT_I, 0DPPNOT_R RSOADSOPAR=data ACTVT= 23 (maintain) 2nd object as above but with RSOADSOPAR=definition ACTVT=03(display)	RSINFOAREA=Z*, whitelist of 0-objects w/o 0BWTCT_DPP RSOADSONM=Z*, whitelist of 0-objects w/o 0DPPNOT_I, 0DPPNOT_R	S_RS_DTP wins for loading, so data protection administrator doesn't need this

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Delete BW data	S_RS_IOBJA	-	-	RSINFOAREA=Z*, whitelist of 0-objects w/o 0BWTCT_DPP RSIOBJ= Z*, whitelist of 0-objects RSIOBJPART=data ACTVT= 03 (display) , 06(delete master data) 2nd object as above but with RSIOBJPART=definition ACTVT=03 (display)	RSINFOAREA=Z*, whitelist of 0-objects w/o 0BWTCT_DPP RSIOBJ= Z*, whitelist of 0-objects	-

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Load data, Activate content, Create notification data flow	S_RS_DTP	RSTLDTPSRC= RSDS, TRCS, DTPA, ADSO RSSTDTPSRC= ATTR RSONDTPSRC= 0DPP_GEN_NOTIF*, 0DPPNOT_I + whitelist of customer sources RSTLDTPTGT= ADSO, TRCS RSSTDTPTGT= ATTR RSONDTPTGT= 0DPPNOT_I, 0DPPNOT_R + whitelist of customer objects ACTVT= 03(display), 23 (maintain)	RSTLDTPSRC= RSDS, TRCS, DTPA, ADSO RSSTDTPSRC= ATTR RSONDTPSRC= 0DPP_GEN_NOTIF*, 0DPPNOT_I + whitelist of customer sources RSTLDTPTGT= ADSO, TRCS RSSTDTPTGT= ATTR RSONDTPTGT= 0DPPNOT_I, 0DPPNOT_R + whitelist of customer objects ACTVT= 03(display), 16 (execute)	-	RSONDTPSRC= Z*, whitelist of 0-objects w/o 0DPP_GEN_NOTIF, 0DPPNOT_I RSONDTPTGT= Z*, whitelist of 0-objects w/o 0DPP_GEN_NOTIF, 0DPPNOT_I	DataSource name contains source system name (concatenated) so authorizing per source system is possible. Problem: custom notification flow consists of Z-objects. Needs namespace concept in Z-names to make sure other does not change custom-part of notification flow

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Load data, Activate content, Create notification dataflow	S_RS_TR (trnsfrmtn)	RSTLDTPSRC= RSDS, TRCS, ADSO RSSTDTPSRC= ATTR RSONDTPSRC= 0DPP_GEN_NOTIF*, 0DPPNOT_I + whitelist of customer sources RSTLDTPTGT= ADSO, TRCS RSSTDTPTGT= ATTR RSONDTPTGT= 0DPPNOT_I, 0DPPNOT_R + whitelist of customer objects ACTVT= 03(display), 23 (maintain)	RSTLDTPSRC= RSDS, TRCS, DTPA, ADSO RSSTDTPSRC= ATTR RSONDTPSRC= 0DPP_GEN_NOTIF*, 0DPPNOT_I + whitelist of customer sources RSTLDTPTGT= ADSO, TRCS RSSTDTPTGT= ATTR RSONDTPTGT= 0DPPNOT_I, 0DPPNOT_R + whitelist of customer objects ACTVT= 03(display), 16 (execute)	-	RSONDTPSRC= Z*, whitelist of 0-objects w/o 0DPP_GEN_NOTIF, 0DPPNOT_I RSONDTPTGT= Z*, whitelist of 0-objects w/o 0DPP_GEN_NOTIF, 0DPPNOT_I	DataSource name contains source system name (concatenated) so authorizing per source system is possible. Problem: custom notification flow consists of Z-objects. Needs namespace concept in Z-names to make sure other does not change custom-part of notification flow

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Create/schedule process chain for data loading	S_RS_PC	RSPCCHAIN=0DPP_LOAD_NOTIF + whitelist of customer notification chains RSPCPART=Definition RSPCAPPLNM = 0BWTCT_DPP + whitelist of customer notification APPLNMs ACTVT=03(display), 06 (delete), 23 (maintain)	RSPCCHAIN=0DPP_LOAD_NOTIF+whitelist of customer notification chains RSPCAPPLNM = 0BWTCT_DPP + whitelist of customer notification APPLNMs RSPCPART=Definition, Runtime, Protocols RSPCPART=Runtime, Protocols ACTVT=03(display), 06(delete protocols), 16 (execute)	-	RSPCCHAIN=Z*, whitelist of 0-objects w/o 0DPP_LOAD_NOTIF RSPCAPPLNM =Z*, whitelist of 0-objects w/o 0BWTCT_DPP	Problem: custom notification flow consists of Z-objects. Needs Namespace concept in Z-names to make sure other does not change custom-part of notification flow
Activate content, create custom DataSource	S_RS_DS data source	RSDS=0DPP_GEN_NOTIF + whitelist of customer sources RSLOGSYS=whitelist of source systems providing notifications RSDSPART=Definition ACTVT=03,23	-	-	RSDS=Z*, whitelist of 0-objects w/o 0DPP_GEN_NOTIF	Problem: custom notification flow consists of Z-objects. Needs namespace concept in Z-names to make sure other does not change custom-part of notification flow

Action	Authorization Object	Authorizations for data protection modeler	Authorizations for data protection administrator	Authorizations for data protection operator	Authorizations for other/ general BW administrator or modeler	Comment
Create/ Update/ Delete/Display data protection worklists	S_RS_DPPWL	ATVT=01,02,03 ,06 or subsets thereof as required by responsibilities and processes in customer implementation	-	-	-	-

6.5 Log Changes to Personal Data

Personal data is subject to frequent changes. Therefore, for revision purposes or as a result of legal regulations, it may be necessary to track the changes made to this data. If these changes are logged, you can check which employee made which change and when at any time. It is also possible to analyze errors in this way.

In SAP BW/4HANA, personal or sensitive data might be stored as transaction data in DataStore objects or as master data in InfoObjects. Personal or sensitive data can be changed by loading new data from a source system or by changing the data in SAP BW/4HANA. A mix of both is also possible.

Transaction Data

Logging changes in transaction data is supported by several types of DataStore objects (aDSO). The following DataStore objects support logging changes:

Object Type	Logging Mechanism
Data Mart DataStore objects	Audit log (audit information are part of the request ID)
Standard DataStore objects (advanced) with modeling property *Write Change Log*	Change log
Local provider (workspaces)	Audit log

For detailed information about logging changes using audits, see section *Related Information*. For more information about Change Logs, see *DataStore Object* in section *Related Information*.

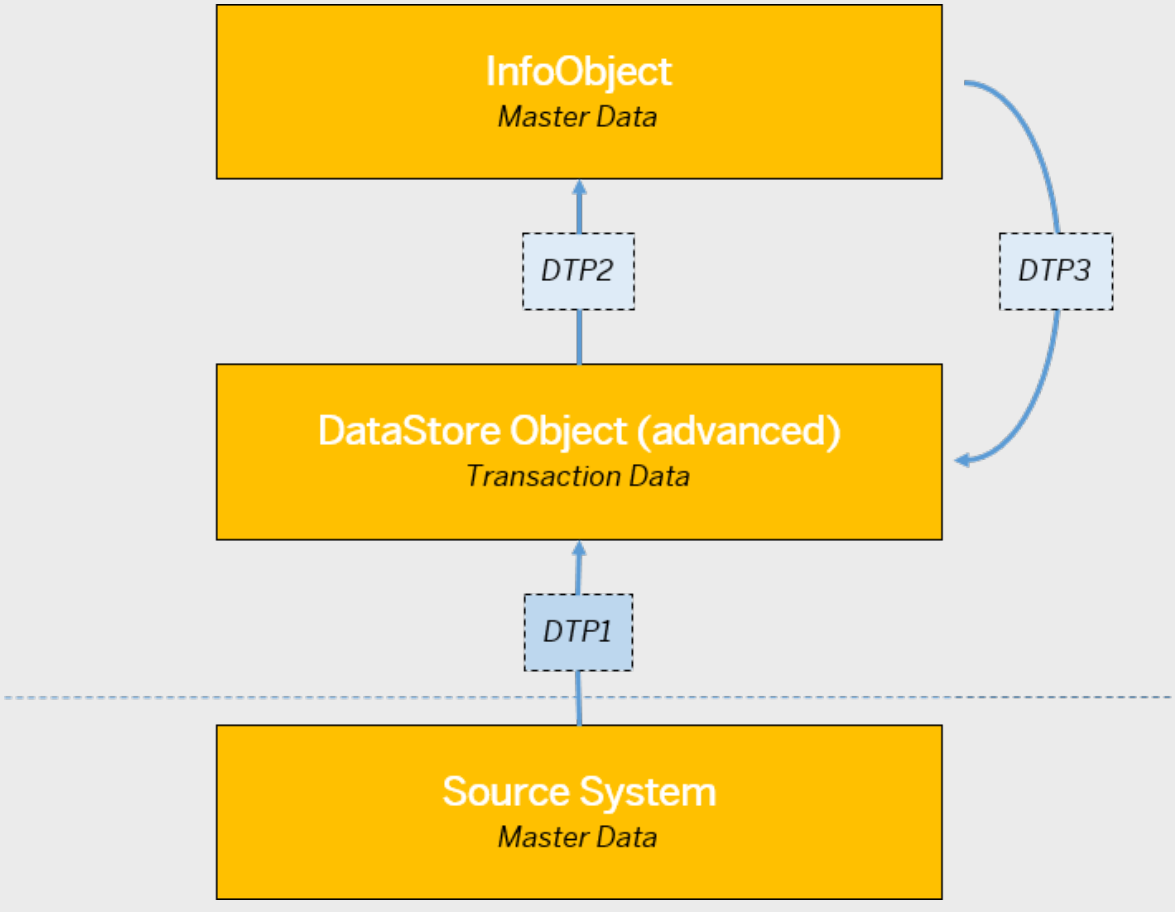
Master Data

If changes in master data are done in the source system and not in SAP BW/4HANA, in SAP Business Suite for example, the changes are logged in the source system and transferred to SAP BW/4HANA.

If changes in master data are done in SAP BW/4HANA master data maintenance, the changes can be logged by using a DataStore object that is modeled in one of the ways described in the table above. Instead of loading the data directly into the InfoObject, you then load the data with a data transfer process (DTP1) into an intermediate DataStore object. You then transfer the data with a second data transfer process (DTP2) into the InfoObject. The intermediate DataStore object has to have the same structure as the InfoObject. It needs to include the InfoObject itself as well as all its attributes. We recommend using a Standard DataStore object with modeling property *Write Change Log*.

> ⓘ Note
>
> This workflow doesn't work for attributes with the flag *Attribute Only*.

> ⓘ Note
>
> If in a scenario changes are done in SAP BW/4HANA (master data maintenance), you can model a data transfer process (DTP3) for a periodic full load from master data to the intermediate DataStore object and check the changes in the change log. If master data additionally is loaded from a source system, the order of loading the data into the intermediate DataStore object is important. The first loaded changes will be overwritten by the changes loaded second.



> **Note**
>
> In the workspace context, change logs are not supported for local data of InfoProviders.

Related Information

Audit
DataStore Object

7 Security-Related Logging and Tracing

Logging Security-Related Changes and Authorization-Related Activities

The following tables are used to log changes to analysis authorizations and other authorization-related activities:

RSUDOLOG

This table contains log information about execution of a query (or other transaction) in the administration transaction for analysis authorizations in Query Monitor (transaction RSRT) by one user for another.

For further information about executing transactions (especially RSRT) with another user, see Management of Analysis Authorizations and Checking Analysis Authorizations as Another User [page 12].

The log data includes the following:

- User name of the user who has executed a transaction under another user name
- User name of the other user
- The transaction that was executed
- Password prompt flag
- Flag to show correct password entered
- Session ID
- Time stamp

RSECVAL_CL

This table contains log information about changes to value authorizations. The log data includes the following:

- The authorization that was changed
- The characteristic that the authorization was changed for
- Object version of the characteristic
- Session ID
- Time stamp for the change

RSECHIE_CL

This table contains log information about changes to hierarchy authorizations. The log data includes the following:

- The authorization that was changed
- The characteristic that the authorization was changed for
- Object version of the characteristic
- Hierarchy-specific data
- Session ID
- Time stamp for the change

RSECUSERAUTH_CL

This table contains log information about the assignment of analysis authorizations by users in the administration transaction for analysis authorizations.

More information: Assigning Information to Users

The log data includes the following:

- Authorization
- Use name of the user whom the authorization was assigned to
- Time stamp
- Session ID

> **Note**
>
> You can analyze changes to value and hierarchy authorizations and to user-user authorization assignments using InfoProviders from the technical content. More information: Change Documents (Legal Auditing).

RSECTXT_CL

This table contains log information about changes to authorization texts. The log data includes the following:

- The authorization that was changed
- The authorization's short, medium and long text
- Session ID
- Time stamp for the change:

RSECSESSION_CL

This table contains log information about user activities in the session, including the date and time of any changes made. You can use this table to find out which user values, hierarchy authorizations or authorization texts have been changed.

Logging LOPD-Relevant Access in Reporting and Planning Applications

SAP BW/4HANA provides a mechanism for logging access in reporting and planning applications, which are security-related in accordance with the Spanish data protection law **L**ey **O**rgánica de **P**rotección de **D**atos de Carácter Personal (LOPD). For more information, see SAP Note 933441.

8 Security Aspects for the Modeling Tools in Eclipse

The following sections explain security aspects that you should bear in mind when using modeling tools for SAP BW/4HANA.

Target Group

- System administrators

Why is Security Important?

With the increasing use of distributed systems and the Internet for managing business data, security requirements are also becoming more prominent. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. It is very important that user errors, negligence, or attempted manipulation do not result in loss of information or affect processing time. These security requirements also apply to Eclipse modeling tools. We have provided this information to help you to make modeling tools more secure.

Related Information

User Authentication on the Front End Client [page 44]
Authorizations for Modeling with the Modeling Tools [page 45]
Protecting Resources on the Front End Client [page 47]
Installing Third-Party Plug-Ins [page 48]

8.1 User Authentication on the Front End Client

In modeling tools, you always work with BW projects in order to access metadata objects from the back end system (SAP BW/4HANA).

A BW project represents a real system connection on the front end client. It therefore requires an authorized user in order to access the back end system. With the standard authentication method, the user enters a user name and password to log on to the back end system.

Risks

Standard authentication with explicit specification of a user name and password means that the user data entered on the front end client is loaded as plain text into the memory of the local host. A password that is saved locally is a potential security breach, as it could be extracted from the memory by third parties.

Security Measures

Activating **Secure Network Communication (SNC)** for the selected system connection is mandatory due to security reasons.

Use **Single Sign-On (SSO)** as well. When used with SNC, SSO also meets the security requirements for working with large-scale BW projects. With SSO, the user does not need to enter a user name and password. S/he can simply access the system as soon as the logon ticket has been checked.

> ⓘ Note
>
> Note that configuring SSO is a general configuration step. There is no difference to the configuration for ABAP Development Tools. If you have already configured SSO for ABAP Development Tools in your landscape, no further configuration is required for modeling tools.

Besides issuing logon tickets, AS ABAP systems can also issue restrictive assertion tickets when system services are accessed. If you use integrated SAP GUI applications in modeling tools, the assertion tickets provide a greater level of security. The back end system does not request a password. Instead it checks the validity of the assertion ticket to permit the user to access system services. We therefore recommend configuring your AS ABAP system to only issue assertion tickets.

More Information

For more information, see the installation guide for BW modeling tools.

8.2 Authorizations for Modeling with the Modeling Tools

Authorizations are assigned to users in the back end system. This assignment is based on roles that are predefined in the system. One or more roles are assigned to a user. These roles are based on authorization objects from a technical viewpoint.

Basis Authorizations

Standard role

The following role is required to use the modeling tools. If role SAP_BC_DBW_ABAPDEVELOPER is already assigned to a user, the role already contains the required authorizations.

Role	Description
SAP_BC_DWB_WBDISPLAY	Roll that contains all authorizations for displaying and searching ABAP development objects. **Note** The users are not allowed to modify ABAP development objects.

Authorization object S_RFC

The modeling tools require remote access to the following function modules that are specified for authorization object S_RFC:

Activity [ACTVT]	Name of RFC Object [RFC_NAME]	RFC Type [RFC_TYPE]
16 (Execute)	DDIF_FIELDINFO_GET RFCPING RFC_GET_FUNCTION_INTERFACE SADT_REST_RFC_ENDPOINT SUSR_USER_CHANGE_PASS-WORD_RFC SYSTEM_RESET_RFC_SERVER	FUNC (Function Module)

Authorization object S_TCODE

The modeling tools need to start specific transactions for SAP GUI integration in Eclipse. The BW modeling tools therefore need access to the following transactions, which are specified in authorization object S_TCODE:

- SADT_START_TCOD
- SADT_START_WB_URI

For more information, read the document Configuring the ABAP Back End for ABAP Development Tools in the SAP Community Network.

SAP BW/4HANA-Specific Roles and Authorizations

When working with BW modeling tools, you can only see or open objects that you have at least display authorization for. The same checks are performed for actions on objects in the modeling tools as for actions in

the back end system or in the query. We therefore recommend the following role templates for users who work with the modeling tools:

Role Template	Description
S_RS_RDEMO	BW role: modeler (development system)

> **Note**
>
> Notes on specific object types:
>
> If the authorization object has subobject field defined for an object type (TLOGO), the user needs to have authorization * or at least *Definition*, in order to see the object in the Project Explorer tree.

In particular, modelers need authorizations that are specified in the following authorization objects:

Authorization Object	Description
S_RS_HCPR (SAP HANA CompositeProvider authorizations)	Authorizations for working with CompositeProviders and their subobjects
S_RS_ODSV (Open ODS view)	Authorizations for working with Open ODS Views
S_ADT_RES	Authorization object for ADT resource access Authorization field URI must have the value */sap/bw/modeling/**. **Note** The placeholder "*" is used for the URI subfolders.

8.3 Protecting Resources on the Front End Client

In the modeling tools, a BW project represents a user-specific view of the BW metadata objects of the back end systems (SAP BW/4HANA).

Like all projects in Eclipse, BW projects also have a local representation of their data on the front end and are managed in a workspace. If you have a BW project, there will therefore be local copies of the SAP BW/4HANA metadata objects on the front end. This means that it is possible to access metadata located outside of the SAP repository at local file system level.

Risks

The SAP BW/4HANA metadata objects can be found by third parties.

Security Measures

To protect local project resources, we recommend creating workspace folders to store project resources locally, in order to prevent third parties from accessing the resources. Use the existing security measures that are available at operating system level.

> ⓘ Note
>
> Files stored under Windows in the personal substructure of a user can only be accessed by that user or by local administrators.

> → Tip
>
> We especially recommend using the default workspace that was created when the integrated development environment (IDE) was installed.

8.4 Installing Third-Party Plug-Ins

Your installation of modeling tools can be enhanced by using additional plug-ins from various third-party providers.

Risks

These plug-ins can take control of your client installation or even take control of your complete front end PC.

Security Measures

Be very careful when deciding which plug-ins to install.

9 Security Aspects for the SAP BW/4HANA Cockpit

The following sections explain security aspects that you should bear in mind when using the SAP BW/4HANA Cockpit.

User Administration and Authentication

SAP BW/4HANA uses the user administration and authentication mechanisms from the Application Server for ABAP. The security recommendations and guidelines for user administration and authentication described in the Security Guide for SAP NetWeaver therefore also apply to SAP BW/4HANA.

Authorizations and Roles

For information about authorizations and roles for working with the SAP BW/4HANA Cockpit, see Authorizations for Working with the SAP BW/4HANA Cockpit.

Network and Communication Security

The network topology for SAP BW/4HANA is based on the topology used by the Application Server for ABAP. The security guidelines and recommendations described in the SAP NetWeaver Security Guide therefore also apply to SAP BW/4HANA. Details that specifically affect SAP BW/4HANA are described in the the relevant sections in the Security Guide for SAP BW/4HANA.

ICF and OData Services

For information about the ICF and OData services required in order to use the SAP BW/4HANA Cockpit, see Configuring the SAP BW/4HANA Cockpit.

Lines of Defense

There are at least two lines of defense against active content.

The first performs a virus scan in order to avoid uploading malicious content in the first place. When performing virus scans, a virus scan interface is provided. You can use this to integrate external virus scanners into the SAP system. For more information, see Virus Scan Interface and Configuration of the Virus Scan Interface in the documentation for *ABAP platform 1809*.

The second line of defense is SAP Web Dispatcher. An alternative is the Internet Communication Manager (ICM). These protect again malicious active content being executed at the front end. This uses additional

HTTP-response headers to instruct browsers to behave in a specific way. SAP Web Dispatcher and ICM both provide the possibility of modifying HTTP response headers..

For more information, see Deleting, Adding, and Enhancing HTTP Header Fields in *Administration of the ICM - SAP NetWeaver*.

SAP recommends adding the following headers:

- `SetResponseHeader X-Content-Type-Options "nosniff"`
  This tells the browser not to try reading the attached file with the assumed MIME type.
- `SetResponseHeader X-XSS-Protection "1; mode=block"`
  This header prevents cross-site scripting.

For the configuration of HTTP Strict Transport Security (HSTS), you can use `Strict-Transport-Security` in the header. For more information, see SAP Note 2202116.

Protection against Clickjacking

Clickjacking is an attack type where an attacker tries to hijack the clicks of an authenticated user in order to trigger malicious actions. This attack is based on framing the attacked page into an attacker-controlled enclosing pageSAP BW/4HANA uses a SAP NetWeaver protection mechanism to prevent click-jacking attacks.

For more information, see Clickjacking Framing Protection in the SAP NetWeaver User Interface Services documentation and under Using a Whitelist for Clickjacking Framing Protection in the SAP NetWeaver Application Server for ABAP Security Guide.

HTTP Session Security Protection

To increase security and prevent access to the SAP logon ticket and security session cookie(s), we recommend activating secure session management. We also highly recommend using SSL to protect the network communications where these security-relevant cookies are transferred.

For more information, a list of the relevant profile parameters, and detailed instructions, see Activating HTTP Security Session Management on AS ABAP in the Application Server for ABAP 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

THE BEST RUN SAP