



SAP NetWeaver '04
Security Guide

SAP Business
Information
Warehouse Security
Guide

Document Version 1.00 – April 29, 2004



SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

© Copyright 2004 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Disclaimer

Some components of this product are based on Java[™]. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java[™] Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.






Documentation in the SAP Service Marketplace

You can find this documentation at the following Internet address:
service.sap.com/securityguide

Typographic Conventions

Type Style	Description
<i>Example Text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example text	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

SAP Business Information Warehouse Security Guide.....	5
1 Technical System Landscape.....	6
2 User Administration and Authentication.....	8
2.1 User Management.....	8
2.2 Authentication.....	12
3 Authorizations.....	12
4 Communication Security.....	13
4.1 Communication Channel Security.....	13
4.2 Communication Destinations.....	14
5 Security with Data Storage.....	14
6 Minimal Installation.....	15
7 Additional Information Relevant to Security.....	15
8 Trace and Log Files.....	15

SAP Business Information Warehouse Security Guide



This guide does not replace the handbook for daily operations that the customer should produce for their productive operations.

This Guide

SAP Business Information Warehouse (SAP BW) is based on the SAP Web Application Server (SAP WAS). Therefore also consult the security information for SAP WAS. This guide only describes additional or anomalous security information. SAP BW can be implemented together with other SAP NetWeaver components. If, for example, you are implementing integration with SAP Enterprise Portal, also consult the security information for these components. BI Content 3.5.1 Add-On is delivered in parallel to SAP BW 3.5. This contains reporting scenarios and pre-defined role and task-related information models that are based on consistent metadata.

The following table provides an overview of the additional security guides and security information that are relevant:

Application	Security Guide
SAP Web Application Server 6.40	SAP Web Application Server Security Guide
SAP Enterprise Portal 6.0	Portal Platform Security Guide
“Data Protection for SAP BW“ guide	Quicklink to SAP Service Marketplace (service.sap.com): <code>germany/aboutSAP/revis/infomaterial.asp</code>

Why Is Security Necessary?

SAP BW serves to integrate, transform, and consolidate data from all areas of an enterprise in order to provide this for analysis and interpretation. This includes confidential corporate data, for example, personal data from Personnel Administration. Decisions are made in all enterprise areas and target-oriented actions are determined on the basis of this data. For this reason, security when accessing data and the ability to guarantee data integrity is of great importance in SAP BW.

The following examples show the dangers to which SAP BW can be exposed:

- Attacks from the Internet or Intranet when using BEx Web functionality and Web Services
- Infringement of data protection guidelines through unauthorized access to personal data

Target Groups

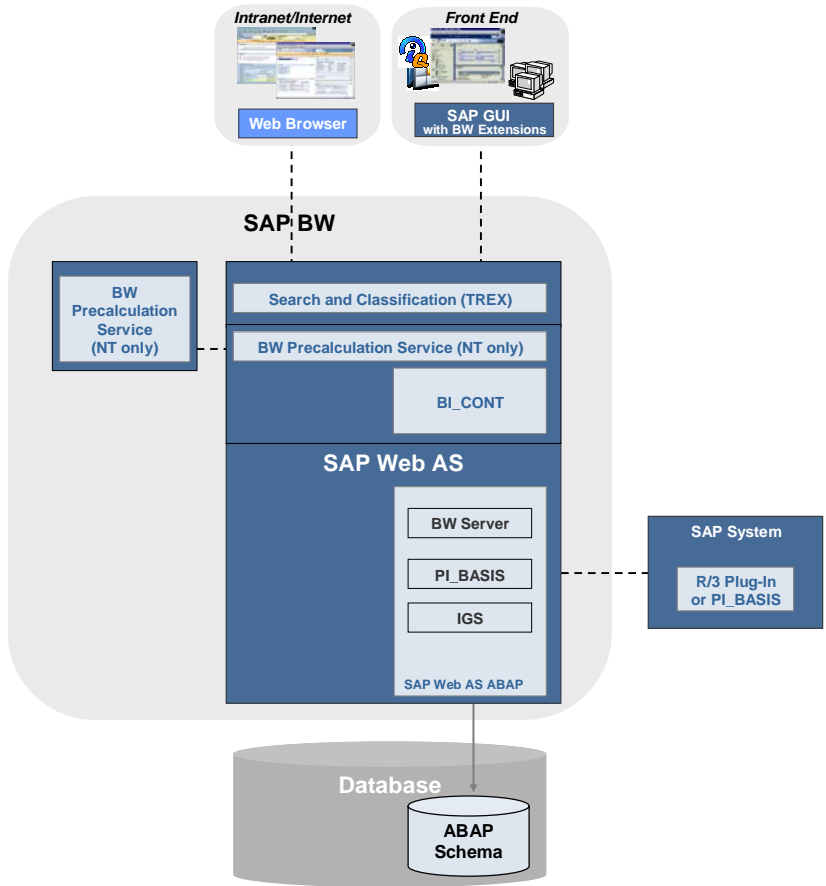
- Technical consultants
- System administration

1 Technical System Landscape

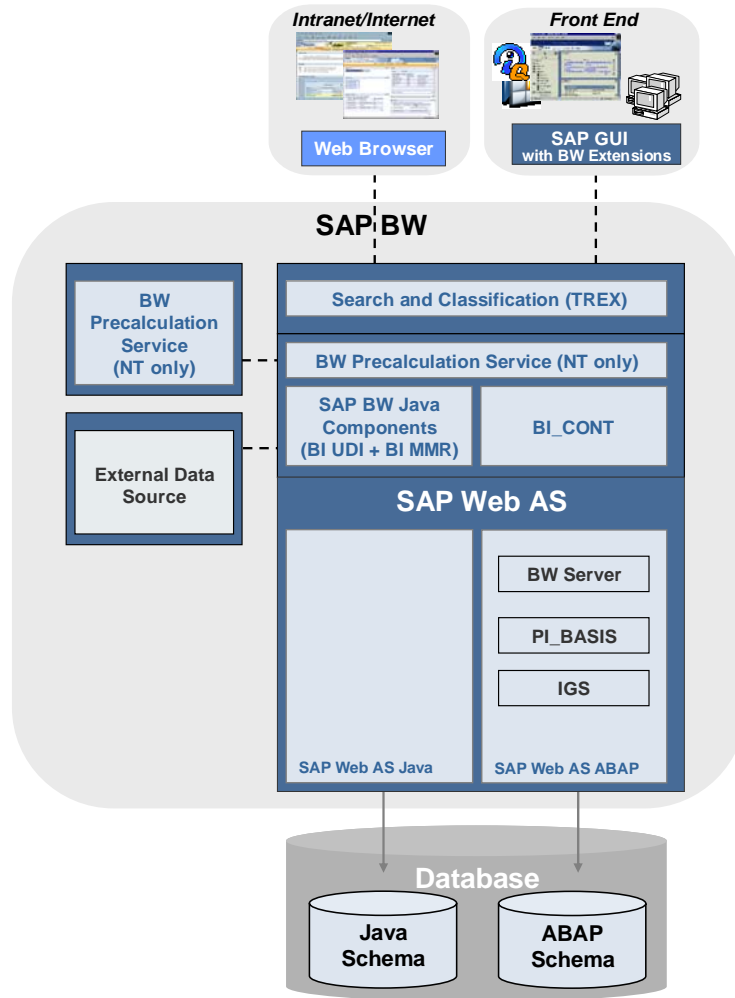
1 Technical System Landscape

The following graphics illustrate the important components that are used when SAP BW is implemented and the communication between these components.

Technical system landscape for SAP BW without external data sources



Technical system landscape for SAP BW with external data sources



More information on the technical system landscape

Topic	Guidelines / Tool	Quick link to SAP Service Marketplace (service.sap.com)
SAP BW 3.5	Master Guide	instguides

2 User Administration and Authentication

See also:

[User Administration and Authentication \[SAP NetWeaver Security Guide\]](#).

2.1 User Management

SAP BW uses the user management delivered for SAP NetWeaver application platforms ABAP and Java (see the tables on user administration tools under [User Management \[SAP NetWeaver Security Guide\]](#)).

You can find information on user management within SAP Enterprise Portal (SAP EP) under *Security* → *Identity Management* → [User Management Engine \[SAP Library\]](#) in the documentation for the SAP NetWeaver components.

You can find information on user management with SAP EP 5.0 in the SAP EP documentation in the SAP Help Portal (help.sap.com), for example, for SP 5 look under *Administration Guide* → *User Management*.

User

The following table provides an overview of the users required when using SAP BW:

System	User	Delivered?	Type	Default Password	Description
SAP BW	SAP*	Yes; System creates user during installation	Standard user	Initial: 06071992	<p>SAP system superuser with the authorization profile SAP_ALL.</p> <p>SAP* is created in clients 000 and 066.</p> <p>To ensure that nobody misuses the standard user SAP* you should define a new superuser and deactivate SAP* in all clients available in table T000.</p> <p>See also:</p> <p>Protecting Standard Users [SAP Web AS Security Guide] and Defining New Superusers and Deactivating SAP* [SAP Web AS Security Guide]</p>

System	User	Delivered?	Type	Default Password	Description
SAP BW	DDIC	Yes; System creates user during installation	Standard user	Initial: 19920706	<p>Superuser for the ABAP Dictionary and Software Logistics with the authorization SAP_ALL.</p> <p>DDIC is created in client 000.</p> <p>To protect the user from unauthorized access, change the default password and assign the user to the group SUPER.</p> <p>See also:</p> <p>Protecting Standard Users [SAP Web AS Security Guide]</p>
SAP BW	Database user				<p>You can find information on database users in Operating System and Database Platform Security Guides [SAP NetWeaver Security Guide]</p>
SAP BW	Background user in SAP BW	No	Technical user	No	<p>The background user in SAP BW is used for communicating with the SAP BW source systems, for extracting data, and for background processes in SAP BW. You create the background user in Customizing in SAP BW and assign it a password (see <i>Administration</i> → <i>Settings</i> → <i>Customizing</i> → <i>Business Information Warehouse</i> → <i>Automated Processes</i> → <i>Create User for Background Processes</i>). SAP recommends that you call the BW background user BWREMOTE. The system asks for a background user password when connecting to the source system. The authorization profile for the background user is S_BI-WHM_RFC.</p> <p>See also:</p> <p>Authorization Profile for Background Users [SAP Library].</p>

2 User Administration and Authentication

System	User	Delivered?	Type	Default Password	Description
SAP source system	Background user in SAP source system	No	Technical user	No	<p>The background user in the SAP source system is used for communicating with SAP BW and for extracting data.</p> <p>If you connect an SAP source system to an SAP BW, the background user is to be created in the source system. You can create the user directly in the source system in user maintenance. You can enter a name in Customizing in SAP BW that will be used as the default name for the background user when you connect a new source system. (See <i>Administration → Settings → Customizing → Business Information Warehouse → Connections to Other Systems → Connections Between SAP Systems and BW → Default for Users in the source system (Maintain ALE Communication)</i>). SAP recommends that you call the BW background user for the source system ALEREMOTE. If the source system you are using is also a BW system, SAP recommends that you create the background user for BW and the background user for the (BW) source system completely separately. The authorization profile for the background user in the source system is S_BI-WX_RFC. See also: Authorization Profile for Background Users [SAP Library].</p>

System	User	Delivered?	Type	Default Password	Description
SAP BW	Administrator	No	Individual user	No	<p>The SAP BW administrator is responsible for the connection to source systems, loading of metadata and implementation of BW statistics, among other things. He develops the data model and plans and monitors the processes in SAP (such as the loading process).</p> <p>See also: Authorization Profile for Working with the AWB [SAP Library]</p>
SAP BW	Authors and analysts	No	Individual user	No	<p>Authors and analysts require advanced analysis functionality and the ability to examine ad-hoc data. In order to accomplish their tasks, they required useful, manageable reporting and analysis tools.</p> <p>See also: Authorizations for Working with the Business Explorer [SAP Library]</p>
SAP BW	Executives and Knowledge Workers	No	Individual user	No	<p>Executives and Knowledge Workers require personalized, context-related information that is accessible via an intuitive user interface. They generally work with pre-defined navigation paths, but require the option of analyzing the summary data more deeply.</p> <p>See also: Authorizations for Working with the Business Explorer [SAP Library]</p>
SAP BW	Information consumers	No	Individual user	No	<p>Information Consumers require specific information (snapshot of a specific data set) in order to be able to execute their operative tasks.</p> <p>See also: Authorizations for Working with the Business Explorer [SAP Library]</p>

3 Authorizations

2.2 Authentication

SAP NetWeaver supports various authentication mechanisms. SAP BW uses a user ID and a password for logon (see [Logon and Password Protection in SAP Systems \[SAP Web AS Security Guide\]](#)).

See also:

[User Authentication \[SAP NetWeaver Security Guide\]](#).

Integration in Single Sign-On Environments

SAP BW supports [Secure Network Communications \(SNC\) \[SAP Web AS Security Guide\]](#).

SAP logon tickets

SAP BW supports SAP logon tickets. To make Single Sign-On available for several systems, users can issue themselves an SAP logon ticket after they have authenticated themselves with 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.

You can find more information under [SAP Logon Tickets \[SAP Web AS Security Guide\]](#).

Client certificates

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

You can find more information under [X509 Client Certificates \[SAP Web AS Security Guide\]](#).

3 Authorizations

The SAP BW authorization concept is based on the standard SAP authorization concept.

BW does not deliver roles but authorization templates. These can be used when creating roles and authorization profiles. Authorization templates are based on authorization objects that are checked when you execute activities in SAP BW. Among the authorization objects delivered are authorization objects of object class *Business Information Warehouse* (RS), and authorization objects for Data Mining. Authorization objects for Data Mining are delivered in their own object class (RSAN). You have to create authorization objects for reporting in the object class *Business Information Warehouse – Reporting* (RSR). You then create roles and authorization profiles in role maintenance. Use the authorization templates and the authorization objects, both those delivered by SAP and those that you have created, as a basis. By assigning roles to users, users obtain the authorizations defined for them in SAP BW.

You can find a detailed description of the SAP BW authorization concept under [Authorizations \[SAP Library\]](#) in the SAP BW documentation.



You can exclude individual InfoProviders from the authorization check for an authorization object in the maintenance for reporting authorization objects (transaction RSSM). To do this, choose the authorization object, select *Check for InfoProvider*, and choose *Change*. In the next screen you get a list of InfoProviders for which the authorization object check can be switched on and off. If the indicator is not set, the authorization object is ignored for this InfoProvider when a query is executed. As authorization assignments can be controlled in an InfoProvider-oriented way here, SAP recommends that you only grant restricted authorizations and do **not** give this authorization to information consumers.

4 Communication Security

4.1 Communication Channel Security

The following table provides an overview of the communication channels and the technology used in each case:

Communication between...	Technology used for communication	How is data protected?
Front end and application server	RFC	See RFC / ICF Security Guide [SAP NetWeaver Security Guide]
Application server and application server	RFC	See RFC / ICF Security Guide [SAP NetWeaver Security Guide]
SAP J2EE Engine and application server	RFC	See RFC / ICF Security Guide [SAP NetWeaver Security Guide]
SAP router and application server	RFC	See RFC / ICF Security Guide [SAP NetWeaver Security Guide]
Connection to database	RFC	See RFC / ICF Security Guide [SAP NetWeaver Security Guide]
Web Browser and application server	HTTP, HTTPS, SOAP	

When using Web applications, we recommend that you switch on encryption for HTTPS.

4.2 Communication Destinations

Connection destinations are particularly important in SAP BW for connecting data sources to SAP BW. These destinations are usually not delivered but are created by customers.

If you want to connect SAP systems and non-SAP data sources as source systems to SAP BW, you usually need RFC destinations. To use UD Connect, you need an RFC destination for the SAP WAS J2EE Engine. Communication between the SAP J2EE Engine and the SAP BW server is undertaken by the JCo. The destination for a Myself BW is created automatically by the system the first time you open the SAP BW Administrator Workbench. XML data is sent to the SAP Web AS SOAP service using specific ports, then into SAP BW. You can find more information under [Sending Data to the SOAP Service \[SAP Library\]](#) in the documentation for SAP BW. Communication between SAP BW and the sources systems is done by the BW background user and the background user in the source system (in the case of SAP source systems). The BW background user requires the authorization profile S_BI-WHM_RFC. The background user in the SAP source system requires the authorization profile S_BI-BW_RFC. You can find more information in the under [Authorization Profile for Background Users \[SAP Library\]](#).

5 Security with Data Storage

In SAP BW, data is stored on the SAP Web application server database.

If an end-user is evaluating data using MS EXCEL, s/he can also store her/his data locally. The end-user has to make sure that no unauthorized person can access the locally stored data.

If BW evaluations and analysis are called using BEx Web applications, data is displayed in a Web Browser. Data is then stored in a browser cache. SAP recommends that you always delete the browser cache when you have evaluated the data.

BEx Web applications can be implemented either as stateful or as stateless applications. Use the BW Web runtime for stateful Web application session cookies to combine independent requests (that is the function calls in a Web application, for example, navigation steps) for a session. Such cookies are called sap-contextid. The cookie contains a generated ID as a value. This ID allows the relevant session to be identified by the server. The session cookie is a temporary cookie and is deleted automatically when the browser window is closed. The server also has a timeout parameter. The session cookie is invalid after the timeout and can no longer be used for navigating in a Web application. You can use the session coding in the URL for the Web application by using the Web template attribute **NO-SESSION_COOKIE**. In this case, no session cookie is generated. So that the Web application uses the session coding in the URL, set x for the attribute **NO-SESSION_COOKIE**. Also see [Object Tag for the Properties of Web Templates \[SAP Library\]](#) in the SAP BW documentation.

Data in SAP BW is predominantly accessed for read purposes. However, in [Business Planning and Simulation \[SAP Library\]](#) data is also changed.

Personal data is also evaluated in SAP BW. SAP recommends that you make personal data anonymous in order to protect it from being accessed by an unauthorized party. You can find more information in the guide "Data Protection for SAP BW".

You can protect data from being accessed by an unauthorized end-user by assigning reporting authorizations. Data is not protected by the standard settings. However, you can flag InfoObjects in BW as being authorization-relevant (also see: [Setting Up Reporting Authorizations \[SAP Library\]](#)). Then data can only be accessed if the user has the required authorizations.

6 Minimal Installation

SAP BW uses JavaScript in the Web Browser when executing Web Applications. You can deactivate JavaScript for a minimal configuration. However, we recommend that you do **not** activate JavaScript, because otherwise all of the Web items and dialogs in the Web will no longer be available without restrictions and the navigation options in Web applications would be quite limited.

7 Additional Information Relevant to Security

Using active code

SAP BW uses JavaScript on the client machine in the Web browser during execution of Web applications. See [Minimal Installation \[Page 15\]](#).

Legal requirements

See the guide "Data Protection for SAP BW".

8 Trace and Log Files

BW Statistics

BW Statistics is a tool that allows you to analyze and optimize the programs running in SAP BW. Various characteristics, key figures, InfoSources, InfoCubes, and queries are available to you for analysis. These are delivered with SAP BW.

Of particular note from a security point of view are InfoCubes **BW Statistics – OLAP** (technical name: 0BWTC_C02) and **BW Statistics – OLAP, Detail Navigation** (technical name: 0BWTC_C03). The InfoCubes contain the data that is generated when you execute a query. By using these InfoCubes, user-specific statements can be reached on, for example, how often which InfoCubes or queries have been used, which selection conditions underlay the query, or how many navigation steps were performed.



To guarantee data protection, SAP recommends that you only activate BW statistics for authorized persons and that you make personal data anonymous. You can make data anonymous by determining constants in the update rules for data about the user.