SAP Catch Weight Management: Security Guide

SAP CWM 2.0

Copyright

Icons in Body Text

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*.

Typographic Conventions

Type Style	Description
Example text	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.

SAP Catch Weight Management: Security Guide

Introduction

This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

Target Audience

- Technology consultants
- System administrators

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

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet to manage business data, the demands on security are also rising. 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. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply also to the SAP Catch Weight Management (CWM) business scenario. We provide this Security Guide to assist you in securing the business scenario.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to the business scenario. If the business scenario consists of several application components, it contains an overall overview as well as the individual guides for each of the underlying application components.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- Before You Start [Seite 8]

  This section provides details about why security is necessary and how to use this document, and contains references to other Security Guides that form the foundation of this Security Guide.

- Technical System Landscape [Seite 10]

  This section provides an overview of the technical components and communication paths that are used by the business scenario.

- User Administration and Authentication [Seite 11]

  This section provides an overview of the following user administration and authentication aspects:

  - Recommended tools to use for user management.
  - User types that are required by the business scenario.
  - Standard users that are delivered with the business scenario.
  - Overview of the user synchronization strategy, if several components or products are involved.
  - Overview of how integration into Single Sign-On environments is possible.

- Authorizations [Seite 16]

  This section provides an overview of the authorization concept that applies to the business scenario.

- Network and Communication Security [Seite 17]

  This section provides an overview of the communication paths used by the business scenario and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- Data Storage Security [Seite 21]

  This section provides an overview of any critical data that is used by the business scenario and the security mechanisms that apply.

- Security for Third-Party or Additional Applications [Seite 22]

  This section provides security information that applies to third-party or additional applications that are used with the business scenario.

- Dispensable Functions with Impacts on Security [Seite 23]

  This section provides an overview of functions that have impacts on security and can be disabled or removed from the system.

- Other Security-Relevant Information [Seite 24]

  This section contains information about, for example, using the Web browser as a user front end.

- Trace and Log Files [Seite 25]

  This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- Appendix [Seite 26]

  This section provides references to further information.

Before You Start

Fundamental Security Guides

The Catch Weight Management (CWM) business scenario is built from the component applications. Therefore, the corresponding Security Guides also apply to the business scenario. Pay particular attention to the most relevant sections or specific restrictions, as indicated in the table below.

Fundamental Security Guides

Application	Guide	Most Relevant Sections or Specific Restrictions
SAP WebAS	SAP NetWeaver Security Guide	In the *SAP NetWeaver Security Guide*, choose *Security Guides for SAP NetWeaver Products* → *SAP Web Application Server Security Guide*.
SAP ECC	SAP ERP 2004 Security Guide	In the *SAP ERP 2004 Security Guide*, choose *Security Guides for SAP ECC 5.0*.
Operating Systems and Database Platforms	SAP NetWeaver Security Guide	In the *SAP NetWeaver Security Guide*, choose *Operating System and Database Platform Security Guides*.

For a complete list of the available SAP Security Guides, see the quick link **`securityguide`** on the SAP Service Marketplace.

Important SAP Notes

The most important SAP Notes that apply to the security of the business scenario are shown in the table below.

Important SAP Notes

SAP Note Number	Title	Comment
827573	Security Guide: Catch Weight Management	The note covers all problems discovered after the publication of the security guide, and provides additional information about security issues.
138498	Single Sign-On Solutions	Information on Single Sign-On Solutions for SAP systems.
30724	Data Protection and Security in SAP Systems	
128447	Trusted/Trusting Systems	Needed for Customizing of RFC connections for trusted/trusting systems.

Additional Information

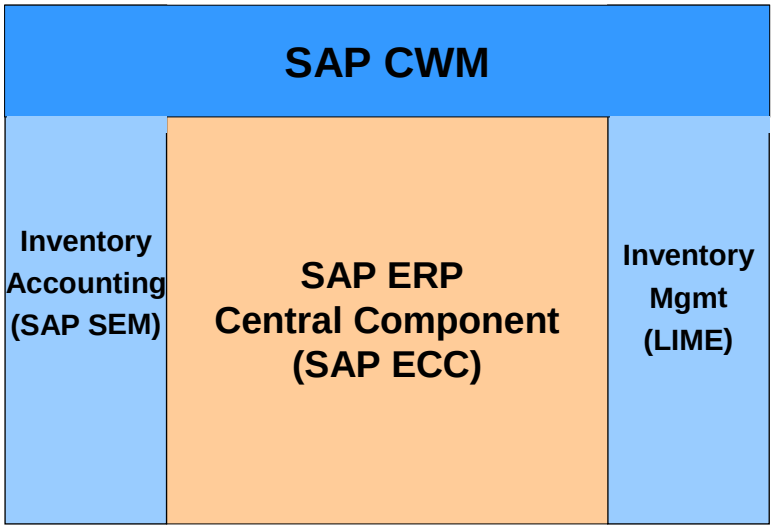
For more information about specific topics, see the quick links in the table below.

Quick Links to Additional Information

Content	Quick Link on the SAP Service Marketplace
Security	**service.sap.com/security**
Security Guides	**service.sap.com/securityguide**
Related SAP Notes	**service.sap.com/notes**
Released platforms	**service.sap.com/platforms**
Network security	**service.sap.com/network** **service.sap.com/securityguide**
Technical infrastructure	**service.sap.com/ti**
SAP Solution Manager	**service.sap.com/solutionmanager**

Technical System Landscape

The figure below shows an overview of the technical system landscape for the Catch Weight Management (CWM) business scenario.



For more information about the technical system landscape, see the resources listed in the table below.

More Information About the Technical System Landscape

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace
Technical description for the CWM business scenario and the underlying technological components such as SAP NetWeaver	Master Guide	`service.sap.com/instguides`
Technical configuration High availability	Technical Infrastructure Guide	`service.sap.com/ti`
Security		`service.sap.com/security`

User Administration and Authentication

The Catch Weight Management (CWM) business scenario uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication described in the SAP Web AS Security Guide for ABAP Technology also apply to the business scenario.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to the business scenario in the following topics:

- User Management [Seite 12]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with the business scenario.

- User Data Synchronization [Seite 14]

  The business scenario shares user data with other sources. This topic describes how the user data is synchronized with these other sources.

- Integration into Single Sign-On Environments [Seite 15]

  This topic describes how the business scenario supports Single Sign-On mechanisms.

User Management

User management for the Catch Weight Management (CWM) business scenario uses the mechanisms provided by the SAP Web Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for the business scenario, see the sections below. In addition, we provide a list of the standard users required for operating the business scenario.

User Administration Tools

The table below shows the tools to use for user management and user administration with the business scenario.

User Management Tools

Tool	Detailed Description
User Management Engine (UME) administration console	Use the Web-based UME administration console to maintain users, roles, and authorizations in Java-based systems that use the UME for the user store, for example, the SAP Web AS Java and the Enterprise Portal. The UME also supports various persistency options, such as ABAP Engine or a directory server.
User Management for the ABAP Engine (transaction code SU01)	Use the user management transaction code SU01 to maintain users in ABAP-based systems.
Profile Generator (transaction code PFCG)	Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.
Central User Administration (CUA)	Use the CUA to centrally maintain users for multiple ABAP-based systems. Synchronization with a directory server is also supported.

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

For more information about these user types, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP WebAS ABAP Security Guide* → *User Types*.

Standard Users

The table below shows the standard users that are necessary for operating the business scenario.

Standard Users

System	User ID	Type	Password	Description
SAP WebAS	<sapsid>adm	SAP System	To be entered	SAP NetWeaver '04 Installation

		Administrator		Guide
SAP WebAS	SAP Service <sapsid>	SAP System Service Administrator	To be entered	SAP NetWeaver '04 Installation Guide
SAP WebAS	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See SAP NetWeaver Security Guide	See SAP NetWeaver Security Guide	SAP NetWeaver Security Guide → *Security Guides for SAP NetWeaver Products* → *SAP Web Application Server Security Guide* → *SAP WebAS Security Guide for ABAP Technology* → *User Authentication* → *Protection Standard Users*
SAP ECC / SAP CWM	SAP ECC / SAP CWM User	See SAP ECC Security Guide	See SAP ECC Security Guide	SAP ERP 2004 Security Guide → *SAP ECC 5.0* → *User Administration and Authentication*

For information about SAP NetWeaver standard users, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *SAP WebAS Security Guide for ABAP Technology* → *User Authentication* → *Protecting Standard Users*.

For information about SAP NetWeaver password rules, see the SAP Help Portal at **`help.sap.com`** → *SAP NetWeaver* → *Release 04* → *Security* → *Identity Management* → *Users and Roles (BC-SEC-USR)* → *User Maintenance* → *Logon and Password Security in the SAP System* → *Password Rules*.

User Data Synchronization

To avoid administrative effort, the use of user data synchronization could be useful in your system landscape. Since the Catch Weight Management (CWM) business scenario is based on SAP NetWeaver-based components, all the mechanisms for user data synchronization of SAP NetWeaver are available for CWM.

For information about user data synchronization, in the SAP Service Marketplace at **`service.sap.com/securityguide`** see *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape*.

Integration into Single Sign-On Environments

The Catch Weight Management (CWM) business scenario and its components support the Single Sign-On (SSO) mechanisms provided by the SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication described in the SAP Web Application Server Security Guide also apply to the CWM business scenario.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides for an SSO environment when using SAP GUI for Windows or Remote Function Calls.

For more information,see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP Web Application Server Security Guide* → *Secure Network Communications (SNC)*.

SAP Logon Tickets

The business scenario and its components support the use of logon tickets for SSO when using a Web browser as the front end client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial 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 Service Marketplace at **`service.sap.com/securityguide`** → *SAP Web Application Server Security Guide* → *SAP Logon Tickets*.

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front end client can also provide X.509 client certificates to use for authentication. 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.

For more information, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP Web Application Server Security Guide* → *Client Certificates*.

Authorizations

The Catch Weight Management (CWM) business scenario uses the authorization provided by the SAP Web Application Server. Therefore, the recommendations and guidelines for authorizations described in the SAP Web AS Security Guide ABAP also apply to the business scenario.

The SAP Web Application Server authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the Profile Generator (transaction code PFCG) on the SAP Web AS ABAP and the User Management Engine's user administration console for SAP Web AS Java.

For information about the use of access control lists, see the relevant security guide for the associated application at **`service.sap.com/securityguide`**. (For example, for access control lists for cProject Suite, see *cProject Suite Security Guide* → *Authorizations*.)

Standard Roles

As the CWM business scenario has no scenario-based standard roles, the standard roles delivered with the underlying components can be used.

Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system 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, there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for the Catch Weight Management (CWM) business scenario is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to the business scenario. Details that specifically apply to the business scenario are described in the following topics:

- Communication Channel Security [Seite 18]

  This topic describes the communication paths and protocols used by the business scenario.

- Network Security [Seite 19]

  This topic describes the recommended network topology for the business scenario. It shows the appropriate network segments for the various client and server components, and where to use firewalls for access protection. It also includes a list of the ports needed to operate the business scenario.

- Communication Destinations [Seite 20]

  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → :

- *Network and Communication Security*
- *Security Aspects for Connectivity and Interoperability*

Communication Channel Security

As communication channels transfer all kinds of your business data, they should be protected against unauthorized access. SAP offers general recommendations and technologies to protect your system landscape based on SAP NetWeaver.

You should activate the Secure Network Communication (SNC) for RFC and Secure Sockets Layer Protocol (SSL) for http within all communication channels in the Catch Weight Management (CWM) business scenario to achieve a secure system landscape.

For information about the communication security of SAP NetWeaver, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

For information about security aspects for connectivity and interoperability of SAP NetWeaver, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Security Aspects for Connectivity and Interoperability*.

The table below shows the communication paths used by the business scenario, the protocol used for the connection, and the type of data transferred.

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using SAP GUI for Windows to application server	DIAG	All application data	For example, passwords, business data
Front end client using a Web browser to application server	HTTP(S)	All application data	For example, passwords, business data
Application server to application server	RFC, HTTP(S)	Integration data	Business data
Application server to third-party application	HTTP(S)	All application data	For example, passwords, business data

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Transport Layer Security*.

Network Security

Your network infrastructure is extremely important in protecting your system. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping.

SAP offers general recommendations to protect your system landscape based on SAP NetWeaver.

For information about the network security of SAP NetWeaver, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

A minimum security requirement for your network infrastructure is the use of a firewall for all your services provided via the Internet.

A more secure variant is to protect your systems (or groups of systems) by locating the different "groups" in different network segments, each protected against unauthorized access by a firewall. (Note: external security attacks can also come from "inside" if the intruder has already taken over control of one of your systems.)

For information about access control using firewalls, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security – Using Firewall Systems for Access Control*.

Communication Destinations

The Catch Weight Management (CWM) business scenario does not use any communication destinations by default. If you are integrating the CWM business scenario with other business scenarios using communication destinations, read the corresponding or the SAP NetWeaver Security Guide.

Data Storage Security

The data storage security of SAP NetWeaver and components installed on this base is described in detail in the SAP NetWeaver Security Guide.

For information about the data storage security of SAP NetWeaver, see SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Operation System and Database Platform Security Guides*.

Security for Additional Applications

For information about the security for additional applications, see the fundamental security guides listed in Before You Start [Seite 8].

Dispensable Functions with Impacts on Security

For information about the dispensable functions with impacts on security, see the fundamental security guides listed in Before You Start [Seite 8].

Other Security-Relevant Information

For information about the other security-relevant information, see the fundamental security guides listed in Before You Start [Seite 8].

Trace and Log Files

All trace and log files for the Catch Weight Management (CWM) business scenario use SAP NetWeaver standard mechanisms.

For information about the security for additional applications, see the fundamental security guides listed in Before You Start [Seite 8].

Appendix

Related Security Guides

You can find more information about the security of SAP applications on the SAP Service Marketplace, quick link **`security`**. Security guides are available under the quick link **`securityguide`**.

Related Information

For more information about topics related to security, see the following quick links:

Quick Links to Related Information

Content	Quick Link on the SAP Service Marketplace
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	**`service.sap.com/instguides`** **`service.sap.com/ibc`**
Related SAP Notes	**`service.sap.com/notes`**
Released Platforms	**`service.sap.com/platforms`**
Network Security	**`service.sap.com/network`** **`service.sap.com/securityguide`**
Technical Infrastructure	**`service.sap.com/ti`**
SAP Solution Manager	**`service.sap.com/solutionmanager`**