Security Guide

SAP® Transportation Management 8.0 Security Guide

Using SAP® TM 8.0, SAP ERP® 6.0 including enhancement package 5, and SAP NetWeaver® 7.0 including enhancement package 2

Target Audience

- Technical Consultants
- System Administrators

PUBLIC
Document version: 1.4 – 2012-03-26

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com

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.

Typographic Conventions

Example	Description
`<Example>`	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your `<User Name>`”.
▶ *Example* → *Example* ◀	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
`Example`	Words or characters that you enter in the system exactly as they appear in the documentation
`http://www.sap.com`	Textual cross-references to an internet address
`/example`	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	■ Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. ■ Cross-references to other documentation or published works
`Example`	■ Output on the screen following a user action, for example, messages ■ Source code or syntax quoted directly from a program ■ File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, `SELECT` and `INCLUDE`
EXAMPLE	Keys on the keyboard

Document History

⚠ CAUTION

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at the following location: `http://service.sap.com/securityguide`.

The following table provides an overview of the most important document changes.

Version	Date	Description
1.0	2010-11-02	Initial version
1.1	2011-06-17	Removed “References” section
1.2	2011-10-10	Paths for freight unit and freight order corrected and line for freight booking added (table in chapter “Activating Change Documents”)
1.3	2011-11-25	Update to textual paths to SAP Help Portal
1.4	2012-03-26	Caution added to Tendering Internet Scenario

Table of Contents

1 Introduction

CAUTION

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

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

Target Audience

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such 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 Necessary

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. 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 likewise to SAP Transportation Management 8.0 (SAP TM 8.0). To assist you in securing your SAP Transportation Management 8.0 system using SAP ERP 6.0 including enhancement package 5 and SAP NetWeaver 7.0 including enhancement package 2, we provide this Security Guide.

About This Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Transportation Management 8.0 using SAP ERP 6.0 including enhancement package 5 and SAP NetWeaver 7.0 including enhancement package 2.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- *Before You Start*

  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- *Technical System Landscape*

  This section provides an overview of the technical components and communication paths that are used by SAP Transportation Management 8.0..
- *Security Aspects of Data Flow and Processes*

  This section provides an overview of security aspects involved throughout the most-widely used processes within SAP TM 8.0.
- *User Administration and Authentication*

  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 SAP Transportation Management 8.0..
  - Standard users that are delivered with SAP Transportation Management 8.0.
  - 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*

  This section provides an overview of the authorization concept that applies to SAP TM 8.0.
- *Session Security Protection*

  This section provides information about activating secure session management, which prevents javascript or plug-ins from accessing the SAP logon ticket or security session cookie(s).
- *Network and Communication Security*

  This section provides an overview of the communication paths used by SAP TM 8.0 and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
- *Internet Communication Framework Security*

  This section provides an overview of the Internet Communication Framework (ICF) services that are used by SAP TM 8.0.
- *Data Storage Security*

  This section provides an overview of any critical data that is used by SAP TM 8.0 and the security mechanisms that apply.
- *Security for Third-Party or Additional Applications*

  This section provides security information that applies to third-party or additional applications that are used with SAP TM 8.0.
- *Dispensable Functions with Impacts on Security*

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

  This section provides an overview about the security aspects that apply to the enterprise services delivered with SAP TM 8.0.
- *Other Security-Relevant Information*

This section contains information about:

  - Integration of SAP Visual Business 1.1

- *Security-Relevant Logging and Tracing*

  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.

- *Services for Security Lifecycle Management*

  This section provides an overview of services provided by Active Global Support that are available to assist you in maintaining security in your SAP systems on an ongoing basis.

- *Appendix*

  This section provides references to further information.

2 Before You Start

Fundamental Security Guides

SAP Transportation Management 8.0 is based on SAP ERP 6.0 including enhancement package 5 and SAP NetWeaver 7.0 including enhancement package 2 Therefore, the corresponding Security Guides also apply to SAP Transportation Management 8.0. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Security Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver 7.0 EhP2 Security Guides (Complete)	Not applicable
SAP Supply Chain Management 7.0 Security Guide	Not applicable
SAP Web Application Server	■ SAP Web AS Security Guide for ABAP Technology ■ SAP Web AS Security Guide for J2EE Technology ■ Internet Transaction Server Security Aspects in Development
SAP Internet Transaction Server Security	Not applicable
SAP Content Server Security Guide	Not applicable
SAP Knowledge Warehouse Security Guide	Not applicable
SAP Event Management 7.0 Security Guide	Not applicable
SAP Mobile Infrastructure Security Guide	Not applicable
SAP NetWeaver Business Intelligence Security Guide	Not applicable
SAP Knowledge Management	■ SAP Knowledge Management Security Guide ■ SAP Content Management Security Guide ■ SAP Trex Security Guide
SAP Process Integration Security Guides	Not applicable
System Management	Security Aspects with System Management

For a complete list of the available SAP Security Guides, see `http://service.sap.com/securityguide`.

Important SAP Notes

The most important SAP Notes that apply to the security of SAP TM 8.0 are shown in the table below.

Important SAP Notes

SAP Note Number	Title	Comment
510007	Setting up SSL on the Web Application Server	Not applicable
149926	Secure e-mail: Encryption, digital signature	This note provides information about how to connect a third party e-mail proxy to your SAP system in order to enable encryption and the use of digital signatures for sending and receiving e-mails from your SAP system
1493710	Texts in the alert inbox are not encoded	This note provides information about how to activate additional settings for the alert inbox.
817623	Integrating a virus scan in your own SAP applications	This note provides information about the SAP virus scan interface.
1514253	Attachment Folder config introduced to allow file uploads	Dependent Object Attachment Folder (/BOBF/ATTACHMENT_FOLDER) is enhanced with new capabilities.
786179	Data security products: Application in the antivirus area	This note provides information about the SAP virus scan interface.
853878	HTTP WhiteList Check (security)	This note provides information about the HTTP white list. This is required if you want to use file upload functionality.

In addition, you can find a list of security-relevant SAP Hot News and SAP Notes on the SAP Service Marketplace at `http://service.sap.com/securityguide`.

Additional Information

For more information about specific topics, see the Quick Links as shown in the table below.

Quick Links to Additional Information

Content	Quick Link on SAP Service Marketplace or SDN
Security	`http://sdn.sap.com/irj/sdn/security`
Security Guides	`http://service.sap.com/securityguide`
Related SAP Notes	`http://service.sap.com/notes`
Released Platforms	`http://service.sap.com/pam`
Network Security	`http://service.sap.com/securityguide`
SAP Solution Manager	`http://service.sap.com/solutionmanager`
SAP NetWeaver	`http://sdn.sap.com/irj/sdn/netweaver`

3 Technical System Landscape

The figure below shows an overview of the technical system landscape for SAP Transportation Management 8.0 using SAP ERP 6.0 including enhancement package 5 and SAP NetWeaver 7.0 including enhancement package 2.

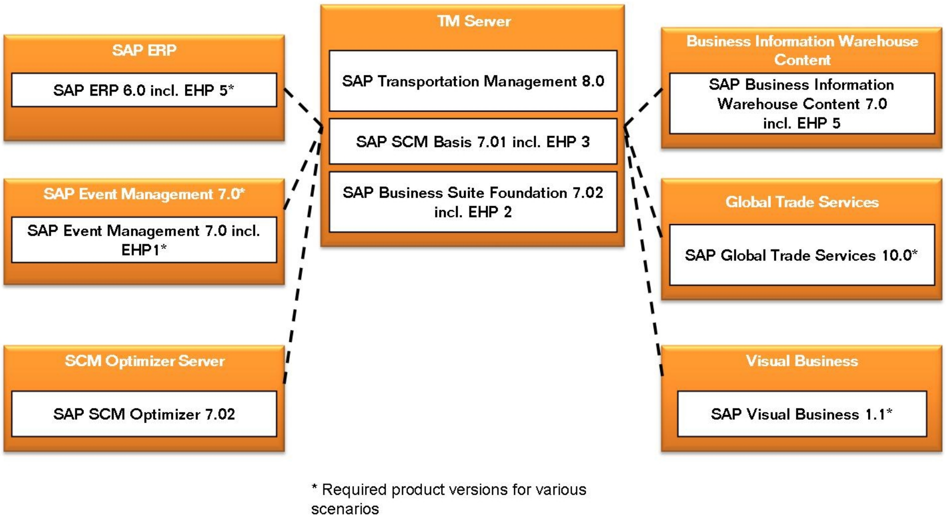

TM Server
SAP Transportation Management 8.0
SAP SCM Basis 7.01 incl. EHP 3
SAP Business Suite Foundation 7.02 incl. EHP 2
SAP ERP
SAP ERP 6.0 incl. EHP 5*
SAP Event Management 7.0*
SAP Event Management 7.0 incl. EHP1*
SCM Optimizer Server
SAP SCM Optimizer 7.02
Business Information Warehouse Content
SAP Business Information Warehouse Content 7.0 incl. EHP 5
Global Trade Services
SAP Global Trade Services 10.0*
Visual Business
SAP Visual Business 1.1*
* Required product versions for various scenarios

Figure 1: Technical System Landscape

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 or Tool	Quick Link to SAP Service Marketplace or SDN
Technical description for SAP Transportation Management 8.0 and the underlying components such as SAP NetWeaver	SAP Transportation Management 8.0 Master Guide	http://service.sap.com/instguides
High availability	*High Availability for SAP Solutions*	http://sdn.sap.com/irj/sdn/ha
Technical landscape design	See applicable documents	http://sdn.sap.com/irj/sdn/landscapedesign
Security	See applicable documents	http://service.sap.com/security

4 Security Aspects of Data Flow and Processes

Some processes being part of SAP Transportation Management 8.0 require special configuration in order to be executed in a secure way. The following list provides an overview about the most critical processes and data flows, along with security measures to be taken into consideration.

E-mail based Tendering Scenario

The figure below shows an overview of the e-mail based tendering scenario for SAP Transportation Management 8.0.

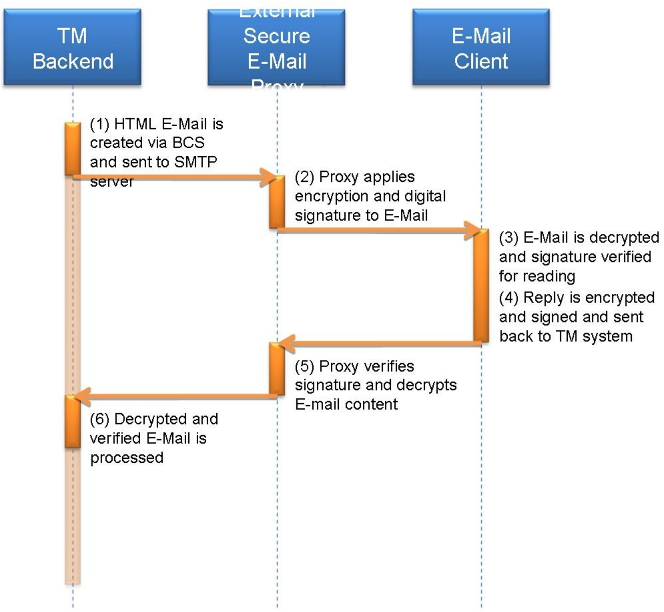

TM Backend
External Secure E-Mail Proxy
E-Mail Client
(1) HTML E-Mail is created via BCS and sent to SMTP server
(2) Proxy applies encryption and digital signature to E-Mail
(3) E-Mail is decrypted and signature verified for reading
(4) Reply is encrypted and signed and sent back to TM system
(5) Proxy verifies signature and decrypts E-mail content
(6) Decrypted and verified E-Mail is processed

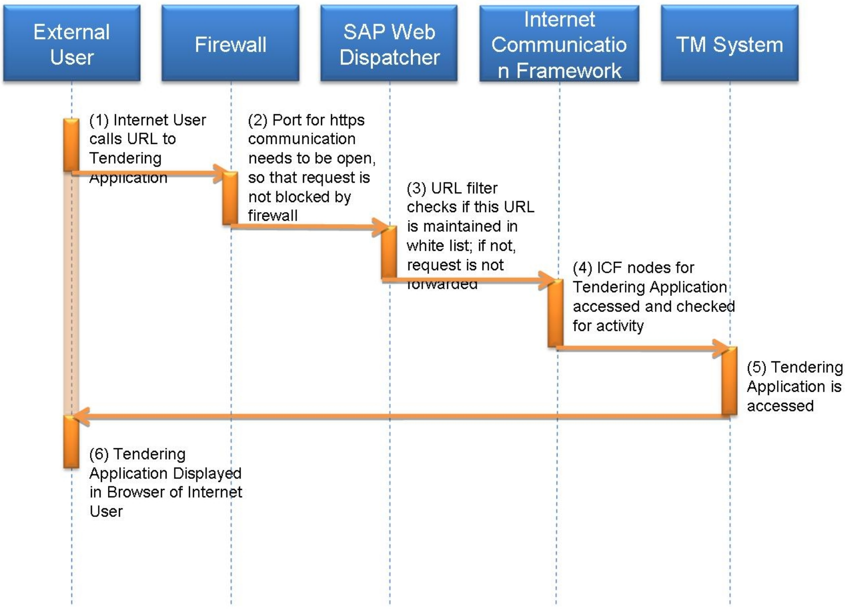
Figure 2:

Step	Description	Security Measure
1	HTML e-mail is created via BCS and sent to SMTP server	In TM application Customizing, use of encryption and digital signatures needs to be enabled. Choose in the SAP TM Customizing ▶ *SAP Transportation Management → Transportation Management → Freight Order Management → Tendering → Define General Settings for Tendering → 03 – E-mail and SMS Content → E-Mail security settings* ◀.
2	Proxy applies encryption and digital signature to e-mail	External secure e-mail proxy needs to be maintained and activated for SAP TM system. For more details, refer to SAP Note 149926 Keys must be exchanged between sender and recipient prior to sending the e-mail. It is strongly recommended to set up the policy of the e-mail proxy in a way that e-mails are only sent if encryption and applying

Step	Description	Security Measure
		digital signatures is possible. If this is not possible, for instance due to missing keys, E-mails must not be sent in an insecure way.
3	E-mail is decrypted and signature verified for reading	Recipient's e-mail client must support encryption and digital signatures and keys must have been exchanged by sender and recipient before
4	Reply is encrypted and signed and sent back to TM system	Refer to step 3
5	Proxy verifies signature and decrypts e-mail content	Refer to step 2
6	Decrypted and verified e-mail is processed	Not applicable

Tendering Internet Scenario

The figure below shows an overview of the tendering internet scenario for SAP Transportation Management 8.0.



(1) Internet User calls URL to Tendering Application

(2) Port for https communication needs to be open, so that request is not blocked by firewall

(3) URL filter checks if this URL is maintained in white list; if not, request is not forwarded

(4) ICF nodes for Tendering Application accessed and checked for activity

(5) Tendering Application is accessed

(6) Tendering Application Displayed in Browser of Internet User

Figure 3:

Step	Description	Security Measure
1	Internet User calls URL to Tendering Application	Internet user needs to be created and maintained for business partner of role “Contact Person” in TM system. We recommend that authentication is done using certificates, which need to be exchanged with external user before, so that the Internet user cannot log on to the system by entering username and password
2	Port for https communication needs to be open, so that request is not blocked by firewall	Firewall needs to be maintained accordingly
3	URL filter checks if this URL is maintained in white list; if not, request is not forwarded	SAP Web Dispatcher needs to be configured as URL filter; only the URLs to ICF services for the carrier POWL, the external tendering quotation application and to the freight order application for tendering must be maintained in the white list, otherwise external users could access internal services for which they are not authorized. For more information, see SAP Library for SAP NetWeaver 2004 on SAP Help Portal at `http://help.sap.com/nwhtm`. In SAP Library, choose ▶ *SAP NetWeaver → Solution Life Cycle Management → SAP Web Dispatcher → Management of the SAP Web Dispatcher → SAP Web Dispatcher as a URL Filter* ◀.
4	ICF node for Tendering Application accessed and checked for activity	ICF nodes for external tendering application (POWL, external tendering quotation application and freight order for tendering) need to be active
5	Tendering Application is accessed	Authorization profile for role of external user needs to be maintained accordingly. Secure HTTP Session Management should be activated on the ABAP AS as described in note 1322944.
6	Tendering Application Displayed in Browser of Internet User	Not applicable

NOTE

If SAP Event Management is part of your scenario and you want to gain external users access to execution information via SAP Event Management, it is strongly recommended to secure the external access to the SAP Event Management accordingly.

CAUTION

If you implement this scenario, a connection is established between your SAP TM server and the Internet. We therefore recommend that you set up tendering-based communication using **asynchronous, message-based B2B communication.**

File Upload Scenario

The figure below shows an overview of the file upload scenario for SAP Transportation Management 8.0.

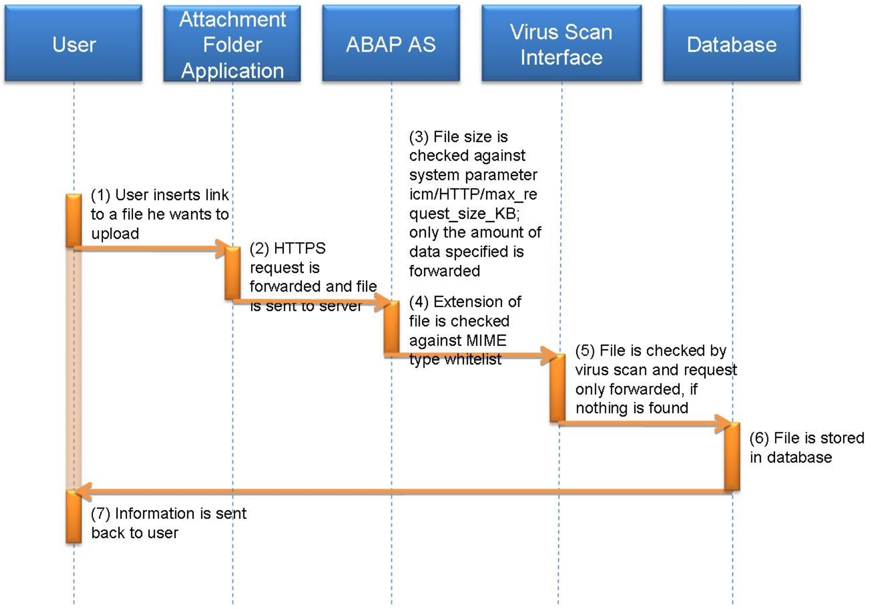

User
Attachment Folder Application
ABAP AS
Virus Scan Interface
Database
(1) User inserts link to a file he wants to upload
(2) HTTPS request is forwarded and file is sent to server
(3) File size is checked against system parameter icm/HTTP/max_request_size_KB; only the amount of data specified is forwarded
(4) Extension of file is checked against MIME type whitelist
(5) File is checked by virus scan and request only forwarded, if nothing is found
(6) File is stored in database
(7) Information is sent back to user

Figure 4:

The table below shows the security aspect to be considered for the process step and what mechanism applies.

Step	Description	Security Measure
1	User inserts link to a file he wants to upload	User needs to be aware of the file he wants to upload
2	HTTPS request is forwarded and file is sent to server	Not applicable
3	File size is checked against system parameter `icm/HTTP/max_request_size_KB`; only the amount of data specified is forwarded	Maximum file size needs to be restricted in order to secure the server. For more information, see SAP Library for SAP NetWeaver 7.0 on SAP Help Portal at `http://help.sap.com/nw`. In SAP Library, choose ▶ *SAP NetWeaver Library → Administrator's Guide → Technical Operations Manual for SAP NetWeaver → Security Guides for SAP NetWeaver According to Usage Types → Security Aspects for Usage Type DI and Other Development Technologies → Security Issues in Web Dynpro for ABAP → Security Notes for FileUpload UI Elements* ◀.
4	MIME type of file is checked against white list	The extension of the uploaded file (but not its content) is checked against MIME type white list; as a prerequisite for using the white list, SAP Note 1514253 must be implemented.
5	File is checked by virus scan and request only forwarded, if nothing is found	Virus scan needs to be active in your system. For more information, see SAP Library for SAP NetWeaver 7.0 on SAP Help Portal at `http://help.sap.com/nw`. In SAP Library, choose ▶ *SAP NetWeaver Library → SAP NetWeaver Developer's Guide → Fundamentals → Making Applications Enterprise-Ready → Secure Programming → Java → Secure Programming → SAP Virus Scan Interface* ◀. We strongly recommend that you create a virus scan profile with linkage type *All steps successful*.
6	File is stored in database	Not applicable
7	Information is sent back to user	Not applicable

CAUTION

Only file extensions are compared to the entries in the white list, not the content of the files. The file upload functionality can be disabled, in order to prevent users from uploading files into your system. Implementation of SAP Note 1514253 is a prerequisite for disabling file upload functionality. It is recommended to disable the upload functionality, if it is not required by your business scenarios.

Always ensure that your virus scan is set up and working correctly, before enabling file uploads. Do not use file upload in case your virus scan is not up and running.

URL Upload Scenario

The figure below shows an overview of the URL upload scenario for SAP Transportation Management 8.0.

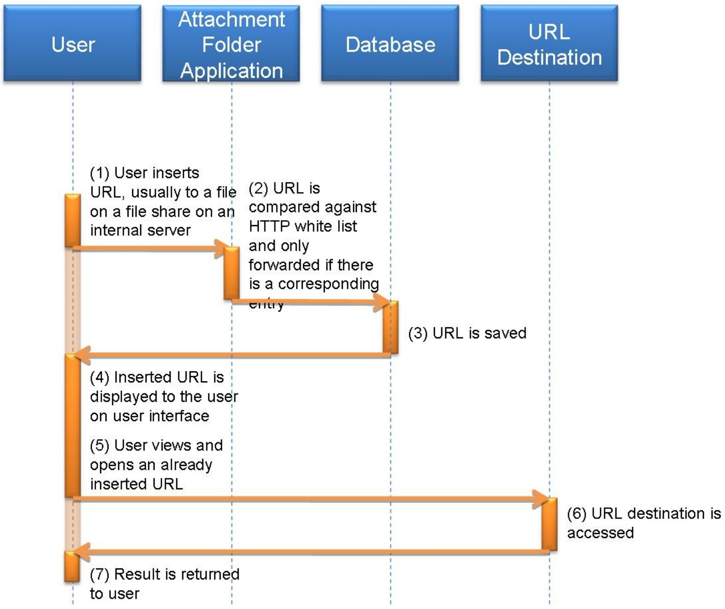

User
Attachment Folder Application
Database
URL Destination
(1) User inserts URL, usually to a file on a file share on an internal server
(2) URL is compared against HTTP white list and only forwarded if there is a corresponding entry
(3) URL is saved
(4) Inserted URL is displayed to the user on user interface
(5) User views and opens an already inserted URL
(6) URL destination is accessed
(7) Result is returned to user

Figure 5:

Step	Description	Security Measure
1	User inserts URL, usually to a file on a file share on an internal server	Secure file shares appropriately
2	URL is compared against HTTP white list and only forwarded if there is a corresponding entry	Maintain HTTP white list according to SAP note 853878 with entry type 01. It is strongly recommended to restrict the access to a secure folder on an internal file share.
3	URL is saved	Not applicable
4	Inserted URL is displayed to the user on user interface	Attachment folder UI configuration should enable displaying column 'URL'
5	User views and opens an already inserted URL	User needs to be aware of the URL he tries to access
6	URL destination is accessed	Not applicable

Step	Description	Security Measure
7	Result is returned to user	Not applicable

5 User Administration and Authentication

SAP Transportation Management 8.0 uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server ABAP Security Guide also apply to SAP Transportation Management 8.0.

For more information, see SAP Service Marketplace at `http://service.sap.com/securityguide` → *SAP Basis / Web AS Security Guides*

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP TM 8.0 in the following topics:

- *User Management* [external document]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with SAP TM 8.0.
- *Integration Into Single Sign-On Environments* [external document]

  This topic describes how SAP TM 8.0 supports Single Sign-On mechanisms.

5.1 User Management

User management for SAP Transportation Management 8.0 uses the mechanisms provided with the SAP NetWeaver Application Server ABAP, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for SAP Transportation Management 8.0, see the sections below. In addition, we provide a list of the standard users required for operating SAP Transportation Management 8.0.

User Administration Tools

The table below shows the tools to use for user management and user administration with SAP TM 8.0.

User Management Tools

Tool	Detailed Description
User Management for the ABAP Engine (transaction `SU01`)	Use the User Management tool to maintain users in ABAP-based systems. For more information, see User and Role Administration of Application Server ABAP [External].

Tool	Detailed Description
Profile Generator (transaction `PFCG`)	Use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems. For more information, see User and Role Administration of Application Server ABAP [External].
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 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 J2EE Engine and the Enterprise Portal. The UME also supports various persistency options, such as the ABAP Engine or a directory server.
SAP J2EE Engine user management using the Visual Administrator	Use the Visual Administrator to maintain users and roles on the SAP J2EE Engine. The SAP J2EE Engine also supports a pluggable user store concept. The UME is the default user store. For more information, see User Management Engine [External].

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.

The user types that are required for SAP TM 8.0 include:

- Individual users:
  - Dialog users are used for business users that are assigned to roles that allow them to work individually on their dedicated tasks in your SAP Transportation Management 8.0 system.
  - Internet users are used for external users that shall be allowed to access your SAP Transportation Management 8.0 system from the internet. If your scenario contains the tendering internet scenario, where carriers shall be able to log on to your SAP Transportation Management 8.0 system in order to view requests for quotations they have received from you and where they shall be able to submit quotations respectively, these external users access your SAP Transportation Management 8.0 system with internet users.
- Technical users:
  - Service users are used for technical purposes, such as service administrators, and are usually available to a larger, anonymous group of users.
  - Communication users are used for dialog-free communication for external RFC calls, for instance for the communication between your SAP Transportation Management 8.0 system and the SAP SCM Optimizer server.
  - Background users are used for running background jobs and executing reports.

For more information about these user types, see *User Types* in the *SAP NetWeaver Application Server ABAP Security Guide* on SAP Service Marketplace at http://service.sap.com/securityguide → *SAP NetWeaver Security Guides 7.0 (complete)* → *SAP NetWeaver 7.0 Security Guides* → *Security Guides for SAP NetWeaver According to Usage Types* → *Security Guide for Usage Type AS* → *SAP NetWeaver Application Server ABAP Security Guide*.

Standard Users

The table below shows the standard users that are necessary for operating SAP TM 8.0.

Standard Users

System	User	Type	Password	Description
SAP TM 8.0	<sapsid>adm	Dialog user	You must specify the initial password during the installation.	SAP TM System Administrator
SAP TM 8.0	SAPService <sapsid>	Service user	You must specify the initial password during the installation.	SAP TM System Service Administrator
SAP TM 8.0	SAPService <sapsid>	Internet user	You must specify the initial password during the installation.	SAP TM carriers, who take part in the tendering process.
SAP SCM 7.0 Server	<sapsid>adm	Dialog user	You must specify the initial password during the installation.	SAP System Administrator For more information, see *SAP SCM Installation Guide* → *Installation Document - SCM Server 7.0* → *<relevant Operating System/DB>* → *Installation Documentation*.
SAP SCM 7.0 Server	SAPService <sapsid>	Service user	You must specify the initial password during the installation.	SAP System Service Administrator For more information, see *SAP SCM Installation Guide* → *Installation Document - SCM Server 7.0* → *<relevant Operating System/DB>* → *Input for the Installation*.
SAP WebAS	SAP Standard ABAP Users	Service users	You must specify the initial password	For more information, see

System	User	Type	Password	Description
	(SAP*, DDIC, EARLYWATCH, SAPCPIC)		during the installation.	▶ *SAP NetWeaver 7.0 Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server ABAP Security Guide → User Authentication → Protecting Standard Users* ◀.
SAP WebAS	SAP Standard J2EE Users (Administrator, Guest, Emergency)	Dialog users	You must specify the initial password during the installation.	For more information, see ▶ *SAP NetWeaver 7.0 Security Guide → Security Guides for SAP NetWeaver According to Usage Types → Security Guide for Usage Type AS → SAP NetWeaver Application Server Java Security Guide → User Administration and Authentication → User Administration and Standard Users → Standard Users and Standard User Groups* ◀.
SAP J2EE Engine	SAPJSF	Communication user	You must specify the initial password during the installation.	For more information, see ▶ *SAP SCM Installation Guide → Installation Document - SCM Server 7.0 → <relevant Operating System/DB> → Installation Process → Input for the Installation* ◀.
SAP SCM 7.0	RFC Communication Users	Communication users	You must specify the initial password during the installation.	The authorizations of the user depend on the business case. For more information, see section *Authorizations* in this Security Guide. You need an RFC communication user for each RFC

System	User	Type	Password	Description
				destination in the section *Communication Destinations*.
SAP SCM 7.0	Business Processing Users	Dialog users	You must specify the initial password during the installation.	You need a user in each component, for each employee working with the system. For more information, see section *Authorizations* in this Security Guide.
SAP Event Management	SAP Event Management Users	Dialog users	You must specify the initial password during the installation.	For more information, see SAP Library for SAP Event Management under *SAP Event Management User*.

RECOMMENDATION

We recommend changing the user IDs and passwords for users that are automatically created during installation.

5.2 User Data Synchronization

To avoid administration effort, you can use user data synchronization in your system landscape. Since SAP Transportation Management 8.0 is based on SAP NetWeaver 7.0 including enhancement package 2, all the mechanisms for user data synchronization of SAP NetWeaver 7.0 including enhancement package 2 are available for SAP TM 8.0.

NOTE

For information about user data synchronization, see the *SAP NetWeaver 7.0 Security Guide* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape*.

5.3 Integration Into Single Sign-On Environments

SAP Transportation Management 8.0 supports the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide [External] also apply to SAP Transportation Management 8.0.

For more information, see the section *Secure Network Communications (SNC)* in the *SAP NetWeaver Application Server ABAP Security Guide* on SAP Service Marketplace at `http://service.sap.com/securityguide` → *SAP Basis / Web AS Security Guides* → *SAP NetWeaver Application Server ABAP Security Guide*.

The following standard mechanisms are supported by SAP Transportation Management 8.0:

- Secure Network Communications (SNC)
  SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.
- SAP logon tickets
  SAP Transportation Management 8.0 supports the use of logon tickets for SSO when using a Web browser as the frontend 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.
- Client certificates
  As an alternative to user authentication using a user ID and passwords, users using a Web browser as a frontend 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.

NOTE

If your scenario contains the tendering internet scenario and external internet users have access to your system, it is recommended to use client certificates instead of authentication with username and password. This way, internet users are prevented from trying to log on with another user's username.

For more information, about the available authentication mechanisms, see SAP Library for SAP NetWeaver Including Enhancement Package 1 on SAP Help Portal at http://help.sap.com/nw. In SAP Library, choose ▶ *SAP NetWeaver → SAP NetWeaver by Key Capability → Security → User Authentication and Single Sign-On* ◀.

6 Authorizations

SAP TM uses the authorization concept provided by the SAP NetWeaver AS ABAP or AS Java. Therefore, the recommendations and guidelines for authorizations as described in the *SAP NetWeaver Application Server ABAP Security Guide, Java Security Guide, ABAP and Java Security Guides* also apply to SAP TM.
The SAP NetWeaver authorization concept is based on assigning authorizations to users based on roles. For role maintenance, use the profile generator (transaction PFCG) on the AS ABAP and the User Management Engine's user administration console for the AS Java.

Role and Authorization Concept for SAP Transportation Management 8.0

Standard roles and authorization objects are delivered with SAP Transportation Management 8.0. In the following, you can find more details about the standard roles and authorization objects and how to use them.

Standard Roles

SAP Transportation Management 8.0 contains standard roles that you must copy to create your own roles. For each of the standard roles, a set of predefined authorization proposals is delivered. As it is not possible to predefine all authorization values because they will strongly depend on your specific business and scenarios, you will have to enhance the proposed authorization values with the missing data. In some cases it might be also required to adopt the proposed values with your values.

CAUTION

We strongly recommend that you always check the delivered authorization proposals carefully.

The list below shows the standard roles that can be used in SAP Transportation Management 8.0.

- /SCMTMS/BOOKING_AGENT
- /SCMTMS/CARRIER_SETTLEMENT_SP
- /SCMTMS/CUSTOMER_SERVICE_AGENT
- /SCMTMS/CUSTOMER_SETTLEMENT_SP
- /SCMTMS/DISPATCHER
- /SCMTMS/DISPLAY
- /SCMTMS/FREIGHT_CONTRACT_SPEC
- /SCMTMS/PLANNER
- /SCMTMS/SERVICE_PROVIDER
- /SCMTMS/TRANSPORTATION_MANAGER
- /SCMTMS/PROCESS_ADMINISTRATOR

For more information, see SAP Library for SAP Transportation Management on SAP Help Portal at `http://help.sap.com/tm`. In SAP Library, choose ▶ *Basic Functions* → *Roles* ◀.

Standard Authorization Objects

For TM 8.0, there are two kinds of authorization objects available: static checks on the technical business objects with their nodes and actions or on organizational data objects, and instance based authorization objects, with which you can check authorization for the defined business documents or other objects depending on business relevant data, as for instance organization information.

For the instance based authorization checks, there are basically two concepts available. First, it is possible to maintain authorization values depending on identifiers for all kinds of profiles or other objects that cannot be classified any further by specific types, but only depending on their identifier. Second, it is possible to define authorization values depending on category, type and further characteristics as for instance organizational data that can classify business documents beyond their identifier.

Besides the standard activities that can be defined for each authorization object for authorization field ACTVT, it is also possible to define whole groups of activities for several authorization actions as an activity area. While you have to maintain only one distinct activity area, this allows or forbids a whole set of actions related to this area. Thus, it is not necessary to define for instance all actions being related subcontracting activities separately for a role being responsible for subcontracting, but only to maintain the activity area for subcontracting.

For information about authorizations in SAP TM, see SAP Library for SAP TM on SAP Help Portal at `http://help.sap.com` under *Authorizations*.

If you want to display the authorization objects in SAP TM, on the *SAP Easy Access* screen, choose ▶ *Tools* → *ABAP Workbench* → *Development* → *Other Tools* → *Authorization Objects* → *Objects* ◀ and open object class SCTS.

NOTE

You can also create your own authorization objects and implement the corresponding checks in BAdIs *Authorization Check* and *Data Retrieval Before Authorization Check*,

For more information, see Customizing for SAP TM under ▶ *Transportation Management* → *Business Add-Ins (BAdIs) for Transportation Management* → *Basic Functions* → *Authorizations* ◀.

The table below shows the security-relevant authorization objects from other components that are used by SAP TM. The list does not include used basis authorization objects for central functions or adminstration.

Standard non-SAP TM 8.0 Authorization Objects

Authorization Object	Field	Value	Description
SAP SCM Basis 7.0			
/SCMB/PESL	ACTVT, USER	(06) Delete or (34) Write In the USER field, you can enter the user for whose selection you want to execute the activities in the ACTVT field.	Define Planning Service Manager (PSM) Selection. The authorization object

Authorization Object	Field	Value	Description
			enables the specified user to save and delete his or her selections.
Business Context Viewer			
BCV_USAGE	ACTVT	(70) Administer (US)	Business Context Viewer usage
APO			
C_APO_DEF	ACTVT, APO_PLNR, APO_DEFT, APO_DEFN	01) Create or generate (02) Change (03) Display (06) Delete	APO Authorization Object: Master Data, Resource Definitions
C_APO_LOC	ACTVT, APO_LOC	01) Create or generate (02) Change (03) Display (06) Delete (16) Execute (32) Save	APO Authorization Object: Master Data, Locations
C_APO_PROD	ACTVT, APO_LOC, APO_PROD	01) Create or generate (02) Change (03) Display (06) Delete (16) Execute	APO Authorization Object: Master Data, Products
C_APO_RES	ACTVT, APO_PLNR, APO_LOC, APO_RES	(01) Create or generate (02) Change (03) Display (06) Delete (16) Execute	APO Authorization Object: Master Data, Resources
EH&S			
C_EHSP_TPP	ACTVT, LANGUAGE, ESECATPIN, ESEPHRGRP, PPSTAT	(02) Change (03) Display	This authorization is checked in the transactions for phrase management for entry into the hit list.
C_SHEP_TPG	ACTVT, ESECATPIN, ESEPHRGRP	01) Create or generate (02) Change (03) Display (59) Distribute	This authorization object is checked in the phrase management transactions when entering and leaving the hit list. The activities 'change' and 'display' are also checked here.
M_MATE_DGM	ACTVT	01) Create or generate (02) Change (03) Display (06) Delete (61) Export (82) Supplement	Using the authorization object M_MATE_DGM, you can restrict the display and editing of the dangerous goods master data.
Formula & Derivation Tool			

Authorization Object	Field	Value	Description
FDT_OBJECT	FDT_APPL, FDT_OBJTYP, FDT_ACT	(1) Create (2) Change (3) Display (4) Delete (5) Activate	You use this authorization object to control the authorization to display, create, change, or delete objects in the Formula & Derivation Tool (including functions, expressions, expression types, filters, and applications).
Human Resources			
PLOG	PLVAR, OTYPE, INFOTYP, SUBTYP, ISTAT, PPFCODE	Not applicable	The present object is used by the authorization check for PD data.
SCM Optimizer 7.0			
S_RFC	ACTVT, RFC_NAME, RFC_TYPE	(16) Execute	Needed authorization to start the SCM Optimizer and use most of the administrator transactions
SAP Event Management 7.0			
X_EM_EH	ACTVT, /SAPTRX/PN, /SAPTRX/PV	(03) Display or (10) Post	Event handler authorization
X_EM_EH_CH	ACTVT, /SAPTRX/SO,	(01) Create or generate, (02) Change, (05) Lock, (06) Delete, (63) Activate, or (95) Unlock	Event handler changes
X_EM_EVM	ACTVT, /SAPTRX/CS, /SAPTRX/CD	(32) Save the sender code set and sender code ID	Event messages
Cross-application Authorization Objects			
CA_POWL	POWL_APPID, POWL_QUERY, POWL_CAT, POWL_LSEL, POWL_TABLE, POWL_RA_AL	POWL_QUERY: (01) the user is allowed to create/change/delete own queries for all POWL object types assigned to him (c.f. customizing tables POWL_TYPE_USR and POWL_TYPE_ROL). (02) the user is only allowed to create own queries on the basis of admin queries assigned to him via customizing tables POWL_QUERY_USR and POWL_QUERY_ROL respectively. (Note:	Specifies the authorities for Personal Object Worklist (POWL) iViews

Authorization Object	Field	Value	Description
		this is also subjected to the user – POWL object type assignments) (03) (and other values): the user is only allowed to change admin queries assigned to him with respect to the select options restrictions of those admin queries (thus creating one own “derivation” per admin query transparently) POWL_CAT: (01) the user is allowed to create/change/delete own categories and assign queries to them (02) the user is only allowed to assign queries to the existing categories and change the order of queries (03) (and other values): the user is not allowed to re-assign queries or change the query order. Note: if field POWL_QUERY is set to 01 or 03, setting POWL_CAT to 03 is not sensible. Therefore, the value will be set to '02' implicitely in that case.	

CAUTION

In order to realize segregation of duties with roles and authorization values in SAP Transportation Management 8.0, it is recommended to restrict the different role’s authorizations to the business related minimum.

With the authorization concept provided by SAP Transportation Management 8.0, it is possible to restrict authorization based on business document categories, such as *Freight Order* or *Freight Booking*, or on business document types, which you can create for the delivered business document categories. Further, all critical business related activities, such as the creation of business documents, displaying business documents or master data, triggering charge calculation, subcontracting freight documents, requesting customs declaration, and others defined as activities or activity areas for the authorization objects of object class SCTS, can be restricted for the different roles. Thus, segregation of duties can be achieved according to your business and scenarios.

Note that it is strongly recommended not to provide one role with full authorization for one business document or process, so that one role is for instance not able to create and maintain a business document, to add charge data to it, to send it to a business partner and to create the invoice for that document. Such activities should be spread over different roles.

Further, one user must not be assigned to different roles that would then also provide him with full authorizations for one business document or process, just as described before

CAUTION

If your scenario contains an approval workflow process, you need to create or maintain user WF-BATCH accordingly.

For general information about the creation or maintenance of user WF-BATCH, refer to SAP Note 1251255.

As described in SAP Note 1251255, you need to also assign a role used for SAP Transportation Management 8.0 to user WF-BATCH. Depending on your specific scenario, this could be a role created according to role template /SCMTMS/TRANSPORTATION_MANAGER, but this can also differ according to your business scenario.

7 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.

Session Security Protection on the AS ABAP

To activate session security on the AS ABAP, set the corresponding profile parameters and activate the session security for the client(s) using the transaction SICF_SESSIONS.

For more information, a list of the relevant profile parameters, and detailed instructions, see *Activating HTTP Security Session Management on AS ABAP* [external document] in the AS ABAP security documentation.

Session Security Protection on the AS Java

On the AS Java, set the properties described in *Session Security Protection* [external document] using the Visual Administrator.

8 Network and Communication Security

Your network infrastructure is 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, then there is no way for intruders to compromise the machines and gain access to the back-end system's database or files. Additionally, if users are unable 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 SAP Transportation Management 8.0 (SAP TM 8.0) 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 SAP TM 8.0. Details that specifically apply to SAP TM 8.0 are described in the following topics:

- *Communication Channel Security* [page 37]
  This topic describes the communication paths and protocols used by the application.
- *Network Security* [page 39]
  This topic describes the recommended network topology for the application. 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 application.
- *Communication Destinations* [page 39]
  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 following sections in the *SAP NetWeaver Security Guide*:

- *Network and Communication Security* [external document]
- *Security Guides for Connectivity and Interoperability Technologi* [external document]

8.1 Communication Channel Security

Since 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.

CAUTION

You should activate the Secure Network Communication (SNC) within all communication channels in SAP Transportation Management 8.0 to achieve a secure system landscape.

For more information, see ▶ http://service.sap.com/security → *SAP NetWeaver* → *SAP NetWeaver in Detail* → *Security* → *Security in Detail* → *SAP Security Guides* → *SAP NetWeaver 7.0 Security Guides (Complete)* → *SAP NetWeaver 7.0 Security Guide* → *Network and Communication Security* → *Transport Layer Security* → *Secure Network Communications (SNC)* ◀.

The table below shows the communication paths used by SAP TM 8.0, 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
Frontend client using a Web browser or SAP NWBC 3.0 to application server	HTTPS	All application data	Business Object information, System information
Upload document	HTTPS	Attachments of all allowed MIME types	Financial data, for instance invoices
Application server to application server	RFC	Application data	No special data, but SNC recommended

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

NOTE

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

For more information, see *Transport Layer Security* [external document] in the *SAP NetWeaver Security Guide*.

Core Interface (CIF) – SAP ERP 6.0 Including Enhancement Package 5

The integration of SAP Transportation Management 8.0 and SAP ERP 6.0 including enhancement package 5 is technically based on the Core Interface (CIF). Since CIF is technically based on the Remote Function Call (RFC) functionality provided by SAP NetWeaver, we strongly recommend that you consult the SAP NetWeaver Security Guide regarding communication channel security. You should at least enable Secure Network Communication (SNC) while configuring the RFC destination for the integration of SAP Transportation Management 8.0 and SAP ERP 6.0 including enhancement package 5.

For more information, see SAP Library for SAP Supply Chain Management on SAP Help Portal at ▶ http://help.sap.com/scm → *SAP SCM Server* ◀. In SAP Library for SAP SCM 7.0, choose ▶ *SAP Advanced Planning and Optimization (SAP APO)* → *Integration via Core Interface (CIF)* → *Technical Integration* ◀.

8.2 Network Security

Your network infrastructure is 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.

NOTE

For information about network security for SAP NetWeaver 7.0 including enhancement package 2, see *Network and Communication Security* in the *SAP NetWeaver 7.0 Security Guide*. You can find this guide on SAP Service Marketplace at ▶ `http://service.sap.com/securityguide` → *SAP NetWeaver 7.0 Security Guides (Complete)* ◀.

A minimum security demand for your network infrastructure is the use of a firewall for all your services provided over 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 with a firewall against unauthorized access. External security attacks can also come from "inside", if the intruder has already taken over control of one of your systems.

NOTE

For information about access control using firewalls, see *Using Firewall Systems for Access Control* [external document]*Using Firewall Systems for Access Control* in the *SAP NetWeaver 7.0 Security Guide*.

Ports

SAP Transportation Management 8.0 runs on SAP NetWeaver 7.0 including enhancement package 2 and uses the ports from the AS ABAP or AS Java. For more information, see the topics for *AS ABAP Ports* [external document] and *AS Java Ports* [external document] in the corresponding SAP NetWeaver Security Guides. For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, also see the document *TCP/IP Ports Used by SAP Applications*, which is located on the SAP Developer Network at `http://sdn.sap.com/irj/sdn/security` under ▶ *Infrastructure Security* → *Network and Communications Security* ◀.

8.3 Communication Destinations

CAUTION

It is strongly recommended not to give SAP_ALL authorizations to communication users. It is extremely important to grant only minimum authorization to these users.

The table below shows an overview of the communication destinations used by SAP Transportation Management 8.0 (SAP TM 8.0)..

Connection Destinations

Destination	Delivered	Type	User, Authorizations	Description
SAPOSCOL_<DB_hostname> (SAP TM central instance - DB instance)	Yes	RFC - TCP/IP		For more information, see SAP Service Marketplace at ▶ http://service.sap.com/instguides → *SAP Business Suite Applications* → *SAP SCM* → *SAP SCM Server* → *Using SAP SCM 7.0 Server* → *Installation Guides* ◀. Choose the appropriate guide for your operating system and data base and in this guide ▶ *Post-Installation Steps* → *Checking the RFC Destination* ◀.
<SAP TM name>CLNT<client> SAP TM –> SAP ERP	No	RFC - ERP	Use the Profile Generator (transaction code PFCG) to define an appropriate profile, and see SAP Notes 447543 **and** 727839.	For more information, see Customizing for SCM Basis under ▶ *Integration* → *Basic Settings for Creating the System Landscape* → *Assign RFC Destinations to Various Application Cases.* ◀
OPTSERVER_<Optimizer>01	No	RFC - TCP/IP		For more information, see the *SCM Optimizer Installation Guide* on SAP Service Marketplace at ▶ http://service.sap.com/instguides → *SAP Business Suite Applications* → *SAP SCM* → *SAP SCM Server* → *Using SAP SCM 7.0 Server* → *Installation Guides* ◀. Choose the appropriate guide for your operating system and data base and in this guide ▶ *Post Installation Steps* → *Performing a Setup Check of the RFC Gateway* ◀.
SAP Event Management –> Application Systems	No	RFC	Use the Profile Generator (transaction code `PFCG`) to define an appropriate profile.	For more information, see Customizing for SAP Event Management under ▶ *Event Management* → *General Settings in SAP Event Management* → *Define Application System* ◀.
SAP Application System –> SAP Event Management	No	RFC	Use the Profile Generator (transaction code `PFCG`) to define an appropriate profile.	For more information, see Customizing for SAP SCM under ▶ *Integration with SAP Components* → *Event Management*

Destination	Delivered	Type	User, Authorizations	Description
				Interface → *Define Application Interface* → *Define SAP EM* ⇤.

NOTE

For more information about communication destinations of SAP NetWeaver, see *Security Guides for Connectivity and Interoperability Technologies* in the *SAP NetWeaver 7.0 Security Guide*.

9 Internet Communication Framework Security

You should only activate those services that are needed for the applications running in your system. For SAP Transportation Management 8.0 the following services are needed:

- /sap/option
- /sap/option/-gui
- /sap/option/-stateful
- /sap/option/-stateless
- /sap/option/-transactional
- /sap/public
- /sap/public/bc
- /sap/public/bc/abap
- /sap/public/bc/icf
- /sap/public/bc/icf/logoff
- /sap/public/bc/icons
- /sap/public/bc/icons_rtl
- /sap/public/bc/its
- /sap/public/bc/its/designs
- /sap/public/bc/its/mimes
- /sap/public/bc/pictograms
- /sap/public/bc/ur
- /sap/public/bc/webdynpro
- /sap/public/bc/webdynpro/adobeChallenge
- /sap/public/bc/webdynpro/mimes
- /sap/public/bc/webdynpro/Polling
- /sap/public/bc/webdynpro/ssr
- /sap/public/bc/webicons/
- /sap/public/bc/workflow
- /sap/public/bsp
- /sap/public/bsp/sap
- /sap/public/bsp/sap/htmlb
- /sap/public/bsp/sap/public
- /sap/public/bsp/sap/

- /sap/public/bsp/sap/alertinbox
- /sap/bc/fpads
- /sap/bc/gui
- /sap/bc/gui/sap
- /sap/bc/gui/sap/its
- /sap/bc/gui/sap/its/webgui
- /sap/bc/icf
- /sap/bc/nwbc
- /sap/bc/soap
- /sap/bc/srt
- /sap/bc/srt/xip
- /sap/bc/srt/xip/scmtms
- /sap/bc/srt/xip/scmtms/cfirsuite_conf
- /sap/bc/srt/xip/scmtms/exportdeclarationsuite
- /sap/bc/srt/xip/scmtms/gettranspdocuri
- /sap/bc/srt/xip/scmtms/icpy_trq_cancln_rq
- /sap/bc/srt/xip/scmtms/icpy_trq_rq
- /sap/bc/srt/xip/scmtms/icpy_trq_simrc
- /sap/bc/srt/xip/scmtms/inbdlvconf_v1
- /sap/bc/srt/xip/scmtms/invoicenotification_in
- /sap/bc/srt/xip/scmtms/outbdlvbulkconf
- /sap/bc/srt/xip/scmtms/tor_invprepcnf
- /sap/bc/webdynpro
- /sap/bc/webdynpro/sap
- /sap/bc/webdynpro/sap/scmtms
- /sap/bc/webdynpro/sap/scmtms/bs
- /sap/bc/webdynpro/sap/scmtms/carrier_sel
- /sap/bc/webdynpro/sap/scmtms/dlvb
- /sap/bc/webdynpro/sap/scmtms/fre_book
- /sap/bc/webdynpro/sap/scmtms/fre_order
- /sap/bc/webdynpro/sap/scmtms/fre_order_tend
- /sap/bc/webdynpro/sap/scmtms/fre_unit
- /sap/bc/webdynpro/sap/scmtms/fub
- /sap/bc/webdynpro/sap/scmtms/fwd_order
- /sap/bc/webdynpro/sap/scmtms/fwd_quot
- /sap/bc/webdynpro/sap/scmtms/layout
- /sap/bc/webdynpro/sap/scmtms/md_drvres
- /sap/bc/webdynpro/sap/scmtms/md_hures

- /sap/bc/webdynpro/sap/scmtms/md_otres
- /sap/bc/webdynpro/sap/scmtms/md_tures
- /sap/bc/webdynpro/sap/scmtms/md_vehres
- /sap/bc/webdynpro/sap/scmtms/pln
- /sap/bc/webdynpro/sap/scmtms/prof_capa
- /sap/bc/webdynpro/sap/scmtms/prof_ccr
- /sap/bc/webdynpro/sap/scmtms/prof_cof
- /sap/bc/webdynpro/sap/scmtms/prof_cond_
- /sap/bc/webdynpro/sap/scmtms/prof_decca
- /sap/bc/webdynpro/sap/scmtms/prof_demh
- /sap/bc/webdynpro/sap/scmtms/prof_dlv
- /sap/bc/webdynpro/sap/scmtms/prof_filter
- /sap/bc/webdynpro/sap/scmtms/prof_fubr
- /sap/bc/webdynpro/sap/scmtms/prof_geosel
- /sap/bc/webdynpro/sap/scmtms/prof_incdef
- /sap/bc/webdynpro/sap/scmtms/prof_incsett
- /sap/bc/webdynpro/sap/scmtms/prof_optsett
- /sap/bc/webdynpro/sap/scmtms/prof_pln
- /sap/bc/webdynpro/sap/scmtms/prof_plncost
- /sap/bc/webdynpro/sap/scmtms/prof_sel
- /sap/bc/webdynpro/sap/scmtms/prof_tspsett
- /sap/bc/webdynpro/sap/scmtms/tal
- /sap/bc/webdynpro/sap/scmtms/tcm_cfir
- /sap/bc/webdynpro/sap/scmtms/tcm_efa_ca
- /sap/bc/webdynpro/sap/scmtms/tcm_efa_cu
- /sap/bc/webdynpro/sap/scmtms/tcm_efa_mu
- /sap/bc/webdynpro/sap/scmtms/tcm_quick_quote
- /sap/bc/webdynpro/sap/scmtms/tcm_rate2_tables
- /sap/bc/webdynpro/sap/scmtms/tcm_rate_tables
- /sap/bc/webdynpro/sap/scmtms/tcm_scale
- /sap/bc/webdynpro/sap/scmtms/tcm_sfir
- /sap/bc/webdynpro/sap/scmtms/tcm_tccs
- /sap/bc/webdynpro/sap/scmtms/tend_resp
- /sap/bc/webdynpro/sap/scmtms/tend_resp_ext
- /sap/bc/webdynpro/sap/scmtms/tend_temp
- /sap/bc/webdynpro/sap/scmtms/tnc
- /sap/bc/webdynpro/sap/scmtms/treq_delb
- /sap/bc/webdynpro/sap/scmtms/treq_ordb

- /sap/bc/webdynpro/sap/scmtms/wda_powl_ovp
- /sap/bc/webdynpro/sap/scmtms/wda_ts_eng_conf
- /sap/bc/webdynpro/sap/scmtms/wdc_ts_eng_conf
- /sap/bc/workflow
- /SAPconnect

> NOTE
>
> For activation of ICF service `/sap/public/bsp/sap/alertsubscription`, refer to instructions described in SAP Note 1080668.

Use the transaction SICF to activate these services.

If your firewall(s) or Web dispatcher(s) use URL filtering, also note the URLs used for the services and adjust your firewall settings accordingly. For more information, see *Activating and Deactivating ICF Services* [external document]in the SAP NetWeaver Library documentation.

For more information about ICF security, see the *RFC/ICF Security Guide* [external document].

10 Data Storage Security

The data storage security of SAP NetWeaver and components installed on that base is described in detail in the *SAP NetWeaver 7.0 Security Guide*.

NOTE

For information about the data storage security of SAP NetWeaver, see *Security Guides for Operating System and Database Platforms* in the *SAP NetWeaver 7.0 Security Guide*.

In general, all business data of SAP Transportation Management 8.0 is stored in the system database. This business data is protected by the authorization concept of SAP NetWeaver and SAP Transportation Management 8.0.

You can use the RSCRDOMA report with the SAP & DS USNAM variant to determine all domains that contain person-related data.

You can check which values the variant uses to filter the result. Proceed as follows:

1. On the SAP Easy Access screen, choose ▶ *Tools* → *ABAP Workbench Development* → *ABAP Editor* ◀.
2. Enter **RSCRDOMA** as the program name.
3. Select the Variants subobject and choose *Display*.
4. Enter the SAP & DS_USNAM variant.
5. Select the Values subobject and choose *Display*.

To find the documentation of the RSCRDOMA report, proceed as follows:

1. On the SAP Easy Access screen, choose ▶ *Tools* → *ABAP Workbench Development* → *ABAP Editor* ◀.
2. Enter **RSCRDOMA** as the program name.
3. Select the Source Code subobject and choose *Display*.

NOTE

Business partner data, which is maintained in the SAP TM system in transaction BP, can contain person related data. In order to delete this business partner data from the database, transaction *Deletion of Business Partners* can be carried out. For more information, refer to the following documentation:

Deleting Business Partners [external document]

11 Other Security-Relevant Information

Integration of SAP Visual Business 1.1

SAP Visual Business 1.1 that is integrated into multiple ABAP web dynpro applications of SAP Transportation Management 8.0, is a digitally signed ActiveX control. In order to make it executable on the front-end clients, ActiveX controls must not be blocked by your Web browser.

In case your security policy does not allow ActiveX controls to be executed on the front-end clients, it will not be possible to display SAP Visual Business 1.1.

11.1 Enterprise Services Security

The following chapters in the NetWeaver 7.0 including enhancement package 2 Security Guide and documentation are relevant for all enterprise services delivered with SAP Transportation Management 8.0:

- Security Guide Web Services
- *Recommended WS Security Scenarios* [external document]
- *SAP NetWeaver Process Integration Security Guide* [external document]

For more information about special security requirements for Web services, see SAP Library for SAP NetWeaver 7.0 on SAP Help Portal at `http://help.sap.com/nw`. In SAP Library, choose ▶ *SAP NetWeaver Library* → *SAP NetWeaver Developer's Guide* → *Fundamentals* → *Using Java* → *Core Development Tasks* → *Providing and Consuming Web Services* → *Web Service Toolset* → *Web Services Security* ◀.

For more information about enterprise services and security, see the Enterprise Services Documentation for SAP Supply Chain Management on SAP Help Portal at `http://help.sap.com/scm`.

For more information about the security of the exchange infrastructure, see the SAP NetWeaver 7.0 Security Guide at ▶ `http://service.sap.com/securityguide` → *Security in Detail* → *SAP Security Guides* → *SAP Process Integration Security Guides* → *SAP NetWeaver Process Integration Security Guide* ◀.

11.2 Data Protection and Privacy

You can use the `RSCRDOMA` report with the `SAP&DS_USNAM` variant to determine all domains that contain person-related data.

You can check which values the variant uses to filter the result. Proceed as follows:

1. On the *SAP Easy Access* screen, choose ▶ *Tools* → *ABAP Workbench* → *Development* → *ABAP Editor* ◀.
2. Enter **`RSCRDOMA`** as the program name.

3. Select the *Variants* subobject and choose *Display*.
4. Enter the **`SAP&DS_USNAM`** variant.
5. Select the *Values* subobject and choose *Display*.

To find the documentation of the `RSCRDOMA` report, proceed as follows:

1. On the *SAP Easy Access* screen, choose ▶ *Tools* → *ABAP Workbench* → *Development* → *ABAP Editor* ◀.
2. Enter **`RSCRDOMA`** as the program name.
3. Select the *Source Code* subobject and choose *Display*.

12 Security-Relevant Logging and Tracing

SAP systems keep a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Audits and logs are important for monitoring the security of your system and to track events, in case of problems.

> NOTE
>
> Auditing and logging for the SAP SCM 7.0 component is described in detail in the *SAP NetWeaver 7.0 Security Guide*. For more information, see *Auditing and Logging* under *Security Aspects for System Management* in the *SAP NetWeaver 7.0 Security Guide (Complete)* on SAP Service Marketplace at `http://service.sap.com/securityguide`.

Security Audit Log triggered by Virus Scan Interface (VSI)

The class `CL_VSI` automatically creates entries in the Security Audit Log for infections and scan errors found, together with the following information:

- Profile
- Profile step allowing the detection of the scanner-group
- Kind of virus found, with internal virus ID of the scan engine, if available
- User name and timestamp

The messages logged are located in the message class `VSCAN`, using the system log messages `BU8` and `BU9` (created in transaction `SE92`). The severities are set to *High* and *Medium*, respectively. The severity of the audit class is set to *Miscellaneous*.

For more information, see Customizing for SAP Supply Chain Management under ▶ *SAP Web Application Server* → *System Administration* → *Virus Scan Interface* ◀.

Audit Information System (AIS)

Information on auditing and logging for the Audit Information System (AIS) is described in detail in the *SAP NetWeaver 7.0 Security Guide*. For more information, see *The Audit Info System (AIS)* in the *SAP NetWeaver 7.0 Security Guide* ▶ *Security Aspects for System Management* → *Auditing and Logging* → *The Audit Info System (AIS)* ◀.

SAP Transportation Management 8.0

Tracing and Logging of Business Objects

In SAP TM, you can log messages raised by business objects in the application log.

In the standard system, logging is deactivated. To activate logging, in Customizing for *Transportation Management*, choose ▶ *Basic Functions* → *User Interface* → *Define Message Settings* ◀.

To access the application log, on the *SAP Easy Access* or in SAP NetWeaver Business Client screen, choose ▶ *Application Administration* → *Application Log: Display Logs* ◀. Alternatively, call transaction `SLG1`.

For more information, see *Application Logging* under *Logging of Specific Activities* in the *SAP NetWeaver 7.0 Security Guide (Complete)* on SAP Service Marketplace at `http://service.sap.com/securityguide`.

Activating Change Documents

In SAP TM, you can activate change documents to log changes to master data, business objects, and so on.

You must activate change documents in Customizing, before the system can store them. For information about the objects that you can activate change documents for and where to activate them, refer to the corresponding section in the SAP TM 8.0 documentation:

You must activate change documents in Customizing, before the system can store them. For information about the objects for which you can activate change documents and where to activate them, see the following table:

Object	Customizing Path
Location	▶ *Transportation Management* → *Master Data* → *Transportation Network* → *Location* → *Activate Change Documents* ◀
Transportation lane	▶ *Transportation Management* → *Master Data* → *Transportation Network* → *Transportation Lane* → *Activate Change Documents* ◀
Product	▶ *SCM Basis* → *Master Data* → *Product* → *Activate Change Documents* ◀
Freight unit	▶ *Transportation Management* → *Planning* → *Freight Unit* → *Define Freight Unit Types* ◀ (*Track Changes* checkbox)
Freight order	▶ *Transportation Management* → *Freight Order Management* → *Freight Order* → *Define Freight Order Types* ◀ (*Track Changes* checkbox)
Freight booking	▶ *Transportation Management* → *Freight Order Management* → *Freight Booking* → *Define Freight Booking Types* ◀ (*Track Changes* checkbox)
Freight agreement	▶ *Transportation Management* → *Master Data* → *Agreements* → *Define Freight Agreement Settings* ◀
Forwarding agreement	▶ *Transportation Management* → *Master Data* → *Agreements* → *Define Forwarding Agreement Settings* ◀
Forwarding order	▶ *Transportation Management* → *Forwarding Order Management* → *Forwarding Order* → *Define Forwarding Order Types* ◀
Forwarding quotation	▶ *Transportation Management* → *Forwarding Order Management* → *Forwarding Quotation* → *Define Forwarding Quotation Types* ◀
Forwarding settlement	▶ *Transportation Management* → *Settlement* → *Forwarding Settlement* → *Define Forwarding Settlement Document Types* ◀
Freight settlement	▶ *Transportation Management* → *Settlement* → *Freight Settlement* → *Define Freight Settlement Document Types* ◀
Order-based transportation requirement	▶ *Transportation Management* → *ERP Logistics Integration* → *Order-Based Transportation Requirement* → *Define Order-Based Transportation Requirement Types* ◀

Object	Customizing Path
Delivery-based transportation requirement	▶ *Transportation Management* → *ERP Logistics Integration* → *Delivery-Based Transportation Requirement* → *Define Delivery-Based Transportation Requirement Types* ◀

SAP SCM Optimizer

For information about the trace and log files for the SAP SCM Optimizer, see the *SAP SCM 7.0 Component Security Guide* on SAP Service Marketplace at `http://service.sap.com/securityguide`.

For further information about the logging and tracing mechanisms from SAP NetWeaver, refer to the following information: *Auditing and Logging* [external document].

13 Services for Security Lifecycle Management

The following services are available from Active Global Support to assist you in maintaining security in your SAP systems on an ongoing basis.

Security Chapter in the EarlyWatch Alert (EWA) Report

This service regularly monitors the Security chapter in the EarlyWarch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing on your system.

In this case, analyze and implement the identified notes, if possible. If you cannot implement the notes, the report should be able to help you decide on how to handle the individual cases.

- Whether an accumulation of critical basis authorizations has been identified.

In this case, verify whether the accumulation of critical basis authorizations is okay for your system. If not, correct the situation. If you consider the situation okay, you should still check for any significant changes compared to former EWA reports.

- Whether standard users with default passwords have been identified on your system.

In this case, change the corresponding passwords to non default values.

Security Optimization Service (SOS)

The Security Optimization Service can be used for a more thorough security analysis of your system, including:

- Critical authorizations in detail
- Security relevant configuration parameters
- Critical users
- Missing security patches.

This service is available as a self service within the SAP Solution Manager or as a remote or on-site service. We recommend you use it regularly (for example, once a year) and in particular after significant system changes or in preparation of a system audit.

Security Configuration Validation

The Security Configuration Validation can be used to continuously monitor a system landscape for compliance to predefined settings, for example, from your company-specific SAP Security Policy. This primarily covers configuration parameters, but it also covers critical security properties like the existence of a non trivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the E2E Solution Operations Standard Security service, a best practice recommendation is available on how to operate SAP systems and landscapes in secure manner. It guides you through the most important security operation areas and links to detailed security information from SAP's knowledge base wherever appropriate.

More Information

For more details on these services see

- EarlyWatch Alert:`http://service.sap.com/ewa`
- Security Optimization Service / Security Notes Report:`http://service.sap.com/sos`
- Comprehensive list of Security Notes:`http://service.sap.com/securitynotes`
- Configuration Validation:`http://service.sap.com/changecontrol`
- RunSAP Roadmap, including the Security and the Secure Operations Standard: `http://service.sap.com/runsap` (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)

A Appendix

A.1 Related Security Guides

You can find more information about the security of SAP solutions on SAP Service Marketplace at `http://service.sap.com/security`.

Security guides are available on SAP Service Marketplace at `http://service.sap.com/securityguide`.

Related Security Guides

Guide	Location on SAP Service Marketplace
SAP SCM 7.0 Security Guide	▶ *Security → Security in Detail → SAP Security Guides → SAP Supply Chain Management* ◀
SAP NetWeaver 7.0 Security Guide	▶ *Security → Security in Detail → SAP Security Guides → SAP NetWeaver 7.0 Security Guides (Complete)* ◀

A.2 Related Information

For more information about topics related to security, see the links shown in the table below.

Content	Quick Link on SAP Service Marketplace
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	`http://service.sap.com/instguides`
Related SAP Notes	`http://service.sap.com/notes`
Released platforms	`http://service.sap.com/platforms`
Network security	`http://service.sap.com/securityguide`
Technical infrastructure	`http://service.sap.com/installnw70`
SAP Solution Manager	`http://service.sap.com/solutionmanager`

Documentation in the SAP Service Marketplace

You can find this document at the following address: `http://service.sap.com/securityguide`

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 34
F +49/18 05/34 34 20
www.sap.com