

SAP® Transportation Management 9.3 Security Guide

Using SAP® TM 9.3, SAP ERP® 6.0, and SAP NetWeaver® 7.4



© Copyright 2015 SAP SE or an SAP affiliate company. Alle Rechte vorbehalten. All rights reserved. Tous droits réservés. Все права защищены.




Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Please see www.sap.com/corporate-en/legal/copyright/index.epx#trademark for additional trademark information and notices.

Typographic Conventions

Table 1

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
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 
<i>Example</i>	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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: service.sap.com/securityguide ↗.

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

Table 2

Version	Date	Description
1.0	2015-05-28	Initial version
1.1	2015-11-12	Formal revision for SP02

Content

1	Introduction	7
2	Before You Start	9
3	Technical System Landscape	11
4	Security Aspects of Data Flow and Processes	12
5	User Administration and Authentication	21
5.1	User Management	21
5.2	User Data Synchronization	24
5.3	Integration into Single Sign-On Environments	24
6	Authorizations	26
7	Session Security Protection	33
8	Network and Communication Security	34
8.1	Communication Channel Security	34
8.2	Network Security	36
8.3	Communication Destinations	36
9	Internet Communication Framework Security	39
10	Data Storage Security	42
11	Other Security-Relevant Information	43
11.1	Enterprise Services Security	43
11.2	Data Protection and Privacy	44
12	Security-Relevant Logging and Tracing	45
13	Services for Security Lifecycle Management	48
A	Appendix	50
A.1	Related Security Guides	50
A.2	Related Information	50



1 Introduction



Caution

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

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 9.3 (SAP TM 9.3). This Security Guide assists you in securing your SAP TM 9.3 system using SAP ERP 6.0 and SAP NetWeaver 7.4.

About This Document

The Security Guide provides an overview of the security-relevant information that applies to SAP TM 9.3 using SAP ERP 6.0 and SAP NetWeaver 7.4.

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 TM 9.3.
- *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 9.3.
- *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 TM 9.3.

- Standard users that are delivered with SAP TM 9.3.
- Overview of the user synchronization strategy if several components or products are involved.
- Overview of how integration with Single Sign-On environments is possible.

- *Authorizations*

This section provides an overview of the authorization concept that applies to SAP TM 9.3.

- *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 9.3 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 9.3.

- *Data Storage Security*

This section provides an overview of any critical data that is used by SAP TM 9.3 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 9.3.

- *Dispensable Functions with Impacts on Security*

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

- *Enterprise Services Security*

This section provides an overview of the security aspects that apply to the enterprise services delivered with SAP TM 9.3.

- *Other Security-Relevant Information*

This section contains information about:

- Integration of SAP Visual Business 2.0
- Enterprise services
- Data protection and privacy

- *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 TM 9.3 is based on SAP NetWeaver 7.4. Therefore, the corresponding Security Guides also apply to SAP TM 9.3. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Table 3: Fundamental Security Guides


Security Guide	Most-Relevant Sections or Specific Restrictions
SAP NetWeaver 7.4 Security Guides (Complete)	
SAP Web Application Server	<ul style="list-style-type: none">• SAP Web AS Security Guide for ABAP 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 Security Guide	
SAP Mobile Infrastructure Security Guide	Not applicable
SAP NetWeaver Business Intelligence Security Guide	
SAP Knowledge Management	<ul style="list-style-type: none">• SAP Knowledge Management Security Guide• SAP Content Management Security Guide• SAP TREX Security Guide
SAP Process Integration Security Guides	
System Management	Security Aspects with System Management





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


Important SAP Notes

The most important SAP Notes that apply to the security of SAP TM 9.3 are shown in the table below.

Table 4: Important SAP Notes

SAP Note Number	Title	Comment
510007 	Setting up SSL on the Web Application Server	







SAP Note Number	Title	Comment
149926 	Secure e-mail: Encryption, digital signature	This SAP Note provides information about how to connect a third party e-mail proxy to your SAP system to encrypt data and use digital signatures when sending and receiving e-mails from your SAP system.
817623 	Integrating a virus scan in your own SAP applications	This SAP Note provides information about the SAP virus scan interface.
786179 	Data security products: Application in the antivirus area	This SAP Note provides information about the SAP virus scan interface.
853878 	HTTP WhiteList Check (security)	This SAP Note provides information about the HTTP white list. This is required if you want to use file upload functionality.

For a list of additional security-relevant SAP Hot News and SAP Notes, see SAP Service Marketplace at service.sap.com/securitynotes .

Additional Information

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

Table 5: Quick Links to Additional Information

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

3 Technical System Landscape

The figure below shows an overview of the technical system landscape for SAP TM 9.3 using SAP ERP 6.0 and SAP NetWeaver 7.4.

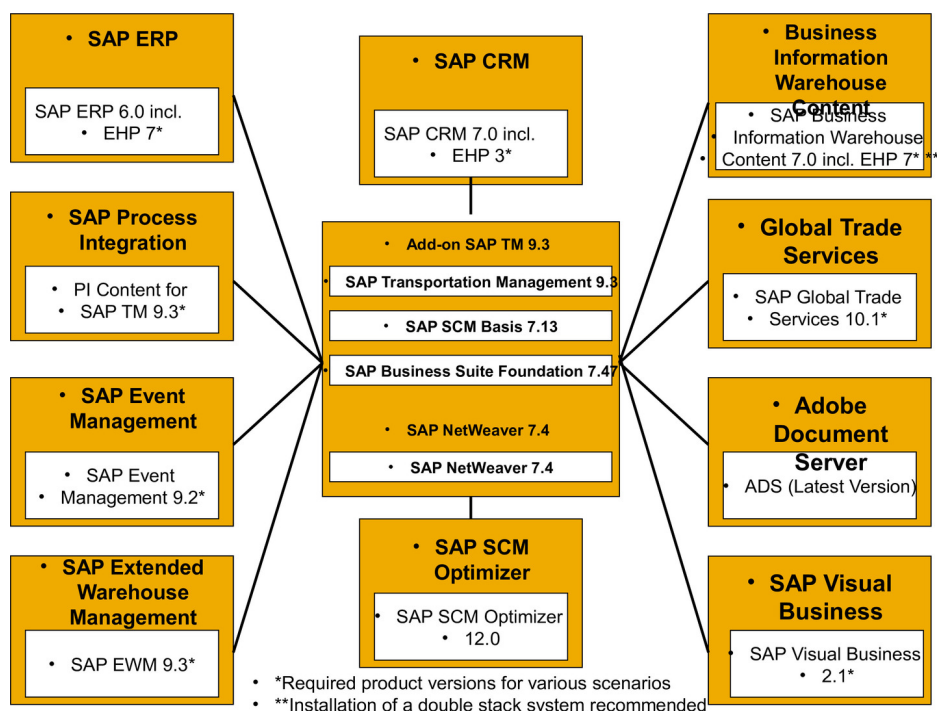


Figure 1: Technical System Landscape

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

Table 6: More Information About the Technical System Landscape

Topic	Guide or Tool	Quick Link to SAP Service Marketplace or SDN
Technical description for SAP TM 9.3 and the underlying components such as SAP NetWeaver	SAP Transportation Management 9.3 Master Guide	service.sap.com/instguides
High availability	High Availability for SAP Solutions	sdn.sap.com/irj/sdn/ha
Technical landscape design	See applicable documents	sdn.sap.com/irj/sdn/landscapedesign
Security	See applicable documents	service.sap.com/security

4 Security Aspects of Data Flow and Processes

Some processes within SAP TM 9.3 must be specially configured so that they can be executed securely. The following list provides an overview of the most critical processes and data flows, along with the 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 TM 9.3.

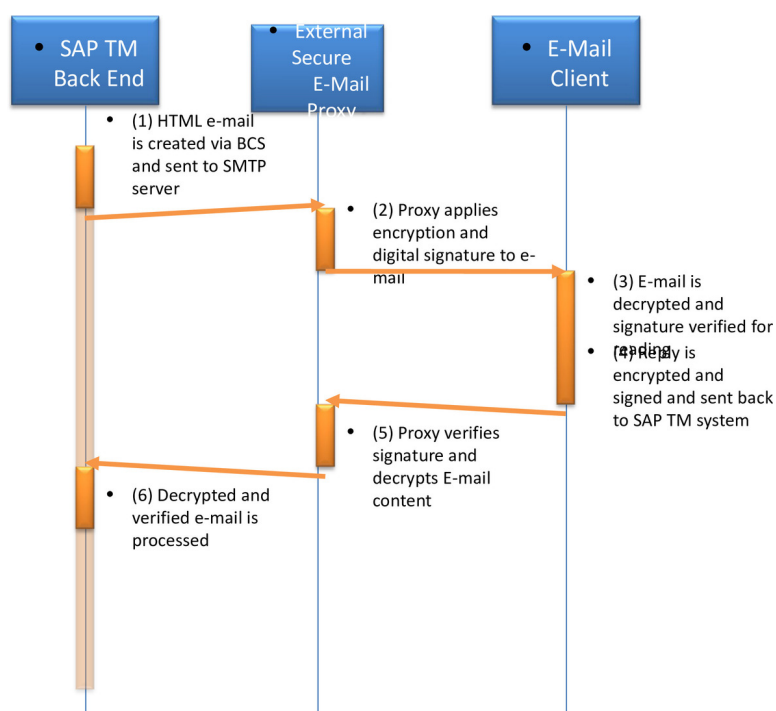


Figure 2: E-Mail-Based Tendering Scenario

Table 7: Steps for E-Mail Based Tendering Scenario

Step	Description	Security Measure
1	HTML e-mail is created via BCS and sent to SMTP server	In Customizing for SAP TM 9.3, the use of encryption and digital signatures needs to be enabled. In Customizing for <i>Transportation Management</i> , choose Freight Order Management > Tendering > Define General Settings for Tendering > 03 – E-mail and SMS Content > E-Mail Security Settings .

Step	Description	Security Measure
2	Proxy applies encryption and digital signature to e-mail	External secure e-mail proxy needs to be maintained and activated for the SAP TM system. For more information, see SAP Note 149926 . Keys must be exchanged between the sender and recipient prior to sending the e-mail. We highly recommend that you set up the policy for the e-mail proxy in such a way that e-mails can be sent only if encryption and digital signatures are enabled. If this is not possible, for example, due to missing keys, e-mails must not be sent in an insecure way.
3	E-mail is decrypted and signature verified for reading	The e-mail client of the recipient must support encryption and digital signatures, and keys must have been exchanged beforehand by the sender and the recipient.
4	Reply is encrypted and signed and sent back to SAP 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

➔ Recommendation

To access the SAP Transportation Management (SAP TM) system externally, we recommend that you define a system alias in the web dispatcher. The web dispatcher redirects the request to the correct hostname and port so that an external user can use a hyperlink, which contains the alias, to access the system.

You create a tendering notification e-mail in the SAP Transportation Management system. The system sends this e-mail to the carrier with a hyperlink to the carrier's worklist in the SAP TM system or in the SAP TM collaboration portal. The hyperlink contains the system alias instead of the physical hostname and port. To use the alias, ensure that you have implemented SAP Note [1748036](#) or [1747651](#), and SAP Note [1783590](#). Subsequently, you need to specify the following settings in the SAP TM system:

1. Create an alias in transaction **SM59** as described in the document *5.10 Remote Systems* [external document] under the section **Target System Names**
2. In the **Target Host** field, enter the system alias as specified in the web dispatcher
3. Enter the alias in the **03 E-Mail and SMS Content** screen in Customizing for **Transportation Management** under **Freight Order Management > Tendering > Define General Settings for Tendering**

Tendering Internet Scenario

➔ Recommendation

The Tendering Internet Scenario is supported with SAP TM 9.3 but we strongly recommend that you use the SAP TM Collaboration Portal instead (see next process).

The figure below shows an overview of the tendering Internet scenario for SAP TM 9.3.

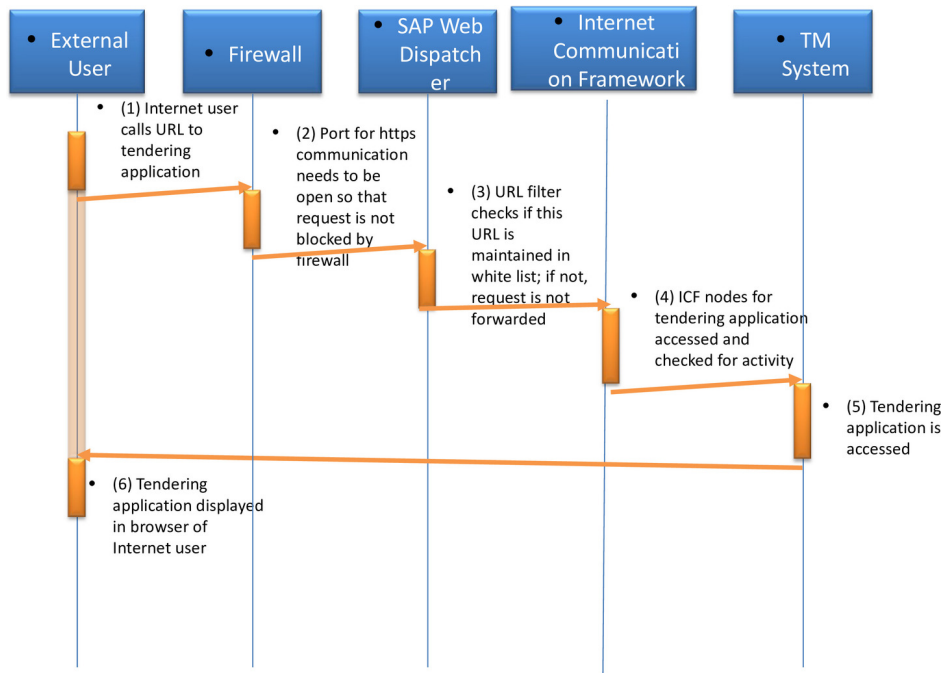


Figure 3: Tendering Internet Scenario

Table 8: Steps for Tendering Internet Scenario

Step	Description	Security Measure
1	Internet user calls URL to tendering application	Internet user needs to be created and maintained for the "Contact Person" role of the business partner in the SAP TM system. We recommend that authentication is done using certificates, which need to be exchanged with the external user beforehand so that the Internet user cannot log on to the system by entering a user name 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 a URL filter; only the URLs to ICF services for the carrier POWL, the

Step	Description	Security Measure
		external tendering quotation application, and 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 7.3 on SAP Help Portal at help.sap.com/nw . In SAP Library, choose SAP NetWeaver > SAP NetWeaver Library: Function-Oriented View > Application Server > Application Server Infrastructure > SAP Web Dispatcher Administration 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 the role of the external user needs to be maintained accordingly. Secure HTTP Session Management should be activated on the ABAP AS as described in SAP Note 1322944 .
6	Tendering application displayed in browser of Internet user	Not applicable

➔ Recommendation

If SAP Event Management is part of your scenario and you want to grant external users access to execution information via SAP Event Management, we strongly recommend that you secure external access to 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**.

SAP TM Collaboration Portal Scenario

The figure below shows an overview of the SAP TM Collaboration Portal scenario for SAP TM 9.3.

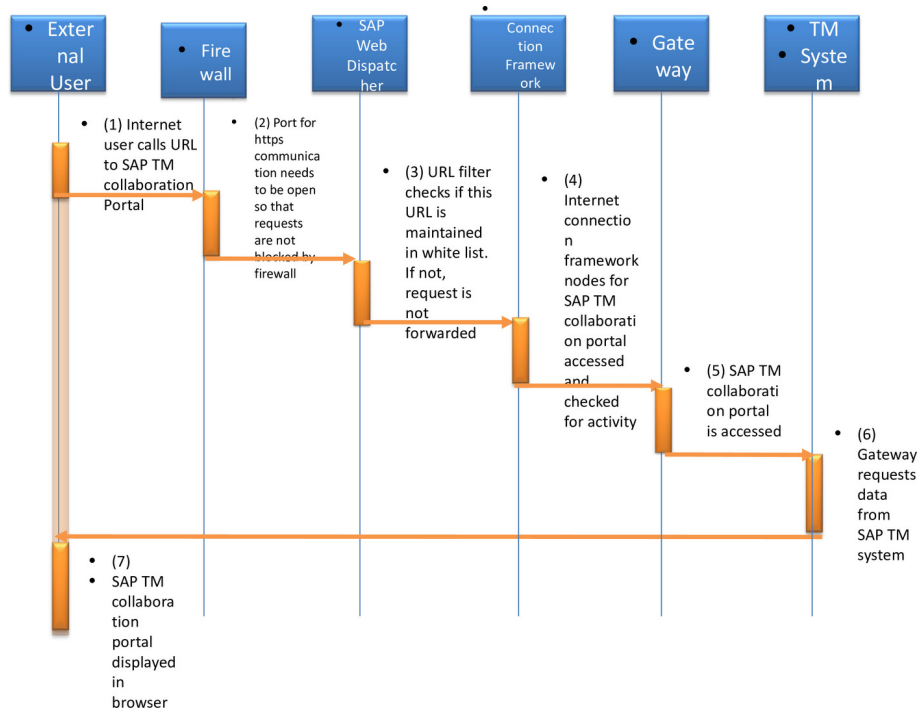


Figure 4: SAP TM Collaboration Portal Scenario

Table 9: SAP TM Collaboration Portal Scenario

Step	Description	Security Measure
1	Internet user calls URL to SAP TM collaboration portal	Internet user needs to be created and maintained for the “Contact Person” role of the business partner in the SAP TM system. We recommend that authentication is done using certificates, which need to be exchanged with the external user beforehand so that the Internet user cannot log on to the portal by entering a user name 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 a URL filter; only the URLs to ICF services for the SAP TM collaboration portal, the Gateway Services for the SAP TM collaboration portal, and for supporting services must be maintained in the white list. Otherwise, external users could access internal services for which they are not authorized. For more information, see

Step	Description	Security Measure
		SAP Library for SAP NetWeaver 7.4 on SAP Help Portal at help.sap.com/nw . In SAP Library, choose SAP NetWeaver > SAP NetWeaver Library: Function-Oriented View > Application Server > Application Server Infrastructure > SAP Web Dispatcher Administration of the SAP Web Dispatcher > SAP Web Dispatcher as a URL Filter .
4	ICF node for SAP TM collaboration portal accessed and checked for activity	ICF nodes for SAP TM collaboration portal (supporting services, gateway services and collaboration portal) need to be active. The relevant services are listed in the chapter Internet Communication Framework Security [page 39]
5	SAP TM collaboration portal is accessed	Authorization profile for the role of the external user needs to be maintained accordingly. Secure HTTP Session Management should be activated on the ABAP AS as described in SAP Note 1322944 .
6	Gateway requests data from SAP TM system	Trusted RFC sent to SAP TM to get the relevant data.
7	SAP TM collaboration portal displayed in browser of Internet user	

➔ Recommendation

To access the SAP Transportation Management (SAP TM) system externally, we recommend that you define a system alias in the web dispatcher. The web dispatcher redirects the request to the correct hostname and port so that an external user can use a hyperlink, which contains the alias, to access the system.

In case the SAP TM Backend Server and Gateway are running on two different physical servers we recommend that secure http connections are used to connect the two.

File Upload Scenario

The figure below shows an overview of the file upload scenario for SAP TM 9.3.

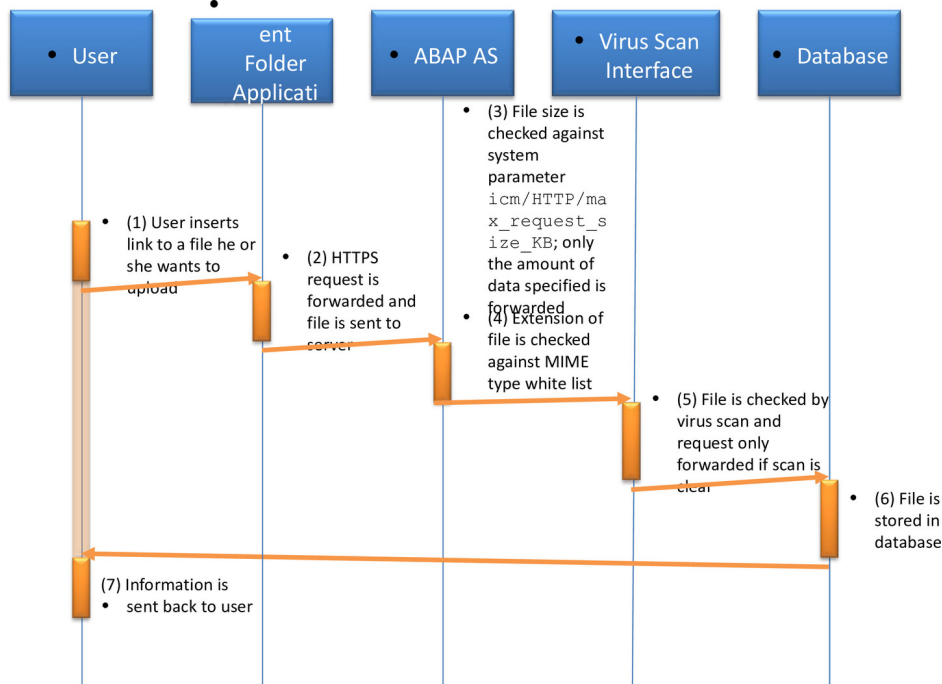


Figure 5: File Upload Scenario

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

Table 10: Steps for File Upload Scenario

Step	Description	Security Measure
1	User inserts link to a file he or she wants to upload	User needs to be aware of the file he or she wants to upload
2	HTTPS request is forwarded and file is sent to server	Not applicable
3	File size is checked against system parameter <code>icm/HTTP/max_request_size_KB</code> ; only the amount of data specified is forwarded	Maximum file size needs to be restricted to secure the server; for more information, see the Security Guide for SAP NetWeaver 7.4 on SAP Service Marketplace at service.sap.com/securityguide . In the Security Guide, choose ► <i>Security Guides for SAP NetWeaver Functional Units</i> ► <i>Security Guides for the Application Server</i> ► <i>Security Guides for the AS ABAP</i> ► <i>Web Dynpro ABAP Security Guide</i> ► <i>Security Notes for FileUpload UI Elements</i> .
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.

Step	Description	Security Measure
5	File is checked by virus scan and request only forwarded if scan is clear	Virus scan needs to be active in your system. For more information, see SAP Library for SAP NetWeaver 7.4 at help.sap.com/nw . In SAP Library, choose ► <i>SAP NetWeaver</i> ► <i>SAP NetWeaver Library: Function-Oriented View</i> ► <i>Security</i> ► <i>Security Developer Documentation</i> ► <i>Secure Programming</i> ► <i>Secure Programming – Java</i> ► <i>Secure Programming</i> ► <i>SAP Virus Scan Interface</i> . We strongly recommend that you create a virus scan profile with linkage type <i>All steps successful</i> .
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 function can be disabled to prevent users from uploading files to your system. To disable the file upload function, you must implement SAP Note [1514253](https://support.sap.com/en/notes/1514253.html). We recommend that you disable the upload function 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. If your virus scan is not up and running, do not use the file upload.

For information about uploading TACT rates to SAP TM 9.3, see SAP Library for SAP Transportation Management at help.sap.com/tm. In SAP Library for SAP TM 9.3, choose ► *Master Data* ► *Charge Management and Service Product Catalogs* ► *Setup of Service Product Catalogs and Charge Management MD* ► *TACT Rates* ► *TACT Rate Upload*.

URL Upload Scenario

The figure below shows an overview of the URL upload scenario for SAP TM 9.3.

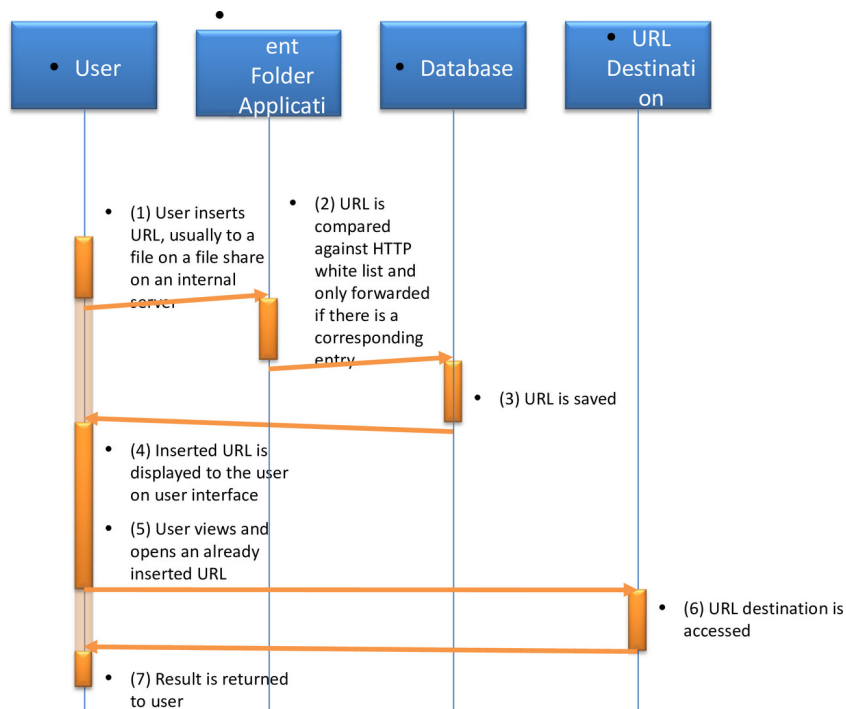


Figure 6: URL Upload Scenario

Table 11: Steps for URL Upload Scenario

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 the HTTP white list according to SAP Note 853878 with entry type 01. We highly recommend that you restrict 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	Configure the Attachment Folder Application user interface to display a column containing the URL.
5	User views and opens an already inserted URL	User needs to be aware of the URL he or she attempts to access.
6	URL destination is accessed	Not applicable
7	Result is returned to user	Not applicable

5 User Administration and Authentication

SAP TM 9.3 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 TM 9.3.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP TM 9.3 in the following topics:

- [User Management \[page 21\]](#)
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 9.3.
- [User Data Synchronization \[page 24\]](#)
SAP TM 9.3 shares data with other sources. This topic describes how the user data is synchronized with these sources.
- [Integration into Single Sign-On Environments \[page 24\]](#)
This topic describes how SAP TM 9.3 supports Single Sign-On mechanisms.

5.1 User Management

User management for SAP TM 9.3 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 TM 9.3, see the sections below. In addition, we provide a list of the standard users required for operating SAP TM 9.3.

SAP TM collaboration portal uses the following user management concepts:

Users in the Back-End System (SU01, PFCG)

Existing users are relevant for the back-end system. The authorizations required for a particular application are provided using a PFCG role delivered for each application. For more information, see [Authorizations \[page 26\]](#).

If you enable users who never directly access the back-end system, you should create these users in the back-end system without a password. This protects them against attacks that exploit incorrect or insecure password handling (these users are unlikely to change the initial password if they do not actually need to).

Users in SAP Gateway (SU01, PFCG)

Users also require a user id for the SAP Gateway layer. They must have the same user name as the users in the back-end system. The user requires certain authorizations that allow the services of the application to be triggered in the back end. If you copy the users from the back-end users, note the following recommendations:

- If you use SSO2 logon tickets to authenticate the requests from a mobile device on SAP Gateway, you should copy the user without any password. This protects against attacks based on incorrect or insecure password handling.

- For information about basic authentication and SSO2 logon tickets, see the User Authentication and Single Sign-On section in this guide.
- For more information about encryption of users, see the Data Protection section in this guide.
- The same recommendations apply if you prefer to create the users from scratch. If users already exist in SAP Gateway because they already use another mobile application, these steps are not relevant. Authentication can be carried out with the same credentials as for the existing application.

To authenticate users, you can set up integration with your existing SSO solution based on SAP Logon Tickets. For more information, see the User Authentication and Single Sign-On section in this guide. The user name in the system that issues the logon tickets has to be the same as the user name for the Gateway system and back-end system.

User Administration Tools

The table below shows the tools for user management and user administration with SAP TM 9.3.

Table 12: 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.
Profile Generator (transaction 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.
SAP NetWeaver Identity Management 7.2	For an overview of the information necessary for securing operations with SAP NetWeaver Identity Management, see the Security Guide available on the SAP Help Portal at help.sap.com/nwidm72 .

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 9.3 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 TM 9.3 system.
 - Internet users are used for external users that are allowed to access your SAP TM 9.3 system from the Internet. If your scenario contains the SAP TM Collaboration Portal, whereby carriers can log on to your SAP TM 9.3 system, view requests for quotations they have received from you, and submit quotations, these external users access your SAP TM 9.3 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 example, for communication between your SAP TM 9.3 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 ► help.sap.com/NW74 ► *Security Information* ► *Security Guide* ► *Security Guides for SAP NetWeaver Functional Units* ► *Security Guides for the Application Server* ► *Security Guides for the AS ABAP* ► *SAP NetWeaver Application Server ABAP Security Guide* ► *User Administration and Authentication* ► *User Management* ►.

Standard Users

The table below shows the standard users that are necessary for operating SAP TM 9.3.

Table 13: Standard Users

System	User	Type	Password	Description
SAP TM 9.3	<sapsid>adm	Dialog user	You must specify the initial password during the installation.	SAP TM System Administrator
SAP TM 9.3	SAPService <sapsid>	Service user	You must specify the initial password during the installation.	SAP TM System Service Administrator
SAP TM 9.3	SAPService <sapsid>	Internet user	You must specify the initial password during the installation.	SAP TM carriers that take part in the tendering process.
SAP TM 9.3	WF-BATCH	Background user	You must specify the initial password during the installation.	
SAP WebAS	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	Service users	You must specify the initial password during the installation.	For more information, see ► <i>SAP NetWeaver Security Guide</i> ► <i>Security Guides for SAP NetWeaver Functional Units</i> ► <i>Security Guides for the Application Server</i> ► <i>Security Guides for the AS ABAP</i> ► <i>SAP NetWeaver Application Server ABAP Security Guide</i> ► <i>User Authentication</i> ► <i>User Administration</i> ► <i>Protecting Standard Users</i> ►.
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 <i>SAP Event Management User</i> .

➔ 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 TM 9.3 is based on SAP NetWeaver 7.4, all the mechanisms for user data synchronization of SAP NetWeaver 7.4 are available for SAP TM 9.3.

i Note

For information about user data synchronization, see SAP Library for SAP NetWeaver 7.4 on SAP Help Portal at help.sap.com/nw. In SAP Library, choose ► *Function-Oriented View* ► *Security* ► *Identity Management* ► *Identity Management for System Landscapes*.

5.3 Integration into Single Sign-On Environments

SAP TM 9.3 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* also apply to SAP TM 9.3.

For more information, see the *Secure Network Communications (SNC)* section of the *SAP NetWeaver Application Server ABAP Security Guide* on SAP Service Marketplace at help.sap.com/NW74. Choose ► *Security Information* ► *Security Guide* ► *Security Guides for SAP NetWeaver Functional Units* ► *Security Guides for the Application Server* ► *Security Guides for the AS ABAP* ► *SAP NetWeaver Application Server ABAP Security Guide* ► *User Administration and Authentication* ► *Integration in Single Sign-On Environments* ► *Secure Network Communications (SNC)*.

The following standard mechanisms are supported by SAP TM 9.3:

- Secure Network Communications (SNC)

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

- SAP logon tickets

SAP TM 9.3 supports 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.

- Client certificates

As an alternative to user authentication using a user ID and passwords, users with 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.

➡ Recommendation

If your scenario contains the SAP TM Collaboration Portal and external Internet users have access to your system, we recommend that you use client certificates instead of authentication with user names and passwords. This way, Internet users are prevented from logging on with another user's details.

For more information about the available authentication mechanisms, see SAP Library for SAP NetWeaver on SAP Help Portal at help.sap.com/nw74. In SAP Library for *SAP NetWeaver 7.4*, choose ► *SAP NetWeaver: Security Information* ► *Security Guide* ► *User Administration and Authentication* ► *User Authentication and Single Sign-On*.

6 Authorizations

SAP TM 9.3 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](#), and [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 `PF03`) 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 9.3

Standard roles and authorization objects are delivered with SAP TM 9.3. For more information about the standard roles and authorization objects and how to use them, see the following section.

Standard Roles

SAP TM 9.3 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. Since it is not possible to predefine all authorization values (these will strongly depend on your specific business and scenarios), you will have to add any missing data to the proposed authorization values. In some cases, you may have to change the proposed values to your own 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 to copy in SAP TM 9.3.

- /SCMTMS/BOOKING_AGENT
- /SCMTMS/CAPACITY_MANAGER
- /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_MGR_V2
- /SCMTMS/PROCESS_ADMINISTRATOR
- /SCMTMS/CAPACITY_MANAGER
- /SCMTMS/COLL_PORTAL
- /TMUI/COLL_PORTAL
- /TMUI/COLL_PORTAL_DEMO

➔ Recommendation

The role /SCMTMS/DISPLAY is designed for an auditor who is able to view all content in a system. For example, master data and transactional data, such as business documents. The role is not allowed to change any data. The role can be assigned to users who conduct security or financial audits.

For more information, see SAP Library for SAP Transportation Management 9.3 on SAP Help Portal at help.sap.com/tm. In SAP Library, choose ► *Basic Functions* ► *Roles*.

Standard Authorization Objects

For SAP TM 9.3, there are two kinds of authorization objects:

- Static checks of the technical business objects along with their nodes and actions, or of organizational data objects
- Instance-based authorization objects, with which you can check authorization for the specified business documents or other objects, depending on business-relevant data such as organization information

For instance-based authorization checks, there are two basic concepts. First, you can define authorization values based on identifiers for all profiles or other objects that cannot be classified any further by specific types, but only depending on their identifier. Second, you can define authorization values based on category, type, and further characteristics such as 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, you can also define whole groups of activities for several authorization actions as an activity area. This means that you can define a distinct activity area, thereby allowing or preventing a whole set of actions related to this area. For example, you do not have to define all actions relating to subcontracting activities separately for a role, but only to define the activity area for subcontracting.

For information about authorizations in SAP TM, see SAP Library for SAP TM on SAP Help Portal at help.sap.com/tm. In SAP Library, choose ► *Basic Functions* ► *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.

i 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 *Transportation Management* under ► *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 9.3. The list does not include basis authorization objects used for central functions or administration.

Table 14: Standard Non-SAP TM 9.3 Authorization Objects

Authorization Object	Field	Value	Description
SAP SCM Basis 7.0			
/SCMB/PESL	ACTVT, USER	(06) Delete (34) Write In the USER field, you can enter the user for which you	Define Planning Service Manager (PSM) Selection. The authorization object enables the specified user to save and delete his or her selections.

Authorization Object	Field	Value	Description
		want to execute the activities in the ACTVT field.	
/SCTM/SCU	/SCMB/SCU ACTVT		Use of supply chain units in routes.
C_MD_SCU	/SCMB/SCU, ACTVT		
Business Context Viewer			
BCV_USAGE	ACTVT	(70) Administer (US)	Business Context Viewer usage
BCV_PERS	ACTVT BCV_CTXKEY BCV_QRYVID		Personalize BCV User Interface for Query View
Business Rules Framework			
FDT_OBJECT	FDT_ACT FDT_APPL FDT_OBJTYP		You use this authorization object to control usage of objects of the specified type in BRFplus.
FDT_WORKB	FDT_WB_ACT		This authorization object controls whether a user is authorized to use the BRFplus workbench and its tools.
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

Authorization Object	Field	Value	Description
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 prevent dangerous goods master data from being displayed or edited.
Formula & Derivation Tool			
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.
SAP SCM Optimizer			
S_RFC	ACTVT, RFC_NAME, RFC_TYPE	(16) Execute	Required authorization to start the SAP SCM Optimizer

Authorization Object	Field	Value	Description
			and use most of the administrator transactions.
SAP Event Management			
X_EM_EH	ACTVT, /SAPTRX/PN, /SAPTRX/PV	(03) Display (10) Post	Event handler authorization
X_EM_EH_CH	ACTVT, /SAPTRX/SO	(01) Create or generate (02) Change (05) Lock (06) Delete (63) Activate (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) Users are allowed to create, change, and delete their own queries for all POWL object types assigned to them (compare with Customizing tables POWL_TYPE_USR and POWL_TYPE_ROL). (02) Users are only allowed to create their own queries on the basis of admin queries assigned to them in Customizing tables POWL_QUERY_USR and POWL_QUERY_ROL respectively. (Note: this is also subject to the user – POWL object type assignments.) (03) (and other values): Users are only allowed to change admin queries assigned to them with respect to the select options restrictions of those admin queries (thus creating a separate “derivation” for	Specifies the authorities for Personal Object Worklist (POWL) iViews

Authorization Object	Field	Value	Description
		<p>each admin query transparently)</p> <p>POWL_CAT:</p> <p>(01) Users are allowed to create, change, and delete their own categories and assign queries to them.</p> <p>(02) Users are only allowed to assign queries to the existing categories and change the order of queries.</p> <p>(03) (and other values): Users are not allowed to reassign queries or change the query order. Note: if field POWL_QUERY is set to 01 or 03, setting POWL_CAT to 03 is not advisable. Therefore, the value is implicitly set to 02 in this case.</p>	
S_SERVICE	SRV_NAME, SRV_TYPE		This authorization object is automatically checked when external services are started. This is required for Gateway Services used by the SAP TM Collaboration Portal
S_RFCACL	RFC_SYSID, RFC_CLIENT,RFC_USER, RFC_EQUUSER, RFC_TCODE, RFC_INFO,ACTVT	(16) Execute	Authorization check for RFC users, especially for trusted systems. This is required for Gateway Services used by the SAP TM Collaboration Portal.
S_WFAR_OBJ	ACTVT OAARCHIV OADOKUMENT OAOBJEKTE	(01) Create or generate	This authorization object is used to control access to archived documents.
S_ARCHIVE	ACTVT APPLIC ARCH_OBJ		This authorization object is used in SAP archiving programs to protect the access to archive files
B_BUFA_RLT	ACTVT RLTYP		With this authorization object you define which BP roles can be edited.

Authorization Object	Field	Value	Description
B_BUPR_BZT	ACTVT RELTYT		With this authorization object you establish which relationship categories can be processed.
S_DATASET	ACTVT FILENAME PROGRAM		You use this object to assign authorizations for accessing operating system files.
S_WF_WI	TASK_CLASS WFACTVT WI_TYPE		Authorization object for working with work items in SAP Business Workflow
S_SCD0	ACTVT		

➔ Recommendation

To segregate duties using roles and authorization values in SAP TM 9.3, we recommend that you restrict the authorizations of the different roles to the business-related minimum.

With the authorization concept provided by SAP TM 9.3, you can 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 supplied business document categories. Furthermore, all critical business-related activities can be restricted for the different roles. These activities include creating business documents, displaying business documents or master data, triggering charge calculations, subcontracting freight documents, requesting customs declarations, and others activities or activity areas for the authorization objects of object class SCTS. Duties can, therefore, be segregated according to your business and scenarios.

Note that we do not recommend providing one role with full authorization for a business document or process, so that one role cannot be used, for example, to create and maintain a business document, add charge data to it, send it to a business partner, and create the invoice for that document. Such activities should be spread over different roles.

In addition, one user must not be assigned to different roles that would provide full authorization for a business document or process as described above.

1 Note

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

For general information about creating and maintaining the WF-BATCH user, see SAP Note [1251255](#) 📄.

As described in SAP Note [1251255](#) 📄, you need to also assign a role used for SAP TM 9.3 to user WF-BATCH. Depending on your specific scenario, this could be a role created according to role template /SCMTMS/TRANSPORTATION_MGR_V2, 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 transaction `SICF_SESSIONS`.

- The [HttpOnly](#) flag instructs the browser to deny access to the cookie through client side script. As a result, even if a cross-site scripting (XSS) flaw exists, and a user accidentally accesses a link that exploits this flaw, the browser will not reveal the cookie to a third party.
- The [Secure](#) flag tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests.

These additional flags are configured through the following profile parameters:

Table 15

Profile Parameter	Recommended Value	Description	Comment
icf/ set_HTTPOnly_flag_on _cookies	0	Add HttpOnly flag	client-dependent
login/ ticket_only_by_https	1	Add Secure flag	Not client-dependent

For more information, a list of the relevant profile parameters, and detailed instructions, see SAP Library for SAP NetWeaver 7.4 at help.sap.com/nw74. In SAP Library, choose ► *Function-Oriented View* ► *Security* ► *User Authentication and Single Sign-On* ► *Authentication Infrastructure* ► *AS ABAP Authentication Infrastructure* ► *Activating HTTP Security Session Management on AS ABAP*.

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 TM 9.3 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 9.3. Details that specifically apply to SAP TM 9.3 are described in the following topics:

- [Communication Channel Security \[page 34\]](#)

This topic describes the communication paths and protocols used by the application.

- [Network Security \[page 36\]](#)

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 \[page 36\]](#)

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

For more information, see the *SAP NetWeaver Security Guide* at help.sap.com/nw74. In Security Information, choose Security Guide and navigate to the following sections:

- [Network and Communication Security](#)
- [Security Guides for Connectivity and Interoperability Technologies](#)

8.1 Communication Channel Security

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

➔ Recommendation

Activate the Secure Network Communication (SNC) within all communication channels in SAP TM 9.3 to achieve a secure system landscape.

For more information, see the *SAP NetWeaver Security Guide* at help.sap.com/nw74. In Security Information, choose Security Guide ► [Network and Communication Security](#) ► [Transport Layer Security](#) ► [Secure Network Communications \(SNC\)](#) ►

The table below shows the communication paths used by SAP TM 9.3, the protocol used for the connection, and the type of data transferred.

Table 16: Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Front end client using a Web browser or SAP NWBC 4.0 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.

➔ Recommendation

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

For more information, see the *SAP NetWeaver Security Guide* at help.sap.com/nw74. In Security Information, choose Security Guide ► *Network and Communication Security* ► *Transport Layer Security* ►

Core Interface (CIF) – SAP ERP 6.0 Including Enhancement Package 4 and Higher

The master data integration of SAP TM 9.3 and SAP ERP 6.0 including enhancement package 4 and higher 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 integration of SAP TM 9.3 and SAP ERP 6.0 including enhancement package 4 and higher.

Demilitarized Zone (DMZ)

The access to your SAP TM back-end system from the SAP TM Collaboration Portal should be secured by means of an application-level gateway in the corporate network Demilitarized Zone (DMZ). This is described in the SAP NetWeaver Security Guide that you can find on SAP Service Marketplace at: <http://service.sap.com/security> under ► *SAP Security Guides* ► *SAP NetWeaver 7.4 Network and Communication Security* ►

The following subsections are also relevant:

- Web Dispatcher under ► *Using Firewall Systems for Access Control* ► *Application-Level Gateways Provided by SAP* ►
- Using Multiple Network Zones

In the following sections of this chapter, the application-level gateway is referred to as the reverse proxy.

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





Note

For information about network security for SAP NetWeaver 7.4, go to service.sap.com/nw74.  Choose [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 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, go to service.sap.com/nw74.  Choose [Security Guide](#)  [Network and Communication Security](#)  [Using Firewall Systems for Access Control](#) .

Ports

SAP TM 9.3 runs on SAP NetWeaver 7.4 and uses the ports from the AS ABAP.

For more information about AS ABAP ports, see the SAP NetWeaver Security Guide and choose [Security Guides for SAP NetWeaver Functional Units](#)  [Security Guides for the Application Server](#)  [Security Guides for the AS ABAP](#)  [SAP NetWeaver Application Server ABAP Security Guide](#)  [Network Security for AS ABAP](#)  [AS ABAP Ports](#) .

For other components, for example, SAPinst, SAProuter, or the SAP Web Dispatcher, also see the *TCP/IP Ports Used by SAP Applications* document, which is located on the SAP Developer Network at sdn.sap.com/irj/sdn/security .

8.3 Communication Destinations

Recommendation

We do not recommend assigning `SAP_ALL` authorization 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 TM 9.3:

Table 17: Connection Destinations

Destination	Delivered	Type	User Authorizations	Description
SAPOSCOL_<DB_host name> (SAP TM central instance – DB instance)	Yes	RFC – TCP/IP		For more information, see SAP Service Marketplace at ▶ service.sap.com/instguides ▶ <i>SAP Business Suite Applications</i> ▶ <i>SAP SCM</i> ▶ <i>SAP SCM Server</i> ▶ <i>Using enhancement package 3 for SAP SCM 7.0 Server</i> ▶ <i>Installation Guides</i> ▶ . Choose the appropriate guide for your operating system and database and in this guide choose ▶ <i>Post-Installation Steps</i> ▶ <i>Checking the RFC Destination</i> ▶ .
<SAP TM name>CLNT<client> SAP TM → SAP ERP	No	RFC – ERP	Use the Profile Generator (transaction code PF03) to define an appropriate profile, and see SAP Notes 447543 ▶ and 727839 ▶ .	For more information, see Customizing for SCM Basis under ▶ <i>Integration</i> ▶ <i>Basic Settings for Creating the System Landscape</i> ▶ <i>Assign RFC Destinations to Various Application Cases</i> ▶ .
OPTSERVER_<Optimizer>01	No	RFC – TCP/IP		For more information, see the <i>SCM Optimizer Installation Guide</i> on SAP Service Marketplace at ▶ service.sap.com/instguides ▶ <i>SAP Business Suite Applications</i> ▶ <i>SAP TM</i> ▶ <i>SAP SCM Optimizer</i> ▶ . Choose the appropriate guide for your operating system and database and in this guide choose ▶ <i>Post-Installation Steps</i> ▶ <i>Performing a Setup Check of the RFC Gateway</i> ▶ .
SAP Event Management → Application Systems	No	RFC	Use the Profile Generator (transaction code PF03) to define an appropriate profile.	For more information, see Customizing for SAP Event Management under ▶ <i>Event Management</i> ▶ <i>General Settings in SAP Event Management</i> ▶ <i>Define Application System</i> ▶ .

Destination	Delivered	Type	User Authorizations	Description
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 TM under ► Integration with other SAP Components ► Event Management Interface ► Define Application Interface ► Define SAP EM ►.

i Note

For more information about communication destinations of SAP NetWeaver, see the *Security Guides for Connectivity and Interoperability Technologies* section in the *SAP NetWeaver 7.4 Security Guide*.

9 Internet Communication Framework Security

You should only activate those services that are required for the applications running in your system. For SAP TM 9.3, the following services are required:

- /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/color_icon
- /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_canceln_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/scmtms
- /sap/bc/workflow
- /SAPconnect

You must activate the following services if you intend to use the Gantt chart in the transportation cockpit:

- /sap/public/bc/ui5_ui5
- /sap/bc/bsp/gntlb
- /sap/bc/scmtms

The following services are required if you intend to use the SAP TM Collaboration Portal:

- /sap/public/bc/ur/
- /sap/public/bc/icf/logoff
- /sap/public/bc/UI2
- /sap/bc/ui2/startup
- /sap/opu/odata/SCMTMS/TENDERING
- /sap/opu/odata/SCMTMS/USER
- /sap/opu/odata/SCMTMS/GENERAL/
- /sap/opu/odata/SCMTMS/EVENT_NOT/
- /sap/opu/odata/SCMTMS/INVOICE_SUBMISSION
- /sap/opu/odata/SCMTMS/FRT_PROCUREMENT
- /sap/opu/odata/SCMTMS/INVOICING

- /sap/opu/odata/UI2/PAGE_BUILDER_CUST/
- /sap/bc/ui5_ui5/tmui/coll_portal/
- /sap/bc/TM_CP_DOCU
- /sap/opu/odata/sap/vbi_appl_def_srv

Note

For information about activating ICF service /sap/public/bsp/sap/alertsubscription, see SAP Note [1080668](#).

Note

The following services are only required in case you want to implement the corresponding business process. Please check the [Administration Guide](#) for SAP TM Collaboration Portal at help.sap.com/tm choose the correct release and choose ► [System Administration and Maintenance Information](#) ► [SAP Service Marketplace](#) ► [Guides](#) for a more detailed description on the services.

Use transaction SICF to activate these services.

Note

Services

- /sap/opu/odata/SCMTMS/TENDERING/ (Business process: Tendering)
- /sap/opu/odata/SCMTMS/EVENT_NOT/ (Business Process: Event Notification)
- /sap/opu/odata/SCMTMS/INVOICE_SUBMISSION/ (Business Process: Invoice Submission)
- /sap/opu/odata/SCMTMS/FRT_PROCUREMENT/ (Business Process: Strategic Freight Procurement)
- /sap/opu/odata/SCMTMS/INVOICING/ (Business Process: Self-Billing)

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, SAP Library for SAP NetWeaver 7.4 at help.sap.com/nw74. In SAP Library, choose ► [Function-Oriented View](#) ► [Application Server](#) ► [Application Server Infrastructure](#) ► [Connectivity](#) ► [Components of SAP Communication Technology](#) ► [Communication Between ABAP and Non-ABAP Technologies](#) ► [Internet Communication Framework](#) ► [Development](#) ► [Server-Side Development](#) ► [Creating and Configuring an ICF Service](#) ► [Activating and Deactivating ICF Services](#).

For more information about ICF security, see the [SAP NetWeaver Security Guide](#) under ► [Security Guides for Connectivity and Interoperability Technologies](#) ► [RCF/ICF Security Guide](#).

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 7.4 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 7.4 Security Guide*.

In general, all business data of SAP TM 9.3 is stored in the system database. This business data is protected by the authorization concept of SAP NetWeaver and SAP TM 9.3.

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. To delete this business partner data from the database, you can use the [Deletion of Business Partners](#) transaction. For more information, see SAP Library for SAP ERP 6.0 Enhancement Package 7 at help.sap.com/erp . In SAP Library, choose ► [SAP ERP](#) ► [SAP ERP Cross-Application Functions](#) ► [Cross-Application Components](#) ► [SAP Business Partner](#) ► [Functions](#) ► [Deleting Business Partners](#) .

11 Other Security-Relevant Information

Integration of SAP Visual Business 2.1

SAP Visual Business 2.1 is a digitally signed ActiveX control that is integrated into multiple ABAP Web dynpro applications of SAP TM 9.3. For it to run on front-end clients, ActiveX controls must not be blocked by your Web browser.

Your security policy must, therefore, allow ActiveX controls to be executed on the front-end clients; otherwise, it is not possible to use SAP Visual Business 2.1.

SAP TM collaboration portal

The SAP TM collaboration portal exposes TM scenarios to external carrier users. Thus, the portal is available in the internet. This increases the need for secure configuration even more. Make sure to not expose the SAP TM server directly to the internet but instead put a Web Dispatcher in place.

➔ Recommendation

To access the SAP Transportation Management (SAP TM) system externally, we recommend that you define a system alias in the web dispatcher. The web dispatcher redirects the request to the correct hostname and port so that an external user can use a hyperlink, which contains the alias, to access the system. As the URL to the portal bears the risk to be forged, the URL should not be published to parties which have no business need for it.

The SAP TM collaboration portal is written in HTML and JavaScript. For these client-side technologies, the source code can be accessed on user clients and it can be potentially manipulated on the client machine if a third party has access to that machine. Thus, it has to be ensured, that only authorized personnel has access to the devices which are running the portal. The SAP TM collaboration portal provides a demo mode which can be used for demo or training purposes. If you want to provide a demo user, make sure that you create an individual user which has only role `/TMUI/COLL_PORTAL_DEMO`.

Special Considerations

Since the tablet devices are at a greater risk of being lost or stolen, it is highly recommended that you perform the following activities.

- Configure your tablet devices to use the security features provided by the relevant tablet device platform
- Configure your tablet devices to restrict access to data
- Configure your tablet to automatically erase data if the device is stolen

We strongly recommend that each tablet device has only a single dedicated user.

11.1 Enterprise Services Security

The following chapters in the [SAP NetWeaver 7.4 Security Guide](#) and related documentation are relevant for all enterprise services delivered with SAP TM 9.3:

Table 18

Chapter	Location
Security Guide Web Services (ABAP)	Security Guide for SAP NetWeaver 7.4 under ► SAP NetWeaver Security Guide ► Security Guides for Connectivity and Interoperability Technologies ► Security Guide Web Services (ABAP) ►
Recommended WS Security Scenarios	SAP Library for SAP NetWeaver 7.4 under ► SAP NetWeaver: Function-Oriented View ► Security ► Recommended WS Security Scenarios ►
SAP NetWeaver Process Integration Security Guide	► service.sap.com/securityguide ► SAP NetWeaver ► SAP NetWeaver PI 7.1 including EhP 1 ►

For more information about special security requirements for Web services, see the Security Guide for SAP NetWeaver 7.4 and choose ► [Security Guides for Connectivity and Interoperability Technologies](#) ► [Security Aspects for Web Services](#) ►.

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

For more information about the security of the exchange infrastructure, see ► help.sap.com/nw ► [SAP NetWeaver](#) ► [SAP NetWeaver PI 7.1 including Enhancement Package 1](#) ► [Security Information](#) ► [Security Guides](#) ►.

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 Netweaver component is described in detail in the *SAP NetWeaver 7.4 Security Guide*. For more information, go to help.sap.com/nw74. Choose ► *Security Guide* ► *Security Aspects for Lifecycle Management* ► *Auditing and Logging*.

Security Audit Log Triggered by Virus Scan Interface (VSI)

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 message class `VSCAN` using 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 about auditing and logging for the Audit Information System (AIS) is described in detail in the *SAP NetWeaver 7.4 Security Guide*.

For more information, see *The Audit Info System (AIS)* at help.sap.com/nw74. Choose ► *Security Guide* ► *Security Aspects for Lifecycle Management* ► *Auditing and Logging* ► *The Audit Info System (AIS)*.

For more information about security logs for the SAP Gateway, see Logging in SAP Gateway section of the SAP Gateway Developer Guide for SAP Gateway SP06.

SAP Transportation Management 9.3

Tracing and Logging of Business Objects

In SAP TM 9.3, 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 7.4 Security Guide* on SAP Help at help.sap.com/nw.

Activating Change Documents

In SAP TM 9.3, 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 for which you can activate change documents and where to activate them, see the corresponding section in the SAP TM 9.3 documentation:

Table 19

Object	Customizing Path
Location	► <i>Transportation Management</i> ► <i>Master Data</i> ► <i>Transportation Network</i> ► <i>Location</i> ► <i>Activate Change Documents</i> ►
Transportation lane	► <i>Transportation Management</i> ► <i>Master Data</i> ► <i>Transportation Network</i> ► <i>Transportation Lane</i> ► <i>Activate Change Documents</i> ►
Product	► <i>SCM Basis</i> ► <i>Master Data</i> ► <i>Product</i> ► <i>Activate Change Documents</i> ►
Freight unit	► <i>Transportation Management</i> ► <i>Planning</i> ► <i>Freight Unit</i> ► <i>Define Freight Unit Types</i> ► (Track Changes checkbox)
Freight order	► <i>Transportation Management</i> ► <i>Freight Order Management</i> ► <i>Freight Order</i> ► <i>Define Freight Order Types</i> ► (Track Changes checkbox)
Freight booking	► <i>Transportation Management</i> ► <i>Freight Order Management</i> ► <i>Freight Booking</i> ► <i>Define Freight Booking Types</i> ► (Track Changes checkbox)
Freight agreement	► <i>Transportation Management</i> ► <i>Master Data</i> ► <i>Agreements and Service Products</i> ► <i>Define Freight Agreement Types</i> ► (Track Changes checkbox).
Forwarding agreement	► <i>Transportation Management</i> ► <i>Master Data</i> ► <i>Agreements and Service Products</i> ► <i>Define FWA and Service Product Catalog Types</i> ► (Track Changes checkbox).
Forwarding order	► <i>Transportation Management</i> ► <i>Forwarding Order Management</i> ► <i>Forwarding Order</i> ► <i>Define Forwarding Order Types</i> ► (Track Changes checkbox).
Forwarding quotation	► <i>Transportation Management</i> ► <i>Forwarding Order Management</i> ► <i>Forwarding Quotation</i> ► <i>Define Forwarding Quotation Types</i> ► (Track Changes checkbox).
Forwarding settlement	► <i>Transportation Management</i> ► <i>Settlement</i> ► <i>Forwarding Settlement</i> ► <i>Define Forwarding Settlement Document Types</i> ► (Track Changes checkbox).
Freight settlement	► <i>Transportation Management</i> ► <i>Settlement</i> ► <i>Freight Settlement</i> ► <i>Define Freight Settlement Document Types</i> ► (Track Changes checkbox).

Object	Customizing Path
Order-based transportation requirement	► <i>Transportation Management</i> ► <i>Integration</i> ► <i>ERP Logistics Integration</i> ► <i>Order-Based Transportation Requirement</i> ► <i>Define Order-Based Transportation Requirement Types</i> ► (Track Changes checkbox).
Delivery-based transportation requirement	► <i>Transportation Management</i> ► <i>Integration</i> ► <i>ERP Logistics Integration</i> ► <i>Delivery-Based Transportation Requirement</i> ► <i>Define Delivery-Based Transportation Requirement Types</i> ►
Service order	► <i>Transportation Management</i> ► <i>Freight Order Management</i> ► <i>Service Order</i> ► <i>Define Service Order Types</i> ► (Track Changes checkbox).

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 service.sap.com/securityguide ►.

For more information about the logging and tracing mechanisms from SAP NetWeaver, go to help.sap.com/nw74 ►. Choose ► *Security Guide* ► *Security Aspects for Lifecycle Management* ► *Auditing and Logging* ►.

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 EarlyWatch Alert report of your system. It tells you:

- Whether SAP Security Notes have been identified as missing from 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 in 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 for 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 a 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 information about these services, see the following locations:

- EarlyWatch Alert: service.sap.com/ewa 
- Security Optimization Service / Security Notes Report: service.sap.com/sos 
- Comprehensive list of Security Notes: service.sap.com/securitynotes 

-
- Configuration Validation: service.sap.com/changecontrol 
 - RunSAP Roadmap, including the Security and the Secure Operations Standard: 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

For more information about the security of SAP solutions, see SAP Service Marketplace at service.sap.com/security.

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

Table 20: Related Security Guides

Guide	Location on SAP Service Marketplace
SAP NetWeaver 7.4 Security Guide	▶ SAP NetWeaver ▶ SAP NetWeaver 7.4 ▶
SAP Visual Business 2.1 Security Guide	▶ Security ▶ Security in Detail ▶ SAP Security Guides ▶ SAP Business Suite Applications ▶ Cross-Application Tools ▶

A.2 Related Information

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

Table 21

Content	Quick Link on SAP Service Marketplace
Master Guides, Installation Guides, Upgrade Guides, Solution Management Guides	service.sap.com/instguides
Related SAP Notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
Network security	service.sap.com/securityguide
Technical infrastructure	service.sap.com/installnw74
SAP Solution Manager	service.sap.com/solutionmanager

Documentation in the SAP Service Marketplace

You can find this document at the following address: help.sap.com/tm93.

www.sap.com