Security Guide | PUBLIC
Document Version: 1.1 – 2024-04-22

Security Guide for SAP Translation Hub

THE BEST RUN SAP

Content

1 Document History

Version	Date	Change
1.0	2024-03	Initial version for Cloud Foundry/multi-environment version.

2 Introduction

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

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the installation guides, configuration guides, technical operation manuals, or upgrade guides. These guides are relevant only for a certain phase of the software life cycle, whereas a security guide provides 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 ensure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Translation Hub. This security guide assists you in securing SAP Translation Hub.

About this Document

The security guide provides an overview of the security-relevant information that applies to SAP Translation Hub (including Document Translation).

3 Before You Start

Fundamental Security Guides

SAP Translation Hub is built on SAP Business Technology Platform and as part of SAP NetWeaver. Therefore, the corresponding security guides also apply to SAP Translation Hub. Pay particular attention to the most relevant sections or specific restrictions as indicated in the following table:

Scenario, Application, or Component Security Guide	Applicable to which option
SAP Business Technology Platform Security Information	Document Translation/Software Translation
RFC/ICF Security Guide	Software Translation
SAP NetWeaver Security Guide	Software Translation

Important SAP Notes

The most important SAP Notes that apply to the security of SAP Translation Hub are shown in the following table:

Title	SAP Note	Comment
STH ABAP API	2349776	ABAP RFC layer for SAP Translation Hub

> **Note**
>
> For a list of additional security-relevant news and SAP Notes, see *SAP Security Notes & News* at https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html.

Additional Information

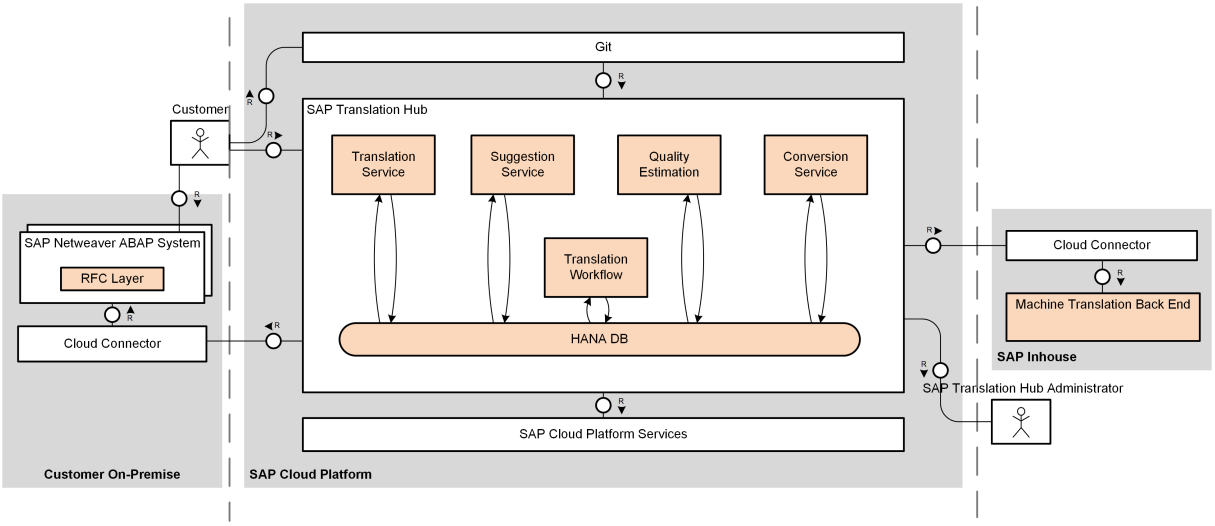
For more information about specific security topics, see the links in the following table:

Content	Link
Security Community	https://www.sap.com/community/topic/security.html
Related SAP Notes	https://support.sap.com/en/my-support/knowledge-base.html and https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Released platforms	https://support.sap.com/en/release-upgrade-maintenance.html#section_1969201630
SAP Solution Manager	https://support.sap.com/en/solution-manager.html
SAP NetWeaver Technology Community	https://www.sap.com/community/topic/netweaver.html

4 Technical System Landscape

This section comprises the main components in SAP Translation Hub.

The following diagram shows an overview of the technical system landscape for SAP Translation Hub.



SAP Translation Hub combines all translations in a cloud-based solution on SAP Business Technology Platform by using an SAP HANA database to increase speed and reduce costs in global roll-outs.

The central multilingual approach, which stores source texts and all corresponding translations together, we can semi-automate the reuse of all existing SAP product languages.

With SAP Translation Hub, you can translate Git content, files that you can upload, and texts in a customer's on-premise ABAP system.

SAP Translation Hub also comprises a suggestion service that is integrated in SAP Web IDE.

Translation Service

The translation service provides translations of short texts based on existing texts and their translations that are used in SAP products. The service looks for suitable translations in the following places:

1. Company multilingual text repository (company MLTR)
2. SAP multilingual text repository (MLTR)
3. SAP machine translation (SAP MT) based on Moses open source toolkit

Each record in the multilingual text repository comprises the source language in English plus translations for a combination of domain and text type, which you can enter as additional request parameters.

Suggestion Service

Provides suggestions for short texts in English based on complete or partial texts and their translations used in SAP products. You can, for example, use the suggestion service to propose texts while you type in a development environment. The texts that the service proposes are already available in additional languages in the multilingual text repository.

Translation Workflow Scenarios

The following steps are performed:

1. Read the translation project.
2. Get translations from the following sequence of translation providers: (to be customizable)
    1. Company multilingual text repository (company MLTR)
    2. SAP Translation Hub's multilingual text repository (SAP MLTR)
    3. SAP machine translation solution (SAP MT)
3. Generate the corresponding translations in the source repository or in an export file.

Machine Translation Back End

In addition to the translations stored in the SAP HANA database (SAP MLTR), SAP Translation Hub can also retrieve proposals from a machine translation back end.

The back end is in the SAP Intranet (Zone3) and connected with a Cloud Connector (SAP HANA Enterprise Cloud) to SAP Business Technology Platform.

Several UIMA pipelines parallelize the calls to the Moses server.

Moses is a statistical machine translation system that can be used to automatically train translation models for any language pair. With the trained models and available algorithms Moses finds the best translation.

Conversion Service

A common issue during software translation is the storage and handling of the source files and translations. Most often every repository and/or development infrastructure handles translatable texts different. The conversion service helps to overcome these issues and provides a service that converts source files, such as .properties files, in a format that can be translated more easily (XLIFF 1.2) and also reconverts the translated file back to the source format.

ABAP RFC Layer

The ABAP RFC layer is deployed in a customer's SAP NetWeaver ABAP system. The RFC layer acts as a wrapper to access ABAP source texts from SAP Business Technology Platform and to write the translated texts back to the ABAP system.

The communication is secured through the Cloud Connector, which is installed in a customer's intranet.

The Cloud Connector communicates with a customer's subscription of SAP Translation Hub on SAP Business Technology Platform. You use destinations to configure the Cloud Connector.

The core SAP Translation Hub services are called from the UI. The services invoke the ABAP client to communicate with a customer's system and the XS importer service to import the ABAP texts to the SAP HANA database.

Integration of Your Own Language Data

You can upload your own translations to SAP Translation Hub based on object lists in on-premise ABAP systems or using XLIFF files. The function accepts XLIFF 1.2 files with SAP-specific metadata.

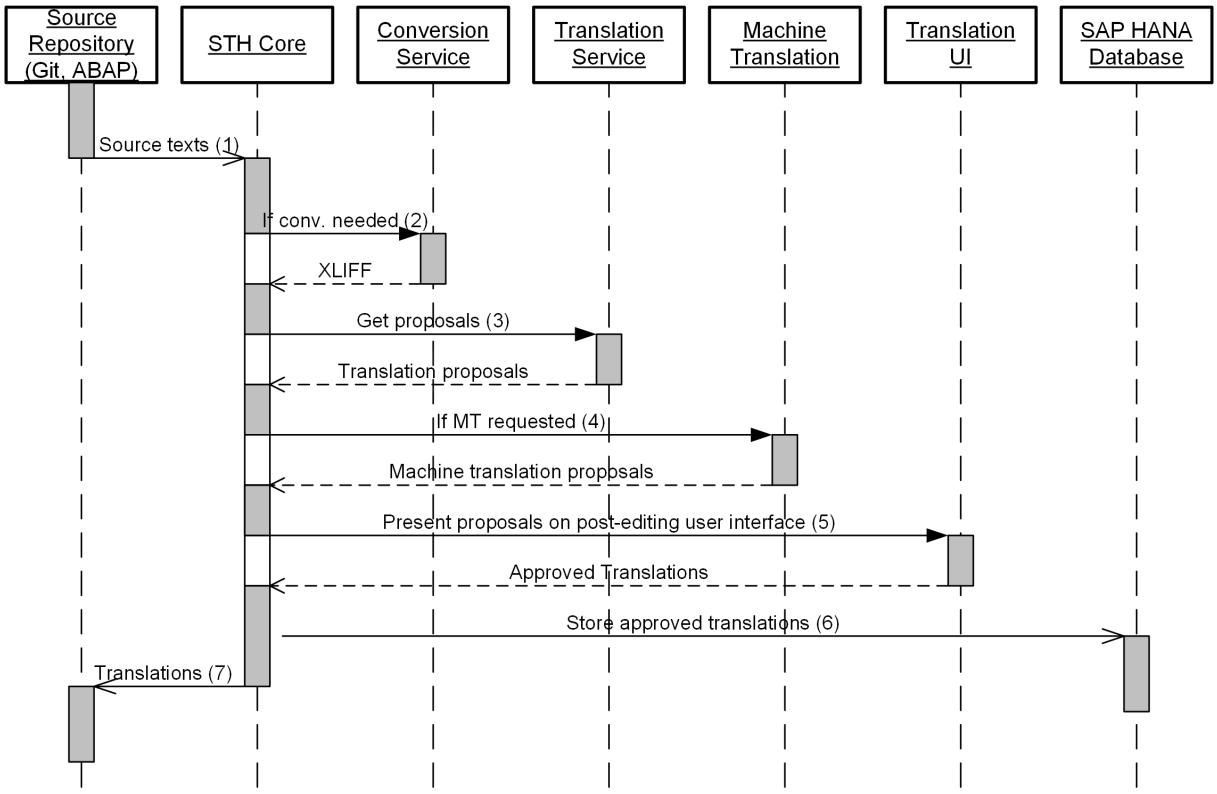
To use this feature, customers create a multilingual text repository known as a company MLTR, which is considered in the retrieval algorithms to provide the best translation for a given text.

Related Information

SAP Business Technology Platform Documentation
Technical Landscape Design
Security Community

5 Security Aspects of Data, Data Flow, and Processes

The following figure shows an overview of the data flow for SAP Translation Hub.

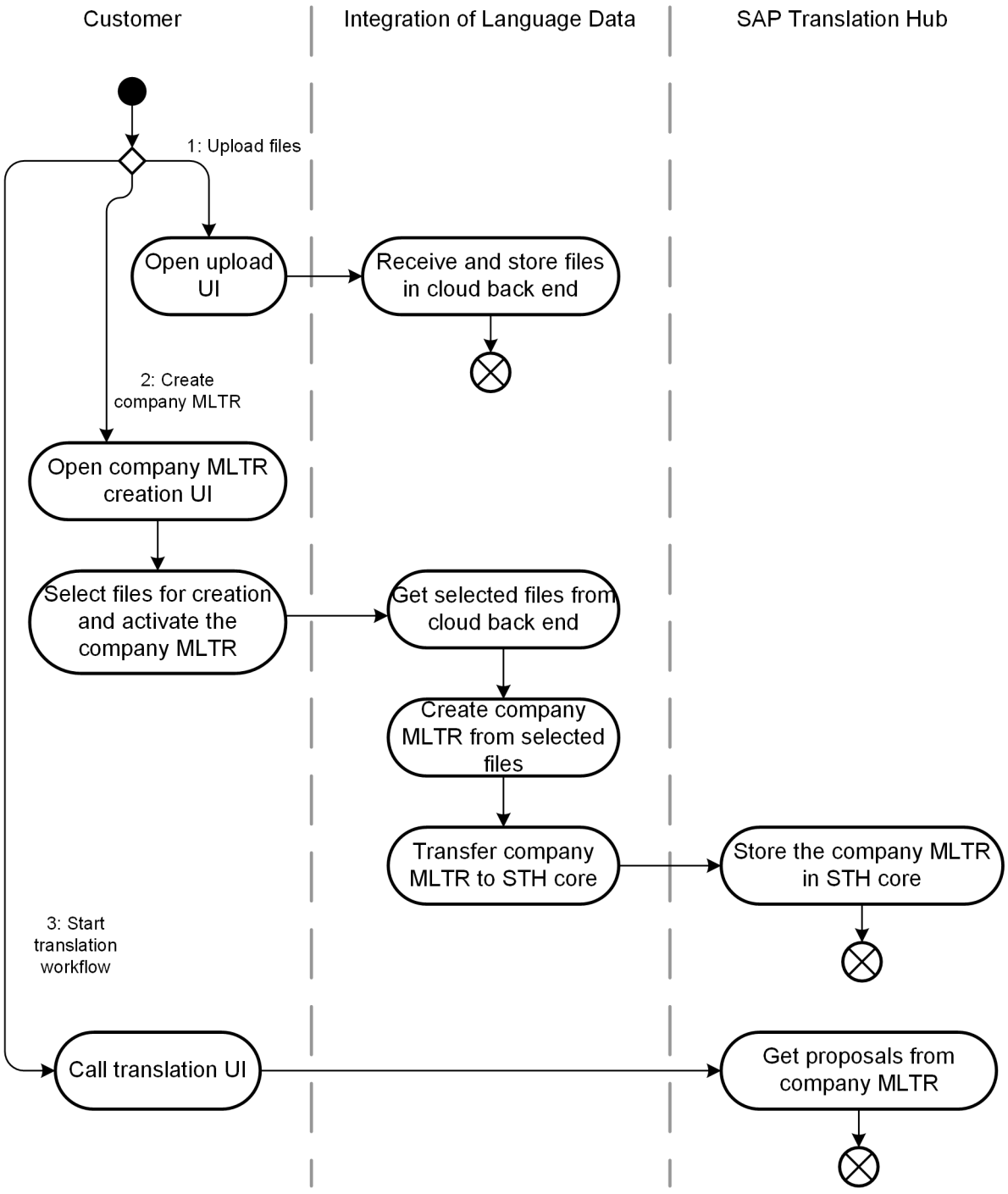


The table below shows the security aspect to be considered for the process step and which security measure applies in each case.

Step	Description	Security Measure
1	SAP Translation Hub core accesses source texts from Git repository/ABAP system	User types: Technical user accesses the repositories. In the ABAP scenario, explicit authorizations are needed. The communication protocol is HTTPS for Git and RFC for ABAP.
2	SAP Translation Hub core to conversion service	HTTPS. Input validation used.
3	SAP Translation Hub core to translation Service	HTTPS.

Step	Description	Security Measure
4	SAP Translation Hub core to machine translation	OAuth authorization, HTTPS.
5	SAP Translation Hub core to post-editing user interface	Input validation.
6	SAP Translation Hub to SAP HANA database	Not applicable.
7	SAP Translation Hub stores target texts in Git repository/ABAP system	User types: Technical user accesses the repositories. In the ABAP scenario, explicit authorizations are needed. The communication protocol is HTTPS for Git and RFC for ABAP.

The following figure shows an overview of the data flow for the integration of your own language data in SAP Translation Hub based on the XLIFF file upload option.


Customer
Integration of Language Data
SAP Translation Hub
1: Upload files
Open upload UI
Receive and store files in cloud back end
2: Create company MLTR
Open company MLTR creation UI
Select files for creation and activate the company MLTR
Get selected files from cloud back end
Create company MLTR from selected files
Transfer company MLTR to STH core
Store the company MLTR in STH core
3: Start translation workflow
Call translation UI
Get proposals from company MLTR

6 User Administration and Authentication

SAP Translation Hub uses SAP Business Technology Platform Identity Authentication service. Therefore, the security recommendations and guidelines for SAP Business Technology Platform apply as well.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to SAP Translation Hub in the topics in this section.

Related Information

User Management for SAP Business Technology Platform [page 14]
User Management for RFC Layer [page 17]
User Management for Machine Translation Back End [page 18]
User Management for Integration of Language Data [page 19]
User Data Synchronization [page 19]
Integration into Single Sign-On Environments [page 20]

6.1 User Management for SAP Business Technology Platform

Use

User management for SAP Translation Hub uses the mechanisms provided with the SAP Business Technology Platform Identity Authentication service for users in the SAP Business Technology Platform. For the SAP HANA XS services, SAP Translation Hub uses the user and role management of the XS back end. For an overview of how these mechanisms apply to SAP Translation Hub, see the sections below. In addition, we provide a list of the standard users required for operating SAP Translation Hub.

User Administration Tools

The following table shows the tools to use for user management and user administration with SAP Translation Hub.

Tool	Detailed Description	Prerequisites
SAP Business Technology Platform Identity Authentication service	User and Role Administration	Registered user on SAP Business Technology Platform
SAP HANA XS database user management	Database user and role management	None.

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 who run background processing jobs.

The user types that are required for SAP Translation Hub include:

- Users in SAP Business Technology Platform
  - SAP Translation Hub Core
    - Developer (specific to SAP Business Technology Platform)
    - Admin (specific to SAP Business Technology Platform)
    - User (application-specific)
  - Integration of own language data
    - User (application-specific)
- SAP HANA XS
  - SAP Translation Hub core
    - Developer (translsvcDev)
    - Read-only (translsvcREADONLY)
    - User (translsvcUSER)

Standard Users

The following table shows the standard users that are necessary to use SAP Translation Hub.

System	User ID	Type	Password	Description
SAP Business Technology Platform	Developer	Developer	SAP Business Technology Platform Identity Authentication service	Specific to SAP Business Technology Platform for provider account.

System	User ID	Type	Password	Description
SAP Business Technology Platform	Admin	Admin	SAP Business Technology Platform Identity Authentication service	Specific to SAP Business Technology Platform for provider account.
SAP Business Technology Platform	READONLY	Read-Only	SAP Business Technology Platform Identity Authentication service	Specific to SAP Business Technology Platform for application.
SAP Business Technology Platform	User (own language data)	User	SAP Business Technology Platform Identity Authentication service	Specific to SAP Business Technology Platform for application.
XS back end	Developer	Database user	DB management	translsvcDev sap.translsvc.xsServices:Full sap.translsvc.xpra:Full sap.translsvc:Full sap.hana.xs.admin.roles:JobAdministator sap.hana.xs.admin.roles:JobSchedulerAdministator
XS back end	READONLY	Database user	DB management	translsvcREADONLY sap.hana.xs.admin.roles:JobAdministator sap.hana.xs.admin.roles:JobSchedulerAdministator sap.translsvc.xsServices:ReadOnly

System	User ID	Type	Password	Description
XS back end	USER	Database user	DB management	translsvcUSER sap.hana.xs.admin.roles:JobAdministator sap.hana.xs.admin.roles:JobSchedulerAdministator sap.translsvc.xsServices:Full

6.2 User Management for RFC Layer

Use

User management for the RFC Layer 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 the RFC Layer, see the sections below. In addition, we provide a list of the standard users required for operating SAP Translation Hub.

User Administration Tools

The following table shows the tools to manage and administer users for the RFC layer.

Tool	Detailed Description
User and role maintenance with SAP NetWeaver AS ABAP (Transactions `SU01`, `PFCG`)	User and Role Administration of Application Server ABAP

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 the RFC Layer include technical users, which are service users that read object lists and source texts, and write translations.

For more information about these user types, search for information about user types in the SAP NetWeaver AS ABAP Security Guide.

Standard Users

The following table shows the standard users that are required to operate the RFC layer.

System	User ID	Type	Password	Description
Customer's on-premise SAP NetWeaver System	To be specified	Service user	The user ID and password are stored in the RFC destination for the connection.	Technical user for connection to your on-premise ABAP system.

> **Note**
>
> Your must create the technical user in your on-premise ABAP system.

Related Information

SAP NetWeaver Guide Finder
User and Role Administration of Application Server ABAP

6.3 User Management for Machine Translation Back End

Use

The user and role for the machine translation back end is predefined in the application. Only the technical user identified via OAuth can use the HLT MT connector service in SAP Business Technology Platform to request machine translation output for a given input text.

User Types and Standard Users

The following table shows the standard users that are necessary for operating the machine translation back end

Standard Users

System	User ID	Type	Password
Machine translation back end	OAuth user	Technical user	OAuth token

6.4 User Management for Integration of Language Data

Use

The user and role for the integration of language data is predefined in the application. Only the technical user identified via OAuth can use the Customer Data Endpoint in the SAP Business Technology Platform.

User Types and Standard Users

The following below shows the standard users that are necessary for integrating language data.

Standard Users

System	User ID	Type	Password
Integration of language data (SAP Business Technology Platform)	OAuth user	Technical user	OAuth token

6.5 User Data Synchronization

Use

The SAP Business Technology Platform Identity Authentication service synchronizes data for users.

Technical users are not synchronized automatically. Due to the limited number of technical users, SAP Translation Hub manages the required users in SAP Business Technology Platform.

6.6 Integration into Single Sign-On Environments

Use

7 Authorizations

Use

SAP Translation Hub uses the authorization concept provided by SAP Business Technology Platform and the SAP HANA XS back-end system.

The SAP Translation Hub RFC layer uses the authorization concept provided by SAP NetWeaver AS ABAP or AS Java. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to the SAP Translation Hub RFC layer.

The SAP NetWeaver authorization concept is based on the assignment of authorizations to users based on roles. To maintain roles, use the profile generator (transaction `PFCG`) in SAP NetWeaver AS ABAP and the User Management Engine's user administration console in SAP NetWeaver AS Java.

Related Information

Role Administration

7.1 Role and Authorization Concept for SAP Business Technology Platform

Standard Roles

The following table shows the standard roles that SAP Translation Hub uses.

Standard Roles

Role	Description
Developer	Developer (specific to SAP Business Technology Platform)
Admin	Admin (specific to SAP Business Technology Platform)

Role	Description
User	User (application-specific) Users translate texts stored in one of the locations that SAP Translation Hub supports, such as the Git repository on SAP Business Technology Platform or an on-premise ABAP system. Users review the translations on the SAP Translation Hub UI before transferring the translations to the source repository.
User (integration of your own language data)	User (application-specific) Users upload translations that are specific to a customer's company or industry so that SAP Translation Hub can use these translations as the first choice translation provider.

7.2 Role and Authorization Concept for SAP HANA XS Back End

Standard Roles

The following table shows the standard roles that SAP Translation Hub uses.

Standard Roles

Role	Description
translsvcDev	Developer
translsvcREADONLY	Read-only
translsvcUser	User

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by the SAP HANA XS back end.

Standard Authorization Objects

Role	Value
translsvcDev	sap.translsvc.xsServices:Full
	sap.translsvc.xpra:Full
	sap.translsvc:Full
	sap.hana.xs.admin.roles:JobAdministator
	sap.hana.xs.admin.roles:JobSchedulerAdministator
translsvcREADONLY	sap.hana.xs.admin.roles:JobAdministator
	sap.hana.xs.admin.roles:JobSchedulerAdministator
	sap.translsvc.xsServices:ReadOnly
translsvcUser	sap.hana.xs.admin.roles:JobAdministator
	sap.hana.xs.admin.roles:JobSchedulerAdministator
	sap.translsvc.xsServices:Full

7.3 Role and Authorization Concept for Machine Translation Back End

Authentication is done at the entry point of the system at the HLT MT connector service running on SAP Business Technology Platform. Users with the role `translation` can use the system. Only a single user with that role exists. It's the technical user authenticated by OAuth that SAP Translation Hub uses: `505eb27b-b830-3365-bd29-78bc73297a49`.

End users are authenticated on the level of SAP Translation Hub, which is the only consumer of the HLT MT connector service.

7.4 Role and Authorization Concept for ABAP RFC

Standard Roles

The following table shows the standard authorizations that the technical user needs:

Role	Description
Role for technical user (you must create this user)	Technical user to connect to the ABAP back-end system

Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used

Standard Authorization Objects

Authorization Object	Field	Value
S_RFC	RFC_TYPE	FUNC
	RFC_NAME	LXE_STH_GET_OBJECT_LISTS LXE_STH_READ_OBJECT_LIST LXE_STH_READ_TEXTS LXE_STH_WRITE_TEXTS
	ACTVT	16 (Execute)
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RFC1, SDIFRUNTIME, SG00, SRFC, SYST, SYSU,
	ACTVT	16 (Execute)
S_ADMI_FCD	TRNR	Translation administration SLWA/ SLWB

8 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.

9 Network and Communication Security

This section describes the network connections and channels that SAP Translation Hub uses.

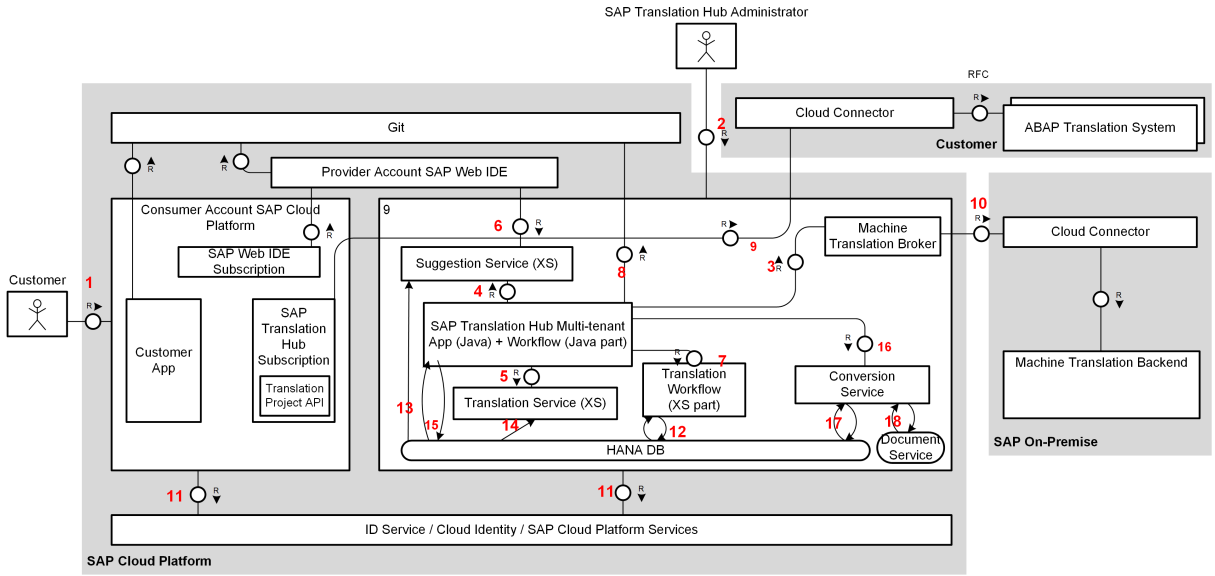
Related Information

Communication Channel Security [page 26]
Network Security [page 30]
Communication Destinations [page 33]

9.1 Communication Channel Security

Overall SAP Translation Hub

The following graphic shows an overview of the network and channels of SAP Translation Hub.



> ### Note
>
> The table below contains an explanation of the numbers in the graphic.

The following table shows the communication channels that SAP Translation Hub uses, the protocol used for the connection, and the type of data that is transferred.

Connection ID (See Graphic Above)	Source System	Destination System	Protocol (only one entry per ID possible)	Port (only one entry per ID possible)	Comment
1	Browser	Consumer account on SAP Business Technology Platform	HTTPS	443	None.
2	Browser	Provider account on SAP Business Technology Platform	HTTPS	443	None.
3	Translation workflow	Machine translation broker	HTTPS	443	Based on the subscription concept of SAP Business Technology Platform
4	SAP Translation Hub multitenant app	Suggestion service	HTTPS	443	Routing from Java to XS
5	SAP Translation Hub multitenant app	Translation service	HTTPS	443	Routing from Java to XS
6	Provider account for SAP Web IDE	Suggestion service	HTTPS	443	Based on the subscription concept of SAP Business Technology Platform
7	Translation workflow Java	Translation workflow XS	HTTPS	443	None.
8	Translation workflow	Git	HTTPS	443	None.
9	Customer subscription	Customer SAP NetWeaver ABAP system	RFC	33XX	Through Cloud Connector
10	Translation workflow	Machine translation broker service	HTTPS	9443	Through Cloud Connector

Connection ID (See Graphic Above)	Source System	Destination System	Protocol (only one entry per ID possible)	Port (only one entry per ID possible)	Comment
11	SAP Business Technology Platform apps	Cloud Identity	HTTPS	443	None.
12	Translation workflow XS	SAP HANA database	Other: XSJS database access HTTPS	Not applicable.	None.
13	Suggestion service	SAP HANA database	Other: XSJS database access HTTPS	Not applicable.	None.
14	Translation service	SAP HANA database	Other XSJS database access HTTPS	Not applicable.	None.
15	Translation workflow Java	SAP HANA database	JDBC	30015	None.
16	SAP Translation Hub	Conversion service	HTTPS	443	None.
17	Conversion service	SAP HANA database	JDBC	30015	None.
18	Conversion service	SAP Business Technology Platform Document Service	CMIS protocol	Not applicable.	None.

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

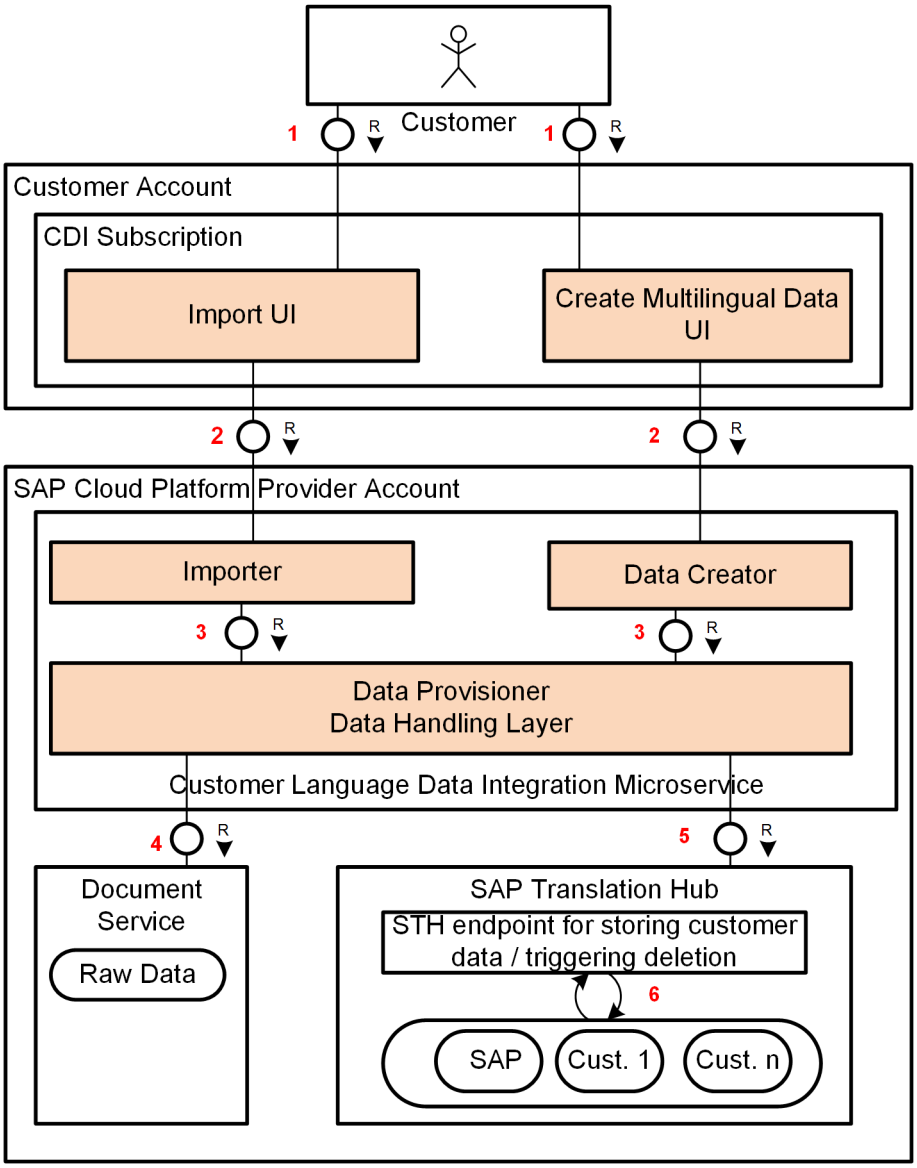
→ Recommendation

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

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

Integration of Your Own Language Data

The following graphic shows an overview of the network and channels specific to the integration of your own language data in SAP Translation Hub.



> **Note**
>
> The table below contains an explanation of the numbers in the graphic.

The table below shows the communication channels, protocol, and type of data transferred when you integrate your language data in SAP Translation Hub.

Connection ID	Related Data Flow (See Graphic Above)	Source System	Destination System	Protocol (only one entry per ID possible)	Port (only one entry per ID possible)	Comment
1	1	Browser	Consumer account on SAP Business Technology Platform	HTTPS	443	None.
2	2	SAP Business Technology Platform customer account UI	Provider account on SAP Business Technology Platform	HTTPS	443	None.
3	3	Import/Data Creator	Data handling in back-end layer	HTTPS	443	None.
4	4	Data Handling Back-End Layer	Document service	HTTPS	443	CMIS Protocol
5	5	Integration of your own language data	SAP Translation Hub	HTTPS	443	None.
6	6	Provider account SAP Web IDE	SAP HANA DB	JDBC	30015	None.

Related Information

SAP NetWeaver Guide Finder

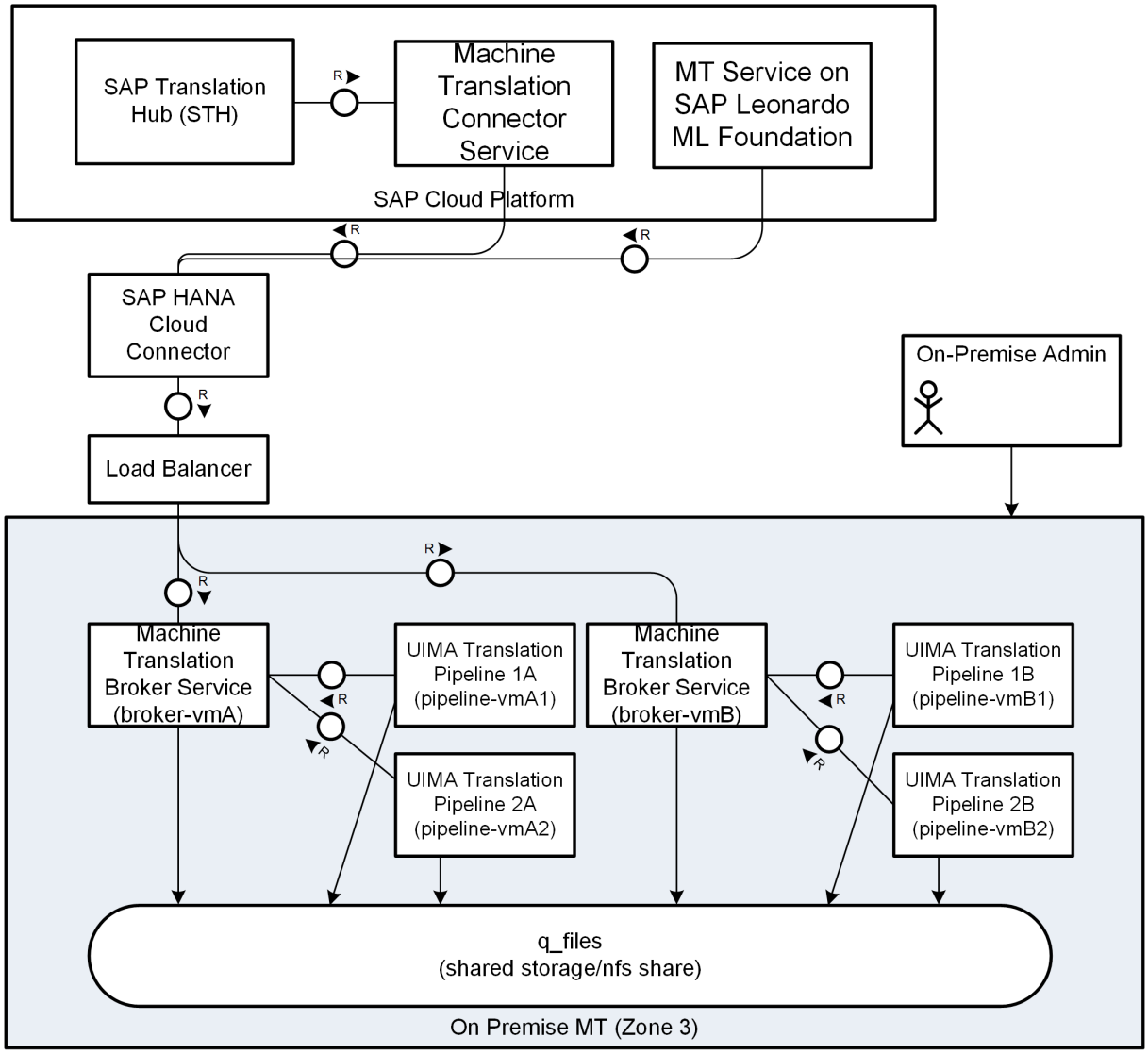
9.2 Network Security

Use

For the parts that ate deployed on SAP Business Technology Platform, SAP Translation Hub relies on the network security of SAP Business Technology Platform.

The SAP machine translation back end resides in zone 3 and uses the Cloud Connector to connect to SAP Business Technology Platform.

The following graphic shows an overview of the network topology for the machine translation parts of SAP Translation Hub.



> **Note**
>
> The table below contains an explanation of the numbers in the graphic.

Ports

The following table describes the individual steps in the overview of the network topology on this page.

Connection ID (from Network Topology Graphic)	Source System	Destination System	Protocol (only one entry per ID possible)	Port (only one entry per ID possible)	Comment
1	SAP Translation Hub ID: STH	Machine Translation Connector Service ID: HLTCS	HTTPS	443	None.
2	Machine Translation Connector Service ID: HLTCS	Cloud Connector ID: CC	HTTPS	Other: 9443	None.
3	Cloud Connector ID: CC	Load Balancer ID: LOAD HLT Broker Service ID: HLTBS	HTTPS	Other: 9443	This connection physically goes through the load balancer which transparently distributes the requests between the two HLTBS instances.
3'	Load Balancer ID: LOAD	Machine Translation Broker Service ID: HLTBS	HTTPS	Other: 9443	Note that this connection "enters" the Zone 3 Network. All communication hereafter is inside of the Zone 3 Network.
4	Machine Translation Broker Service ID: HLTBS	UIMA-AS activeMQBroker ID: UIMAAS	HTTP	Other: 8080	Communication happens locally on Machine
5	UIMA Pipeline(s) ID: UIMAP	UIMA AS ID: UIMAAS	Other: TCP	Other: dynamic	None.
6	UIMA Pipeline(s) ID: UIMAP	Moses Server ID: MOSES	Other: XML-RPC	Other: dynamic	Communication happens locally on Machine
7	<HLTBS>	Q_files shared NFS storage ID: QFILES	Other: NFS	Other: 111 and 2049	None.

Connection ID (from Network Topology Graphic)	Source System	Destination System	Protocol (only one entry per ID possible)	Port (only one entry per ID possible)	Comment
8	<UIMAP>	Q_files shared NFS storage ID: QFILES	Other: NFS	Other: 111 and 2049	None.
9	Admin User (inside SAP employee network)	All on-premise machine translation systems	Other:SSH	Other:22	The administrative user can access the root account of all On-Premise VMs via SSH (using their global user).
10	Machine Translation Service on SAP Leonardo Machine Learning Foundation	Cloud Connector ID: CC	HTTPS	Other: 9443	None.

9.3 Communication Destinations

Use

The following destinations in SAP Business Technology Platform are necessary for productive usage.

9.3.1 converterMS

Connection to the conversion service with basic authentication and the *Internet* proxy type.

9.3.2 Git

Connection to the Git repository on SAP Business Technology Platform with no authentication and the *Internet* proxy type.

9.3.3 SAP Business Technology Platform Metering

Connection to the SAP Business Technology Platform metering service with InternalSystemAuthentication and the *Internet* proxy type.

9.3.4 ABAP Translation Back End

Connection to an ABAP translation system as part of the ABAP workflow scenario with jCo parameters *client*, *mshost*, and *r3name*.

9.3.5 XS Back End

Connection to the XS back end with basic authentication and the *Internet* proxy type.

10 Application-Specific Virus Scan Profile (ABAP)

The SAP Translation Hub RFC layer makes use of the SAP RFC protocol only, therefore no virus scanner is required for the ABAP part.

11 Data Storage Security

Data is stored in the following locations and secured by the means mentioned in each section.

11.1 SAP HANA Database

SAP Translation Hub stores translations, log files, project metadata, and customer translations in a dedicated SAP HANA database.

Translations are loaded during a specific loading process and transported using Smart Data Access to the test and production systems.

Log files are written when you execute business functions.

Customer translations and project metadata are stored during the translation workflow scenarios.

SAP Translation Hub relies on the database-management system (DBMS) and the specific roles to restrict data access where necessary.

11.2 SAP Business Technology Platform

Git repositories are cloned to a temporary folder that is connected to SAP Business Technology Platform. SAP Translation Hub ensures that the data can be accessed only as a technical process within the application.

No user can access the data directly.

11.3 Customer ABAP System

After SAP Translation Hub translates the content of object lists in your on-premise ABAP system, confirmed translations are stored in the ABAP system.

The data is protected by standard SAP NetWeaver functions.

11.4 Data Protection and Privacy

Governments place legal requirements on industry to protect data and privacy. We provide features and functions to help you meet these requirements.

> ⓘ Note
>
> SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and data protection-relevant functions, such as blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws is not covered by a product feature. Furthermore, this information should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements. Definitions and other terms used in this documentation are not taken from a specific legal source.

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

This section and any other sections in this security guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

> ⚠ Caution
>
> The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

11.4.1 Glossary

The following terms are general to SAP products. Not all terms may be relevant for this SAP product.

Term	Definition
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Business purpose	The legal, contractual, or in other form justified reason for the processing of personal data to complete an end-to-end business process. The personal data used to complete the process is predefined in a purpose, which is defined by the data controller. The process must be defined before the personal data required to fulfill the purpose can be determined.

Term	Definition
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Data subject	An identified or identifiable natural person, defined in relation to applicable data protection legislation, for example, the EU GDPR.
Deletion	Deletion of **personal data** so that the data is no longer available.
End of business	Defines the end of active business and the start of residence time and retention period.
End of purpose (EoP)	End of purpose and start of blocking period. The point in time when the primary processing purpose ends, for example, a contract is fulfilled.
End of purpose (EoP) check	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization, for example, tax auditors.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"), defined in relation to applicable data protection legislation, for example, the EU GDPR.
Purpose	The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.
Residence period	The period of time between the end of business and the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Retention period	The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.

Term	Definition
Personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation. • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts
Technical and organizational measures (TOM)	Some basic requirements that support data protection and privacy are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and privacy and require appropriate TOMs, for example: • **Access control:** Authentication features • **Authorizations:** Authorization concept • **Read access logging** • **Transmission control / Communication security** • **Input control / Change logging** • **Availability control** • **Separation by purpose:** Is subject to the organizational model implemented and must be applied as part of the authorization concept.
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.

11.4.2 Read-Access Logging

SAP Translation Hub stores only the user name, user ID, and subaccount ID as part of the business requirement. Therefore tools to monitor and log read access to personal data are not applicable.

11.4.3 Personal Data Record

SAP Translation Hub stores only the user name, user ID, and subaccount ID as part of the business requirement.

There are no functions to alter user names and other data. Values are retrieved as part of SAP Business Technology Platform and SAP Business Technology Platform Identity Authentication service tools.

11.4.4 Change Log

SAP Translation Hub stores only the user name, user ID, and subaccount ID as part of the business requirement.

There are no functions to alter user names and other data. Values are retrieved as part of SAP Business Technology Platform and SAP Business Technology Platform Identity Authentication service tools.

11.4.5 User Consent

SAP Translation Hub stores only the user name, user ID, and subaccount ID as part of the business requirement. No explicit consent is required as this is part of account creation.

There are no functions to alter user names and other data. Values are retrieved as part of SAP Business Technology Platform and SAP Business Technology Platform Identity Authentication service tools.

11.4.6 Translation of Personal Data

SAP Translation Hub is strictly not intended for translating personal data.

> ⓘ Note
>
> If you translate personal data intentionally, SAP is not responsible for any activities related to this matter and there is no read-access logging.

11.4.7 Deletion of Personal Data

Use

SAP Translation Hub processes following personal data such as `user name`, `email ID`, and `subaccount ID` that is subject to the data protection laws applicable in specific countries.

As a legal basis, SAP Translation Hub has a legitimate interest to store the user name of the translation and, for technical reasons, a clone of the customer's Git repository when you translate texts stored in a Git repository. Furthermore, SAP Translation Hub acts as a service provider.

Data subjects are business customers, partners, and employees. The first and last name of the translator that changes a translation in the post-editing user interface are currently stored for future reference.

The affected IT system is the SAP Business Technology Platform account and the physical location of the data is the SAP HANA Cloud database and the temporary attached storage to SAP Business Technology Platform for the Git clones.

Relevant Processes and Available Deletion Functionality

Process	Detailed Description	Deletion Functionality	Deletion Process
Git cloning	When you translate the contents of a Git repository, SAP Translation Hub connects to the Git repository and clones the complete Git repository to a temporary folder. Although there are possibilities in Git to check out only files that match a certain file pattern, such as `.properties` files, this sparse checkout approach is not available in Eclipse for Git (EGit) or GJIT, and is not an option for SAP Translation Hub. For more information, see https://bugs.eclipse.org/bugs/show_bug.cgi?id=383772 . SAP Translation Hub must clone the complete Git repository to the local file share to get the files that need to be translated. This step includes your own customer coding and user information. Access to this file share is possible only through the SAP Translation Hub conversion service. There is no direct file access possible for SAP Translation Hub users.	Manual deletion process after 6 months.	1. You request the deletion of personal data by sending an e-mail to the SAP Translation Hub team (translation-hub@sap.com) **Note** To verify the originator of the deletion request, the SAP Translation Hub team will call the administrator of the customer account to verify the origin and legitimacy of the request. 2. SAP Translation Hub starts the manual deletion process using reasonable database queries for the relevant data centers and informs you after the data has been deleted successfully.

Process	Detailed Description	Deletion Functionality	Deletion Process
Post-editing	SAP Translation Hub stores the first and last name of the translator that manually changes a translation on the post-editing user interface.	Manual deletion process after 6 months.	1. You request the deletion of personal data by sending an e-mail to the SAP Translation Hub team (translation-hub@sap.com) **Note** To verify the originator of the deletion request, the SAP Translation Hub team will call the administrator of the customer account to verify the origin and legitimacy of the request. 2. SAP Translation Hub starts the manual deletion process using reasonable database queries for the relevant data centers and informs you after the data has been deleted successfully.

Process	Detailed Description	Deletion Functionality	Deletion Process
Integration of your own language data	You integrate your own language data in SAP Translation Hub by uploading translations and terminology to SAP Translation Hub. For administrative purposes, SAP Translation Hub stores the user ID of the user who uploads the data.	Manual deletion process after 6 months.	1. You request the deletion of personal data by sending an e-mail to the SAP Translation Hub team (translation-hub@sap.com) **Note** To verify the originator of the deletion request, the SAP Translation Hub team will call the administrator of the customer account to verify the origin and legitimacy of the request. 2. SAP Translation Hub starts the manual deletion process using reasonable database queries for the relevant data centers and informs you after the data has been deleted successfully.

12 Security for Additional Applications

The following components are used in SAP Translation Hub. Since they are all SAP components, the security information for that product applies.

- SAP HANA DB 1.0
- SAP Business Technology Platform
- SAPUI5
- SAP NetWeaver 7.4
- SAP jConnect

> → Tip
>
> You can find the security information on http://help.sap.com.

13 Dispensable Functions with Impacts on Security

Use

Only needed functions are delivered with SAP Translation Hub. Functions that are required only to train the machine translation engines have been removed from the scope to secure the application.

14 Other Security-Relevant Information

Bad HTML Formatting

In a typical translation workflow scenario, it is common to upload and translate source texts that contain HTML and XML markup. SAP Translation Hub cannot check poorly formatted HTML or XML markup.

It is the responsibility of the consumer to check that their HTML or XML markup is consistent.

15 Security-Relevant Logging and Tracing

This section describes the functions that the individual applications and components in SAP Translation Hub use to log and trace data.

15.1 SAP Business Technology Platform

SAP Translation Hub uses the built-in logging and tracing functions in SAP Business Technology Platform.

16 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 the following:

- Whether SAP Security Notes have been identified as missing on your system.
  In this case, analyze and implement the identified SAP Notes if possible. If you cannot implement the SAP 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 nondefault values.

Security Optimization Service (SOS)

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

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

This service is available as a self-service within SAP Solution Manager, as a remote service, or as an on-site service.

> → Recommendation
>
> We recommend that 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 with predefined settings, for example, from your company-specific SAP Security Policy. The validation primarily covers configuration parameters, but it also covers critical security properties like the existence of a nontrivial Gateway configuration or making sure standard users do not have default passwords.

Security in the RunSAP Methodology / Secure Operations Standard

With the end-to-end 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.

- EarlyWatch Alert
- Security Optimization Service / Security Notes Report
- Comprehensive list of Security Notes
- RunSAP Roadmap, including the Security and the Secure Operations Standard
- Early Watch Alert

Related Information

Early Watch Alert
Security Optimization Service / Security Notes Report
Comprehensive list of Security Notes
RunSAP Roadmap, including the Security and the Secure Operations Standard

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP