Security Guide | PUBLIC
2021-05-27

Generator Security Guide

SAP 3D Visual Enterprise

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

Document History - Security Guide

> ⚠ Caution
>
> Before you start the implementation, make sure that you have the latest version of the document. You can find the latest version at the following location: http://help.sap.com *SAP 3D Visual Enterprise Generator*

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

Version	Date	Description
1.00	December 20, 2013	First version
1.10	June 26, 2014	Minor updates for Service Pack
2.00	December 10, 2014	Minor updates for Service Pack
2.10	May 21, 2015	Minor updates for Service Pack
2.20	November 12, 2015	Minor updates for Service Pack
2.30	March 10, 2016	Minor updates for SP05
3.00	June 23, 2016	Major updates for version 9.0
3.10	November 24, 2016	Minor updates for version 9.0 FP01
3.20	April 27, 2017	Minor updates for version 9.0 FP02
3.30	September 07, 2017	Minor updates for version 9.0 FP03
3.40	December 15, 2017	Minor updates for version 9.0 FP04
3.50	October 25, 2018	Update for 9.0 FP06.
3.60	May 23, 2019	Update for 9.0 FP07.
3.70	October 20, 2019	Update for 9.0 FP08.
3.80	May 28, 2020	Update for 9.0 FP09.
3.90	December, 2020	Update for 9.0 FP10.
3.91	May, 2021	Update for 9.0 FP11.
3.92	November, 2021	Update for 9.0 FP12.

1 Introduction

> **i Note**
>
> This guide does not replace the administration or operation guides that are available for productive operations.

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, 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 of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP 3D Visual Enterprise Generator. To assist you in securing the SAP 3D Visual Enterprise Generator, we provide this Security Guide.

About This Document

The Security Guide provides an overview of the security-relevant information that applies to SAP 3D Visual Enterprise Generator.

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 3D Visual Enterprise Generator.
- Security Aspects of Data, Data Flow and Processes
  This section provides an overview of security aspects involved throughout the most widely-used processes within SAP 3D Visual Enterprise Generator.
- 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 3D Visual Enterprise Generator

    - Standard users that are delivered with SAP 3D Visual Enterprise Generator
    - Overview of the user synchronization strategy, if several components or products are involved
    - Overview of how integration into Single Sign-On environments is possible
- Authorizations
  This section provides an overview of the authorization concept that applies to SAP 3D Visual Enterprise Generator.
- 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 cookies.
- Network and Communication Security
  This section provides an overview of the communication paths used by SAP 3D Visual Enterprise Generator and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
- Data Storage Security
  This section provides an overview of any critical data that is used by SAP 3D Visual Enterprise Generator and the security mechanisms that apply.
- Data Protection
  This section provides information about how SAP 3D Visual Enterprise Generator protects personal or sensitive data.
- Dispensable Functions with Impacts on Security
  This section provides an overview of functions that have impacts on security and can be disabled or removed from the system.
- Enterprise Services Security
  This section provides an overview of the security aspects that apply to the enterprise services delivered with SAP 3D Visual Enterprise Generator.
- 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 occurs.

2 Before You Start

Additional Information

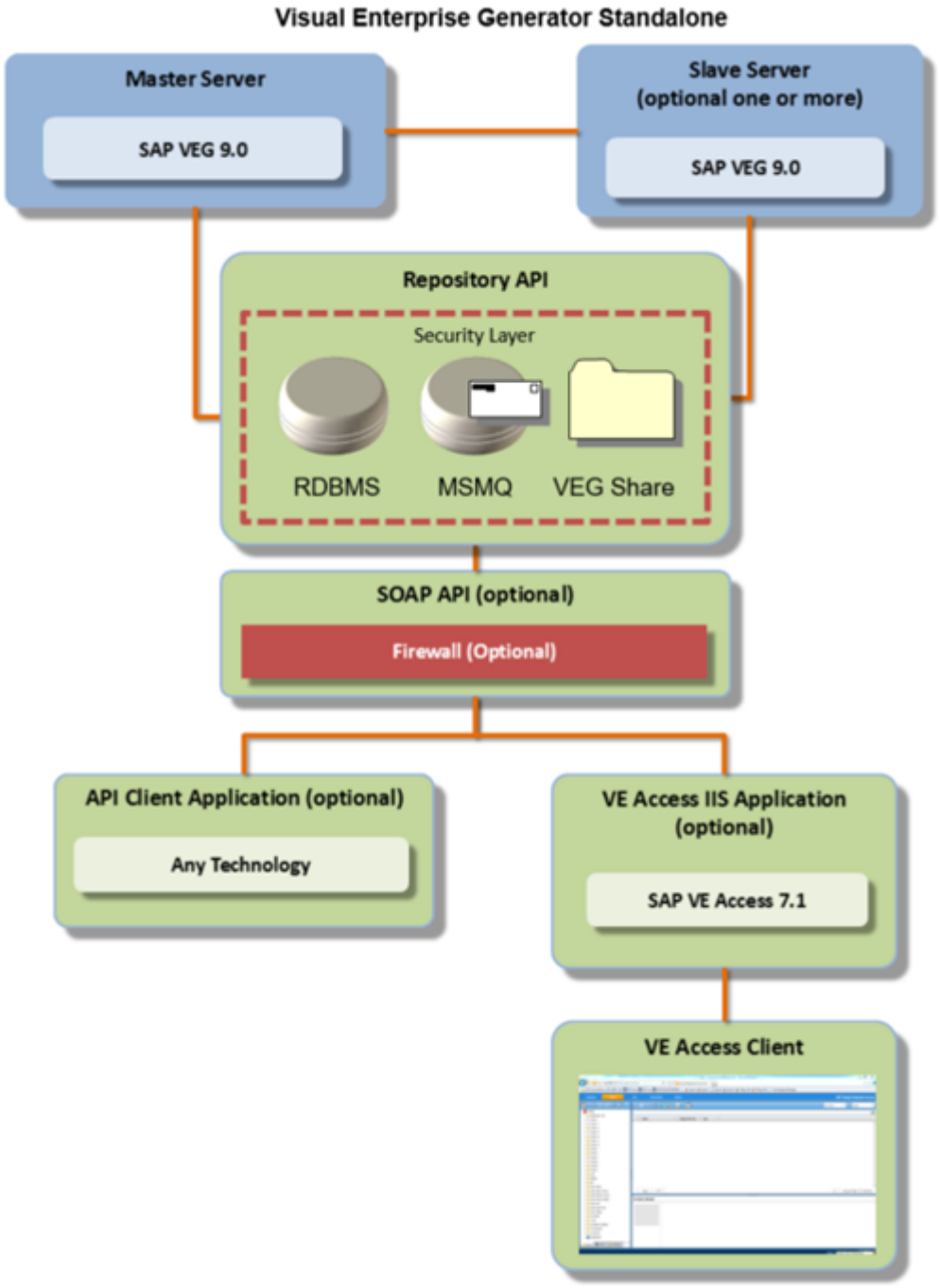
For more information about specific topics, see the Quick Links as shown in the table below.

Quick Links to Additional Information

Content	Quick Link
Security	http://sdn.sap.com/irj/sdn/security
Related SAP Notes	https://support.sap.com/notes
Released Platforms	https://www.sap.com/products.html To access the Platform Availability Matrix directly, enter http://support.sap.com/pam
SAP Solution Manager	https://support.sap.com/solutionmanager
System sizing	https://www.sap.com/about/benchmark/sizing.quick-sizer.html#quick-sizer
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver

3 Standalone Setup - System Landscape

The following is the system landscape for SAP 3D Visual Enterprise Generator with the required software units and the required business functions for a standalone configuration:



Standalone System Landscape

To install SAP 3D Visual Enterprise Generator, you need the following:

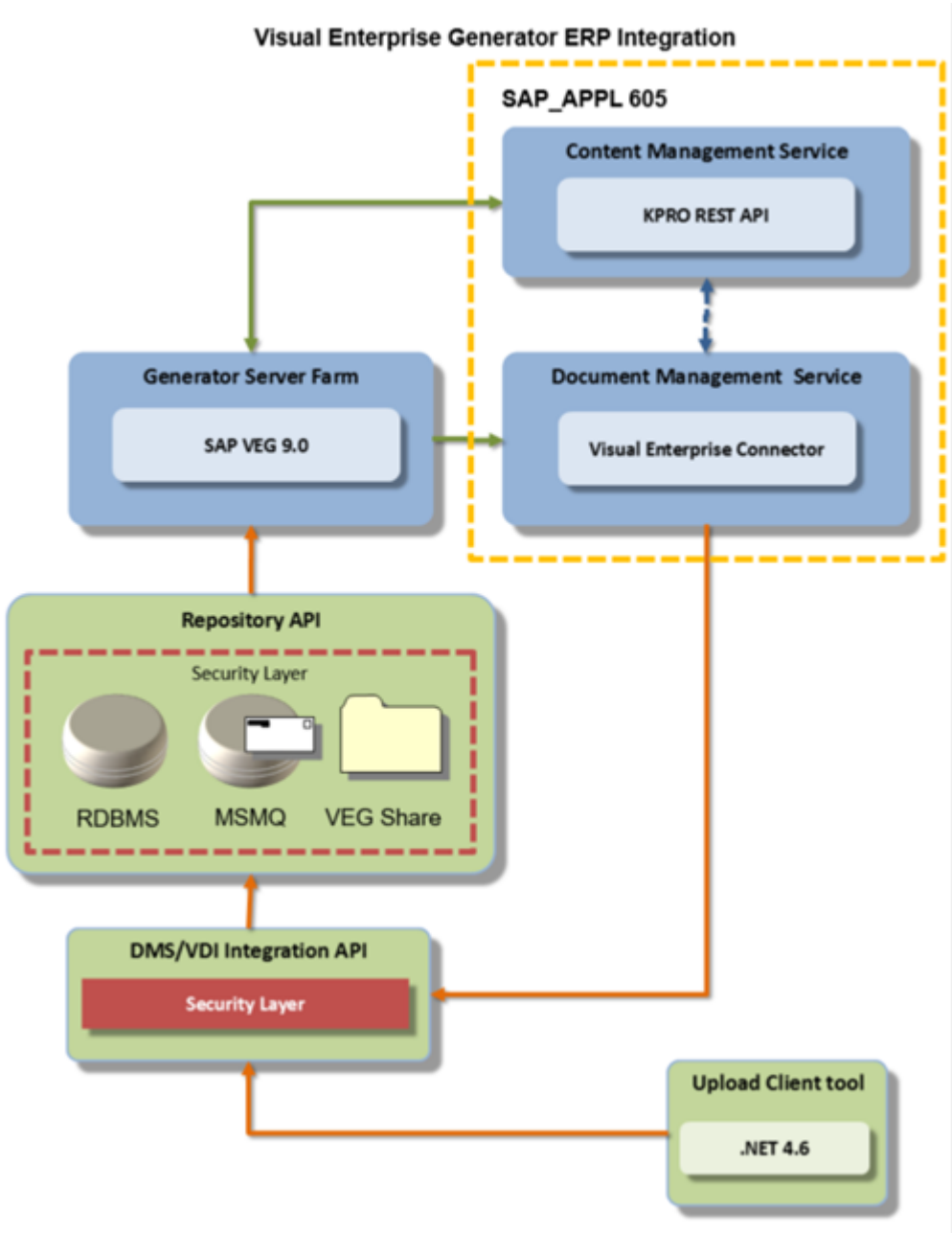
- Microsoft Windows Server 2008 R2, 2012 R2, or 2016 with
- Internet Information Server (IIS)
- Microsoft Message Queuing (MSMQ)
- Microsoft .NET Framework 4.8
- Microsoft SQL Server 2019 (recommended)

  > ⚠ Caution
  >
  > The Microsoft SQL Server instance must be configured with **Accent-Sensitive**, **Case-Insensitive Collation**, and **Mixed Mode Authentication**.

- File Sharing enabled

4 SAP ERP Integration Setup - System Landscape

The following graphic shows the system landscape for SAP 3D Visual Enterprise Generator with the required software units and the required business functions for an ERP-Integrated workflow (including the Visual Data Integration Upload Client):



ERP Integration Landscape

> ⚠ Caution
>
> The landscape depicted in the preceding graphic requires Microsoft Windows Server 2008 R2, 2012 R2, 2016, or 2019, and doesn't fully support some CAD formats. Before attempting to implement this landscape, make sure you are familiar with supported CAD formats. You can see the full list of CAD formats at SAP 3D Visual Enterprise Generator.

4.1 DMS Integration - System Landscape

To install SAP 3D Visual Enterprise Generator in an SAP DMS-integrated system landscape, you need the following:

- Microsoft Windows Server 2008 R2, 2012 R2, or 2016 with
- Internet Information Server (IIS)
- Microsoft Message Queuing (MSMQ)
- Microsoft .NET Framework 4.8
- File Sharing enabled

4.2 Visual Data Integration - System Landscape

To install SAP 3D Visual Enterprise Generator in a Visual Data Integration system landscape, you need the following:

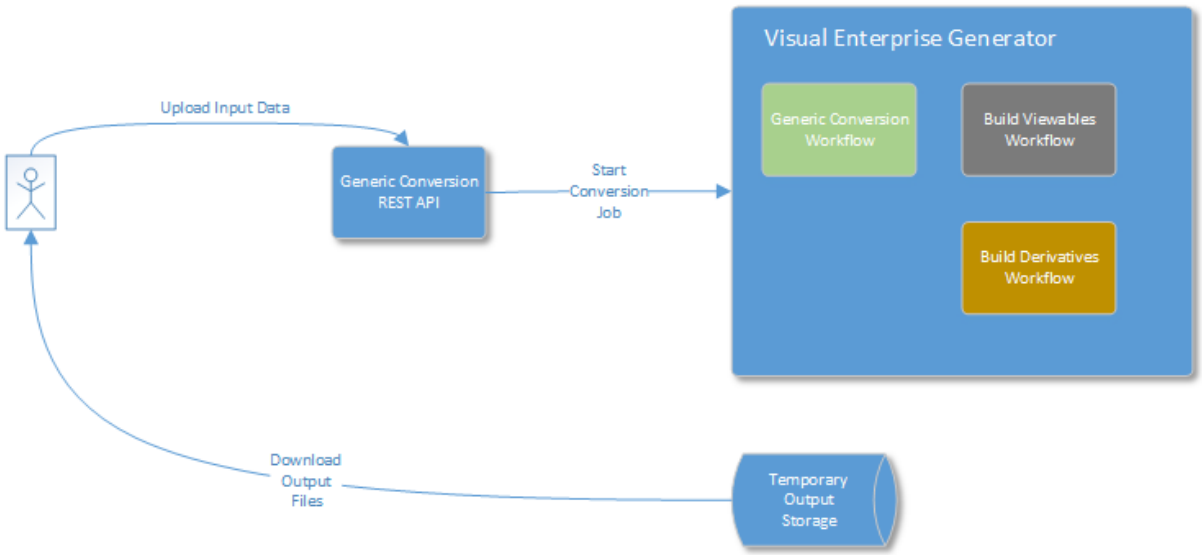
- Microsoft Windows Server 2008 R2, 2012 R2, or 2016 with
- Internet Information Server (IIS)
- Microsoft Message Queuing (MSMQ)
- Microsoft .NET Framework 4.8
- File Sharing enabled

5 System Landscape: Generic Conversion

To install SAP 3D Visual Enterprise Generator in a Generic Conversion system landscape, you need the following:

- Microsoft Windows Server 2008 R2 or 2012 R2 with
- Internet Information Server (IIS)
- Microsoft Message Queuing (MSMQ)
- Microsoft .NET Framework 4.8
- File Sharing enabled

The graphic below shows the system landscape for SAP 3D Visual Enterprise Generator for a Generic Conversion workflow.



Generic Conversion Landscape

Communication Destinations

The table below shows an overview of the communication destinations used by the SAP 3D Visual Enterprise Generator:

Communication Destinations

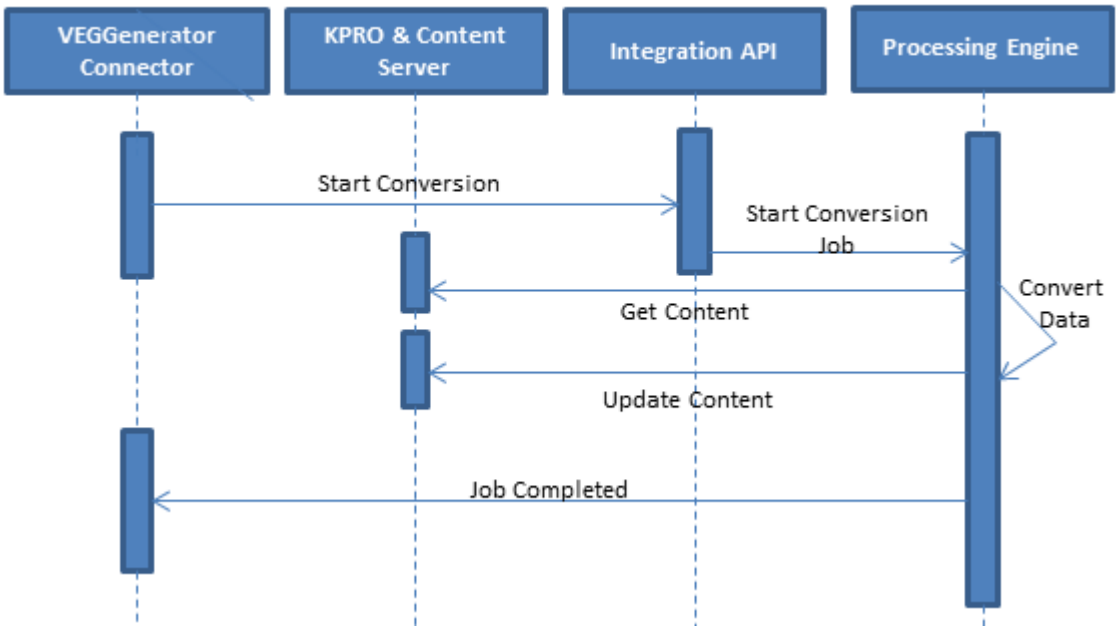
Destination	Type	User, Authorizations	Description
Processing Engine	TCP	SAP 3D Visual Enterprise Generator Processing Engine Service user	Engine to Engine Communication, File Transfer

Destination	Type	User, Authorizations	Description
Processing Engine Administration	TCP	SAP 3D Visual Enterprise Generator Administration user	Administration
WebAPI (optional, standalone mode only)	HTTP or HTTPS	Any SAP 3D Visual Enterprise Generator user	General Programming Interface
SAP Integration WebAPI (optional, Integrated mode only)	HTTP or HTTPS	Configured user, user certificate or basic or digest	Integration with SAP ERP
Generic Conversion REST API (optional)	HTTPS	Any SAP 3D Visual Enterprise Generator user – multitenancy is fully supported	General Programming Interface

6 Security Aspects of Data, Data Flow and Processes

6.1 Overview

The figure below shows an overview of the data flow for the integrated processing of SAP 3D Visual Enterprise Generator.



The table below shows the communication channels and security measures that apply in each processing step.

Step	Description	Security Measure
Documents are sent to Conversion by sending a message to Integration API.	The SAP 3D Visual Enterprise Generator Integration Web service is called to start the task or job for conversion.	Communication is secured using TLS protocol, authenticated by X.509 certificate.
Conversion job is started.	The Integration API sends a Job Start message to the Processing engine.	Integration API uses configured protocol to connect to Microsoft SQL Server database.
Content is retrieved from KPro/Content Server.	Processing engine retrieves location URLs from KPro and then downloads content from Content Server.	KPro is responsible for security aspects in this step.

Step	Description	Security Measure
Content is converted.	Processing engine saves working files in SAP 3D Visual Enterprise Generator share, uses Microsoft Message Queues for communication between processing components and stores results and reports in Microsoft SQL Server.	The share is accessed using the SMB protocol. Microsoft Message Queues are accessed using configured protocols. Microsoft SQL Server accessed using configured client/server protocols.
Content is updated in KPro/Content Server	KPro provides target URLs that are going to be used for storing the results. Converted files are uploaded to Content Server.	Communication is secured using TLS protocol, authenticated by X.509 certificate.
Job is completed.	Web service is called and job report is sent from processing engine.	Communication is secured using TLS protocol, authenticated by X.509 certificate.

> **i** Note
>
> If you do not have a web server certificate, you can use HTTP protocol instead of HTTPS for Integration API. You can use Username and Password Authentication instead of X.509 Certificate Authentication. Configuring usernames and passwords can be done in SAP 3D Visual Enterprise Generator Administrator, SAP Integration.

6.2 Integrated Mode

The communication is initiated from `SAP_APPL. SAP_BS_FND` then communicates with SAP 3D Visual Enterprise Generator to start the processing jobs. SAP 3D Visual Enterprise Generator stores the resulting files in the content server.

Step	Description	Security Measure
The documents containing CAD files that need to be converted are registered	The documents are registered in the database	N/A
The registered documents are sent for conversion to SAP 3D Visual Enterprise Generator.	A Web service from SAP 3D Visual Enterprise Generator is called to start the task/job for conversion.	Communication is secured using TLS protocol, authenticated by X.509 certificate.

Step	Description	Security Measure
For each job and for each file the location of the file is obtained.	A web service from DMS is called to get the HTTPS URLs of the file locations.	Communication is secured using TLS protocol, authenticated by X.509 certificate.
SAP 3D Visual Enterprise Generator retrieves the content of the file using the URL obtained from the previous step.	The URL provided is a rest service by which the content for the file is retrieved.	Security aspects are taken care by the KPRO.
The file is converted to the customized format by SAP 3D Visual Enterprise Generator.	New files are created after conversion using the content from the source file.	N/A
The create/update URL for the converted files is obtained.	A Web service from DMS is called to get the HTTPS URLS of the file locations.	Communication is secured using TLS protocol, authenticated by X.509 certificate.
The converted files are created/ updated in the target locations obtained in the previous step.	The URL provided is a rest service by which the content is created/updated into the target URLs.	Security aspects are taken care by KPRO.
Complete the conversion process by setting some properties and attaching the files to the document	A Web service from DMS is called to complete the process of check-in and assigning the converted files to the document.	Communication is secured using TLS protocol, authenticated by X.509 certificate
Set the status of job as complete	A Web service from SAP 3D Visual Enterprise Generator is called to set the status of the job as completed.	Communication is secured using TLS protocol, authenticated by X.509 certificate.

7 Example: Security Aspects of Data, Data Flow and Processes

The figure below shows an overview of the data flow for the CRM Web request application.

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

Step	Description	Security Measure
1	User submits PDF-, BSP- form	User types: Either dialog or Internet user with dialog user as alias
2	Import	Stateless BSP application recommended Communication protocol HTTPS
3	Convert form into XML data	XML encryption
4	One Order processing using the API CRM_ORDER_MAINTAIN	not applicable
5	Store XML data in KPRO	Customizing
6	Save data in CRM (backend COMMIT)	not applicable
7	Inform user with a confirmation page	not applicable

8 User Administration and Authentication

8.1 User Management

SAP 3D Visual Enterprise Generator has its own authentication mechanism, but can be configured to use LDAP server for authentication. For an overview of how these mechanisms apply to SAP 3D Visual Enterprise Generator, see the sections below. A list of the standard users required to operate the SAP 3D Visual Enterprise Generator is also provided.

User Administration Tools

The table below shows the tools to use for user management and user administration with SAP 3D Visual Enterprise Generator:

User Management Tools

Tool	Description	Prerequisites
SAP 3D Visual Enterprise Generator Administrator, the *Security* tab page	SAP 3D Visual Enterprise Generator application help	SAP 3D Visual Enterprise Generator installed configured and started. SAP 3D Visual Enterprise Generator Administrator user must be administrator (security administrator).

Security management with regards users is fully described in the application help for SAP 3D Visual Enterprise Generator. Here you will find information relating to:

- Permission Levels
- Asset Management
- Managing Users (creation, editing and importing)
- Creating LDAP Server Connections

The appropriate section can be found at http://help.sap.com/ *Product Lifecycle Management* > *SAP 3D Visual Enterprise* > *SAP 3D Visual Enterprise Generator* > *SAP 3D Visual Enterprise Generator 9.0* > *Application*

Help > *Working with SAP 3D Visual Enterprise Generator* > *Security Management in SAP 3D Visual Enterprise Generator* >:

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 the special user accounts used by the system.

Note that access to individual objects (projects, folders, assets) is controlled using Access Control Lists (ACLs) and may differ from object to object.

SAP 3D Visual Enterprise Generator has a number of users that are required by the system.

SAP 3D Visual Enterprise Generator also supports a set of roles for user accounts to be used by end users. These roles are described in the section

The following user types are able to log on for SAP 3D Visual Enterprise Generator:

User Type	Description
Security administrator	The only user initially available in the system that is not a system user. This user can create other users, groups and projects, as well as configuring LDAP Server. This user also assigns users to groups and groups to projects.
Administration users	Administration users have full access to the system and have full access to SAP 3D Visual Enterprise Generator Administration program
User group users	User group users have access to assets (search and browse), derivatives (create and edit), personal dashboard, jobs and reports.
Auditing users	Auditing users have read-only access to parts of the assets (search and browse), as well as the *Jobs* page.
Support users	Support users have read-only access to parts of the assets (search and browse), as well as the *Jobs* page.
Service users	Used for running processing engine and Web APIs
Communication users	Used for integrated installation to communicate with SAP ERP system

- Individual users:
  Security Administrator is the only user initially available in the system that is not a system user. This user can create other users, groups and projects, as well as configuring LDAP Server. This user also assigns users to groups and groups to projects.
  Administration users have full access to the system and have full access to SAP 3D Visual Enterprise Generator Administration program.

User group users have access to assets (search & browse), derivatives (create & edit), personal dashboard, jobs and reports.
Auditing users have read-only access to parts of the Assets (search & browse), as well jobs page.
Support users have read-only access to parts of the Assets (search & browse), as well jobs page.

- Technical users:
  Service users are used for running processing engine and Web APIs.
  Communication users are used for integrated installation to communicate with SAP ERP system.

Required Users

The table below describes the special users that are required by SAP 3D Visual Enterprise Generator:

System	User ID	Password	Description
Microsoft Windows	`VEGRunner`	Customer specified	Used by: • SAP 3D Visual Enterprise Generator Windows Service • IIS Application Pool for the Web APIs
Microsoft SQL Server	`deepserver`	Customer specified	Account used by VEG engine to connect to SQL Server
SAP 3D Visual Enterprise Generator	`deepserver`	System controlled	• This is a special user account used by the VEG engine only. • It is not possible for a user to log onto VEG using this account. • This user is not visible in the Administration tool.
SAP 3D Visual Enterprise Generator	`SecurityAdministrator`	Customer specified	• This is the only account created during the installation that can be used to log onto the VEG Administration tool. • This account is used for security administration (for example, creating user accounts).

You need to create the `VEGRunner` user before starting the installation. Use a domain account if you are creating a SAP 3D Visual Enterprise Generator farm or if you intend to expand to using a server farm in the future, otherwise you can use a local account.

The `VEGRunner` user needs the following Microsoft Windows-based user rights:

- Logon as service
- Logon as batch job

These rights can be assigned using Domain or Local Security Policy. See Microsoft Windows Administration guide for more information.

The Microsoft SQL Server `deepserver` account can be created before installing SAP 3D Visual Enterprise Generator or you can let the configuration program create it for you.

The SAP 3D Visual Enterprise Generator `deepserver` account password is stored encrypted in the `farm.config` file in the SAP 3D Visual Enterprise Generator share.

User Logging

User login attempts are audited in the standard `VE Generator` log. For more information, see the section Security-Relevant Logging and Tracing [page 36]

8.2 User Data Synchronization

SAP 3D Visual Enterprise Generator can be configured to authenticate users using an LDAP server.

Once LDAP Authentication is setup, the following user data will be imported to SAP 3D Visual Enterprise Generator:

- Full name
- E-mail

Every time user tries to authenticate in SAP 3D Visual Enterprise Generator, the system will forward the authentication request to the configured LDAP server.

8.3 Integration Into Single Sign-On Environments

If SAP 3D Visual Enterprise Generator is installed in Integrated mode, it can be configured to use client certificates for mutual authentication with the SAP ERP system.

SAP 3D Visual Enterprise Generator can support 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 [SAP Library] also apply to the SAP 3D Visual Enterprise Generator.

For more information about the available authentication mechanisms, see User Authentication and Single Sign-On in the SAP NetWeaver Library.

9 Authorizations

SAP 3D Visual Enterprise Generator uses Microsoft Windows ACLs to control access to SAP 3D Visual Enterprise Generator share and SAP 3D Visual Enterprise Generator ACLs to control access to the objects inside SAP 3D Visual Enterprise Generator database.

The SAP 3D Visual Enterprise Generator Administration program must be launched using a Microsoft Windows user with write access to the SAP 3D Visual Enterprise Generator share.

Additionally the SAP 3D Visual Enterprise Generator Administration program applies authorization rules according the role of the authenticated SAP 3D Visual Enterprise Generator user.

Role and Authorization Concept for SAP 3D Visual Enterprise Generator

The following two sections describe the role types used by SAP 3D Visual Enterprise Generator.

Standard Roles

The table below shows the standard roles that are used by SAP 3D Visual Enterprise Generator:

Standard Roles

Role	Description
Administration	Full access granted
Security Administration	System Administration
Users	Asset search *Browse* page Create or edit derivatives *Dashboard* page *Jobs* page *Reports* page
Auditing	Asset search *Browse* page *Jobs* page

Role	Description
Support	Asset search *Browse* page *Jobs* page

SAP 3D Visual Enterprise Generator Administrative Users

By default, the `SecurityAdministrator` user can perform both security administration and project administration.

The administrator can specify whether separate users are required for these tasks during configuration when the SAP 3D Visual Enterprise Generator database is created.

Standard Permissions

The table below shows the security-relevant authorization objects that are used by SAP 3D Visual Enterprise Generator:

Authorization Object	Permission	Description
SAP 3D Visual Enterprise Generator Administrator	System Administration	Can do the following: • Monitor server operations: jobs, tasks, server in the farm, alerts • Configure server: Create or modify workflows, processes, derivative types, derivative groups, metadata categories, behavior of some metadata fields, pick lists, file types, hot folders and scheduled activities • Create and modify users, groups, projects, LDAP integration
SAP Visual Enterprise Access	Asset search	*Subscriptions* list page
	Browse page	Can use *Browse* page
	Checked out assets page	Can view checkouts from all users and undo their checkouts
	Create or edit derivatives	Can create and modify existing derivatives

Authorization Object	Permission	Description
	Dashboard page	Can view personalized *Dashboard* page
	Jobs page	Can view jobs in the system
	Reports page	Can view reports in the system
	Subscriptions list page	Can view subscriptions in the system

Standard Authorization Objects

SAP 3D Visual Enterprise Generator ACLs

SAP 3D Visual Enterprise Generator uses Access Control Lists to secure access to folders and assets inside SAP 3D Visual Enterprise Generator projects.

Access Control Lists consist of Access Control Entries, which are mapping of user groups to access rights. Access rights can be granted or not granted. Effective user rights are union of all access rights granted to all user groups user is a member of.

The table below shows the security-relevant access rights that are used by SAP 3D Visual Enterprise Generator and objects they apply to:

Authorization Object	Field	Description
Folder/Asset	Grant	Allows changing Access Control Lists of an object
Asset	Read Asset	Allows reading of asset, versions, instances, metadata, derivatives, and notes Users not having this right will not be able to see this asset in the system
	Update Asset	Allows updating asset: creating a new version, editing metadata, creating/editing derivatives, changing notes
	Delete Asset	Allows deleting asset, derivatives
	Download Original Asset	Allows downloading of original file (if stored)
Folder	Create	Allows creation of subfolders and uploading of assets

Authorization Object	Field	Description
	Read Folder	Allows viewing content of the folder Users not having this right can still search for the assets in the folder that they have *Read Access* right to.
	Update Folder	Allows editing of folder name/description
	Delete Folder	Allows deleting of the folder

SAP 3D Visual Enterprise Generator Object Ownership

In SAP 3D Visual Enterprise Generator, each object has a single user that is the object owner. By default, owner can do the following:

- Transfer ownership to any other user
- Owner can always delete folders/assets he owns

The administrator can specify whether these permissions are granted to object owners during configuration when the SAP 3D Visual Enterprise Generator database is created.

SAP DMS Authorization Objects

The table below shows the standard authorization objects that are already created by DMS. The authorizations are reused in integration of DMS with SAP 3D Visual Enterprise Generator. To see authorization objects, use transaction **SU21**.

Authorization Object	Field	Value	Description
C_DRAW_TCD	ACTVT	03	Display authorization for document activities
C_DRAW_DOK	ACTVT	52	Change application start authorization for document access

10 Session Security Protection

We highly recommend using SSL to protect the network communications.

Session Security Protection on the AS ABAP

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

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

Session Security Protection on the AS Java

On the AS Java, set the HTTP Provider properties as described in *Session Security Protection* [SAP Library].

11 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system level and application level) or network attacks such as eavesdropping.

11.1 Communication Channel Security

The table below shows the communication channels used by SAP 3D Visual Enterprise Generator, the protocol used for the connection, and the type of data transferred:

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Processing Engine to Microsoft SQL Server (standalone mode only)	This is configured by Microsoft SQL Server Administrator	All application data	
Processing Engine to Share	SMB	Workspace containing users' models	User's models are stored in here temporarily, process definitions, encrypted passwords
Processing Engine to another Processing Engine	Encrypted TCP	Processing Engine Communication	
Administration program to Processing Engine	Encrypted TCP	Administration data	Passwords being set for users and for third-party services
Web API to Processing Engine	Encrypted TCP	Processing information	
SAP ERP to Integration API	HTTP or HTTPS	Username/password for authentication (if certificate not configured) and Model Data	Username/password if used and model data

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*.

Configuring SSL in IIS

By default, SAP 3D Visual Enterprise Generator will try to configure SSL for WinAPI or IntegrationAPI.

To use SSL you will need to configure server SSL certificate using Microsoft Internet Information Server (IIS) Manager as follows:

1. Open the site you will use to install SAP 3D Visual Enterprise Generator and select the *Bindings* action.
2. Check that the https binding for the selected site exists. If there is none, add it using the *Add* button.
3. Select https as a type and select SSL certificate to use
   - You can generate server certificate from local certification authority or order one from internet certification authorities.
     Note that when connecting to HTTPS endpoint, you will need to use DNS name as specified in SSL certificate.

11.2 Network Security

Ports

SAP 3D Visual Enterprise Generator uses the following TCP ports:

- 8085
- 8086
- 8087
- 8090
- 8091
- 8099 (lock manager)
- 8433 (integrated mode database server)

11.3 Communication Destinations

The table below shows an overview of the communication destinations used by SAP 3D Visual Enterprise Generator:

Destination	Type	User, Authorizations	Description
Processing Engine	TCP	SAP 3D Visual Enterprise Generator Processing Engine Service user	Engine to Engine Communication, File Transfer
Processing Engine Administration	TCP	SAP 3D Visual Enterprise Generator Administration user	Administration
WebAPI (optional, standalone mode only)	HTTP/HTTPS	Any SAP 3D Visual Enterprise Generator user	General Programming Interface
SAP Integration WebAPI (optional, Integrated mode only)	HTTP/HTTPS	Configured user, user certificate or basic or digest	Integration with SAP ERP
Generic Conversion REST API	HTTPS	Any SAP 3D Visual Enterprise user	General Programming Interface

12 Data Storage Security

Data Storage

Database

SAP 3D Visual Enterprise Generator stores user data inside a Microsoft SQL database.

In Integrated mode, a self-managed database is used for configuration and job management.

KPRO/DMS

When SAP 3D Visual Enterprise Generator is integrated with an SAP ERP system, generated and original files are stored in the HTTP content server. The content server is provided by SAP for storing files checked in from DMS. The security aspects for this are managed by KPRO.

Share

SAP 3D Visual Enterprise Generator share access should not be granted to anyone except SAP 3D Visual Enterprise Generator Service user account and administrators.

The SAP 3D Visual Enterprise Generator share stores the following:

- Configuration data for Processing Engine components, including encrypted passwords for Microsoft SQL Server account, SAP 3D Visual Enterprise Generator internal system account (deepserver)
- Processing Engine scripts (process definitions, operations and notifications) as well as job-in progress data
- Some user data, while being processed, is stored inside share's working folder

All SAP 3D Visual Enterprise Generator components need write access to SAP 3D Visual Enterprise Generator share.

Users who want to author or modify processes using SAP 3D Visual Enterprise Generator Administration program, need write access to SAP 3D Visual Enterprise Generator share.

Program Data

Inside the `%PROGRAMDATA%\SAP\Visual Enterprise Generator` folder, we store the following data:

- Log files
- Trace files (if configured)
- Local processing engine task data (temporary)

Inside the `%ProgramData%\SAP\Visual Enterprise Generator Configurator` folder, we store the following data:

- Configuration log files
- Configuration audit trail file
- Current SAP 3D Visual Enterprise Generator configuration with encrypted passwords
- Pending SAP 3D Visual Enterprise Generator configuration (if exists) with encrypted passwords

Configuration File

Inside the installed application folder, we store DeepServer.config file which contains the following:

- Path to the SAP 3D Visual Enterprise Generator share
- Prefix used to address MSMQs that processing engine is using (optional)

Data Protection

Database

The database should be accessible only by `deepserver` SQL account, and by the database administrator.

By default, the `deepserver` account is given minimum privileges needed to operate the database.

Personal data stored includes the following:

- Usernames
- Full names
- E-mails (optional)
- Password hashes
- User data stored includes the following:
  - Assets the user has stored in the system
  - Metadata extracted or added to those assets

The SAP 3D Visual Enterprise Generator Administration program allows you to create and delete user accounts as well as to create and delete projects that store users' assets.

Deleting a user account does not delete any of user's assets.

Share

Access to the share is given to the account used for the SAP 3D Visual Enterprise Generator Windows service and the Microsoft Windows account that was used to run the SAP 3D Visual Enterprise Generator Configurator tool when the share was created.

Write access to the share should be given to any additional users that might be authoring SAP 3D Visual Enterprise Generator processes.

No one else must have any access to SAP 3D Visual Enterprise Generator share.

Since the share contains executable code (SAP 3D Visual Enterprise Generator process scripts and operations), any user granted write access to this location has the ability to execute arbitrary code and operations in the context of the SAP 3D Visual Enterprise Generator service account.

The SAP 3D Visual Enterprise Generator share is also used to store working folders while processing. In the default configuration, all working data is deleted once a processing job has completed.

If the SAP 3D Visual Enterprise Generator share is not created before the first configuration, one will be automatically created in `%ProgramData%\SAP\Visual Enterprise Generator\VEGShare` during the configuration process.

Program Data

Program Data access is given to the SAP 3D Visual Enterprise Generator's service account and older data is deleted after configurable amount of time.

13 Security for Additional Applications

SAP 3D Visual Enterprise Generator uses the following third party application:

- Microsoft SQL Server

SAP 3D Visual Enterprise Generator uses the following Windows components:

- File Sharing
- Microsoft Message Queuing
- Internet Information Server
- Windows Certificate Store and CryptoAPI

SAP 3D Visual Enterprise Generator can be integrated with:

- SAP ERP

14 Dispensable Functions with Impacts on Security

File Referencing

File referencing can be used with few SAP 3D Visual Enterprise Generator workflows. This setting is turned off by default.

Using file referencing allows users to upload files from network shares without the need to read and compress all of the data upfront, allowing for faster file uploads.

This feature has the potential to create a security issue, whereby a user executing these workflows can instruct the process to read any file that the SAP 3D Visual Enterprise Generator service account has access to, including folders and files on the server.

This requires that service account under which SAP 3D Visual Enterprise Generator runs has at least read-only access to those shares.

If you choose to enable and use file referencing make sure that service account for SAP 3D Visual Enterprise Generator has only access to the areas that should be visible to users that can be using workflows that use file referencing.

File Referencing for Standalone Assembly and Standalone Asset

SAP 3D Visual Enterprise Generator workflows for assembly and asset upload have the *Allow file referencing* setting set to *False* by default.

PLM Workflows

Default configuration of SAP 3D Visual Enterprise Generator ships with disabled PLM Workflows (Default Translation, Default Replace Parts). These workflows are disabled because the file referencing feature is essential to their operation.

Hot Folders

Configuring SAP 3D Visual Enterprise Generator for hot folder processing allows any user with write access to the file system location being monitored to upload or modify data in SAP 3D Visual Enterprise Generator.

Hot folder processing is a very common way to submit data for processing with SAP 3D Visual Enterprise Generator and is an easy integration point.

> **i Note**
>
> Ensure that hot folders can be written only to Microsoft Windows accounts that should have ability to upload and modify data inside SAP 3D Visual Enterprise Generator.

Enterprise Services Security

For SAP 3D Visual Enterprise Generator-specific enterprise security issues, note the following:

- SAP 3D Visual Enterprise Generator can be installed with SAP 3D Visual Enterprise Generator Web API and Generic Conversion REST API in standalone mode or it will be installed with Integration API and Generic Conversion REST API in integrated mode. APIs will install with HTTPS by default (if the server has a Web server certificate).
- Make sure that APIs are additionally secured using Microsoft Internet Information Services Manager and available only to users, computers, and networks where these APIs are going to be used.

If you are installing any APIs on a public Web server, make sure that the root of your Web site contains a `robots.txt` file.

Example `robots.txt` file:

```
User-agent: *Disallow: /
```

15 Services for Security Lifecycle Management

Use

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 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 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 SAP Solution Manager, as a remote service, or as an 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 with 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 more information about these services, see:

- EarlyWatch Alert: https://support.sap.com/en/offerings-programs/support-services/earlywatch-alert.html
- Security Optimization Service / Security Notes Report: https://support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html
- Comprehensive list of Security Notes: http://support.sap.com/securitynotes
- RunSAP Roadmap, including the Security and the Secure Operations Standard: https://support.sap.com/support-programs-services/methodologies/implement-sap.html (See the RunSAP chapters 2.6.3, 3.6.3 and 5.6.3)

16 Security-Relevant Logging and Tracing

SAP 3D Visual Enterprise Generator Logging

By default, SAP 3D Visual Enterprise Generator logs to the file system, Microsoft Windows's event logs and the SQL Server database.

The logging level can be configured using the SAP 3D Visual Enterprise Generator Configuration program.

Location of Log and Trace Files

Log and trace files are stored under the `%PROGRAMDATA%\SAP\Visual Enterprise Generator` folder.

Log files have a `.log` file extension and trace files have a `.trace` extension.

Older log and trace files are periodically deleted. By default, log and trace files older than 14 days are deleted.

To change this value, use the SAP 3D Visual Enterprise Generator configuration application.

Microsoft Windows Event Logs

SAP 3D Visual Enterprise Generator uses the following Microsoft Windows event logs:

Event Log	Events Logged
VE Configuration	Actions taken using SAP 3D Visual Enterprise Generator Configuration program
VE Generator	Events from all other SAP 3D Visual Enterprise Generator components

You can use the Microsoft Windows Event Viewer to clear these logs or change their behavior.

Database Logs

The SAP 3D Visual Enterprise Generator log for individual tasks (instances of processes) is stored in the `DS_LogMessage` table, which is cleared periodically. Include any reference information that is appropriate to include as an appendix, for examples, summarized lists of security-transactions or reports, or checklists.

Security Logs

Any changes to personal data are logged to the Windows Event Log under the category **Applications** by default. The log stores the name of the user who changed the data, the date of the change, and the attribute of personal data to which it refers. Logging can be disabled by setting to `0` a `DWORD` value in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SAP\SAP 3D Visual Enterprise\VEGSecurityAudit`:

Value	Description
`LogFullNameChange`	Controls logging full name changes

Value	Description
`LogEmailChange`	Controls logging e-mail changes
`LogPasswordChange`	Controls logging password changes
`LogERPUserNameChange`	Controls ERP User Name changes
`LogERPUserPasswordChange`	Controls ERP Password changes

A Reference

The Main SAP Document Types

The following is an overview of the most important documentation types that you need in the various phases in the life cycle of SAP software.

Cross-Phase Documentation

SAPterm is SAP's terminology database. It contains SAP-specific vocabulary in over 30 languages, as well as many glossary entries in English and German

- Target group:
  - Relevant for all target groups
- Current version:
  - On SAP Help Portal at *http://help.sap.com* > *Glossary*
  - In the SAP system in transaction `STERM`

SAP Library is a collection of documentation for SAP software covering functions and processes.

- Target group:
  - Consultants
  - System administrators
  - Project teams for implementations or upgrades
- Current version:
- - On SAP Help Portal at http://help.sap.com (also available as documentation DVD)

The **security guide** describes the settings for a medium security level and offers suggestions for raising security levels. A collective security guide is available for SAP NetWeaver. This document contains general guidelines and suggestions. SAP applications have a security guide of their own.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Help Portal at http://help.sap.com > *[Product Name]* > *[Version Number]*

Implementation

The **master guide** is the starting point for implementing an SAP solution. It lists the required installable units for each business or IT scenario. It provides scenario-specific descriptions of preparation, execution, and follow-up of an implementation. It also provides references to other documents, such as installation guides, the technical infrastructure guide and SAP Notes

- Target group:
  - Technology consultants

    - Project teams for implementations
- Current version:
    - On SAP Help Portal at http://help.sap.com *[Product Name]* *[Version Number]*

The **Installation guide** describes the technical implementation of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration

- Target group:
    - Technology consultants
    - Project teams for implementations
- Current version:
    - On SAP Help Portal at http://help.sap.com *[Product Name]* *[Version Number]*

Configuration Documentation in SAP Solution Manager – SAP Solution Manager is a life-cycle platform. One of its main functions is the configuration of business scenarios, business processes, and implementable steps. It contains Customizing activities, transactions, and so on, as well as documentation

- Target group:
    - Technology consultants
    - Solution consultants
    - Project teams for implementations
- Current version:
    - In SAP Solution Manager

The **Implementation Guide (IMG)** is a tool for configuring (Customizing) a single SAP system. The Customizing activities and their documentation are structured from a functional perspective. (In order to configure a whole system landscape from a process-oriented perspective, SAP Solution Manager, which refers to the relevant Customizing activities in the individual SAP systems, is used.)

- Target group:
    - Solution consultants
    - Project teams for implementations or upgrades
- Current version:
    - In the SAP menu of the SAP system under *Tools* *Customizing* *IMG*

Production Operation

The **technical operations manual** is the starting point for operating a system that runs on SAP NetWeaver, and precedes the application operations guides of SAP Business Suite. The manual refers users to the tools and documentation that are needed to carry out various tasks, such as monitoring, backup/restore, master data maintenance, transports, and tests.

- Target group:
    - System administrators
- Current version:
    - On SAP Help Portal at http://help.sap.com *[Product Name]* *[Version Number]*

The **application operations guide** is used for operating an SAP application once all tasks in the technical operations manual have been completed. It refers users to the tools and documentation that are needed to carry out the various operations-related tasks.

- Target group:
  - System administrators
  - Technology consultants
  - Solution consultants
- Current version:
  - On SAP Help Portal at http://help.sap.com ▸ *[Product Name]* ▸ *[Version Number]* ▸

Upgrade

The **upgrade master guide** is the starting point for upgrading the business scenarios and processes of an SAP solution. It provides scenario-specific descriptions of preparation, execution, and follow-up of an upgrade. It also refers to other documents, such as upgrade guides and SAP Notes

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Help Portal at http://help.sap.com ▸ *[Product Name]* ▸ *[Version Number]* ▸

The **upgrade guide** describes the technical upgrade of an installable unit, taking into account the combinations of operating systems and databases. It does not describe any business-related configuration.

- Target group:
  - Technology consultants
  - Project teams for upgrades
- Current version:
  - On SAP Help Portal at http://help.sap.com ▸ *[Product Name]* ▸ *[Version Number]* ▸

Release notes are documents that contain short descriptions of new features in a particular release or changes to existing features since the previous release. Release notes about ABAP developments are the technical prerequisite for generating delta and upgrade Customizing in the Implementation Guide (IMG).

- Target group:
  - Consultants
  - Project teams for upgrades
- Current version:
  - On SAP Help Portal at http://help.sap.com ▸ *[Product Name]* ▸ *[Version Number]* ▸
  - In the SAP menu of the SAP system under ▸ *Help* ▸ *Release Notes* ▸ (only ABAP developments).

Typographic Conventions

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

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 a 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

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

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

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

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

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 https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP