

PUBLIC
SAP Single Sign-On
Document Version: 1.1 – 2020-03-17

Secure Login for SAP Single Sign-On 3.0 - Sizing Guide

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Introduction. . . . 3
1.1 Functions of SAP Single Sign-On. . . . 3
1.2 System Overview. . . . 4
1.3 Conclusion. . . . 5
1.4 Factors That Influence Performance. . . . 5

2 Sizing Fundamentals and Terminology. . . . 7

3 Initial Sizing for SAP Single Sign-On. . . . 9
3.1 Minimum Hardware Requirements for SAP Single Sign-On. . . . 9
CPU Load. . . . 10
Disk Space. . . . 10
RAM. . . . 11
3.2 Sizing Guideline for the Creation of User Certificates. . . . 11
Secure Login Server with Secure Login Client and Secure Login Web Client. . . . 11
3.3 Conclusion. . . . 13

4 Appendix. . . . 14
4.1 Testing Conditions. . . . 14
4.2 Results for Secure Login Server. . . . 15
CPU Load. . . . 15
4.3 Results for the Secure Login Client and Secure Login Web Client. . . . 15
RAM. . . . 16
Disk Space for Secure Login Client. . . . 16
Disk Space for Secure Login Java Applet Web Client. . . . 16
Conclusion. . . . 16

5 Comments and Feedback. . . . 17

1 Introduction

This document provides initial sizing information for the SAP Single Sign-On. Precise recommendations for each customer will be determined on a case-by-case basis for each customer's specific requirements. The SAP sales/support team, your internal IT department, and your hardware vendor can help to define the best configuration for your environment.

> **i** Note
>
> The calculations in this document should be regarded as guidelines based on assumed average usage. If the end results seem unrealistic, contact SAP for further guidelines.

1.1 Functions of SAP Single Sign-On

Secure Login is an innovative software solution created specifically to improve user and IT productivity and to protect business-critical data in SAP business solutions through secure single sign-on to the SAP environment.

Secure Login provides strong encryption, secure communication, and single sign-on between a wide variety of SAP components.

Examples:

- SAP GUI and SAP NetWeaver platform with Secure Network Communications (SNC)
- Web GUI and SAP NetWeaver platform with Secure Socket Layer – SSL (HTTPS)
- Third party application server supporting X.509 certificates

In a default SAP setup, users enter their SAP user name and password into the SAP GUI logon screen. SAP user names and passwords are transferred through the network without encryption. To secure networks, SAP provides a Secure Network Communications interface (SNC) that enables users to log on to SAP systems without entering a user name or password. The SNC interface can also direct calls through the Secure Login Library to encrypt all communication between the SAP GUI and the SAP server, thus providing secure single sign-on to SAP.

Secure Login allows you to benefit from the advantages of SNC without being forced to set up a Public Key Infrastructure (PKI). Secure Login allows users to authenticate with one of the following authentication mechanisms:

- Microsoft Windows domain (Active Directory Server)
- RADIUS server
- LDAP server
- RSA SecurID token
- SAP NetWeaver server
- Smart Card authentication
- Authentication at kiosk PCs using RFID tokens

If a PKI has already been set up, the digital user certificates of the PKI can also be used by Secure Login.

Secure Login also provides single sign-on for Web browser access to the SAP Enterprise Portal (and other HTTPS-enabled Web applications) with SSL.

1.2 System Overview

Secure Login is a client/server software system integrated with SAP software to make single sign-on, alternative user authentication, and enhanced security easy for distributed SAP environments. The Secure Login solution includes the following components:

- Secure Login Server
  Central service that provides X.509v3 certificates (out-of-the-box PKI) to users and application servers. The Secure Login Web Client is an additional function. Secure Login Server also provides fast RFID identification for users of kiosk PCs on the shop floor.
- Secure Login Library
  Crypto library for the AS ABAP system. Secure Login Library supports both X.509 and Kerberos technology.
- Secure Login Client
  Client application that provides security tokens (Kerberos and X.509 technology) for a variety of applications.

You do not necessarily need to install all components. This depends on the use case. For further information about Secure Login Client and Secure Login Library see the corresponding Installation, Configuration and Administration Guide.

The Secure Login Client is split into the following variants:

Secure Login Client

Secure Login Client can either be used with an existing public key infrastructure (PKI) or together with the Secure Login Server. You can use it for certificate-based authentication without being obliged to set up a PKI.

The stand-alone Secure Login Client can use the following authentication methods:

- Smart Cards and USB tokens with an existing PKI certificate
  Secure Login Server and Authentication Server are not necessary.
- Microsoft Crypto Store with an existing PKI certificate
  Secure Login Server and Authentication Server are not necessary.
- Microsoft Windows credentials

The Microsoft Windows domain credentials (Kerberos token) can be used for authentication. The Microsoft Windows credentials can also be used to receive a user X.509 certificate with Secure Login Server.

- User name and password (several authentication mechanisms)
  The Secure Login Client prompts the user for a user name and a password and uses these credentials for authentication at the Secure Login Server to receive an X.509 certificate for the user.

All of these authentication methods can be used in parallel. A policy server provides authentication profiles that specify how to log on to the desired SAP system.

Secure Login Web Client (Java Applet Web Client)

This client is based on a Web browser (Web GUI) and is part of the Secure Login Server. The Secure Login Web Client has the same authentication methods as the standalone Secure Login Client, but with the following limited functions:

- Limited integration with the client environment (interaction required)
- Limited client policy configuration

Secure Login Web Client (JavaScript Web Client)

With SAP Single Sign-On 3.0 the JavaScript Web Client was introduced. In contrast to the Java Applet based Secure Login Web Client, the JavaScript Web Client requires a full Secure Login Client installation, hence Disk and RAM consumption are the same as for the Secure Login Client.

1.3 Conclusion

Key capabilities of SAP Single Sign-On:

- Single sign-on for SAP GUI for Windows, SAP GUI for Java, Web applications
- Integration capabilities (Microsoft Active Directory Server; Microsoft Certificate Store)
- SNC Client Encryption: Strong encryption of communication channels between client and SAP application server
- Single sign-on for legacy systems
- Support of additional authentication methods (RADIUS, smart cards)
- The one-time password solution in SAP Single Sign-On enables strong authentication for access to corporate resources, for example, using time-based passcodes.

1.4 Factors That Influence Performance

The main influencing factors for performance are the following:

- Size of the user CA keys
- CPU power of your server
- Using SSL to protect the communication

- Type of CA
- Login module used

The following minor influencing factors have an effect on the time needed for the creation of certificates.

- Performance of the remote back end, for example an authentication server, and network bandwidth to the back end
- Bandwidth of the network connection in general

The main task of SAP Single Sign-On is creating user certificates when users log on to a system either with the Secure Login Web Client or with a Microsoft Windows client. The performance-intensive transaction is the signing by the CA. The key length of the user CA private keys may vary. It can be, for example, 2048 or 4096 bits. The kind of CA (internal or based on a hardware security module) also influences the speed of signing certificates. Of course, the whole operation from a user's logon until a signed certificate is granted takes longer because the authentication procedure at the back end, for example at an RSA authentication server, has an influence on performance (due to user interaction using a one-time password token).

Using SSL influences the performance significantly due to additional cryptographic operations protecting the communication. However, we strongly recommend that you exclusively use SSL connections to keep the security level high.

If performance at peak times is not sufficient, you can enhance performance by adding hardware to form a cluster with a new system and a dispatcher for load balancing.

Other influencing factors are the login modules, for example, LDAP or basic password login module (UME).

The SAP NetWeaver release does not influence the performance.

2 Sizing Fundamentals and Terminology

SAP provides general sizing information on the SAP Service Marketplace. For the purpose of this guide, we assume that you are familiar with sizing fundamentals. You can find more information at http://service.sap.com/sizing *Sizing Guidelines* *General Sizing Procedures*.

This section explains the most important sizing terms, as these terms are used extensively in this document.

Sizing

Sizing means determining the hardware requirements of an SAP application, such as the network bandwidth, physical memory, CPU processing power, and I/O capacity. The size of the hardware and database is influenced by both business aspects and technological aspects. This means that the number of users using the various application components and the data load they put on the server must be taken into account.

Benchmarking

Sizing information can be determined using SAP Standard Application Benchmarks and scalability tests (http://sap.com/benchmark). Released for technology partners, benchmarks provide basic sizing recommendations to customers by placing a substantial load upon a system during the testing of new hardware, system software components, and relational database management systems (RDBMS). All performance data relevant to the system, user, and business applications are monitored during a benchmark run and can be used to compare platforms.

SAPS

The SAP Application Performance Standard (SAPS) is a hardware-independent unit that describes the performance of a system configuration in the SAP environment. It is derived from the Sales and Distribution (SD) Benchmark, where 100 SAPS is defined as the computing power to handle 2,000 fully business processed order line items per hour. For more information about SAPS, see http://www.sap.com/benchmark *Measuring in SAPS*.

Initial Sizing

Initial sizing refers to the sizing approach that provides statements about platform-independent requirements of the hardware resources necessary for representative, standard delivery SAP applications. The initial sizing guidelines assume optimal system parameter settings, standard business scenarios, and so on.

Expert Sizing

This term refers to a sizing exercise where customer-specific data is analyzed and used to put more detail on the sizing result. The main objective is to determine the resource consumption of customized content and applications (not SAP standard delivery) by comprehensive measurements. For more information, see http://service.sap.com/sizing *Sizing Guidelines* *General Sizing Procedures* *Expert Sizing*.

Configuration and System Landscaping

Hardware resource and optimal system configuration greatly depend on the requirements of the customer-specific project. This includes the implementation of distribution, security, and high-availability solutions by different approaches using various third-party tools. In the case of high availability through redundant resources, for example, the final resource requirements must be adjusted accordingly. There are some "best practices" that are valid for specific combinations of operating system and database. To provide guidance, SAP created the SAP NetWeaver configuration guides http://service.sap.com/instguides *SAP NetWeaver*.

3 Initial Sizing for SAP Single Sign-On

3.1 Minimum Hardware Requirements for SAP Single Sign-On

The following table gives you an overview of the disk space and RAM needed for the application (server and Secure Login Client).

Server Requirements

Minimum Requirements	
Server	Your server must run with SAP NetWeaver 7.2x or higher. For more information, see the SAP Single Sign-On 3.0 Product Availability Matrix in the related link.
RAM for Secure Login Server	Maximum of 26 to 32 MB per certificate request. After the creation of the certificate, the RAM is available again because the server is stateless.

Client Requirements

Client with 32-Bit Operating System	Minimum Requirements
Disk Space for Secure Login Client	Installation: >=11.8 MB The storage of registry entries requires less than 1 KB.
RAM for Secure Login Client	The Secure Login Client itself requires 14 to 16 MB per user.
RAM for Secure Login service	The Secure Login service requires about 12 MB per system for the policy download agent.

Client with 64-Bit Operating System	Minimum Requirements
Disk Space for Secure Login Client	Installation: >=21.6 MB The storage of registry entries requires less than 1 KB.
RAM for Secure Login Client	The Secure Login Client itself requires 24 to 28 MB per user

Client with 64-Bit Operating System	Minimum Requirements
RAM for Secure Login service	The Secure Login service requires about 12 MB per system for the policy download agent.

> **i** Note
>
> The default requirements also apply for installations on Microsoft terminal servers or Citrix servers. For more information, see the relevant documentation.

Related Information

https://support.sap.com/pam

3.1.1 CPU Load

The Secure Login Server must have the minimum CPU power that is required for running with SAP NetWeaver 7.2x or higher.

3.1.2 Disk Space

Disk space for the Secure Login Client varies according to the operating system. If you use a 32-bit operating system, less disk space is required than if you use a 64-bit operating system.

The storage of registry entries requires less than 1 KB.

3.1.3 RAM

In a 32-bit operating system, the Secure Login Client requires 14 to 16 MB. However, in an 64-bit operating system, the Secure Login Client requires 24 to 28 MB per user.

3.2 Sizing Guideline for the Creation of User Certificates

The tables below show you how many user certificates you can generate per hour on a system (depending on the system's SAPS value). To ensure high performance, you can increase computing power by using a server with a higher SAPS value or form a cluster.

> **i** Note
>
> Your security policy determines the lifetime of the user certificates. Usually the lifetime of a user certificate is approximately 1 day. If the lifetime of your user certificates is very short, for example 10 minutes to ensure very high security, you must keep in mind that Secure Login must almost permanently re-generate user certificates for new sessions that are closed, for example after 12 minutes. In this case, you need a number of certificates that is considerably higher than the number of users.

When the system generates user certificates, the CPU load increases linearly until 100% CPU load is reached. Depending on your system setup and on the user CA key size used, this corresponds to 15 to 30 user certificates per second. If you want to generate more user certificates, it simply takes more time, or you must use a system with more computing power.

3.2.1 Secure Login Server with Secure Login Client and Secure Login Web Client

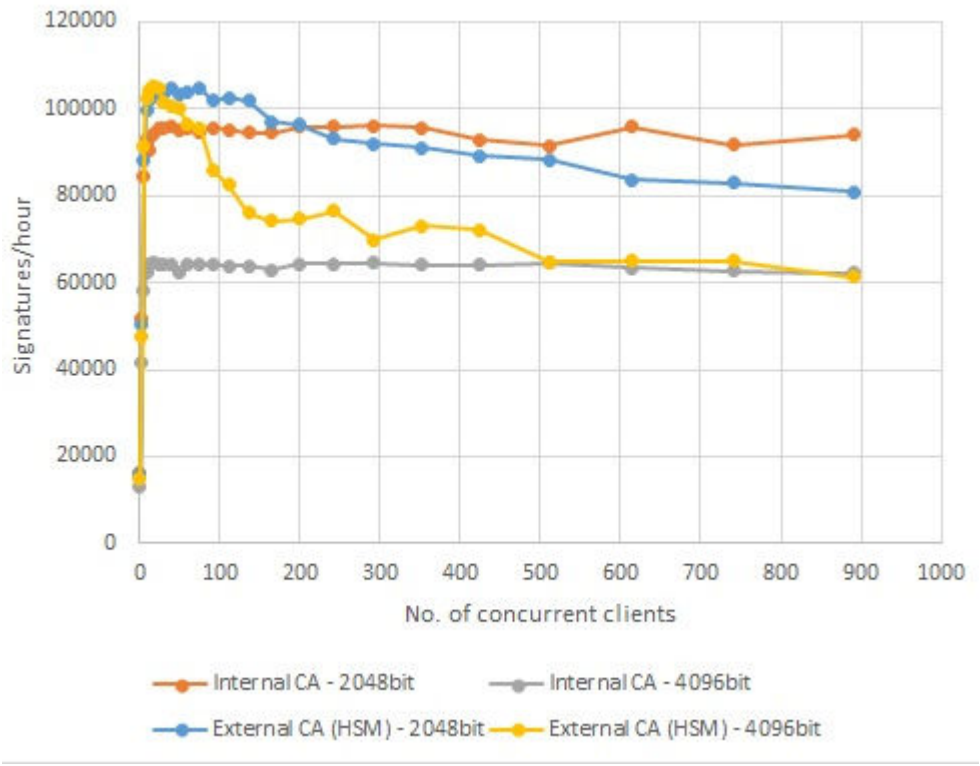
This table displays the quantity of user certificates signed per hour if you are using SSL-protected communication between Secure Login Server and Secure Login Client. The results for Secure Login Web Client are almost identical with those of the Secure Login Client.

Back End: Active Directory (LDAP Protocol)

User Certificates Signed per Hour

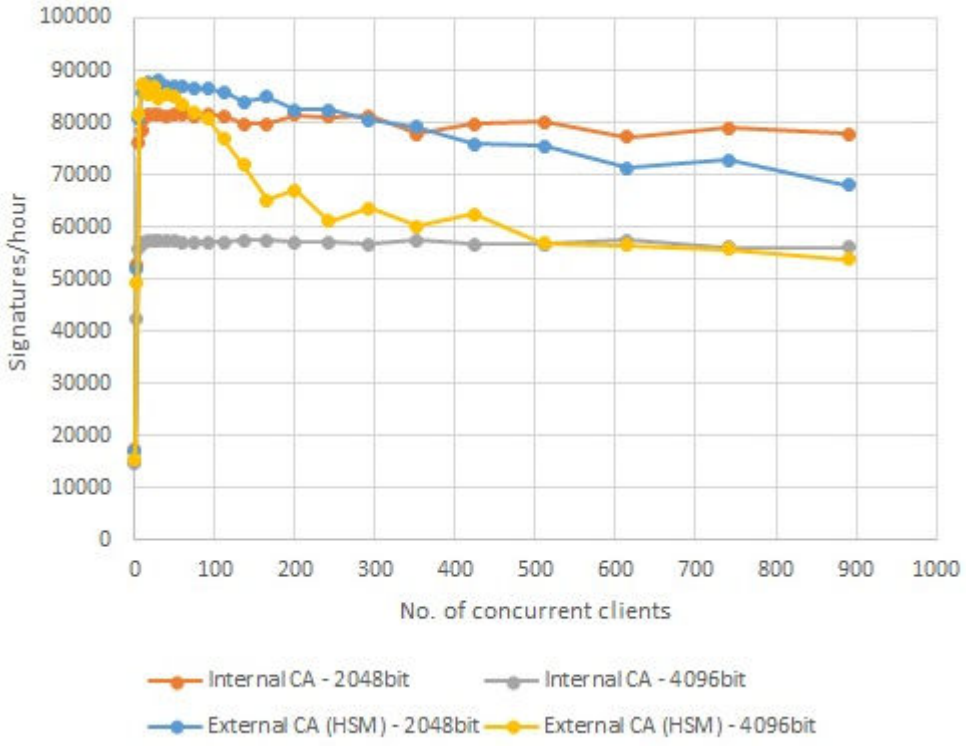
SAPS	Secure Login Server with Secure Login Client (with SSL)			
	2048 Bit (User CA Key Size)	2048 Bit (HSM User CA Key Size)	4096 Bit (User CA Key Size)	4096 Bit (HSM User CA Key Size)

User Certificates Signed per Hour				
3,700	89,000	91,000	60,000	80,000
4,700	113,000	116,000	77,000	101,000



Back End: UME Database

User Certificates Signed per Hour				
SAPS	Secure Login Server with Secure Login Client (with SSL)			
	2048 Bit (User CA Key Size)	2048 Bit (HSM User CA Key Size)	4096 Bit (User CA Key Size)	4096 Bit (HSM User CA Key Size)
3,700	76,000	78,000	54,000	69,000
4,700	97,000	99,000	69,000	88,000



3.3 Conclusion

The results listed in the tables above demonstrate the scalability and performance of a server with a given number of SAPS with respect to user certificates created per hour.

To draw conclusions from your own business requirements you should take your required number of user certificates created per hour into consideration. Comparing these numbers against the performance results of the tables above should provide the baseline to derive the required hardware for your implementation project.

4 Appendix

The method used in this sizing guide is throughput-based sizing. This model is quite accurate because it relies on actual throughput per second of user certificates signed with user CA certificates. However, this model is based on certain testing conditions.

4.1 Testing Conditions

The tests have run on a server with the following performance data:

Test System Used

CPU	1 dual-core Intel Core i5-660 processor
Clock Speed	3.33 GHz
Memory	16 GB
SAPS	3700
Hardware Security Module	Thales nShield Solo
Application Server	SAP NetWeaver Application Server for Java 7.30 including Enhancement Package 1, Support Package Stack 12

The application server used is an SAP NetWeaver Application Server for Java 7.30 including Enhancement Package 1, Support Package Stack 12, and the Internet Communication Manager was specially configured for high load. For more information, see the *Application Server with a High Expected Load* section of the SAP NetWeaver Library on the SAP Help Portal under *Function-Oriented View* > *Application Server* > *Application Server Java* > *Administering Application Server Java* > *Administration* > *ICM Administration* > *Internet Communication Manager (ICM)* > *Administration of the Internet Communication Managers* > *Parameterization of the ICM and the ICM Server Cache* > *Sample Profile for the ICM*.

The Secure Login Server issued user certificates and signs them with a user CA with key lengths of 2048 bits and 4096 bits over a dedicated period of time.

Tests were run using SSL protocol. The SSL protocol has an influence on the Secure Login's system performance. The Secure Login system shares a certain amount of CPU load with the SSL engine of SAP NetWeaver. For more information, see the sizing guide for SAP NetWeaver.

> **i Note**
>
> Signing the user certificates with a large key is a CPU-intensive operation, especially at peak times. Customers must weigh security against performance and decide whether they want high security and

make CPU power available accordingly or whether they are prepared to sacrifice security to a certain extent and use a small key size.

The tests were performed either with LDAP login modules (Active Directory) or basic password login modules. Using the basic password login module has an influence on the Secure Login Server's performance because it is using the User Management Engine of SAP NetWeaver AS for Java, where the Secure Login Server is running.

Secure Login Server used internal Certification Authorities or Certification Authorities based on a hardware security module (HSM) for signing the certificates. Providing keys using a hardware security module has an influence on performance.

4.2 Results for Secure Login Server

The CPU load on the Secure Login Server depends primarily on the user CA key size and on the back end used. Secure Login Client and Secure Login Web Client exert the same CPU load on the Secure Login Server.

4.2.1 CPU Load

Using SSL for the communication between Secure Login Server and Secure Login Client or Secure Login Web Client has an influence on the CPU load used.

The CPU power needed is insignificant.

With SAP Single Sign-On 3.0, there is no longer a significant difference in the CPU load between Secure Login Client and Web Client. Since the Secure Login Web Client creates the private key on client side, the CPU load on the Secure Login Server side is approximately the same as the CPU load caused by the Secure Login Client.

Secure Login Server with Secure Login Client or Secure Login Web Client with LDAP back end and SSL (SSL Server key size is 2048 Bit)

User CA Key Size in Bits	CPU Load in %	Signatures per Second
2048	100	30
4096	100	20

4.3 Results for the Secure Login Client and Secure Login Web Client

The Secure Login Client and Secure Login Web Client is located on one computer and provides security tokens (Kerberos and X.509 technology) for a variety of applications.

4.3.1 RAM

The Secure Login Client or the Secure Login Web Client itself requires 14 to 16 MB in a 32-bit operating system or 24 to 28 MB per user in a 64-bit operating system.

The Secure Login service (policy download agent) requires about 12 MB per system.

The Secure Login Client runs processes, for example for loading the cryptographic store provider, the SNC library, or sbuspkcs11. They need 2.5 MB of additional memory at runtime. Most of this memory is shared by multiple processes. This means that the first process needs 2.5 MB and all other processes need 200 to 500 KB.

4.3.2 Disk Space for Secure Login Client

For installation, the Secure Login Client needs the amount of disk space specified in the table below. The disk space varies depending on the operating system. If you use a 32-bit operating system, less disk space is required than if you use a 64-bit operating system. This is also valid for the Secure Login JavaScript Web Client.

Component	With 32-Bit Operating System	With 64-Bit Operating System
Complete installation (all components)	11.8 MB	21.6 MB

Optional Components	With 32-Bit Operating System	With 64-Bit Operating System
Start during Windows login	0.0 MB	0.0 MB
Secure Login Server Support	1.5 MB	2.3 MB
Kerberos Single Sign-On	0.4 MB	0.8 MB

In operating mode, the Secure Login Client only needs less than 1 KB of disk space for the storage of registry entries. This value was determined when logging was switched off.

4.3.3 Disk Space for Secure Login Java Applet Web Client

The Secure Login Java Applet Web Client runs with zero footprint. So, when the Secure Login Web Client starts for the first time, it initially downloads the SNC library. The download temporarily requires 5.1 MB disk space.

4.3.4 Conclusion

We recommend that you reserve 24 to 28 MB RAM per user in total.

5 Comments and Feedback

Both are very welcome. Send them to SAP Single Sign-On support (component BC-IAM-SSO-SL).

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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

© 2020 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