

SAP Business One Integration Framework

Configure Connectivity to SAP Business One Service Layer

PUBLIC



Global Roll-out

August 2018, Krisztián Pápai

THE BEST RUN



TABLE OF CONTENTS

1.	OBTAIN A VALID CERTIFICATE.....	3
1.1	Purchase a Signed Certificate from a Trusted Third-Party Certification Authority (CA) Vendor ..	3
1.2	Create a Self-Signed Certificate Using the Certificate Tool	3
2.	COPY THE CERTIFICATE TO A LINUX SERVER LOCATION	4
2.1	Prepare Certificate File - <i>server.crt</i>	4
2.2	Prepare Public and Private key file - <i>server.key</i>	4
2.3	Move the Certificate and the Key File to the Linux Machine	4
3.	APPLY THE CERTIFICATE TO THE SERVICE LAYER	5
3.1	Back Up the Default Certificate and Key of the Service Layer	5
3.2	Copy the Certificate and the Key File to the Service Layer Folder.....	5
3.3	Restart the Service Layer Service.....	5
4.	STORE THE KEYS IN THE JAVA KEYSTORE	6
4.1	Download and Save the Certificate from the Service Layer.....	6
4.2	Generate the Java KeyStore	6
5.	IMPORT JAVA KEYSTORE TO THE INTEGRATION FRAMEWORK.....	8
5.1	Upload the Java KeyStore to the Integration Framework BizStore	8
5.2	View the Java KeyStore Content in the Integration Framework BizStore	8
6.	CONFIGURE SLD ENTRY FOR THE SAP BUSINESS ONE SYSTEM IN THE INTEGRATION FRAMEWORK.....	9
6.1	Configure the SDL	9
6.2	Test the Connection	9
7.	ENSURE THE DNS ADDRESS FORWARDING TO THE LINUX HOST (OPTIONAL).....	10
7.1	Check the Connectivity to the Linux Host from the Integration Framework	10
7.2	Edit the hosts File on the Integration Framework Machine	10
8.	REFERENCES	11

The Service Layer is only available for SAP Business One, version for SAP HANA.

1. OBTAIN A VALID CERTIFICATE

SAP cannot give recommendations for when to use a self-signed certificate or a signed certificate from a trusted third party. The selection depends on the specific use and the selected environment, for example, VPN, dev/test systems, intranet/internet solutions, value/type of transferred information, an incentive for someone to attack the connection, security needs, etc.

1.1 Purchase a Signed Certificate from a Trusted Third-Party Certification Authority (CA) Vendor

Follow the steps provided by the CA vendor to receive a trusted CA-signed certificate for the system.

1.2 Create a Self-Signed Certificate Using the Certificate Tool

1.2.1 Get the host name of the Linux server, where the Service Layer service is running.

```
calhost:/ # hostname
calhost
calhost:/ #
```

1.2.2 Open the Certificate Tool in the integration framework and generate the certificate based on the previously identified host name.

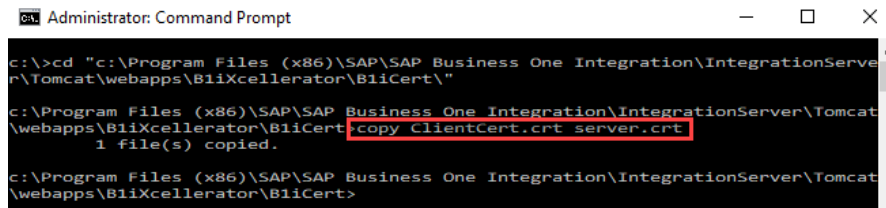
The screenshot shows the SAP Integration Framework user interface. At the top, a navigation bar includes 'COCKPIT', 'SLD', 'MAINTENANCE', 'SCENARIOS', 'MONITORING', 'TOOLS' (highlighted with a red box and a '1' annotation), and 'HELP'. On the left, a 'Tools' sidebar lists various utilities, with 'Certificate Tool' highlighted by a red box and a '2' annotation. The main area is titled 'Certificate Tool' and contains a 'Domain Name' input field with 'calhost' entered (annotated with a red box and a '3' annotation). Below this is an 'Actions' section with 'Create Certificate' (annotated with a red box and a '4' annotation) and 'Reset Certificate' buttons. An 'Explanations' section at the bottom provides details: 'Domain Name: Enter Domain Name the Certificate Is Issued to', '[Create Certificate]: Create and Deploy Certificate', and '[Reset Certificate]: Reset Certificate to Default'.

2. COPY THE CERTIFICATE TO A LINUX SERVER LOCATION

The following section demonstrates how to copy the self-signed certificate, because for the trusted third-party authority certificate, the file names and certificate structure might have a different format, based on the provider.

2.1 Prepare Certificate File - *server.crt*

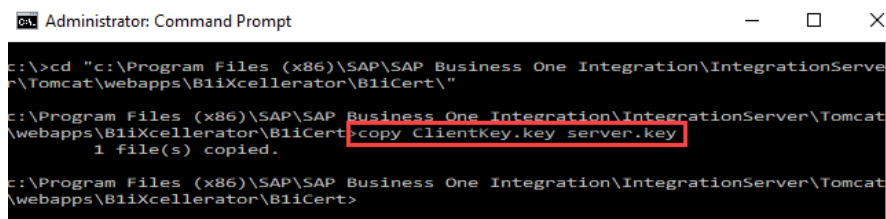
Copy the *ClientCert.crt* file to the *server.crt* file in the */B1iXcellerator/B1iCert* folder of the integration framework installation folder.



```
Administrator: Command Prompt
c:\>cd "c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert\"
c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert>copy ClientCert.crt server.crt
1 file(s) copied.
c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert>
```

2.2 Prepare Public and Private key file - *server.key*

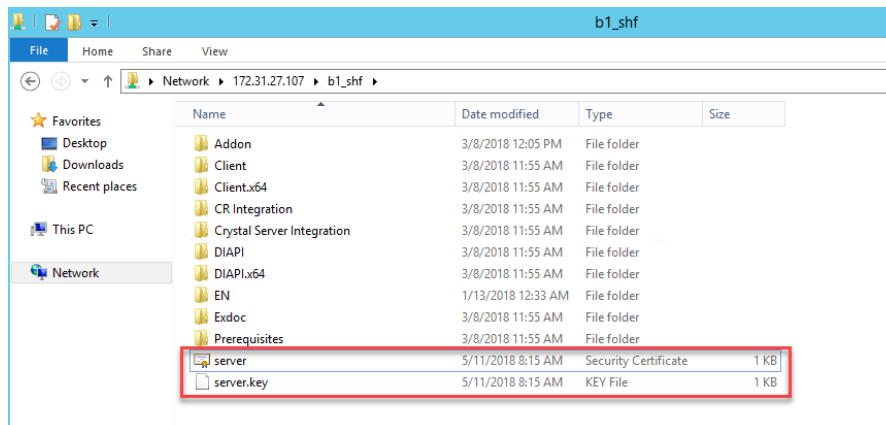
Copy the *ClientCert.key* file to the *server.key* file in the */B1iXcellerator/B1iCert* folder of the integration framework installation folder.



```
Administrator: Command Prompt
c:\>cd "c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert\"
c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert>copy ClientCert.key server.key
1 file(s) copied.
c:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\B1iCert>
```

2.3 Move the Certificate and the Key File to the Linux Machine

You can use the SAP Business One shared folder to transfer the *server.crt* and *server.key* files to the Linux server.



3. APPLY THE CERTIFICATE TO THE SERVICE LAYER

To establish a secure connection to the Service Layer, apply the previously generated certificate and key.

3.1 Back Up the Default Certificate and Key of the Service Layer

By default, certificated-related information for the Service Layer is stored in the `/usr/sap/SAPBusinessOne/ServiceLayer/conf` folder. If you installed the Service Layer to a different path, change the commands accordingly.

Rename the `server.key` and `server.crt` files to `server.key.old` and `server.crt.old`

```
calhost:/ # cd /usr/sap/SAPBusinessOne/ServiceLayer/conf
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # ls
Bl_ServiceLayer.xml      httpd-bls-lb-member-50002.conf  httpd-bls-lb.conf
bls.conf                 httpd-bls-lb-member-50003.conf  server.crt
demo.schema             httpd-bls-lb-member-50004.conf  server.key
httpd-bls-lb-member-50001.conf  httpd-bls-lb-member-common.conf
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # mv ./server.crt ./server.crt.old
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # mv ./server.key ./server.key.old
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # ls
Bl_ServiceLayer.xml      httpd-bls-lb-member-50002.conf  httpd-bls-lb.conf
bls.conf                 httpd-bls-lb-member-50003.conf  server.crt.old
demo.schema             httpd-bls-lb-member-50004.conf  server.key.old
httpd-bls-lb-member-50001.conf  httpd-bls-lb-member-common.conf
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf #
```

3.2 Copy the Certificate and the Key File to the Service Layer Folder

Previously, we used the SAP Business One shared folder to copy the certificate and the key file from the integration framework host to the Service Layer host. Now, we work with the shared folder directory to move the certificate-related files to the Service Layer.

```
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # cp /usr/sap/SAPBusinessOne/Bl_SHF/server.crt ./
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # cp /usr/sap/SAPBusinessOne/Bl_SHF/server.key ./
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # ls
Bl_ServiceLayer.xml      httpd-bls-lb-member-50002.conf  httpd-bls-lb.conf  server.key.old
bls.conf                 httpd-bls-lb-member-50003.conf  server.crt
demo.schema             httpd-bls-lb-member-50004.conf  server.crt.old
httpd-bls-lb-member-50001.conf  httpd-bls-lb-member-common.conf  server.key
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf #
```

3.3 Restart the Service Layer Service

To apply the certificate changes to the Service Layer, restart the Service Layer service.

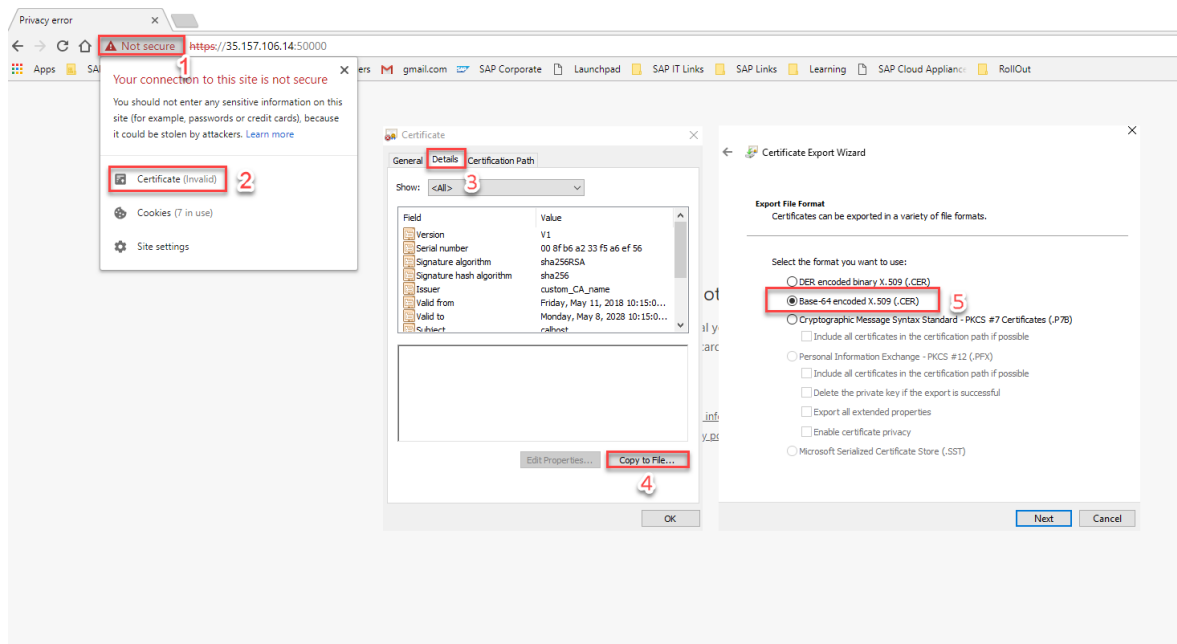
```
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf # /etc/init.d/bls restart
awk: cmd. line:1: fatal: cannot open file `/var/opt/.hdb/calhost/installations.client' for reading (No such file
or directory)
Restarting Service Layer...
Stopping service with port 50001.
Stopping service with port 50002.
Stopping service with port 50003.
Stopping service with port 50004.
Stopping service with port 50000.
Starting service with port 50001.
Starting service with port 50002.
Starting service with port 50003.
Starting service with port 50004.
Starting service with port 50000.
Restarted.
calhost:/usr/sap/SAPBusinessOne/ServiceLayer/conf #
```

4. STORE THE KEYS IN THE JAVA KEYSTORE

You cannot use the Microsoft Certificate Manager to store the certificates used by the integration framework, because the integration framework uses the Java KeyStore. A Java KeyStore (JKS) is a repository of security certificates – either authorization certificates or public key certificates – plus the corresponding private keys, used for instance in SSL encryption.

4.1 Download and Save the Certificate from the Service Layer

- On the integration framework server, open the Service Layer using Microsoft Internet Explorer or Google Chrome using the following address: <https://<ServiceLayerHost>:50000>
- To display the certificate in the Web browser, open the *Certificates* information of the Web browser.
- Click the *Certificate* information link.
- To save the certificate to **servicelayer.cer**, choose the *Details* tab and then, click the *Copy to file* button.
- In the *Certificate Export* wizard, set the format to *Base-64 encoded X.509 (.CER)*.
- Save the file to a folder and finish the wizard. For example, the file **servicelayer.cer** will be saved to the **C:\tmp** folder.



4.2 Generate the Java KeyStore

Use the **keytool** utility to generate the Java KeyStore. The utility is installed by the integration framework setup by default.

```
c:\>cd "c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin\"
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>keytool -import -file "c:\tmp\servicelayer.cer" -keystore "
c:\tmp\servicelayer.jks"
Enter keystore password:
Re-enter new password:
Owner: CN=calhost
Issuer: CN=custom_CA_name
Serial number: 8Fb6a233f5a6ef56
Valid from: Fri May 11 10:15:07 CEST 2018 until: Mon May 08 10:15:07 CEST 2028
Certificate fingerprints:
    MD5: DD:1D:FB:42:D2:30:C6:17:E2:B6:69:25:89:F3:3C:C6
    SHA1: 4A:7B:B2:20:AC:83:CF:76:B9:F3:0D:73:77:6A:A6:85:2D:CB:23:1C
    SHA256: C3:2B:6E:F9:EF:95:53:70:F3:CF:DF:0F:A9:8B:90:83:D5:02:CF:90:24:56:6A:CE:7A:D1:BB:4E:27:05:7E:4B
Signature algorithm name: SHA256withRSA
Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>
```

It is necessary to define the password for the keystore. Enter **yes** to confirm the trust for the certificate.

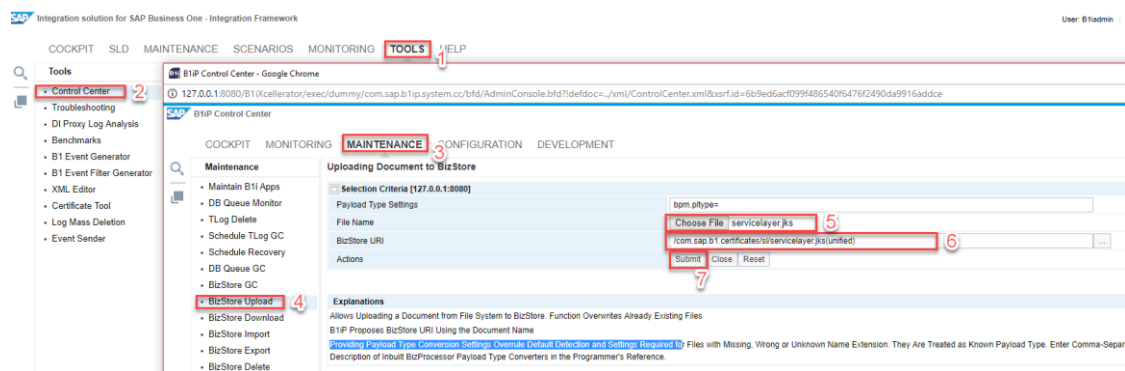
5. IMPORT JAVA KEYSTORE TO THE INTEGRATION FRAMEWORK

5.1 Upload the Java KeyStore to the Integration Framework BizStore

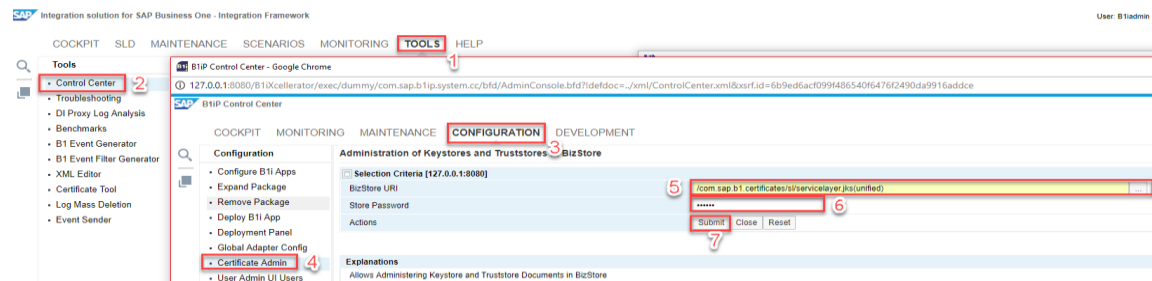
The upload enables the access to the certificate using the Java KeyStore in the SAP Business One.

In the integration framework, we save the Java KeyStore to the following BizStore URI:
`/com.sap.b1.certificates/sl/servicelayer.jks(unified)`

Since this address is not yet available in the BizStore, we generate the address by entering the information.



5.2 View the Java KeyStore Content in the Integration Framework BizStore



6. CONFIGURE SLD ENTRY FOR THE SAP BUSINESS ONE SYSTEM IN THE INTEGRATION FRAMEWORK

The Service Layer connectivity configuration is part of the SLD section of the integration framework. Define the properties for the Service Layer, which are listed for each company database SLD entry.

6.1 Configure the SDL

SAP Integration solution for SAP Business One - Integration Framework

COCKPIT **SLD** MAINTENANCE SCENARIOS MONITORING TOOLS HELP

SLD

B1i Server

- SBODemoHU
- SBODemoDE
- SBODEMOUS**
- HTTP-B1System
- XMLFileSystem
- WSforMobile
- HAnyforXcelsius
- SBO-COMMON
- HAnyforCampaignMa...
- HAnyforRFQ
- HAnyforXcelsiusPortal
- B1A Server
- B1A DB
- WSforCustomerCheck...
- CustomerCheckoutDb
- CustomerCheckoutHttp
- eDocWS

SBODEMOUS

General Information

Type: B1.9.0

Description: SAP Business One 9.0 and Minor Releases

Name: SBODEMOUS

ID: 0010000102

Common Fields

b1Server: calhost

company: SBODEMOUS

Connectivity List (Active)

B1DI

B1SL

b1Server: calhost

company: SBODEMOUS

destProtocol: https

destHost: calhost

destPort: 50000

destPath: /b1s/v1

user: manager

password:

trustStoreURI: /com.sap.b1.certificates/s1/serviceLayer.jks(unified)

JDBC

6.2 Test the Connection

SAP Integration solution for SAP Business One - Integration Framework

COCKPIT **SLD** MAINTENANCE SCENARIOS MONITORING TOOLS HELP

SLD

B1i Server

- SBODemoHU
- SBODemoDE
- SBODEMOUS**
- HTTP-B1System
- XMLFileSystem
- WSforMobile
- HAnyforXcelsius
- SBO-COMMON
- HAnyforCampaignMa...
- HAnyforRFQ
- HAnyforXcelsiusPortal
- B1A Server
- B1A DB
- WSforCustomerCheck...
- CustomerCheckoutDb
- CustomerCheckoutHttp

SBODEMOUS

General Information

Common Fields

Connectivity List (Active)

B1DI

B1SL

b1Server: calhost

company: SBODEMOUS

destProtocol: https

destHost: calhost

destPort: 50000

destPath: /b1s/v1

user: manager

password:

trustStoreURI: /com.sap.b1.certificates/s1/serviceLayer.jks(unified)

Test Connection

Test Connection

Test Connection - Google Chrome

127.0.0.1:8080/B1IXcellerator/exec/dummy/com.sap.b1.system.iae/bfd...

☒ Connect to SBODEMOUS(B1SL) successfully

Detailed Information

7. ENSURE THE DNS ADDRESS FORWARDING TO THE LINUX HOST (OPTIONAL)

If the host name of the Linux machine cannot be resolved on the integration framework host, perform the following steps.

7.1 Check the Connectivity to the Linux Host from the Integration Framework

You can use the ping command to check the connection.

```
C:\> ping calhost
ping request could not find host calhost. Please check the name and try again.
C:\>
```

7.2 Edit the hosts File on the Integration Framework Machine

- On the integration framework host, run notepad.exe with the *Run as Administrator* option.
- Open the `c:\Windows\System32\drivers\etc\hosts` file.
- Enter the IP address of the Service Layer together with the hostname according to the example available in the `hosts` file.
- Save the file.
- Test the connectivity again.

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
192.168.1.1 calhost
```



8. REFERENCES

SAP Note [2209825](#) - Providing valid certificate for service layer access from integration framework

SAP Note [2607373](#) - Service Layer (SL) Troubleshooting Guide

www.sap.com/contactsap

© 2018 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.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

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. See <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

THE BEST RUN

