

Integration Framework for SAP Business One

Setup of Secured Connection to SAP Business One Mobile App

Android, iPhone, iPad and iPod Touch

PUBLIC



Global Roll-out

October 2018, Krisztián Pápai

THE BEST RUN



Table of Contents

1.	INTRODUCTION	3
2.	COMPATIBILITY CONCEPT	3
3.	VERSION INFORMATION	3
3.1	Version Check for SAP Business One Mobile App for iOS	3
3.2	Version Check for SAP Business One Mobile App for Android	3
4.	DOWNLOAD AND INSTALL THE SAP BUSINESS ONE MOBILE APP	4
4.1	Download SAP Business One Mobile App for iOS to your iOS device	4
4.2	Download SAP Business One Mobile App for Android to Your Android Device	4
5.	RETRIEVING THE MOBILE DEVICE ID	5
5.1	Get the Mobile Device ID on iOS	5
5.2	Get the Mobile Device ID on Android	6
6.	LICENSE ASSIGNMENT FOR SAP BUSINESS ONE USER B1I	7
7.	CONFIGURE SAP BUSINESS ONE MOBILE USER	8
8.	LICENSE ASSIGNMENT FOR SAP BUSINESS ONE MOBILE USER	9
9.	CHECK THE COMMUNICATION FROM INTEGRATION FRAMEWORK TO SAP BUSINESS ONE	10
9.1	Login to the Integration Framework for SAP Business One	10
9.2	Verify the Communication to SAP Business One Using the JDBC Connection	10
9.3	Verify the Communication to SAP Business One Using the DI	11
9.3.1	<i>Company Database Is Missing</i>	11
9.3.2	<i>The Communication Fails with Some Specific Error</i>	11
10.	OBTAIN A VALID CERTIFICATE	12
10.1	Implement a Signed Certificate from a Trusted Third-Party Certification Authority (CA)	12
10.2	Create a Self-Signed Certificate Using the Certificate Tool	12
10.3	Create a Self-Signed Certificate Manually	12
11.	DEPLOY THE CERTIFICATE TO MOBILE DEVICE	18
11.1	Deploy a Certificate from a Trusted Third-Party Certification Authority (CA)	18
11.2	Deploy Manually Created or Through Certificate Tool Certificate for iOS	18
11.3	Deploy Certificate Manually Created of Through Certificate Tool for Android	20
12.	SCENARIO PACKAGE SETUP FOR MOBILE	21
12.1	Deactivate the Scenario Package	21
12.2	Set the Secured Transport for the Scenario Package	21
12.3	Activate the Scenario Package	22
13.	CONFIGURE CONNECTION IN SAP BUSINESS ONE MOBILE APP	23
13.1	SAP Business One Mobile App Setup for iOS	23
13.2	SAP Business One Mobile App Setup for Android	23
14.	REFERENCES	25

1. INTRODUCTION

The SAP Business One mobile app is available for SAP Business One and SAP Business One, version for SAP HANA. The certificate is deployed in the integration framework for SAP Business One, which is acting as the middleware between the mobile app and SAP Business One. The configuration is the same for SAP Business One and SAP Business One, version for SAP HANA.

2. COMPATIBILITY CONCEPT

SAP regularly ships minor releases or patches for the app containing new functions as well as improvements and bug fixes. To benefit from this, the latest version of the app and the backend software must be run. As updates on mobile devices are not typically managed by a central IT department, it is the responsibility of end users to update the app to the latest version. Because the mobile app is both backward and forward compatible, it is always safe to upgrade the app on the mobile device; the backend server can remain on the current release of SAP Business One. However, if the backend is installed on an older version of SAP Business One that does not support the latest functions of the most recent mobile app, some new functions will not work. When the user accesses such a function a popup window appears, informing the user that the backend must be upgraded to enable the selected function. All mobile app functions that were supported by the older version of SAP Business One still work. In the reverse case, if the backend is installed on a later version of SAP Business One than the mobile app, the functionality of the mobile app is fully maintained and works as designed.

To view the iOS compatibility information with mobile application, go to [Apple Store downloading page](#) → *Compatibility*.

To view the Android compatibility information with mobile application, go to [Google Play downloading page](#) → *Additional Information* → *Required Android*.

3. VERSION INFORMATION

3.1 Version Check for SAP Business One Mobile App for iOS

To check the changes made in each version of the SAP Business One mobile app, please refer to SAP Note [1602674](#) (login required). In this note you will see, how the SAP Business One mobile app is aligned with the SAP Business One releases and patches as well.

3.2 Version Check for SAP Business One Mobile App for Android

To check the changes made in each version of the SAP Business One mobile app, please refer to SAP Note [1924930](#) (login required). In this note you will see, how the SAP Business One mobile app is aligned with the SAP Business One releases and patches as well.

4. DOWNLOAD AND INSTALL THE SAP BUSINESS ONE MOBILE APP

4.1 Download SAP Business One Mobile App for iOS to your iOS device

You can search for mobile app on Apple App store. Alternatively, follow this link

<http://itunes.apple.com/app/sap-business-one-mobileapplication/id392606876> or use the QR code:



4.2 Download SAP Business One Mobile App for Android to Your Android Device

You can search for mobile app on Google Play. Alternatively, follow this link



<https://play.google.com/store/apps/details?id=b1.mobile.android> or use the QR code:

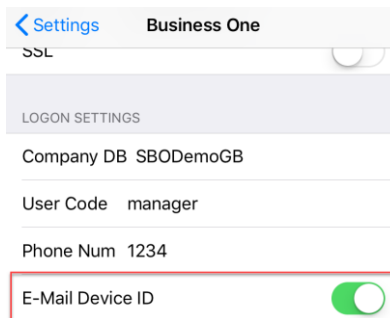



5. RETRIEVING THE MOBILE DEVICE ID

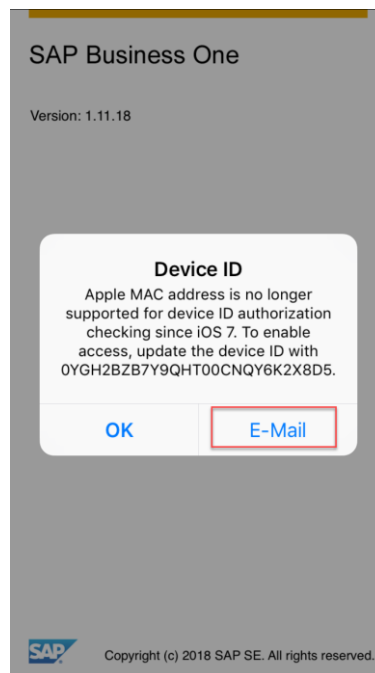
The Mobile Device ID is a unique ID generated based on the device's hardware configuration by the SAP Business One mobile app. This ID will be part of the multi-channel authentication.

5.1 Get the Mobile Device ID on iOS

- Tap the *Settings* icon on your iOS device 
- Tap the *SAP Business One* entry  Business One >
- Turn on the *E-Mail Device ID* option

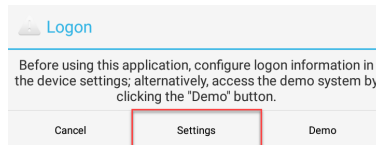


- Tap the *SAP Business One* icon on your iOS device 
- Tap *Email*. An email message containing the device ID in the email body appears. Enter your email address in the *To* field, and tap *Send*

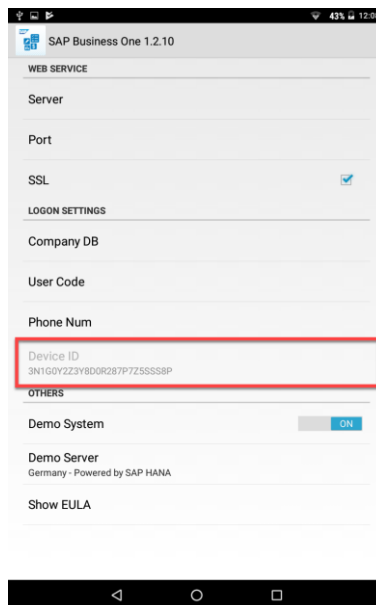


5.2 Get the Mobile Device ID on Android

- Tap the *SAP Business One* icon on your Android device
- Tap the *Settings* button



- The *Mobile Device ID* is available under the *LOGON SETTINGS* section

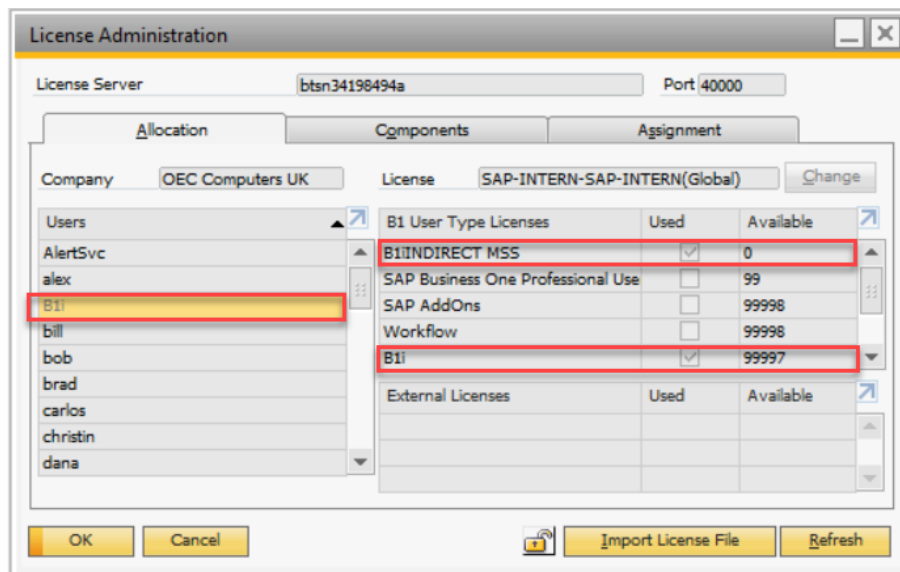


6. LICENSE ASSIGNMENT FOR SAP BUSINESS ONE USER B1I

Each SAP Business One Company Database has a specific B1i user, which is created automatically. This user supports to ensure the communication between the company database and the integration framework for SAP Business One.

Open the *License Administration* form in *SAP Business One* → *Administration* → *License* and assign the following license types for the B1i user:

- B1iINDIRECT MSS
- B1i



7. CONFIGURE SAP BUSINESS ONE MOBILE USER

The SAP Business One user that wants to use the SAP Business One mobile app, must have some additional settings, which will ensure the communication.

The following properties must be filled in SAP Business One → Administration → Setup → General → Users section:

- Select the *Mobile User* checkbox
- Enter the user's mobile phone number in the *Mobile Phone* field
- Enter the device ID of your iOS device into the *Mobile Device ID* field. To get the *Mobile Device ID*, please refer to the chapter 6 in this document.

The screenshot shows the 'Users - Setup' dialog box in SAP Business One. The 'Mobile User' checkbox is checked and highlighted with a red box. The 'Mobile Phone' field contains '+421123456789' and the 'Mobile Device ID' field contains '0YGH2BZB7Y9QHT00CNQY6K2X8D9', both fields are also highlighted with a red box. Other fields include User Code (manager), User Name (Jayson Butler), Branch (Main), and Department (General). The dialog box has tabs for General, Services, and Display. At the bottom, there are buttons for OK, Cancel, and Copy Form Settings.

To enable a user to use the app on two different mobile devices, enter the device ID of both devices. Use "/" as the separator. For example: AE45FG67816ET98ZV6523BNH81 /1QAZXSW23EDCVFR45TGB678YHN.

8. LICENSE ASSIGNMENT FOR SAP BUSINESS ONE MOBILE USER

Open the *License Administration* form in *SAP Business One* → *Administration* → *License* and assign the B1i license type in addition to the normal license types for the user who is going to use the SAP Business One mobile app.

The screenshot shows the 'License Administration' window with the following details:

- License Server: btn34198494a
- Port: 40000
- Company: OEC Computers UK
- License: SAP-INTERN-SAP-INTERN(Global)
- Users list: john, juan, julie, keiko, keith, leo, linda, **manager**, maria
- Selected license type: B1i
- Used: Available: 99997

B1 User Type Licenses		Used	Available
B1i	<input checked="" type="checkbox"/>	99997	
B1iINDIRECT MSS	<input type="checkbox"/>	0	
SAP Business One Professional Use	<input checked="" type="checkbox"/>	99	
SAP AddOns	<input type="checkbox"/>	99999	
Workflow	<input type="checkbox"/>	99999	

Buttons: OK, Cancel, Import License File, Refresh

9. CHECK THE COMMUNICATION FROM INTEGRATION FRAMEWORK TO SAP BUSINESS ONE

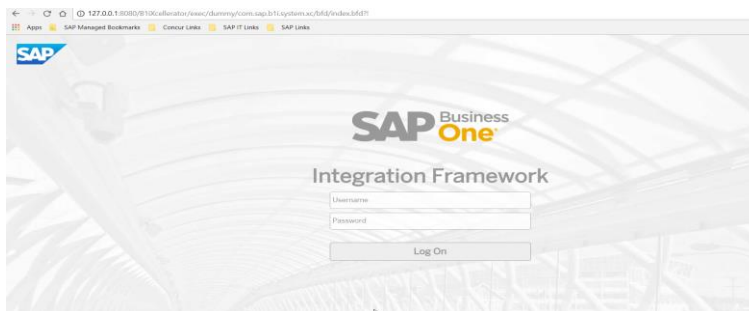
Verify the communication between the integration framework and SAP Business One or SAP Business One, version for SAP HANA.

9.1 Login to the Integration Framework for SAP Business One

Default http address is <http://<FQDN>:8080> (e.g. <http://127.0.0.1:8080>)

Default https address is <https://<FQDN>:8443> (e.g. <https://127.0.0.1:8443>)

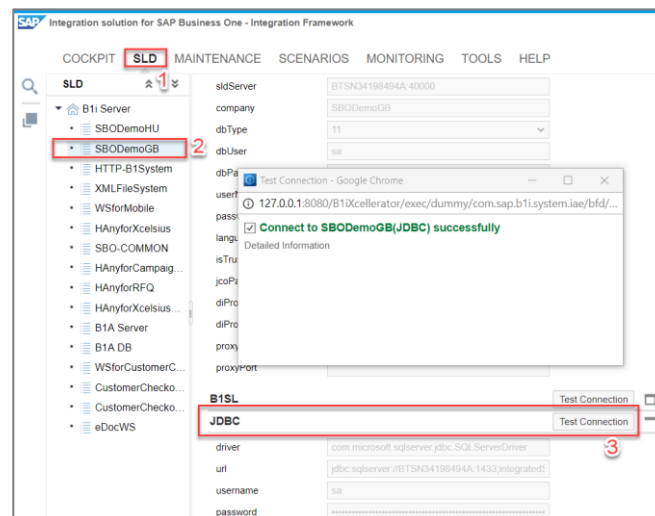
Default administrator user for login is *B1iadmin*. The password for this user was defined during the installation process of the integration framework for SAP Business One.



9.2 Verify the Communication to SAP Business One Using the JDBC Connection

The integration framework uses the *JDBC* connection to retrieve the information from the *Company Database*.

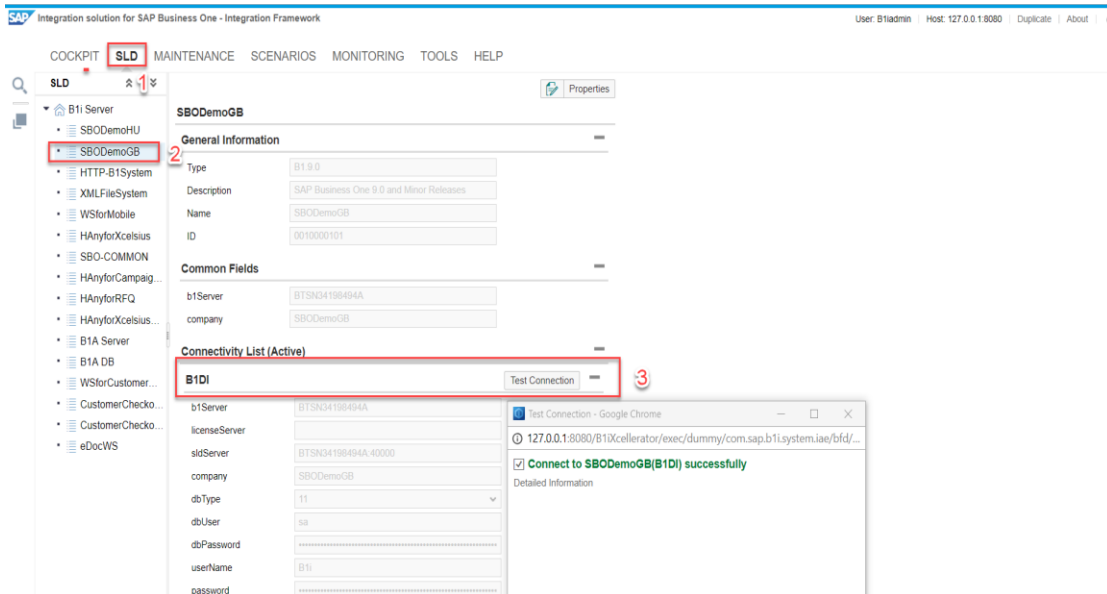
- (1) In the integration framework, choose *SLD* → *B1i Server*
- (2) Select the company database.
- (3) In *Connectivity List (Active)*, find the *JDBC* section and press the *Test Connection* button



9.3 Verify the Communication to SAP Business One Using the DI

The integration framework uses the *SAP Business One DI API* connection to add information to the *Company Database*.

- (1) In the integration framework, choose *SLD* → *B1i Server*
- (2) Select the company database.
- (3) In the *Connectivity List (Active)*, find the *B1DI* section and press the *Test Connection* button



You might encounter the following issues:

9.3.1 Company Database Is Missing

The SAP Business One Company database entry is not listed in the integration framework SLD section.

To solve this issue, please refer to SAP Note [2032666](#) (login required).

9.3.2 The Communication Fails with Some Specific Error

To solve this issue, please refer to SAP Note [2029714](#) (login required).

10. OBTAIN A VALID CERTIFICATE

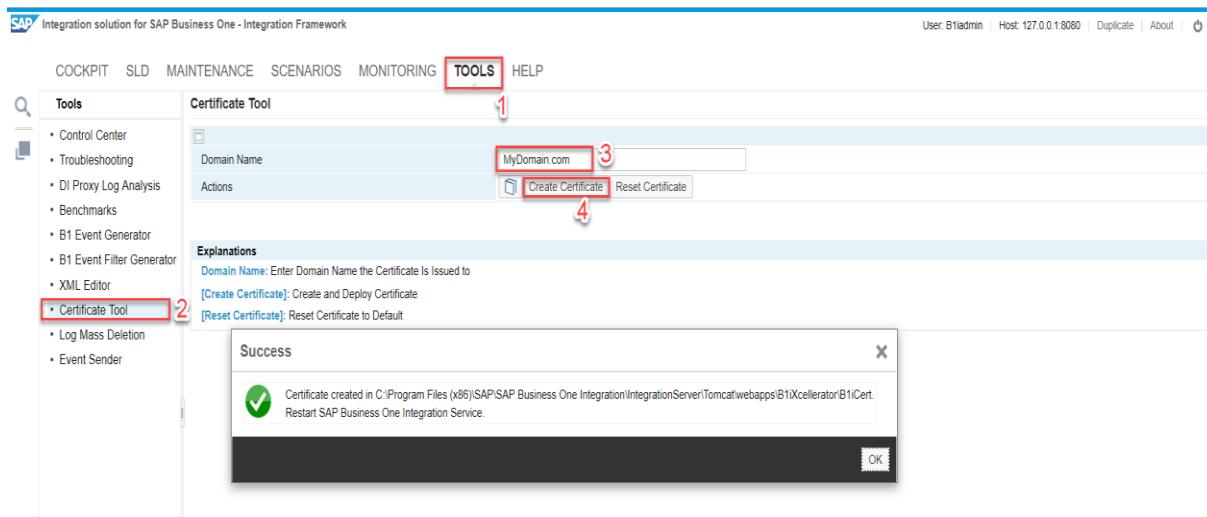
SAP cannot give recommendations for when to use a self-signed certificate or a signed certificate from a trusted third party. The selection depends on the specific use and the selected environment, for example, VPN, dev/test systems, intranet/internet solutions, value/type of transferred information,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

10.1 Implement a Signed Certificate from a Trusted Third-Party Certification Authority (CA)

Please refer to SAP Note [2019275](#) (login required) that documents how you can implement a certificate from a Trusted Certification Authority. The note provides some general guidelines. Each authority has an individual certificate format and structure and the deployment might be different based on the authority's deliveries.

10.2 Create a Self-Signed Certificate Using the Certificate Tool

Open the Certificate Tool in the integration framework and generate the certificate based on the domain name of the customer. The integration framework creates the certificate in the `... \B1iXcellerator\B1iCert` folder. The path depends on where you have installed the integration framework.



After certificate creation, restart the SAP Business One Integration Service.

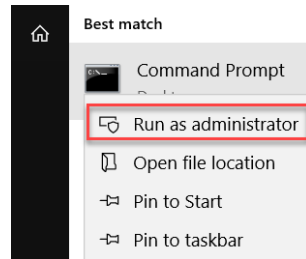
10.3 Create a Self-Signed Certificate Manually

10.3.1 OpenSSL Check

Since SAP Business One 9.1 PL08, the OpenSSL binaries are included in the integration framework for SAP Business One installation. You can verify it in the folder `... \SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin\`.

If the OpenSSL is not shipped with your integration framework installation, you can manually download and install from: <https://www.openssl.org/community/binaries.html>

10.3.2 Open the *Command Prompt as Administrator*.



10.3.3 Set the Path for OpenSSL Configuration File

Execute the command: **set OPENSSL_CONF=<OpenSSL install directory>\bin\openssl.cfg**

```
c:\>set OPENSSL_CONF=C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin\openssl.cfg
c:\>
```

Example command: set OPENSSL_CONF=C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin\openssl.cfg

10.3.4 Create Working Directory for Output Files

Execute the command: **mkdir <your working directory>**

```
C:\>mkdir c:\temp\MyCertificates
C:\>
```

Example command: mkdir c:\temp\MyCertificates

10.3.5 Change Directory to OpenSSL Executable File

Execute the command: **cd <OpenSSL installation directory>\bin**

```
c:\>cd C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>
```

Example command: cd C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin

10.3.6 Create Server Private Key File for CA Server

Execute the command: **openssl genrsa -out <your working directory>\ServerKey.key 1024**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl genrsa -out c:\temp\MyCertificates\ServerKey.key 1024
Generating RSA private key, 1024 bit long modulus
..+++++
.....+++++
e is 65537 (0x10001)
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>
```

Example command: openssl genrsa -out c:\temp\MyCertificates\ServerKey.key 1024

10.3.7 Create the Certificate from the CA Server's Private Key

Execute the command: **openssl req -new -x509 -key <your working directory>\ServerKey.key -out <your working directory>\myCA.cer -days 3650 -subj /CN="<issuer name>"**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl req -new -x509 -key c:\temp\MyCertificates\ServerKey.key -out c:\temp\MyCertificates\myCA.cer -days 3650 -subj /CN="custom_CA_name"
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>
```

Example command: **openssl req -new -x509 -key c:\temp\MyCertificates\ServerKey.key -out c:\temp\MyCertificates\myCA.cer -days 3650 -subj /CN="custom_CA_name"**

10.3.8 Create Client Private Key File

Execute the command: **openssl genrsa -out <your working directory>\ClientKey.key 1024**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl genrsa -out c:\temp\MyCertificates\ClientKey.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
```

Example command: **openssl genrsa -out c:\temp\MyCertificates\ClientKey.key 1024**

10.3.9 Create the Client Signing Request (CSR)

Execute the command: **openssl req -new -key <your working directory>\ClientKey.key -out <your working directory>\CertReq.csr -subj /CN="<server_domain_name or ip_address>"**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl req -new -key c:\temp\MyCertificates\ClientKey.key -out c:\temp\MyCertificates\CertReq.csr -subj /CN="10.16.18.68"
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>
```

Example command: **openssl req -new -key c:\temp\MyCertificates\ClientKey.key -out c:\temp\MyCertificates\CertReq.csr -subj /CN="192.168.1.100"**

10.3.10 Create the Client Certificate based on the CSR, Server Certificate and CA Server's Private Key

Execute the command: **openssl x509 -req -days 3650 -in <your working directory>\CertReq.csr -CA <your working directory>\myCA.cer -CAkey <your working directory>\ServerKey.key -CAcreateserial -out <your working directory>\ClientCert.crt**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl x509 -req -days 3650 -in c:\temp\MyCertificates\CertReq.csr -CA c:\temp\MyCertificates\myCA.cer -CAkey c:\temp\MyCertificates\ServerKey.key -CAcreateserial -out c:\temp\MyCertificates\ClientCert.crt
Signature ok
subject=/CN=10.16.18.68
Getting CA Private Key
```

Example command: **openssl x509 -req -days 3650 -in c:\temp\MyCertificates\CertReq.csr -CA c:\temp\MyCertificates\myCA.cer -CAkey c:\temp\MyCertificates\ServerKey.key -CAcreateserial -out c:\temp\MyCertificates\ClientCert.crt**

10.3.11 Create a Temporary PKCS12 Keystore for Client Private Key and Client Certificate

The default password for the integration framework keystore is sapB1iP. The temporary PKCS12 keystore must have the same keystore password, as it is defined for the integration framework keystore.

Execute the command: **openssl pkcs12 -export -inkey <your working directory>\ClientKey.key -in <your working directory>\ClientCert.crt -out <your working directory>\keystore.pkcs12 -passout pass:<temporary keystore password>**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>openssl pkcs12 -export -inkey c:\temp\MyCertificates\ClientKey.key -in c:\temp\MyCertificates\ClientCert.crt -out c:\temp\MyCertificates\keystore.pkcs12 -passout pass:sapB1iP
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>
```

Example command: `openssl pkcs12 -export -inkey c:\temp\MyCertificates\ClientKey.key -in c:\temp\MyCertificates\ClientCert.crt -out c:\temp\MyCertificates\keystore.pkcs12 -passout pass:sapB1iP`

10.3.12 Change Directory to Integration Framework Java Runtime Path

Execute the command: **cd <Integration Framework installation directory>\<sapjre folder>\bin**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>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>
```

Example command: `cd c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin\`

10.3.13 Delete the Original Self-Signed Certificate from the Integration Framework Keystore

Execute the command: **keytool -delete -alias tomcat -keystore <Integration Framework installation directory>\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass <keystorepassword>**

```
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>keytool -delete -alias tomcat -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>
```

Example command: `keytool -delete -alias tomcat -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP`

10.3.14 Import Certificates from Temporary Keystore into the Integration Framework Keystore

Execute the command: **keytool -importkeystore -srckeystore <your working directory>\keystore.pkcs12 -srcstoretype PKCS12 -destkeystore <Integration Framework installation directory>\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -deststoretype JKS -deststorepass <Integration Framework's keystore password> -srcstorepass <temporary keystore password>**

```
C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin>keytool -importkeystore -srckeystore c:\temp\MyCertificates\keystore.pkcs12 -srcstoretype PKCS12 -destkeystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -deststoretype JKS -deststorepass sapB1iP -srcstorepass sapB1iP
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

Example command: `keytool -importkeystore -srckeystore c:\temp\MyCertificates\keystore.pkcs12 -srcstoretype PKCS12 -destkeystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -deststoretype JKS -deststorepass sapB1iP -srcstorepass sapB1iP`

10.3.15 Change Default Alias Name for the Integration Framework Keystore Certificate Entry

Execute the command: **keytool -changealias -alias 1 -destalias tomcat -keystore keytool -changealias -alias 1 -destalias tomcat -keystore <Integration Framework installation directory>\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore -storepass <Integration Framework's keystore password> -keypass <password defined for temporary keystore password>**

```
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>keytool -changealias -alias 1 -destalias tomcat -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP -keypass 1234
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>
```

Example command: `keytool -changealias -alias 1 -destalias tomcat -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP -keypass 1234`

10.3.16 Verify the Integration Framework Keystore Content

Execute the command: **keytool -list -keystore <Integration Framework installation directory>\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore -storepass <Integration Framework's keystore password>**

```
c:\Program Files (x86)\SAP\SAP Business One Integration\sapjre_32\bin>keytool -list -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP

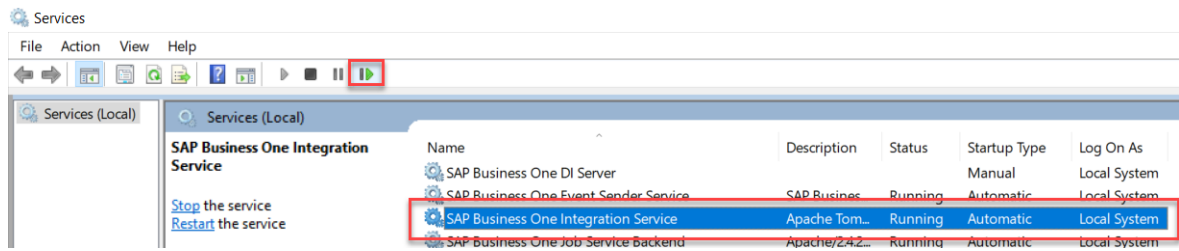
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

tomcat, 31.7.2018, PrivateKeyEntry,
Certificate fingerprint (SHA1): 11:BB:99:29:63:4F:3F:E7:56:7F:EA:BC:09:F6:54:AA:C5:CA:00:AB
```

Example command: `keytool -list -keystore "C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\keystore" -storepass sapB1iP`
 The keystore should contain a key entry with alias name tomcat and the date should be the creation date of the certificate.

10.3.17 Restart the SAP Business One Integration Service



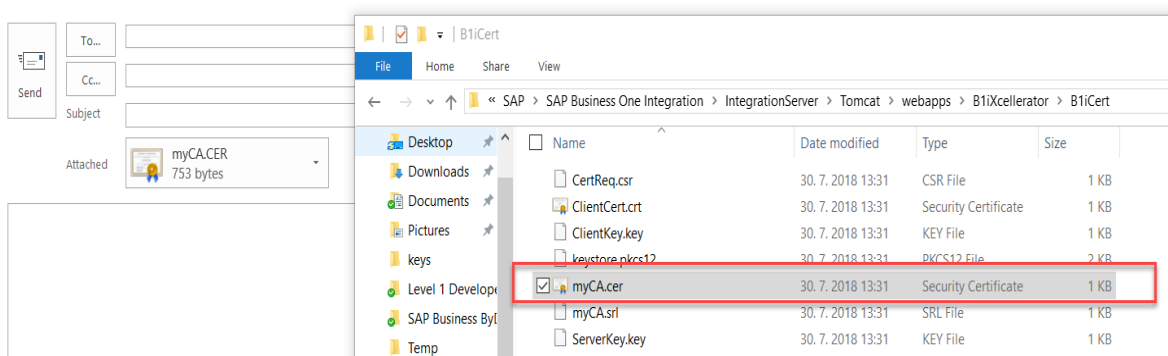
11. DEPLOY THE CERTIFICATE TO MOBILE DEVICE

11.1 Deploy a Certificate from a Trusted Third-Party Certification Authority (CA)

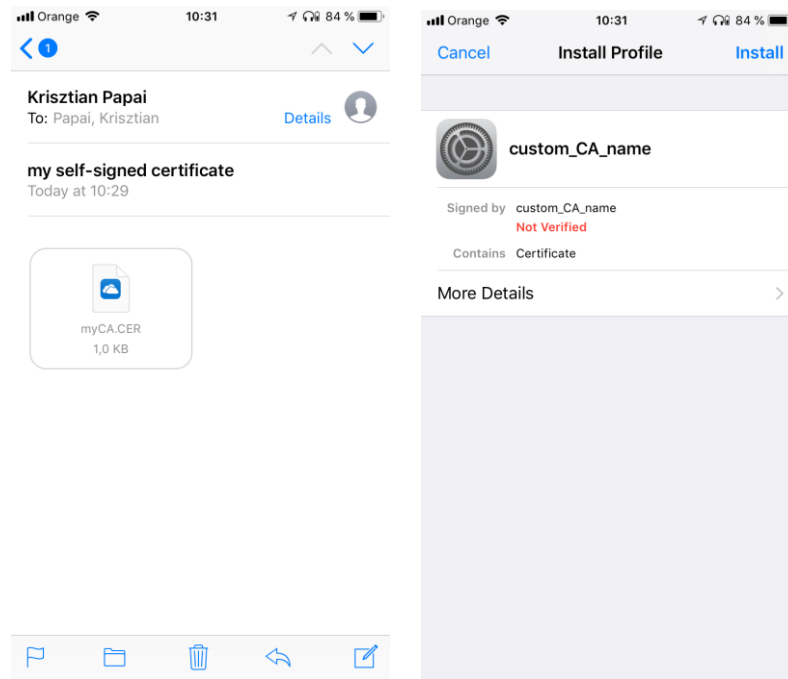
This type of certificate is not needed to be deployed to the mobile device, because the root certificate from the provider is already preinstalled into the mobile device's operating system.

11.2 Deploy Manually Created or Through Certificate Tool Certificate for iOS

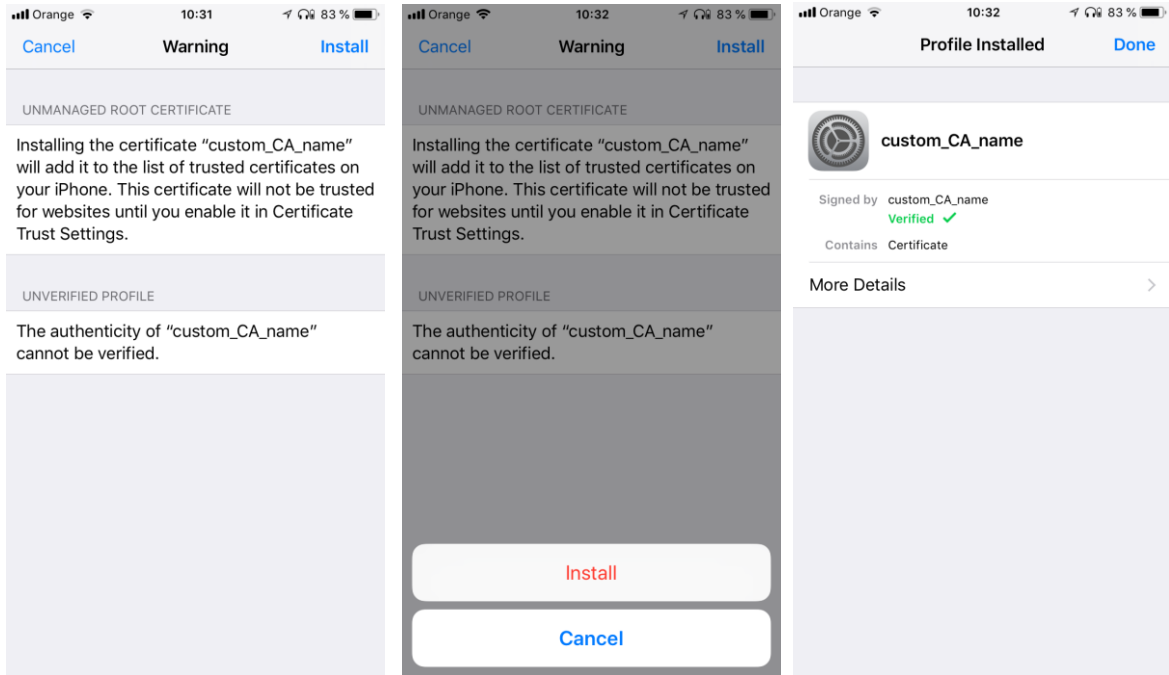
- Send the **myCA.cer** certificate generated by following the sections 11.2 and 11.3.7 via e-mail to the mobile device.



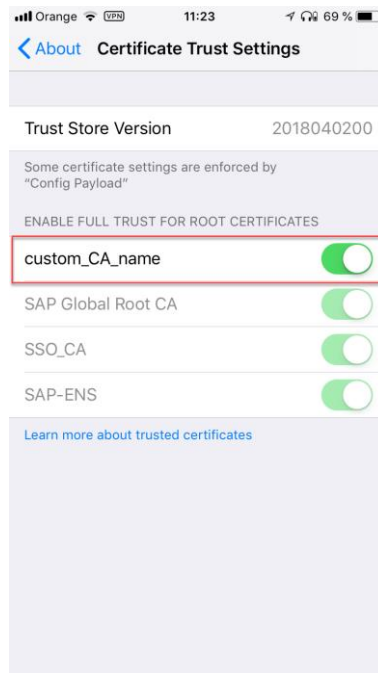
- Open the e-mail, click to the attached file and press the **install** button



- After entering your security code of your device, you can continue with the installation.

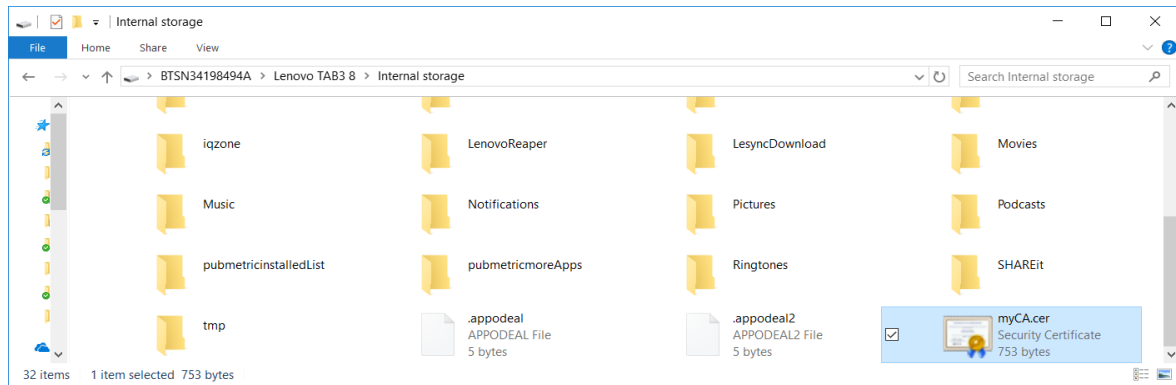


- Enable the certificate in the mobile device by navigating to *Setting* → *General* → *About* → *Certificate Trust Settings* and selecting the exact certificate.

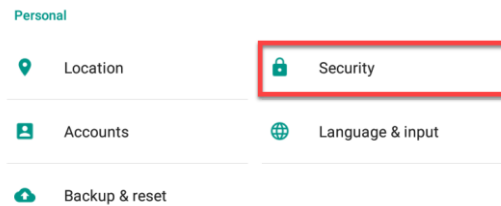


11.3 Deploy Certificate Manually Created of Through Certificate Tool for Android

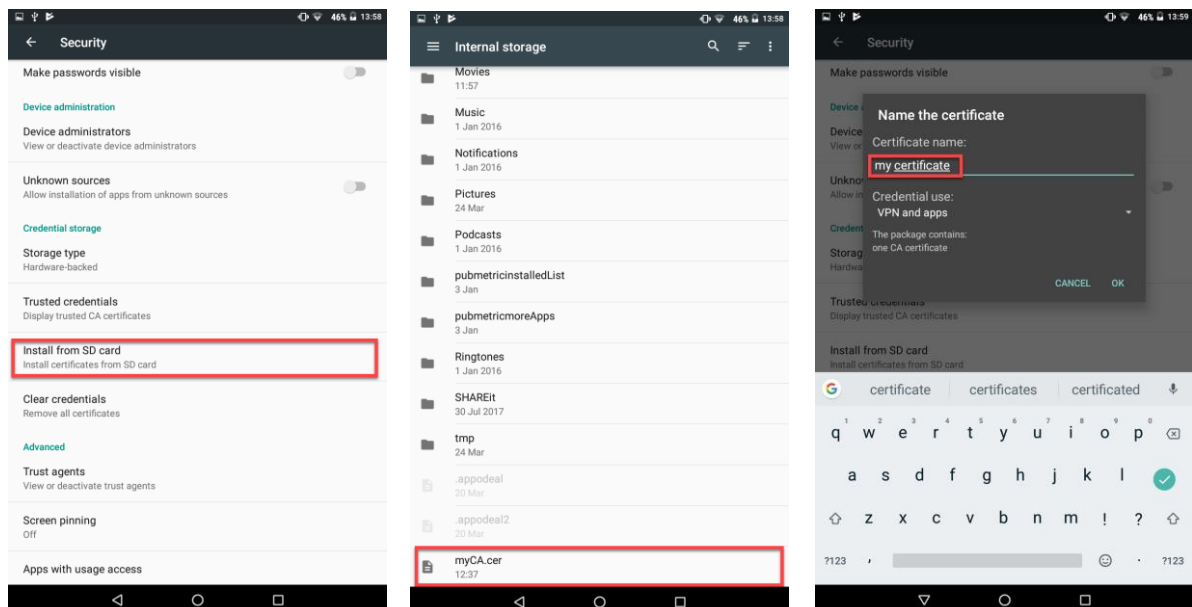
- Copy the **myCA.cer** certificate generated according chapters 11.2 and 11.3.7 to the mobile device internal or external storage (microSD)



- Tap the **Settings** icon on your Android device
- **Security** option in the **Personal** section



- Navigate to the **Credential Storage** → **Install from SD card** and install the myCA.cer certificate by defining the certificate name as well.



12. SCENARIO PACKAGE SETUP FOR MOBILE

The **sap.B1Mobile** scenario package for the SAP Business One mobile app communicates with the company database and the mobile app.


12.1 Deactivate the Scenario Package

- (1) (2) In the integration framework, choose *SCENARIOS* → *Setup*.
- (3) In the *Scenario Package Identifier* field, select the **sap.B1Mobile** value clicking the [...] button.
- (4) Press the **[Deactivate]** button.

The screenshot shows the SAP Integration Framework interface. The top navigation bar includes COCKPIT, SLD, MAINTENANCE, SCENARIOS (highlighted with a red box and '1'), MONITORING, TOOLS, and HELP. On the left, the 'Scenarios' menu is open, with 'Setup' highlighted (red box and '2'). The main area displays the 'Scenario Package Setup' for 'sap.B1Mobile'. The 'Scenario Package Identifier' field is highlighted with a red box and '3'. At the bottom, the 'Deactivate' button is highlighted with a red box and '4'. The table below shows the following data:

Field	Value
Scenario Package Identifier	sap.B1Mobile
Version Number	2.0.0
Status	active
Scenario Steps	119 of 119
Sender System Types	ws
Receiver System Types	
Activate Job List	<input type="checkbox"/>
Actions	Steps Sender Receiver Deactivate Data Mgt. Setup Tools

12.2 Set the Secured Transport for the Scenario Package

- (1) (2) In the integration framework, choose *SCENARIOS* → *Authentication*.
- (3) In the *User-Defined Authentication Identifier* field, select the **sap.B1Mobile** value clicking the [...] button.
- (4) In the *Enforce Secure Transport* field, choose the value **true** clicking the [...] button.
- (5) Press the  button to save the settings

The screenshot shows the SAP Integration Framework interface. The top navigation bar includes COCKPIT, SLD, MAINTENANCE, SCENARIOS (highlighted with a red box and '1'), MONITORING, TOOLS, and HELP. On the left, the 'Scenarios' menu is open, with 'Authentication' highlighted (red box and '2'). The main area displays the 'Scenario User-Defined Authentication' settings for 'sap.B1Mobile'. The 'User-Defined Authentication Identifier' field is highlighted with a red box and '3'. The 'Enforce Secure Transport' field is highlighted with a red box and '4'. At the bottom, the save icon is highlighted with a red box and '5'. A 'Success' dialog box is visible in the foreground, indicating 'Configuration saved'. The table below shows the following data:

Field	Value
User-Defined Authentication Identifier	sap.B1Mobile
Handover of User Name and Password	
User List	
Session Timeout	10
Enforce Secure Transport	true
On_Session xsl	
On_Authenticate bfd	GetUsrPwd bfd
On_Authenticate Event bfd	
Authentication bfd	Authenticate bfd
Actions	Save ...

12.3 Activate the Scenario Package

- (1) (2) In the integration framework, choose *SCENARIOS* → *Setup*.
- In the *Scenario Package Identifier* field, select the **sap.B1Mobile** value clicking the [...] button
- Press the **[Activate]** button
- Press again the **[Activate]** button on the Scenario Setup Result form
- At the end the **[OK]** button will force the final phase of the scenario package activation

SAP Integration solution for SAP Business One - Integration Framework

COCKPIT SLD MAINTENANCE **SCENARIOS** MONITORING TOOLS HELP

Scenarios

- Business Processes
- Package Design
- Step Design
- Setup**
- Control
- Reports
- Import
- Export
- Authentication

Scenario Package Setup

Scenario Package Identifier	sap.B1Mobile
Version Number	2.0.0
Status	design
Scenario Steps	119 of 119
Sender System Types	ws
Receiver System Types	
Activate Job List	<input type="checkbox"/>
Actions	<input type="button" value="Steps"/> <input type="button" value="Sender"/> <input type="button" value="Receiver"/> <input type="button" value="Activate"/> <input type="button" value="Data Mgt."/> <input type="button" value="Setup Tools"/>

Integration solution for SAP Business One - Integration Framework - Scenario Setup Result

Identifier	sap.B1Mobile
Setup	ok
Status	ok



Notification

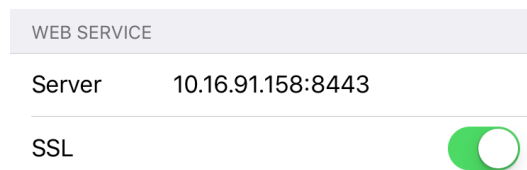
Preparation completed.
Activate scenario package?

OK Cancel

13. CONFIGURE CONNECTION IN SAP BUSINESS ONE MOBILE APP

13.1 SAP Business One Mobile App Setup for iOS

- Tap the *Settings* icon on your iOS device 
- Tap the *SAP Business One* entry  Business One >
- Define *Web Service* settings
 - Enter the Server address and port (either IP or server name) in the format <server>:<port> into the **Server** field. The default https port of the integration framework is **8443**
 - Turn on the **SSL** switch

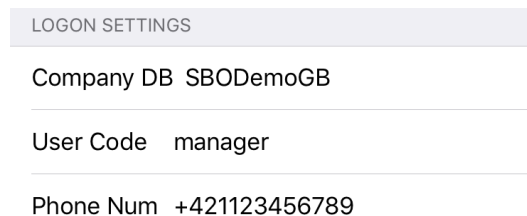


WEB SERVICE

Server 10.16.91.158:8443

SSL

- Define the *Logon Settings*
 - Enter the company database name or schema name into the **Company DB** field
 - Enter in the **User Code** field the exact SAP Business One user code
 - Define the **Phone Number** of the user. The phone number must match the number defined in the *User Master Data* form. Please refer to the [chapter 8](#) in this document.




LOGON SETTINGS

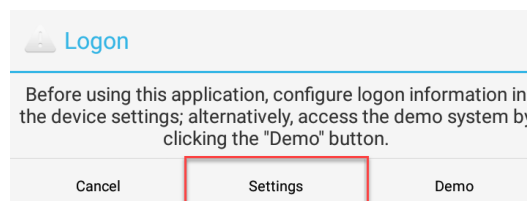
Company DB SBODemoGB

User Code manager

Phone Num +421123456789

13.2 SAP Business One Mobile App Setup for Android

- Tap the *SAP Business One* icon on your Android device. 
- Tap the *Setting* button

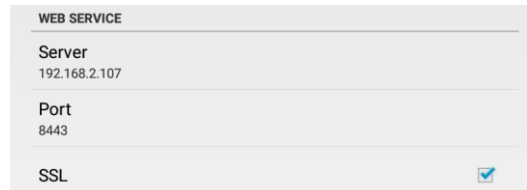


Logon

Before using this application, configure logon information in the device settings; alternatively, access the demo system by clicking the "Demo" button.

Cancel Settings Demo

- Define *Web Service* settings
 - Enter the **Server** address (either IP or server name)
 - Enter the **Port** number. The default https port of the integration framework is **8443**
 - Check the **SSL** checkbox



WEB SERVICE

Server
192.168.2.107

Port
8443

SSL

- Define the *Logon Settings*
 - Enter the company database name or schema name into the **Company DB** field
 - Enter in the **User Code** field the exact SAP Business One user code
 - Define the **Phone Number** of the user. The phone number must match the number defined in the *User Master Data* form. Please refer to the [chapter 8](#) in this document.



LOGON SETTINGS

Company DB
SBODemoGB

User Code
manager

Phone Num
+421123456789

Device ID
3N1G0Y2Z3Y8D0R287P7Z5SS8P



14. REFERENCES

SAP [Online Help](#) – Working with SAP Business One Mobile App for iOS

SAP [Online Help](#) – Working with SAP Business One Mobile App for Android

SAP Note [1602674](#) – SAP Business One mobile app for iOS - Troubleshooting and Compatibility Information (login required)

SAP Note [1924930](#) – SAP Business One mobile app for Android - Troubleshooting and compatibility (login required)

SAP Note [2019275](#) – SAP Business One mobile app for iOS or Android require a valid SSL certificate (login required)

Apple Support [HT204132](#) – Lists of available trusted root certificates in iOS

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.