SAP Business One

PUBLIC

Administrator's Guide for the Integration Component

Release Family 8.8

Applicable Release:

SAP Business One 8.82

All Countries

English

September 2011

Table of Contents

1. Introduction

The Administrator's Guide for the integration component for SAP Business One provides a central point of reference, both before and during the technical implementation of the component.

Prerequisites

To administer the installed SAP Business One integration component, you need to have SAP Business One 8.82 and the integration component installed.

 Note

For information about installing the integration component, see section *Installing Integration Component for SAP Business One* in *Administrator's Guide for SAP Business One* (AdministratorGuide_SQL.pdf).

 Note

To avoid conflicts with TCP/IP ports used on the SAP Business One Server machine, make sure to read SAP Note 1536119 *(Port assignment in the B1 Integration Component landscape.)*

Section 2.7 of this document describes how to change two of the ports.

 Note

For the latest information, see the central SAP Note 1477984.

See also:

For information about dashboards and improvements in 8.81, see SAP Note 1549326 *(Dashboards and Integration Component: Improvements ver. 8.81)*.

For information about cockpits, see *Working with the Cockpit* (attached to SAP Note 1471016).

For information about creating dashboards, see *How to Develop Your Own Dashboards for SAP Business One.*

For additional documentation about operations, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations.*

For information about the dashboard services in the integration framework, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Scenarios* → *Scenario Package Control* → *Report* → *sap.Xcelsius* → *Documentation.*

 Note

After the installation is completed, use the **`B1iadmin`** user and the password provided during the installation. Note that the user **`B1iadmin`** is case sensitive.

2. Performing Post-Installation Activities

2.1. Maintenance and Monitoring

Integration framework is implemented as a Microsoft Windows service under the identifier “SAP Business One Integration Service” and starts automatically after a successful setup.

NOTE

You find the services by choosing *Start* → *Control Panel* → *Administrative Tools* → *Services.*

For monitoring purposes, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Monitoring*. Here you can use the *Message Log*, access the *Error Inbox*, and use other monitoring features.

NOTE

For optimal performance, the *Message Log* is deactivated by default. SAP does not recommend activating it in a productive environment.

For additional documentation, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations, chapter 2.*

For maintenance purposes, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration Framework*, and then choose *SLD* (System Landscape Directory), *Maintenance,* or *Scenarios*.

SAP recommends that you check the performance aspects in the related documentation, as follows:

Choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations, chapter 5*.

For information about the dashboard services in the integration framework, choose *Scenarios* → *Scenario Package Control* → *Report* → *sap.Xcelsius* → *Documentation* and then choose the document *vpac.pdf*, and refer to chapters 3 and 4.

In the case where the Integration framework is installed on top of an existing SAP Business One (B1) installation, and this SAP Business One installation is connected as a subsidiary to an SAP Business One integration for SAP NetWeaver (B1iSN) server, it is necessary to add entries to the Event Dispatcher manually. Refer to the latest B1iSN documentation for details of how to pass the SAP Business One events, relevant for your subsidiary integration processing, to your centralized B1iSN server, and how to register B1 events in the Event Dispatcher.

Note

RAM for Tomcat (64 Bit Windows):

When using 64 Bit Windows, to improve performance when larger amounts of data or a high number of parallel accesses need to be handled, you can assign more RAM to the Integration framework server by double-clicking the *tomcat6w.exe* on your local drive

C:\Program Files\SAP\SAP Business One Integration\B1iServer\tomcat\bin\tomcat6w.exe, if C:\Program Files\SAP\SAP Business One Integration is the installation directory. In *SAP Business One Integration Service Properties*, select the *Java* tab, and increase the *Maximum memory pool* amount as follows:

Tomcat supports max. 1024 MB on a 32 Bit OS, which is also the default setting. On a 64 Bit OS, the *Maximum memory pool* amount for Tomcat is 2048 MB.

Note

In the SLD (system landscape directory) make sure to keep the entry for *b1Server* in the SAP Business One system in sync with *associatedSrvIP* for the *HAnyforXcelsius* and *WSforMobile* systems.

2.2. Licensing

Ensure that the user *B1i* has been assigned with the following two (free) licenses:

- B1iINDIRECT_MSS
- B1i

No further license is required for the *B1i* user.

Note

These licenses should be assigned automatically to user *B1i* starting with B1 8.8 PL15 and B1 8.81 PL00 when initially importing the license file.

2.3. Technical User B1i

A user with code *B1i* is created for every new company database. Ensure that the password for this user is properly initialized since it is required for B1 Integration Component to connect to SAP Business One, for example for authentication when using dashboards.

It is recommended to change the password for the *B1i* user through the user “Manager” or another super user. Starting with this version it is not necessary to connect with user *B1i* and change the password again.

This action can also be performed after the installation is completed.

2.4. Activating Dashboard Widgets for the Cockpit

From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *General Settings*.

Note

If the *B1i* user password is not correct or licenses are not properly assigned to this user, the error *401 not authorized* will be displayed in the Dashboard widgets.

To fix this, correct the *B1i* user password in the SLD (system landscape directory) within the Integration framework and ensure licenses are assigned as specified in section Licenses in this document.

Note

In case Dashboards have been activated, but not deployed properly within the SAP Business One integration component (or more precisely, within the B1i Server), the error *404 file not found* mentioning the word *DASHBOARD* is displayed.

To fix this, check that all services mentioned in the *Installation Guide for the Integration Component* are running. First deactivate the Dashboard widgets, logoff and logon again, and activate the Dashboard widgets.

Note

Ensure that Adobe Flash Player 10.0 is installed on the client workstation to support the display of dashboards.

See also:

For information about cockpits, see *Working with the Cockpit* (attached to SAP Note 1471016).

For information about creating dashboards, see *How to Develop Your Own Dashboards for SAP Business One.*

For troubleshooting information, refer to SAP Note 1495563 *(SAP Business One Integration component troubleshooting guide).*

2.5.Upgrading

If any components of SAP Business One integration for SAP NetWeaver (B1iSN) were previously installed on your server, you need to uninstall them manually before installing the Integration Component delivered with SAP Business One 8.81. This step is required due to compatibility reasons. The integration component installer supports integration component upgrades.

For more information about uninstalling components of B1iSN, see the *SAP Business One integration for SAP NetWeaver Installation and Upgrade Guide*.

2.6.B1 Event Subscriber UI

You access the B1 Event Subscriber from the SAP Business One integration framework (B1iF) main page by choosing *Maintenance* → *Cfg B1 Event Subscriber*.

B1 Event Subscriber is the main page of the *B1 Event Subscriber UI:*

Button Name	Purpose
Create	Create a new remote B1i node to connect to a remote B1i server.
Edit	Edit a selected remote B1i node.
Delete	Delete a selected remote B1i node.
Subscriber	Maintain the subscriber of the selected remote B1i node.


Note

If the integration framework (B1iF) is newly installed, then there is no remote B1i node.

Creating a remote B1i node

To add a new remote B1i node, choose *Create*. The *Remote B1i* web page dialog is displayed. Enter the following values for the parameters listed:

Field Name	Description	Sample Value	Remark
TargetHost	The server host of the remote B1i, can be either the server name or IP address	“Pvgd50073426a” or “10.58.0.25”	This is the primary key of the remote B1i, so it cannot be empty or duplicated. Once created, it cannot be changed anymore.
TargetPort	The server port of the remote B1i	8080	
Protocol	The protocol that is used to connect to the remote B1i	http / https	
ProxyHost	If you need a proxy to connect to the remote B1i, then you need to maintain the proxy host here.	proxy.wdf.sap.corp	
ProxyPort	The port number of the proxy host.	8080	
Authentication	The authentication mode that is used by the remote B1i.	basic	B1iSN 8.8 and most B1iSN 2007 patches use basic authentication. Only B1iSN 2007 PL00 and PL01 use Filter authentication.
Target B1i User	The user name to logon to the remote B1i.	B1iadmin	
Target B1i Password	The password for the B1i user.		
SSL TrustStore Path	The path of the SSL TrustStore.		Only to be specified if protocol is https
SSL TrustStore Password	The password of the SSL TrustStore.		Only to be specified if protocol is https

When you have entered all necessary values, save your entries. A new remote B1i node is created.

If you wish to cancel this operation, choose *Cancel*.

Note

When a new remote B1i node is created, a default subscriber is also created inside this remote B1i node with all filter criteria set to “*”. This means, all B1 events coming to this local B1i server will be sent to the remote B1i server as well.

Editing a remote B1i node

To edit a remote B1i Node, first select a remote B1i node by clicking the radio box in front of it, and then choose *Edit*. Edit the parameters in the *Remote B1i* dialog, and save your entries.

If you wish to cancel this operation, choose *Cancel*.

Note

The *TargetHost* field is not editable.

Deleting a remote B1i node

To delete a remote B1i node, first select a remote B1i node by clicking the radio box in front of it, and then choose *Delete.* Confirm by choosing *OK*. The remote B1i node is deleted.

Editing the subscriber of a remote B1i

A subscriber is a B1i application which subscribes B1 events. In this Event Subscriber UI the subscriber is hard-coded to the entry point of the remote B1i’s Event Dispatcher, which is responsible for receiving and dispatching incoming B1 events.

To edit a remote B1i node’s subscriber, first select a remote B1i node by clicking the radio box in front of it, and then choose *Subscriber*.

In the *Edit Subscriber* web page dialog, you can maintain the filter criteria:

Field Name	Explanation	Sample Value
SysId	The SysId of a local B1i’s SLD. Its value can be either “*” or a concrete SysId. If specified as “*”, then all incoming B1 events will pass; if specified as a concrete SysId, then only the B1 events from this SysId can pass.	“0010000100” or *
Local object type id	The B1 object id. Its value can be either “*” or a concrete object id, or an object id list separated by “,”.	“2” or “2,4,17” or “*”
Event task	The transaction type (explained as a “task”) of the B1 event, can be either * or one or more of the following concrete values: A (add), U (update), C (cancel), L (close), and D (delete)	“A” or “AUC” or “*”

To add filter criteria, choose *Add Condition*.

To delete filter criteria, first select the check box button in front of it, and then choose *Delete Condition*.

To save the subscriber, choose *Save*.


Note

If you delete all filter criteria, then the result is the same as disabling this remote B1i node. No B1 event will be sent to the remote B1i server.

2.7. Configuration of B1i Server Ports

B1i Server uses ports 8080 and 8443 (among others).

In case these ports are already used by other applications, it is possible to change the ports.

To change the ports, changes are required in three places in the following order:

1. Stop the *SAP Business One EventSender Service*.
2. Choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Maintenance* → *Cfg Runtime* to change the ports as required.
3. Change the server.xml file for Tomcat – for example at: C:\Program Files (x86)\SAP\SAP Business One Integration\B1iServer\Tomcat\conf


Note

Make sure to change only the values of the ports.
Changing other data may have severe impact on server security.

4. Restart the *SAP Business One Integration Service*.
5. Choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *EventSender* → *Setup* and follow the steps, change the B1i Server port, and test the connection.
6. Restart the *SAP Business One EventSender Service*.
7. Change the properties for the menu entry, using the correct port number: *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework.*

2.8.RFQ Scenario with Online Quotation

As of SAP Business One 8.81 PL06, SAP Business One customers can send purchase quotations to business partners electronically. The process of sending and gathering purchase quotations is implemented in SAP Business One using the integration component in a process called the RFQ process. This process allows customers to generate a web-based quotation submission form which is hosted on the B1i Server. Business partners can directly submit their offers over this web-based interface to the buyer. This section describes the process itself, how to customize certain parts of the process, and how maintain it.

Prerequisites

To administer the SAP Business One integration component, you need to have SAP Business One 8.81 PL06 and the integration component installed.

Note

For information about installing the integration component, see section *Installing Integration Component for SAP Business One* in *Administrator's Guide for SAP Business One* (*AdministratorGuide_SQL.pdf*).

1. After you have successfully installed SAP Business One, the SAP Business One administrator or user (SAP Business One user) must make sure that business partner details are maintained in the system. Most importantly the email address of the contact person from the business partner.
2. The current version (8.81 PL06) supports language-dependent settings for sending emails to business partners. The following section describes how to customize language-dependent settings in the respective languages.

2.8.1. Performing Post-Installation Activities

2.8.1.1. Contact Details in SAP Business One

The RFQ process is split in two child processes. One is generating a purchase quotation that is automatically sent to the business partner. In the second step, the original purchase quotation document is updated by the business partner. Contact details of the Business partner and the SAP Business One user play a vital role for the successful execution of the RFQ process.

NOTE

You can find the business Partner contact details by choosing *Modules* → *Business Partners*. Then choose the business partner code, and select the contact person and edit the email address or add new contacts. Ensure that the default contact person details are maintained. Choose *Modules* → *Administration* → *General Settings* → *Users*, to select the SAP Business One user, and to maintain the user's contact details.

NOTE

If the email address of the contact person is not provided and the checkbox *Create Online Quotation* is enabled, the SAP Business One user will get a message in the *Alerts* box about this error. If the email address is not correct, outdated, or if the recipient has an active out of office alert, the SMTP email client (for example, Outlook Express) would be notified of this error.

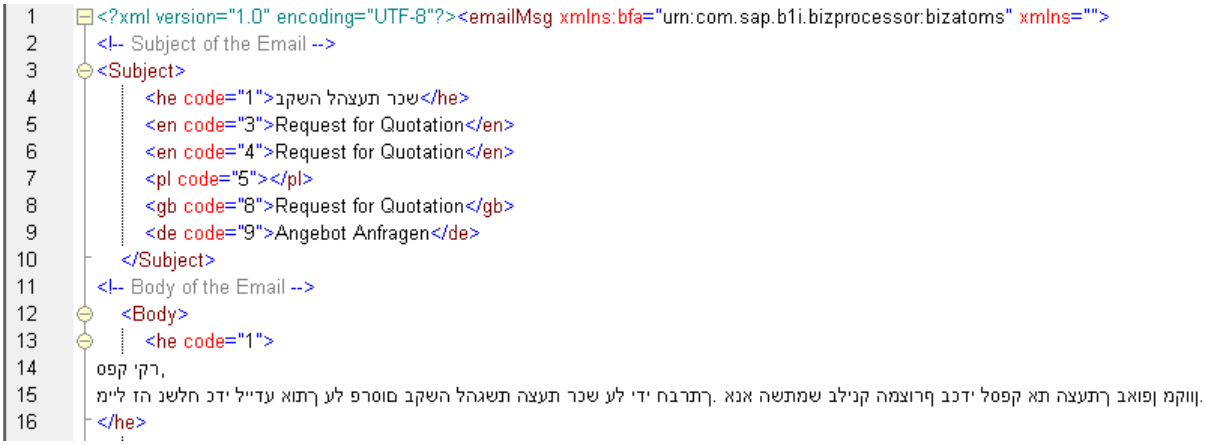
2.8.1.2. Email Text in the Integration Component

When creating a new purchase quotation, the customer has the option to send the quotation to the respective partner electronically. This option is disabled by default. It can be enabled by selecting the check box *Create Online Quotation* under the *Logistics* tab of the *Purchase Quotation Screen*. The RFQ process is designed to be triggered once this check box is selected, and the purchase quotation is created. The RFQ process will take certain parts of the document and generate a web page that will be hosted in the B1i server BizStore. Once this page is generated, the page URL is wrapped along with some text and emailed to the business partner contact person. The contents of this email will be derived from a XML template that is available for modification in the BizStore. Customers can change the contents of this email by adding or editing their own text in their own respective language(s).

Note

Do not change the name or the location of the XML template in the BizStore.

To open the email document EmailContent.xml, use a WebDav client such as Microsoft Windows Explorer (Windows XP and above) and open the file under the BizStore path http://YOUR_B1i_SERVER:PORTl//B1iXcellerator/exec/dummy/com.sap.b1.webapps/PurchaseQuote using a text editor. Alternatively, you can open the document using an XML editor and browsing to the BizStore path mentioned above.



```
<?xml version="1.0" encoding="UTF-8"?><emailMsg xmlns:bfa="urn:com.sap.b1i.bizprocessor:bizatoms" xmlns="">
<!-- Subject of the Email -->
<Subject>
    <he code="1">שכר תעצהל השקב</he>
    <en code="3">Request for Quotation</en>
    <en code="4">Request for Quotation</en>
    <pl code="5"></pl>
    <gb code="8">Request for Quotation</gb>
    <de code="9">Angebot Anfragen</de>
</Subject>
<!-- Body of the Email -->
  <Body>
    <he code="1">
רקי קפס,
.ווקמ ופואב רתעצה תא קפסל ידכב חרוצמה קנילב שמתשה אנא .רתרבח ידי לע שכר תעצה תשגהל השקב סוסרפ לע רתוא עדייל ידכ חלשנ הז ליימ
</he>
```

The XML template can be accessed through the C*ontrol Center* → *Maintenance* → *BizStore Download* menu path of the Integration Framework in the package *com.sap.b1.webapps.PurchaseQuote*. The template is called *EmailContent.xml* and contains four major parts:

Language Culture Name – This is a two letter ISO name as defined in http://msdn.microsoft.com/en-us/library/ee825488%28v=cs.20%29.aspx Take the first two letters written in lower case only. The language code attribute is the one that is available in SAP Business One in the table OLANG for language codes.

<emailMsg> <subject> <**en code**=”3”></en>

Subject – This is the subject of the email sent. In English the subject is *“Request for Quotation”*. Take care to enter your customized text for the subject between the corresponding culture names.

<emailMsg> <**Subject**> <en code=”3”>Request for Quotation</en>**</Subject>**

Body – This is the body text of the email sent along with the link to the web-based purchase quotation form. Take care to enter your customized text for the body between the corresponding culture names.

<emailMsg> <**Body**> <en code=”3”>Some text</en>**</Body>**

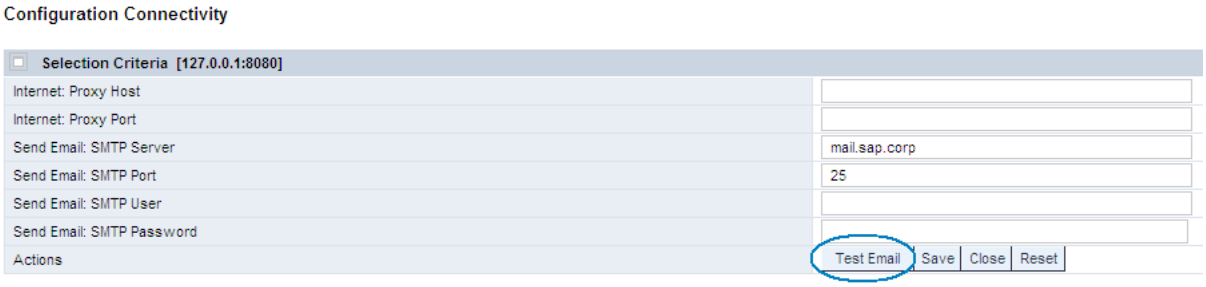
Closing – This is the closing greeting of the email sent. Take care to enter your customized text for the subject between the corresponding culture names.

<emailMsg> <**Closing**> <en code=”3”>Some text</en>**</Closing>**

2.8.1.3. Server Information in the Integration Component

You must specify the connectivity parameters and the runtime parameters in the Integration Component.

1. Start the Integration Framework and go to *Maintenance* → *Cfg Connectivity*.
2. Specify the SMTP server and port details. Without these details, an email would not be sent to the business partner. You might need to specify the user and password if the SMTP server requires authentification. Installations after patch level 07 have the possibility to test the connectivity to this server with the provided *Test Email* button.



3. Specify *Maintenance* → *Cfg Runtime* for the HTTP port and the B1i Server name.

> **Note**
>
> If the integration framework (B1iF) is newly installed, there is no remote B1i node. Refer to the *Administrator's Guide for the Integration Component* on how to configure the B1i Server to receive events from the SAP Business One system. You must activate the EventSender for the particular company database.

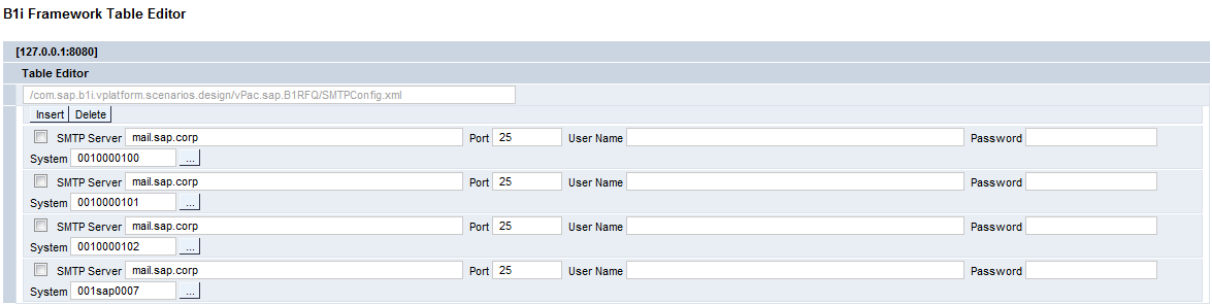
> **Note**
>
> When a new remote B1i node is created, a default subscriber is also created inside this remote B1i node with all filter criteria set to “*”. This means that all B1 events coming to this local B1i server will be sent to the remote B1i server as well.

Valid at 8.81 PL09

You can define the SMTP server properties for individual scenarios:

1. Go to *Scenarios* → *Setup* → *Data Mgt*.
2. Choose the document *SMTPConfig.xml*.

   A window opens that allows you to define the SMTP settings for this particular scenario.



3. Choose the *System ID* from the *SLD*.
4. Enter appropriate parameters for the SMTP Server port, and the associated user credentials for this particular system.
5. Save your changes. The RFQ Scenario will now use these details when sending e-mails.

2.8.1.4. Custom Logo on the RFQ template

Valid at 8.81 PL09

If required, you can change the SAP Business One logo on the html page viewed by the vendor.

To change the SAP Business One logo:

1. Create a folder called *rfq* in the `<B1i installation folder>\Tomcat\webapps\B1iXcellerator` folder.
2. Create a PNG file containing your logo with the name *logo.png* (note that you must use lower case letters only for the file name).
3. Copy the file containing your logo to the folder `<B1i installation folder>\Tomcat\webapps\B1iXcellerator\rfq`.

   For example, `C:\Program Files (x86)\SAP\SAP Business One Integration\B1iServer\Tomcat\webapps\B1iXcellerator\rfq\logo.png`

When you create a new purchase requisite, your logo will be added to the HTML page viewed by the vendor.

2.8.2. Maintenance

Once the purchase quotation has been sent, the business partner fills it out and submits it using the UI available in the web page. Data is parsed and directly updated in the existing purchase quotation document on reception.

Simultaneously, a message alert is created in the SAP Business One user's inbox. The alert is linked to the respective purchase quotation document. Clicking on this message would then open the purchase quotation document.

The process remains the same when generating bulk quotations using the Wizard. The BizStore *com.sap.b1.webapps.PurchaseQuote.Data* stores the generated purchase quotations that are visible to the business partner. A SAP Business One Administrator can delete old requests from this folder using a *WebDav* client.

Note

For more information, see the chapter *Security Aspects Related to the RFQ Scenario with Online Quotation* within this guide.

3. Managing Security

This section explains how to implement a security policy and provides recommendations for meeting security demands. Choose *Start → All Programs → Integration solution for SAP Business One → Integration framework,* and then choose *Help → Ref 04 – Operations, chapter 6.*

3.1. Secure Deployment and Operation of Integration framework

3.1.1. Deployment

Once Integration framework is installed and deployed, it is necessary to protect the whole installation against unauthorized access and modification. This process begins with protecting the directories, where the Integration framework-related software parts (TOMCAT, Integration framework itself, and the operating system level configuration files) reside, against unauthorized modification and even read-access. Only the services that make up Integration framework need to have access to these files; end users and even Integration framework-level administrators do not.

This prevents the unintended modification of Integration framework (for example, for the purposes of spying out data or changing its behavior) through the replacement of some software parts with forged ones (for example, replacing a regular database driver with a forged version that is put in place solely to fraudulently retrieve database credentials).

As another measure, the changing of the password of the Integration framework default user (**`B1iadmin`**) to an individual value is enforced during installation. All passwords within Integration framework are stored in an encrypted manner (whether in configuration files at the operating system level or in configuration documents based on the database).

To further enhance the security level, it is possible to specify a private key which will be used to encrypt passwords at in the file enckey.cfg which is located for example at: C:\Program Files (x86)\SAP\SAP Business One Integration\B1iServer\Tomcat\webapps\B1iXcellerator.

 NOTE

By installation default:

- Administrative Web access is limited to the local machine only. After installation, it is possible to manually allow access by remote machines by changing the particular setting in the operating system configuration file (Xcellerator.cfg).

  For additional documentation, choose *Start → All Programs → Integration solution for SAP Business One → Integration framework,* and then choose *Help → Ref 04 – Operations, chapter 6.2.*

- WebDAV-based access to BizStore content is disabled. SAP does not recommend enabling this kind of access for productive systems, as this is typically needed for development systems only.

  For additional documentation, choose *Start → All Programs → Integration solution for SAP Business One → Integration framework,* then go to *Help → Ref 01 – Dev Environment, chapter 3.*

3.1.2. Transport Level Security

3.1.2.1. HTTP/WebService/WebDAV Clients to Integration framework


RECOMMENDATION

SAP recommends, but does not enforce, the use of HTTPS.


NOTE

For additional documentation, choose *Start → All Programs → Integration solution for SAP Business One → Integration framework,* and then choose *Help → Ref 04 – Operations, chapter 6.3.*

All necessary preparation for basic HTTPS support is done during the installation of Integration framework. This means that a self-signed server-side certificate is generated in which the issuer is called “B1iP”. Consequently, because the certificate is self-signed, a Web browser-based client raises a security warning when connecting to the Integration framework server for the first time. SAP recommends letting the browser accept this certificate for future use so that such warnings are no longer issued.

Alternatively, the customer can purchase certificates issued by a well-known certification authority.


NOTE

At this time, the use of HTTPS in Integration framework is intended only for plain transport-level security purposes. Neither client authentication nor server authentication through HTTPS is supported.

3.1.2.2. SAP Business One to Integration framework

This transport level is comprised of three components:

3.1.2.2.1. Event-Sender Calling Integration framework Through HTTP(S)

SAP recommends configuring the event sender to use HTTPS. The reason for this is that authentication information is passed on by the event sender; however, the data passed over is non-critical. It is just information about changed objects but not the data of these objects. On the other side, because event sender communication typically happens inside the intranet, the need for protection through HTTPS might not be too strong when working within a local network or via VPN.

3.1.2.2.2. Integration framework Calling the DI Proxy Through JAVA RMI

JAVA RMI is a TCP/IP-based protocol used for remote object communication between Java programs.

The Integration framework DI adapter once used this protocol in order to communicate with the assigned proxy. Currently, there is no encryption of the data and connection credentials passed on to SAP Business One. It is possible to tunnel RMI communication through HTTP for when firewalls become an issue. (However, it is not possible to tunnel it through HTTPS.) As this communication also typically happens within the intranet, or through VPN, on remote communication, this should not be a critical issue. SAP does not recommend exposing the plain communication between the DI adapter and the proxy to the intranet without using a VPN.

NOTE

For future releases, it is also planned to secure the RMI communication through SSL (secure socket layer) TCP/IP communication.

3.1.2.2.3. Communication from DI API to Database

DI API communicates with the database through the native database transport wire-level protocol. As this communication also typically happens in the intranet, or through VPN, on remote communication, this should not be a critical issue. SAP does not recommend exposing the plain communication between the DI adapter and the proxy to the intranet without using a VPN. From a performance perspective, a remote communication between DI API and the database is not recommended.

3.1.2.3. Communication Between SAP ERP and Integration framework

For communication with SAP ERP, Integration framework uses SAP's JCO (java connector), which in turn uses SAP's RFC technology for communication. Any transport level security measures have to be taken at the RFC level. In order to secure RFC communication, customers can purchase third-party encryption solutions to use with SAP ERP. As this communication also typically happens in the intranet, or through VPN, on remote communication, this should not be a critical issue. SAP does not recommend exposing the plain communication between SAP ERP and Integration framework to the intranet without using a VPN.

3.1.2.4. Communication/Data Transfer Between Integration framework and File System Content

As data files used for data transfer by the various solutions typically contain data in an unencrypted and readable form, it is necessary to protect the directories in which they reside against unauthorized access (reading and modification).

For this purpose, to control the appropriate user-based access, it is necessary to use the means provided by the relevant operating system (Windows NT-based or newer). SAP does not recommend using FAT-based file systems as they do not allow user-access control.

3.1.3. Operation

3.1.3.1. Administration Concept

Integration framework is structured around a three-fold administration concept and provides the choice to implement the following concepts:

3.1.3.1.1. Operating System Level

Administrators at this level must have operating system level access rights to the Integration framework-based directories, and must be able to install and uninstall the application, as well as start/stop the appropriate services. There is no need for the administrators to have a deep working knowledge of Integration framework itself; they can see Integration framework as a "black box". There is also no need for them to know the database password (in fact, they do not even have a chance to become aware of it). Furthermore, these administrators do not need to have access to Integration framework itself (in fact, they have no chance of gaining access to Integration framework itself by knowing the environment, unless they unlawfully reconfigure parts of the Integration framework software in order to spy out the necessary information).

3.1.3.1.2. Database Administration Level

Database administrators are only in charge of making sure that the Integration framework database is operating on top. They have to maintain the database use (table space, recovery model, backup, and so on) and to enter/supply the intended database password on the Integration framework level where necessary. There is no need to give the password to another person, but database administrators can obtain access to the necessary screens in order to enter the database password themselves (for example, the database password prompt in the installer, or the connectivity credentials in the system landscape directory). Database administrators also do not need to be aware of the detailed functionality of Integration framework itself.

3.1.3.1.3. Integration framework Level

The Integration framework-level administrators act solely on the Integration framework level itself, using the HTTP-based access tools (for example, browser-based administration tools or WebDAV-based development tools).

They do not need file access at the operating system level (except if needed for a particular use case, such as DATEV-HR), or access to the Integration framework services. Nor do they need access to the database password.

Integration framework-level administrators all have the same access rights on the Integration framework level (every administrator can perform the same activities); however, they cannot repudiate their activities due to the non-repudiation measures taken by Integration framework (initiator concept): any activity in Integration framework - be it initiation of an execution or the storage of data - is flagged with the respective initiator who caused the activity. Therefore, any (malicious) change can be traced back to the person who caused it.

Recommendation

In order to make this concept work, create individual administrator accounts instead of using the default Integration framework administrator (**`B1iadmin`**). In addition, delete the initially created default Integration framework administrator (**`B1iadmin`**) entirely.

If the logon of a particular administrator fails on more than 5 consecutive attempts, the relevant administrator account is deactivated automatically and must subsequently be unlocked by another administrator.

If the last (or only) administrator account had been locked, or if the sole administrator has forgotten his password, it is necessary to start B1iP in safe mode. To do this, settings must be changed in the operating system configuration file (Xcellerator.cfg). For more information, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations, chapter 2.4.*

When B1iP operates in safe mode:

- Any adapters in use are disabled.
- Any user authentication in use is disabled.
- Access is only possible from the local machine, regardless of the settings in the normal mode.
- The relevant administration tools still work, and in turn, allow the assignment of a new password or the unlocking of an account.

3.1.4. Security Aspects Related to the DATEV-HR Solution

Since personal data is exported, maximum levels of data security and sensitivity are required.

The DATEV-HR scenario generates employee data for DATEV eG out of SAP Business One data that is then provided in a specified directory of the file system. Make sure that these files are provided in a folder to which only authorized persons have access.

Ensure that the Integration framework administration screens are accessible to authorized persons only. Alternatively, collect confirmations from all users who have access that they are aware that this data is sensitive, and that they may not distribute any data to third parties or make data accessible to non-authorized persons.

3.1.5. Security Aspects Related to the Mobile Solution

Before being authorized to use the system, the mobile user has to be added into the mobile user list from the SAP Business One user administration.

From the SAP Business One Main Menu, choose → *Administration* → *Definition* → *Setup* → *Users* → *Users – Setup*. Provide the user mobile phone number, mobile device ID (IMEI), and relevant SAP Business One user code and user name. In the SAP Business One user administration *Users - Setup* screen, the user must be flagged as a *Mobile User*.

After launching the SAP Business One mobile front end from the mobile device, the user is asked to enter a user name and password, which is the same user name and password for logging on to the SAP Business One application. After the user enters the correct user name and password, the front-end application passes the mobile phone number and mobile device ID (IMEI), together with the user name and password, to Integration framework.

After receiving the information, Integration framework verifies the following:

- Whether the phone number and IMEI pair can be found in the SAP Business One user administration
- Whether the user name matches the phone number and IMEI
- Whether the user has been blocked by the SAP Business One system
- Whether the password is the correct one

If the information is verified, the user is allowed to access the system.

The password is encrypted while it is transmitted to Integration framework, which decrypts the password after receiving it.

3.1.5.1. HTTPS

To make communication safer, the user has the option to use HTTPS for the sessions with Integration framework. On the server side, the communication protocol (HTTP or HTTPS) can be configured. On the client side, the user has the option to switch to the HTTPS protocol. By default, the solution runs with HTTPS, and Integration framework allows incoming calls through HTTPS only. This can be modified by settings in Integration framework.

NOTE

For additional documentation, choose *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations, chapter 6.3.*

Consider that HTTPS is the basis for a secure interaction. Check options to use certificates for enhanced security.

3.1.5.2. License Control

All mobile users have to be licensed before being allowed to access the SAP Business One system through the mobile channel. License administration is integrated with the SAP Business One user and license.

As well as being assigned an SAP Business One application license, the user must also be assigned with a mobile user license. Authorization within the SAP Business One application depends on the user's SAP Business One application license.

3.1.6. Security Aspects Related to the Dashboards Solution

Permission and authentication rules for dashboards:

- The system administrator can decide whether to grant each user full or no permission, for each dashboard, in the Authorizations form.
- By default, with a new company and for all dashboards, a non-super user has no permissions.
- At runtime, the user should be able to view the full dashboard even if this user does not have permissions for underlined user-defined queries.

During the SAP Business One startup, the SAP Business One username and password are sent with basic authentication through HTTP or HTTPS to the Integration framework server. The Integration framework server uses the username and password to authenticate the user and to return the session.

After that, SAP Business One pings the Integration framework server from time to time to keep the session active. The dashboard retrieves the data through the connection through HTTP post functions.

3.1.7. Security Aspects Related to the RFQ Scenario with Online Quotation

You must provide vendors included in the RFQ process access to the online purchasing document on the B1iFramework server.

This is accomplished by restricting access to the server to a minimum. To restrict access to the server, you must configure network (NAT) firewall as shown below:

- Only allow external access to the particular hostname / IP-address
- Only allow external access to the configured server port.
  Default: port 8080 for HTTP, or port 8443 for HTTPS
- If applicable / available for the particular firewall, configure the restricting URL:
  `http://<hostname>:<portnumber>/B1iXcellerator/exec/ipo/vP.0010000100.in_HCSX/com.sap.b1i.vplatform.runtime/INB_HT_CALL_SYNC_XPT/INB_HT_CALL_SYNC_XPT.ipo/proc?`

Copyrights, Trademarks, and Disclaimers

The current version of the copyrights, trademarks, and disclaimers at http://service.sap.com/smb/sbocustomer/documentation is valid for this document.