SAP Business One

PUBLIC

Administrator's Guide for the Integration Component

Applicable Release:

SAP Business One 8.8

Patch Level 12 and Higher

All Countries

English

June 2010

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

You have SAP Business One PL12 and the integration component installed.


Note

For information about installing the integration component, see *Installation Guide for the Integration Component.*


Note

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

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 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 to activate 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 *tomcat5w.exe* on your local drive

C:\Program Files\SAP\SAP Business One Integration\B1iServer\tomcat\bin\tomcat5w.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.

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.

To achieve this, you first change the *B1i* user password and then to log on to the SAP Business application as *B1i*. This action can also be performed after the installation is completed.

2.4. Activating Dashboard Widgets for the Cockpit

1. From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *General Settings*.
2. On the *Cockpit* tab, enter the following address for the company specified during the installation into the *B1i Server Address* field:

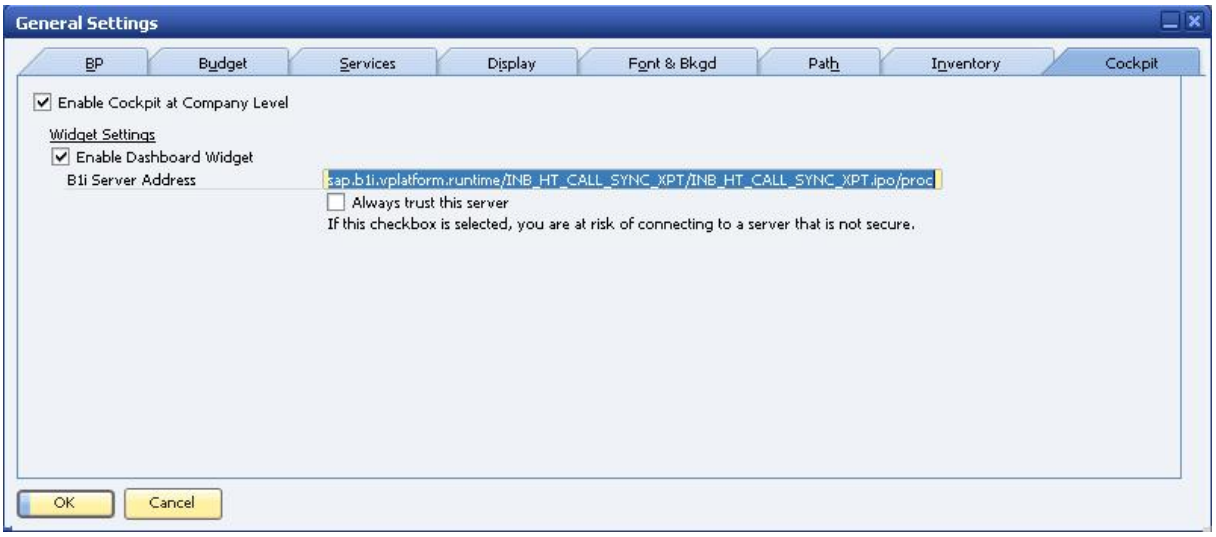
   http://<**server name**>:8080/B1iXcellerator/exec/ipo/vP.001sap0004.in_HCSX/com.sap.b1i.vplatform.runtime/INB_HT_CALL_SYNC_XPT/INB_HT_CALL_SYNC_XPT.ipo/proc.

    Note

   Remember to replace the <**server name**> with the actual name of the server where the SAP Business One integration component is installed.

   001sap0004 is the system ID of the *HanyForXcelsius* system that has been created in the SLD (system landscape directory) within the Integration framework.

   Also for additional companies, the system ID *001sap0004* in the *B1i Server Address* is the same for all company databases.



Note

If the address is not entirely correct, SAP Business One will report the error *500 Internal Server Error*, which is the typical error code and message used with HTTP connections. To fix this, correct the *B1i Server Address*.

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

If no error message appears, but only placeholder graphics are displayed in the Dashboard widget, ensure that the Adobe Shockwave Flash Player 9.0 or higher is installed on the system.

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.*

2.5. Using Further Companies With SAP Business One Integration Component

During the installation you may specify for which company you like to use the integration component features.

To add references to further databases to the system, proceed as described below. This generic description may vary depending on the features of the specific scenario(s).

1. Choose *All Programs* → *Integration solution for SAP Business One* → *Integration Framework* → *SLD.*
2. Create a new entry in the *Integration Framework* system landscape: Copy an existing system, enter a new company in node *B1i Server* (*Connectivity List* → *B1DI*) and in the URL in section JDBC, set the B1i user password, ensure the database server is correct, and save the new system.

    CAUTION

   Ensure the company name is less than 32 characters.
3. Add the new system to the scenario package in the *Integration framework* by choosing *Scenarios* → *Scenario Package Setup*, then deactivate the scenario, add the new system to the *Sender List*, and activate the scenario package.
4. Choose *All Programs* → *Integration solution for SAP Business One* → *EventSender* → *Setup.*
5. Run the *EventSender Setup*, choose a new database and enter the filter criteria (by using the same criteria as for the existing database).
6. Restart the *EventSender service*.

For additional documentation, refer to the Operations guide by choosing *Start* → *All Programs* → *Integration solution for SAP Business One* → *Integration framework,* and then choose *Help* → *Ref 04 – Operations.*

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, 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).

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 as urgent as when using the Internet.

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.

RECOMMENDATION

Partners should configure HTTPS to communicate with SAP Business One and Integration framework.

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.