**Integration Framework**

**Operations Part Two**

**System Administration**

**Last Modified: July 26, 2022**

[1 Integration Framework Administration 4](#_Toc109747320)

[1.1 Displaying System Information and Setting Profiles 4](#_Toc109747321)

[1.2 Importing BizStore Content 7](#_Toc109747322)

[1.3 Configuring the Development Environment 8](#_Toc109747323)

[1.4 Runtime Configuration 11](#_Toc109747324)

[1.4.1 Changing Integration Framework Server Ports 11](#_Toc109747325)

[1.4.2 Setting Up Scenario Step Instances 13](#_Toc109747326)

[1.5 Configuring Connectivity to the Internet and E-Mail Server 16](#_Toc109747327)

[1.6 Configuring Metadata 18](#_Toc109747328)

[1.7 Configuring the SAP Business One Cloud Setup 18](#_Toc109747329)

[1.8 Configuring the SAP Business One Event Filter 23](#_Toc109747330)

[1.9 Configuring the SAP Business One Event Subscriber 25](#_Toc109747331)

[1.10 Configuring Business Process Management 29](#_Toc109747332)

[1.11 Configuring the Message Log 29](#_Toc109747333)

[1.12 Configuring Error Handling 34](#_Toc109747334)

[1.12.1 Error Handling Overview 34](#_Toc109747335)

[1.12.2 Configuring Error Handling Default Settings 36](#_Toc109747336)

[1.12.3 Defining Overall Actions 39](#_Toc109747337)

[1.12.4 Defining Error Actions for the Outbound Phase 40](#_Toc109747338)

[1.12.5 Configuring the Garbage Collection for Error Information 46](#_Toc109747339)

[1.13 Configuring the Audit Control Function 48](#_Toc109747340)

[1.14 Configuring Daily Actions 51](#_Toc109747341)

[1.14.1 Configuring the Log Summary 52](#_Toc109747342)

[1.14.2 Configuring Message Log Deletion 54](#_Toc109747343)

[1.14.3 Monitoring Scenario Package Processes 54](#_Toc109747344)

[1.15 SAP Business One Offline Support 56](#_Toc109747345)

[1.16 User and Session Administration 57](#_Toc109747346)

[1.16.1 User Administration 58](#_Toc109747347)

[1.16.1.1 Managing Runtime Users 59](#_Toc109747348)

[1.16.1.2 Managing Administration Users 62](#_Toc109747349)

[1.16.1.3 Adding Views to Administration Users 65](#_Toc109747350)

[1.16.1.4 Enabling the Password Reset Process 68](#_Toc109747351)

[1.16.2 Session Control 70](#_Toc109747352)

[1.16.3 Authentication Events 72](#_Toc109747353)

[2 Using Integration Framework Tools 74](#_Toc109747354)

[2.1 Generating SAP Business One Events 74](#_Toc109747355)

[2.2 Displaying Benchmarks 78](#_Toc109747356)

[2.3 Using the SAP Business One Event Filter Generator 79](#_Toc109747357)

[2.4 Displaying Documentation 81](#_Toc109747358)

[2.5 Using the Embedded XML Editor in Scenario Design 83](#_Toc109747359)

[2.6 Performing Mass Deletion of Log Entries 85](#_Toc109747360)

[2.7 Stopping, Starting the Event Sender and Changing Settings 86](#_Toc109747361)

[2.8 Configuring Garbage Collection in Control Center 89](#_Toc109747362)

[3 Further Configuration Tasks 90](#_Toc109747363)

[3.1 Enabling Systems to Use HTTPS 90](#_Toc109747364)

[3.2 Exchanging a Certificate in the Tomcat Keystore 91](#_Toc109747365)

[3.3 Parameters of the Xcellerator File 92](#_Toc109747366)

[3.4 Creating Keystores and Truststores in the BizStore 100](#_Toc109747367)

[3.5 Setting Up HTTPS Between Integration Framework Servers 103](#_Toc109747368)

[3.6 Setting Up JDBC Connections with SSL between Framework and SAP HANA 104](#_Toc109747369)

[3.7 Enabling a Secure Connection between Framework and SAP HANA 105](#_Toc109747370)

[3.8 Enabling Secure Connections between Framework and Company Databases 106](#_Toc109747371)

[3.9 Database Maintenance Tasks 106](#_Toc109747372)

[3.10 Working in Safe Mode 107](#_Toc109747373)

[3.11 Options for Calling Framework Functions 108](#_Toc109747374)

[3.11.1 Enhancing the Framework URL 108](#_Toc109747375)

[3.11.2 Using Short URLs 109](#_Toc109747376)

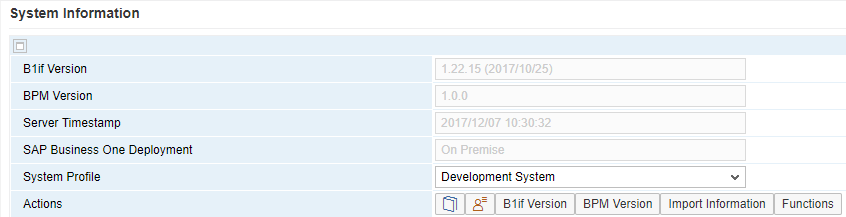
[Copyrights, Trademarks, and Disclaimers 111](#_Toc109747377)

# 1 Integration Framework Administration

After installation, the integration framework is configured for a productive system environment. The following sections provide information about how to change the system default settings. This is relevant, if you want to use the integration framework as a development environment. The following sections describe the functions of the maintenance menu.

## 1.1 Displaying System Information and Setting Profiles

System information provides details about the integration framework version and available functions of the version. Additionally, you can define and switch between system profiles. The system profiles offer settings for a development and a production system. To display system information, choose *Maintenance* → *System Info*.



B1if Version

The system information displays the version number of the integration framework. It is helpful information for the SAP support.

BPM Version

System information displays the BPM version.

Server Timestamp

The integration framework displays the timestamp of the integration framework server.

SAP Business One Deployment

Displays whether the integration framework is installed with SAP Business One on premise or the cloud version.

System Profile

After installation, the integration framework is configured for a production landscape. If you want to use the integration framework as a development environment, change some settings. The integration framework provides default definitions for a production and a development system. To change the default settings, click the  (Define Profiles for Production and Development) button.

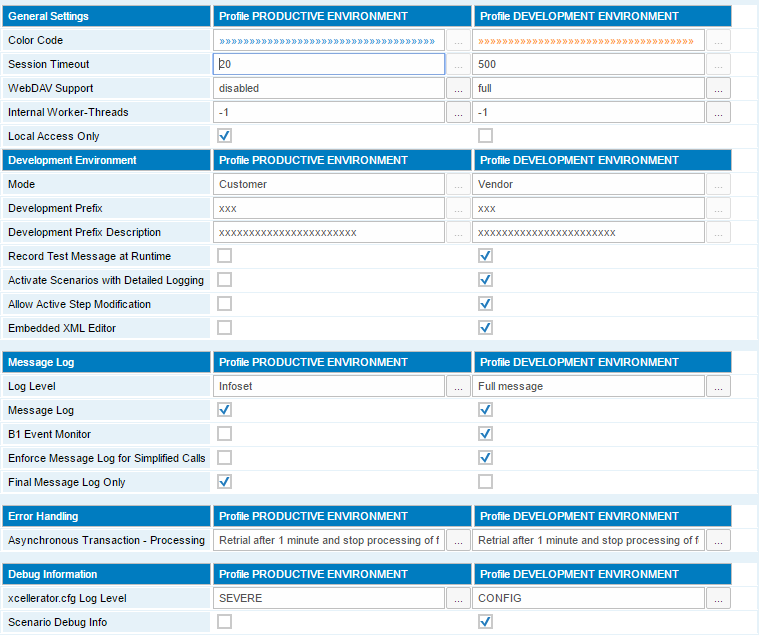
To switch settings for a development or production system, select the according profile. The integration framework requires you to restart the integration service.

Note that the color of the upper line of the integration framework user interface is blue for a production system and yellow for a development system.

 (Define Profiles for Production and Development)

To change settings of your production and development system profile, click the button.

The integration framework opens the *Set System Profiles* user interface. Profiles make the definition of all relevant settings available in one place for the productive and development environment. You can change the default settings.



[B1if Version], [BPM Version]

To display the added features and bug fixes that are available with each version, click the button. In the *Filter Text* field, enter a search term. The framework displays information for the term. In the *Filter Version* field, select a version and display information for the version.

[Import Information]

To display imports of an integration framework version with version number and timestamp, click the button.

[Functions]

To display the overview of supported inbound and outbound channels, available flow atoms, and framework features in the current version of the integration framework, click the button.

Inbound Channels

The inbound channels marked as not available are introduced successively with upcoming patches or upgrades.

Outbound Channels

The outbound channels marked as not available are introduced successively with upcoming patches or upgrades.

Available Process Atoms

Atoms marked as not available are introduced successively with upcoming patches or upgrades. Based on customer requirements SAP adds further atoms on demand.

Framework Functions

There are functions available for the administration user interface and for the runtime. Functions marked as not available are introduced successively with upcoming patches or upgrades.

## 1.2 Importing BizStore Content

The function allows to import documents in an archive to different locations in the BizStore. Upgrades for the integration framework use the function. It is the standard way for SAP support to provide error corrections.

For more information, see the *Development Environment Guide*, section *Document Handling*, *Importing a ZIP with Multiple Documents*

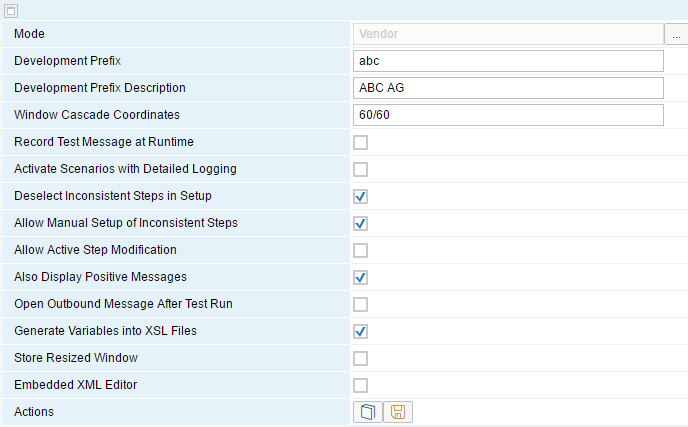
For more information about importing scenario packages, see section *Importing a Scenario Package or a Scenario Step* in the *Operations, Part 1* guide

## 1.3 Configuring the Development Environment

The function is only relevant, if you use the integration framework for scenario package development. After installation, the integration framework default configuration is for a productive environment. To configure the development environment, choose *Maintenance* → *Cfg Dev Environment*.

To define a profile for the productive environment, choose *Maintenance* → System Info.

The following settings support the development process.



Mode

The mode defines the namespace for scenario packages that you develop. If you are a scenario vendor, select Vendor. If you are a customer and you develop your scenario package, select Customer. Customers use the z namespace.

Development Prefix

Enter the development prefix for scenario development. Enter a short prefix. You only have limited space available for scenario package and step names. Do not use a point (.) as part of the prefix. If you are a customer, the integration framework sets the prefix to Z.

Development Long Description

Enter a description for the development prefix for the scenario package documentation.

Window Cascade Coordinates

Enter the position the integration framework uses to open additional windows of the user interface. The default position is 60/60.

Record Test Message at Runtime

To switch on the creation of test messages at runtime, select the checkbox. Use test messages in scenario package design for testing your development. In this way, you can test your scenario without connecting to sender systems and creating test messages in the connected systems. The integration framework saves test messages in the scenario step folder in the scenarios design area. By default, the integration framework does not record test messages at runtime. Do not activate the recording of test messages in a productive system, the function has impact on performance.

Activate Scenarios with Detailed Logging

To activate detailed logging for the design phase, select the checkbox. By default, the detailed logging is deactivated.

note.gif NOTE

Do not activate detailed logging in your productive system.

Deselect Inconsistent Steps in Setup

The integration framework deselects scenario steps in the step list of the setup user interface that are inconsistent, if you select the checkbox. This is the default.

Allow Manual Setup of Inconsistent Steps

To enable manually selection of inconsistent steps for setup, select the checkbox.

Allow Active Step Modification

If you work in the design phase and want to avoid repeated activation and deactivation of a scenario package, select the checkbox. It allows changing activated steps.

Also Display Positive Messages

If you want the integration framework to only display negative alerts, deselect the checkbox. The selected checkbox is the default.

Open Outbound Message After Test Run

If you want the integration framework to display the result message after each processing, select the checkbox. This is only relevant for the design phase. It is the default that the checkbox is not selected.

Generate Variables into XSL Files

The integration framework generates defined variables in each XSL stylesheet as XSL variables, if you select the checkbox. By default, the integration framework generates variables into XSL stylesheets.

Store Resized Window

The graphical flow designer saves all resizing changes. This function does not work for all browsers. If it does not work for your browser, this checkbox allows you to switch it off.

Embedded XML Editor

If you have an embedded XML editor available in the /com.sap.b1i.vplatform.directory/external folder. the integration framework opens the embedded editor and does not open a browser window, if you select the checkbox.

As of integration framework version 1.21.0, the integration framework provides an internal embedded XML edior. If you have not integrated an external XML editor and you select the checkbox, the integration framework opens the internal XML editor when clicking the xform or final atoms.

Additionally, the integration framework displays the  icon in several user interfaces for editing required XML documents, for example, format control documents. Clicking the icon opens the editor.

If you are currently using an external embedded XML editor and you want to use the internal XML editor instead, do the following:

* Deselect the checkbox and click *Save*.
* Select the checkbox again and click *Save*.

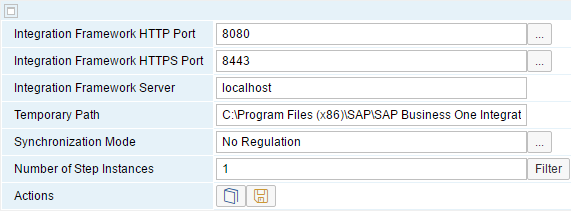
The integration framework offers you the option to select the external or the internal XML editor.

* Select the internal XML editor.

For more information, see the *Using the Embedded XML Editor in Scenario Design* section of this guide.

## 1.4 Runtime Configuration

Use the function to configure settings for the integration framework runtime.



### 1.4.1 Changing Integration Framework Server Ports

By default, the integration framework server uses port 8080 for http and 8443 for https. If another application already uses the ports, or you do not want to use the default ports, change the integration framework ports.

note.gif NOTE

It is not sufficient to change the server port in the Runtime Configuration function. Also change the port in the event sender setup, in the Tomcat server file and in the menu entry to call the integration framework.

If you change settings in the Runtime Configuration function, the integration framework updates the SAP Business One SLSP and SLSPP tables.

**Procedure**

1. If the SAP Business One Event Sender Service is already running, stop the service.
2. In the …\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\conf folder, open the server.xml Tomcat file and change the settings in the first two Connector port tags. Do not change any other settings.
3. Restart the SAP Business One Integration Service.
4. Call the integration framework using the changed port in the URL, log on, choose *Maintenance* → *Cfg Runtime*. and change the port or ports.

The integration framework updates the SLSPP table in SAP Business One.

1. Choose Start → All Programs → Integration Framework for SAP Business One → SAP Business One Event Sender Setup, follow the steps of the wizard, and in the Configure Integration Framework Parameters section, change the Framework Server Port entry, and test the connection.
2. Restart the SAP Business One Event Sender Service.
3. To update the properties for the menu entry with the new port number, choose Start → All Programs → Integration Framework for SAP Business One → Integration Framework.

**Additional Fields**

Integration Framework Server Name

You can change the integration framework server name. The integration framework sets the computer name by default. Change the name, for example, to localhost.

Temporary Path

The integration framework uses the temporary folders for internal tasks, for example, to create large outbound files. If it has written the complete file to the temporary folder, it copies the file to the dedicated outbound folder for further processing.

The default folder is: …\Tomcat\temp. If you change the default folder, make sure that the integration framework service has the required rights to write to the folder.

Synchronization Mode

Use the parameter to influence the synchronization behaviour of the integration framework, if you define to synchronize data, for example, between an on premise and cloud solution, and users can change data in both solutions.

You have the following options:

* No Regulation (default)

The integration framework processes messages, how you have defined it in the scenario packages.

* Return to Sender

If you select the option, the integration framework always sends back changes to the original sender. You can avoid that changes in different solutions lead to overall inconsistent data.

* Filter Sender

If you select this option, the integration framework does not send back changes to the original sender.

Number of Step Instances

To configure the number of instances the integration framework uses for scenario step processing, enter a number. The default is 1, and the integration framework uses one instance for each scenario step at runtime. You can change the value at runtime. The setting is valid for all scenario steps. To use more than one instance, make sure that a scenario step cannot become a bottleneck, locking, for example, a resource.

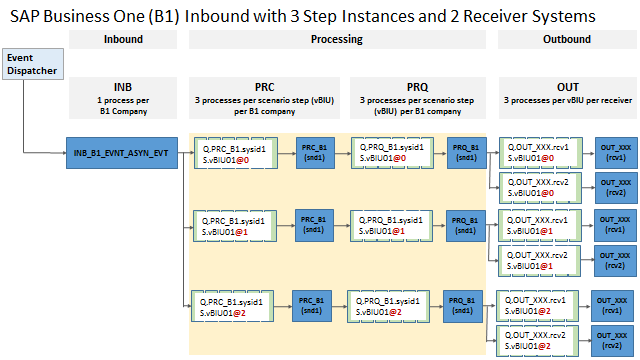
[Filter]

To exclude scenario steps from parallel processing at runtime, click the button and select the steps.

### 1.4.2 Setting Up Scenario Step Instances

For different scenario steps and different sender and receiver system combinations, the integration framework processes messages in parallel by default.

Additionally, you can enable parallel processing of scenario steps for specific sender and receiver combinations for the processing and outbound phases. The parallel processes are called scenario step instances. Use the additional option, for example, to initially load messages of one B1 object type to one or several receiver systems. Parallel processing is available for all inbound types the integration framework supports.

SAP Business One Inbound Example

The illustration above displays an example for SAP Business One inbound. The integration framework receives a B1 event that triggers the scenario step. In processing and outbound, the integration framework uses three instances of the step (@0, @1, @2) to process messages to the two receiver systems.

If you use more than one instance in processing and outbound, ensure that a scenario step cannot become a bottleneck by locking, for example, one resource.

**Prerequisites**

* Check the number of available processors of the machine where the integration framework runs.
* In the integration framework, choose Tools → Troubleshooting.
* In the *Functional Group* field, select B1i Framework and click the [Submit] button.
* In the *Memory Usage* section, click the [Start] and then the [Display] button.
* The integration framework displays the number of available processors in the *Number of Processors* field.
* All parallel processes share the same memory. Keep it in mind when allocating memory to the integration framework. To allocate memory to the integration framework, open   
  C:\Program Files (x86)\SAP\SAP Business One Integration\IntegrationServer\Tomcat\bin\_64\tomcat6w.exe, click the *Java* tab and in the *Maximum memory pool field*, provide the memory assigned to the integration framework.
* For parallel processing, enter the following setting in xcellerator.cfg:

xcl.threads=n

A positive number defines the number of threads, a negative number defines the number of threads or processes for each processor. The -1 default value enables one thread or process for each available processor.

**Design Time**

* By default, existing scenario steps are enabled to support more than one instance for the processing and outbound phases. To use one instance for scenario step processing and outbound, choose Scenarios → Step Designand deselect the *Allow Parallel Processing* checkbox. Note that for new scenario steps, parallel processing is enabled by default.
* If a scenario step asynchronously triggers another scenario step using the *Put to Internal Queue* atom, select the *Use Instances* checkbox, and the integration framework creates queue instances at runtime. The triggered scenario step uses instances for parallel processing.
* If you use the *Call Scenario Step* atom to asynchronously call another scenario step, the atom enables parallel processing.

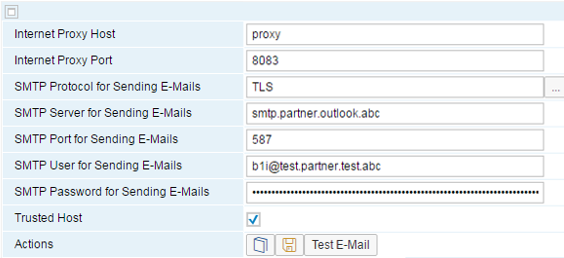
**Runtime**

To configure the number of step instances for the integration framework runtime, choose Maintenance → Cfg Runtime. In the *Number of Step Instances* field, enter the number of instances. The setting is valid for all scenario steps selected for parallel processing at design time. You can change the number of instances any time, it takes effect immediately. No further changes are required.

To exclude scenario steps from parallel processing at runtime, click the [Filter] button and in the list, select the scenario steps you want to exclude from parallel processing. The integration framework displays scenario steps that are already excluded from parallel processing in step design with a selected and disabled checkbox.

## 1.5 Configuring Connectivity to the Internet and E-Mail Server

Define e-mail server settings for sending e-mails, and define proxy settings. To configure setting, choose *Maintenance*→*Cfg Connectivity*.



Internet Proxy Host

If there is a firewall between your system and the internet, enter the proxy host name.

Internet Proxy Port

Enter the proxy port number.

**Settings for Sending E-Mails**

SMTP Protocol for Sending E-Mails

Select one of the following protocols:

* SMTP
* SMTPS
* TLS

SMTP Server for Sending E-Mails

Enter the name or IP address of the SMTP server, you want to connect to.

SMTP Port for Sending E-Mails

Enter the port of the SMTP server. The default is 25.

SMTP User for Sending E-Mails

Enter the user for connecting to the e-mail server.

SMTP Password for Sending E-Mails

Enter the password for connecting to the e-mail server.

Trusted Host

To add the name of the e-mail server to the list of trusted hosts, select the checkbox. If the e-mail server requires a certificate for a secure connection, you do not need to import the certificate to the Java keystore.

If the e-mail server requires a secure connection and you do not select the checkbox, import the certificate to the Java keystore using the keytool program.

[Test E-Mail]

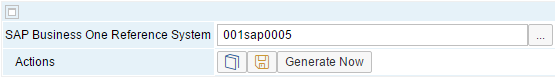
* To test the connection, click the button.
* Enter the sender e-mail address and click [Select].
* Enter the receiver e-mail address and click [Select].

The integration framework triggers to send an e-mail from the sender to the receiver. The e-mail subject is: B1if Test Email

For more information about the connection information, refer to the documentation of your e-mail provider

## 1.6 Configuring Metadata

Use the function to retrieve metadata from a reference SAP Business One system. You need metadata of B1 objects, B1 functions and B1 services to define inbound and outbound channels and for the B1 atoms of the processing phase. The installation already provides basic information. To update the information including user-defined fields, select an SAP Business One reference system and generate the metadata into the BizStore. To update metadata, choose *Maintenance*→*Cfg Metadata*.



SAP Business One Reference System

Select an SLD system as the reference system for metadata generation and click Save.

[Generate Now]

To generate metadata, click the button.

The integration framework retrieves metadata including the object ID, name list, schema, and so on. Display the information in the following places:

* In the *B1 object* and *B1 service* atoms, click the [Help] button.
* In the integration framework, choose *Help* and display the *B1 Object Help* or *B1 Service Help*.

To check the running process, choose Tools → Control Center → Monitoring → Execution Status /vPlatformIDE/com.sap.b1i.vplatform.ide/ipo/vPlatform.ide.ipo/RetrieveB1MetaDataQ.

## 1.7 Configuring the SAP Business One Cloud Setup

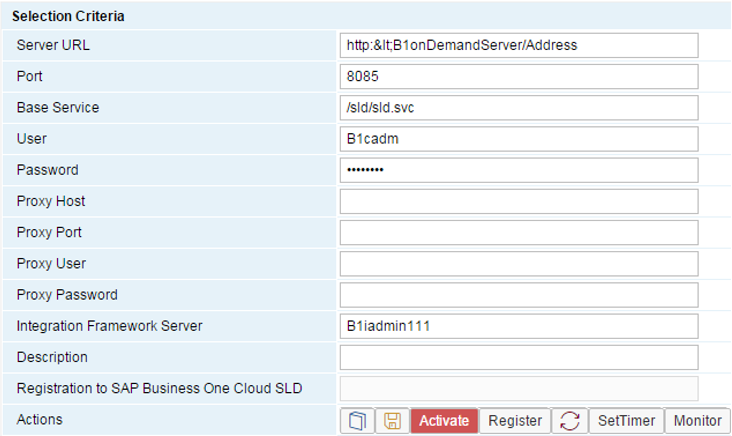
caution.gif CAUTION

Only use the function, if you have installed SAP Business One Cloud and the integration framework (SAP Business One integration). The function is not relevant for the standard on premise solution.

Provide connectivity parameters for the SAP Business One Cloud server and register at the server. The SAP Business One Cloud Control Center administrator can provide you with the required information. After providing the information, click the [Register] button. Without registration the connection between SAP Business One and the integration framework does not work.

This function is based on the sap.B1System2 package that is responsible for technical communication between SAP Business One Cloud and the integration framework. The package retrieves information from the SAP Business One Cloud SLD and synchronizes the integration framework System Landscape Directory (SLD).

To open the *SAP Business One Cloud Setup*, choose *Maintenance*→*Cfg B1 Cloud*.



Server URL

Enter the complete server URL of the SAP Business One Cloud server.

Port

Enter the port of the SAP Business One Cloud server.

Base Service

Enter the base service of the server URL.

User

To access the SAP Business One Cloud server, enter the user name. Only use plain US ASCII characters. The default user name is b1cadm.

Password

To access the SAP Business One Cloud server, enter the password. Only use plain US ASCII characters.

Proxy Host

If you use a proxy server in the network for connecting to the SAP Business One server, enter the IP address of a proxy server. Leave the field empty, if a proxy is not required.

Proxy Port

If you use a proxy, enter the port number. Leave the field empty, if a proxy is not required.

Proxy User

To access the proxy, enter the user name.

Proxy Password

To access the proxy, enter the password.

Integration Framework Server

Enter the name of the integration framework server. It must be identical with the one in the SAP Business One Cloud SLD.

Description

Optionally add a description for the integration framework (B1i) server.

Registration to B1OD SLD

The integration framework displays the date and time, when it has registered to the SAP Business One Cloud SLD.

The following functions are available:

[Activate or Deactivate]

To activate or deactivate the sap.B1System2 scenario package, click the button. The default is that the package is active after installation in the SAP Business One Cloud environment.

If you activate the sap.B1System2 scenario package, the integration framework gives you an overview of the activation status.

For more information, see the *Operations Guide, Part One*, section *Activation and Deactivation*

[Register]

To register the integration framework to the SAP Business One Cloud server, click the button.

 (Synchronize SLD Settings)

To manually synchronize the settings in SLD with the settings in the SAP Business One Cloud SLD, click the button.

[SetTimer]

To define scheduler settings for automated synchronization of SLD settings with the SAP Business One Cloud SLD, click the button. The integration framework triggers synchronization every five minutes by default. You have the following options:

* Synchronization to B1OD SLD

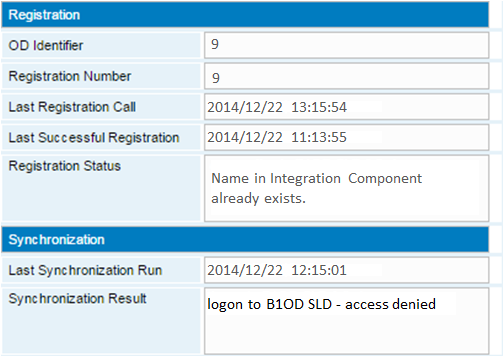
The integration framework synchronizes SLD entries with the SAP Business One Cloud SLD.

* Synchronization with SLSP/SLSPP tables

The integration framework synchronizes SLD entries with the SLSP and SLSPP tables of SAP Business One.

[Monitor]

To display information about the registration and the last synchronization details, click the button.



Information in the *Registration* section is provided by the SAP Business One Cloud registration service.

OD Identifier

This is the unique numeric identifier of the integration framework in the SAP Business One Cloud control center.

Registration Number

This value is currently identical with the *OD Identifier*.

Last Registration Call

This displays the date and time of the last registration call to the registration service.

Last Successful Registration

This displays the date and time of the last successful registration call to the registration service.

Registration Status

The registration status can be:

* success
* Name in IntegrationComponent already exists; specify a unique value for Name

The name defined for the Integration Component in the Cloud Control Center for SAP Business One already exists. Ask the SAP Business One Cloud Control Center administrator to provide another name.

* Connection to B1OD SLD failed

Last Synchronization Run

This displays the date and time when the integration framework has triggered the last synchronization.

Synchronization Result

This gives you a summary about the last synchronization. The following options are possible:

* logon to B1OD SLD successful: <no> actions triggered

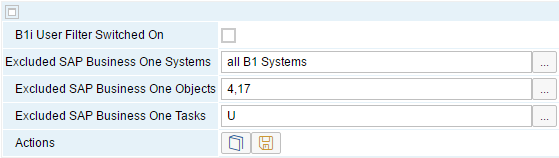
<no> is the number of actions

* logon to B1OD SLD - access denied
* logon to B1OD SLD failed

## 1.8 Configuring the SAP Business One Event Filter

Using the SAP Business One event filter, you can bypass the default filter that lets the integration framework filter events caused by the technical B1i user in SAP Business One.

To configure the SAP Business One event filter, choose *Maintenance*→*Cfg B1 Event Filter*.



B1i User Filter Switched on

It is the default setting and avoids endless loops that the integration framework filters all events caused by the technical B1i user in SAP Business One. The B1i user handles the login to the company database of SAP Business One in SLD.

It is possible that special scenario steps require processing such events. To bypass the filter for a combination of SAP Business One systems, objects and tasks, deselect the *B1i User Filter Switched on* checkbox. If a vendor of a scenario package needs events caused by the B1i user, look up information in the scenario package description.

For more information, refer to the *SLD* documentation, SAP Business One, about the *userName* parameter.

If you deselect the checkbox, select the filter exclusion fields clicking the […] button. To select multiple entries, press *ctrl* and right-mouse click. The integration framework checks all exclusion field definitions and processes an event, if all conditions are true.

Excluded SAP Business One Systems

Select one, more or all SAP Business One systems available in SLD.

Excluded SAP Business One Objects

Select all, one or several SAP Business One objects. The list displays all SAP Business One standard objects. To consider individual objects or user-defined tables, add them to the list. Separate entries by a comma.

Excluded SAP Business One Tasks

Define the exclusion based on the task the event refers to. Select all tasks, if the exclusion is valid for all events or you select one or more tasks. I defines insert, U defines update and D defines delete.

**Example**

In the example above, the integration framework filters all events caused by the B1i user, except events for updates of items and orders.

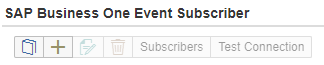
## 1.9 Configuring the SAP Business One Event Subscriber

To send SAP Business One events to a remote integration server, configure the SAP Business One event subscriber.

**Prerequisites**

If you want to use HTTPS for the connection to the remote integration framework, import the certificate of the remote integration framework to the BizStore. For more information, see section *Setting Up HTTPS Between Integration Framework Servers* in this guide

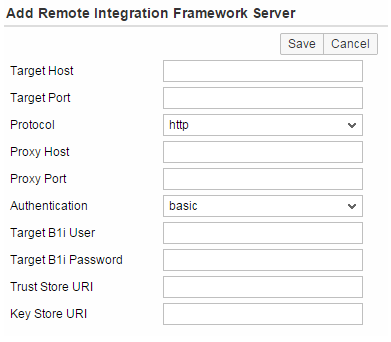
To configure the B1 (SAP Business One) event subscriber, choose *Maintenance*→*Cfg B1 Event Subscriber*.



[Create]

To create a remote integration framework server node, click the button. The integration framework creates a remote integration framework server node for the remote integration server and a default subscriber for this node. The integration framework sets the filter criteria to \*. The integration framework sends all B1 events also to the remote server node.

To define the remote integration framework, the integration framework opens the following user interface:



TargetHost

Enter the primary key of the remote integration framework server. Enter either the server name or the IP address.

TargetPort

Enter the port of the remote integration framework server. The standard HHTP port is 8080. The standard HTTPS port is 8443.

Protocol

Select the protocol, http or https. Ensure that the protocol selection matches the port entry.

ProxyHost

If there is a proxy host available for the remote integration framework server, enter the proxy host name.

ProxyPort

If there is a proxy host available for the remote integration framework server, enter the proxy port.

Authentication

Select the authentication method for connecting to the remote integration framework server. For remote access, use basic.

TargetB1i User

Enter the user name to logon to the remote integration framework server.

TargetB1i Password

Enter the password to logon to the remote integration framework server.

SSL TrustStore Path

If you use HTTPS to connect to the remote integration framework server, enter the path to the SSL trust store.

SSL TrustStore Password

If you use HTTPS to connect to the remote integration framework server, enter the password to access the SSL trust store.

In the B1 Event Subscriber user interface, select a remote integration framework server node and click one of the following buttons:

[Edit]

To edit a server mode, click the button. You cannot change the *TargetHost* entry.

[Delete]

To delete a remote server node, click the button.

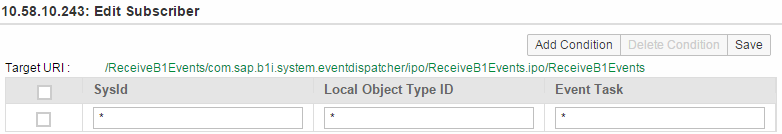
[Test Connection]

To test the connection to the remote integration framework, click the button.

[Subscribers]

In the subscriber, you define the system and the message type or types, the local integration framework sends to the remote integration framework.

The following user interface opens:



SysId

Enter the SysId of a system in the local SLD. The local integration framework forwards messages from this system to the remote integration framework. Enter \* and the local integration framework forwards messages coming from all systems to the remote integration framework.

Local Object Type ID

Enter either one or several B1 (SAP Business One) object IDs, separated by comma. If you want to forward all B1 objects, enter \*.

Event Task

Enter the transaction type of the B1 event. You have the following options: A (add), U (update), C (cancel), L (close), D (delete), and \* for all event types.

example.gif Example

Enter AUC for additions, updates and cancellations.

[Add Condition]

To add a condition, click the button.

[Delete Condition]

To delete a condition, select it at the beginning of the row and click the button.

[Save]

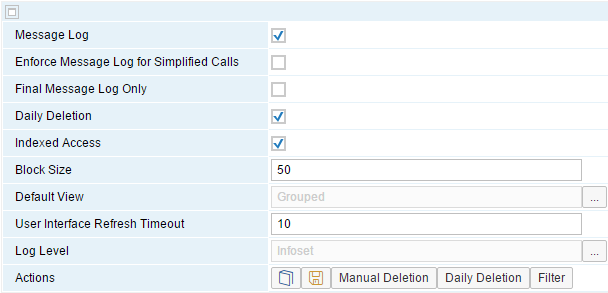
To save settings, click the button.

## 1.10 Configuring Business Process Management

For more information about configuring the garbage collection for business process management, see the *Business Process Management Guide*

## 1.11 Configuring the Message Log

Message logs are important for analyzing problems. Use the function, to switch on message logging and define the message log level. Manually delete message logs and define the scheduler for automatic deletion. To configure the message log, choose *Maintenance*→*Cfg MsgLog*.



Message Log

To switch on the generation of message logs at runtime, select *Message Log*. By default, the message log is switched off.

Enforce Message Log for Simpified Calls

To enforce the production of message log entries for simplified HTTP and Web service calls, although the settings have been disabled in the call, select the checkbox.

Final Message Log Only

If the integration framework creates message logs, it starts writing entries as soon as messages enter the integration framework. The integration framework updates initial message log entries when processing messages. If you select the option, the integration framework only creates the final message log. It does not update log entries during processing. This has an impact on the integration framework performance. Note that you cannot display messages with the Processing status in the message log, if you enable the function.

Daily Deletion

To activate daily deletion (garbage collection) of message logs, select the checkbox. The integration framework only activates daily deletion, if you have defined the correct configuration for daily deletion. To define the configuration, click the [Daily Deletion] button. If the message log is switched on, we recommend scheduling the automatic daily deletion. By default, daily deletion is switched on.

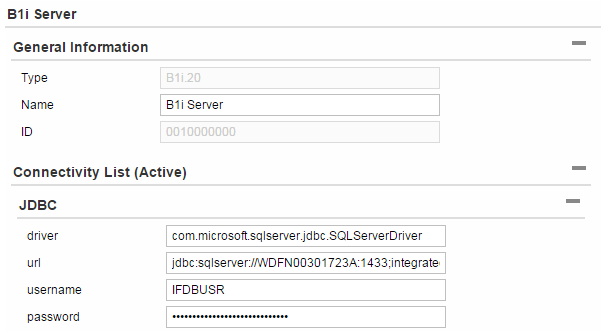
Indexed Access

If the message log is switched on, the integration framework writes entries to the BizStore that you can access in the message log monitor.

As of integration framework version 1.20.0, the integration framework offers indexed access to message log information. As of integration framework version 1.21.0, the integration framework uses the message log with indexed access by default.

To switch on indexed access to the message log, select the checkbox. If the MSGLOG table is abvailable, the integration framework starts writing index information to the MSGLOG table. The installation of the integration framework creates the table. The IFDBUSR provides access to the table. The user has the permission to select, update, insert, and delete records in the MSGLOG database table.

Find the connection parameters in SLD in the *B1i Server* entry:



If you switch on indexed access, the integration framework displays the advanced message log in the *Monitoring* section. It provides more selection criteria and more options to display message log entries. For more information, see the *Operations Guide 1*, section *2.1 Message Logs*

note.gif NOTE

In the advanced message log, you can only display the entries that the integration framework creates with index. If you switch off the indexed access and switch it on again after some time, the message log entries without index are not displayed in the advanced message log.

Block Size

If you switch on indexed access to the message log, enter the block size. The default block size is 50. It is the number of messages displayed in the message log list on one page.

Default View

If you switch on indexed access to the message log, choose the default view.

You have the following options:

* List

Displays message logs in a list.

* Grouped

Groups message logs by *Success*, *Failure*, *Processing* and *Filtered*.

User Interface Refresh Timeout

Define for how long the message log screen remembers the timestamps in the filter setting. If you enter 0, the user interface opens with the default values to display the information of the current day.

Log Level

Define the level of information the integration framework generates for the message log. The following levels are available

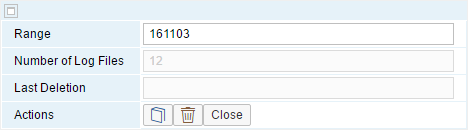
* Infoset
* Full message
* Full message incl. binary data

note.gif NOTE

For a productive environment, we recommend switching off the message log or only switching it on with the lowest level (Infoset). If you develop scenario steps, switch on the full message log (Full message).

[Manual Deletion]

To delete the message log manually without waiting for the daily scheduler, click the button.



Range

Enter the range of message logs you want to delete. The default is today. If the field is empty, the integration framework selects all message logs. You can use a substring of the date, for example, 1005 to select message logs for May 2010. You can define a start and an end date using – between both dates, for example, 100501-100518.

Number of Log Files

The field displays the number of message logs available for the selected range.

Last Deletion

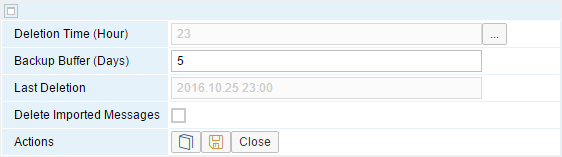
The field displays the timestamp of the last manual deletion.



To generate jobs that trigger the deletion of message logs in the background, corresponding to the selected range, click the button.

[Daily Deletion]

To configure the daily deletion click the button.



Deletion Time (Hour)

Select the deletion time. The integration framework deletes the log on the hour. By default, the integration framework deletes the message log at the 23rd hour.

Backup Buffer (Days)

Enter a number to specify for how many days you do not want any deletion. The default is 5 days.

Last Deletion

The field displays the timestamp of the last automatic daily deletion.

Delete Imported Messages

To include messages you have imported from other integration frameworks in the automatic deletion, select the option.



To save the configuration, click the button. If automatic deletion is switched on, the integration framework reactivates the scheduler with the new settings.

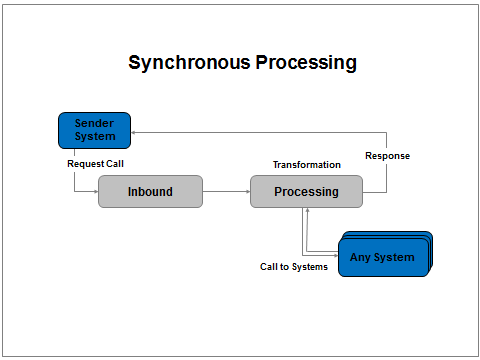
[Filter]

To display the *Message Log Exclusion Filter*, click the button. The integration framework displays all scenario steps. To exclude a scenario step from message log, select the checkbox. Use the filter list, if the message log is switched on in general, and you want to switch it off for certain scenario steps.

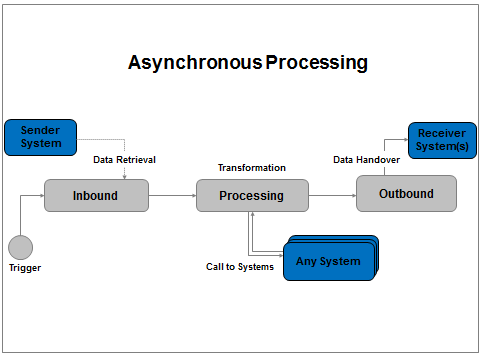
## 1.12 Configuring Error Handling

### 1.12.1 Error Handling Overview

For error handling, the integration framework distinguishes between synchronous and asynchronous scenario steps.



Synchronous scenario steps consist of an inbound IPO step, and a processing (vBIU) IPO step. The processing IPO step returns the result to the original sender. If an error occurs, the integration framework sends a notification to the sender system and writes the message to the Failure section of the message log by default.



Asynchronous scenario steps consist of an inbound, a processing and an outbound phase. Internal message processing differs, depending on whether you have one or more than one receivers for the message. The different phases of asynchronous processing hand over messages using internal queues.

In default error handling for asynchronous message processing, you can define settings that influence the error handling or notify you, if a certain situation occurs.

For a more detailed overview of asynchronous message processing, see the *Scenario Development Guide*, section *5 Developing an Individual Error Handling*

On scenario package level, you have additional error handling options available.

The integration framework writes all error handling configurations to the following document in the BizStore:

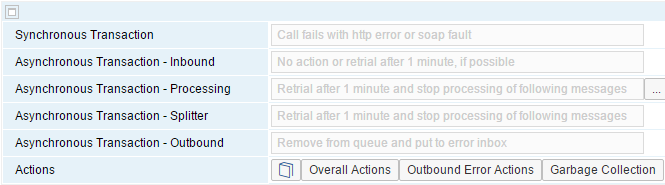
…/com.sap.b1i.vplatform.repository/ErrorHandler/eh.xml

### 1.12.2 Configuring Error Handling Default Settings

Use the function to get an overview of the default error handling of the integration framework. Additionally, you can define settings for the following:

* For the processing phase, define how the integration framework handles messages blocking internal queues. You can either process the message again after one minute or choose to remove the message from the queue.
* Define settings for receiving notifications about messages blocking queues.
* For the outbound phase, define specific error actions that the integration framework performs if errors occur.

To open the configuration for default error handling, choose *Maintenance* → *Cfg Error Handling*.



**Synchronous Transaction**

The default error handling for synchronous transactions is that the integration framework sends an HTTP or SOAP fault error to the sender system and writes an entry to the *Failure* section of the message log. You cannot change the default behavior.

**Error Handling Option on Scenario Package Level**

On scenario package level, you can define an individual error handling step that replaces the default error handling. For more information, see the *Scenario Development Guide*, section *5 Developing an Individual Error Handling*.

**Asynchronous Transaction – Inbound**

For asynchronous transactions, the integration framework provides the following default behavior that you cannot change:

* No error action for the inbound database trigger and inbound trigger, because the inbound steps do not handle critical data processing.
* The inbound dispatcher that distributes messages from sender systems to the subscribed scenario steps automatically triggers the deactivation and subsequent activation of the instance after one minute, if possible. This avoids high load on the integration framework server, if problems occur in the inbound channel. An example for such a situation is that the integration framework tries to pick up a corrupt file from the file system. The integration framework writes an entry to the *Failure* section of the message log.

**Error Handling Option on Scenario Package Level**

On scenario package level, it is not possible to define an individual error handling step.

**Asynchronous Transaction – Processing**

If an error occurs in the processing phase, the integration framework writes an entry to the *Failure* section of the message log. You have the following options to set the default behavior of the integration framework:

* Retrial after one minute and stop processing of following messages
* Remove from queue and continue with next message.

The integration framework writes messages removed from queues to an internal integration framework table.

**Error Handling Option on Scenario Package Level**

On scenario package level, define an individual error handling step to change the default behavior of the integration framework. Additionally, you can overlay the deletion of messages from the queue on scenario package level. For more information, see the *Scenario Development Guide*, section *5 Developing an Individual Error Handling*.

**Asynchronous Transaction – Splitter**

If a message has more than one receiver and an error occurs, the integration framework writes an entry to the *Failure* section of the message log. It tries to process the message after one minute. The integration framework does not process messages that are behind the erroneous message in the queue. You cannot change the default behavior.

**Error Handling Option on Scenario Package Level**

On scenario package level, it is not possible to define an individual error handling step.

**Asynchronous Transaction – Outbound**

If an error occurs in the outbound phase, the integration framework writes an entry to the *Failure* section of the message log. It removes the message from queue and moves it to the error inbox. This is the default behavior. You can define outbound error actions. For more information, see the section *Defining Error Actions for the Outbound Phase*

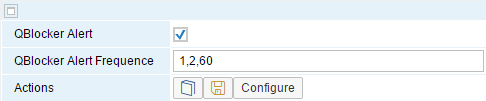
**Error Handling Option on Scenario Package Level**

On scenario package level, it is not possible to define an individual error handling step.

### 1.12.3 Defining Overall Actions

If messages block queues in the integration framework, you can configure to receive e-mail notifications.

To configure notifications, choose *Maintenance* → *Cfg Error Handling*→*[Overall Actions]*.



QBlocker Alert

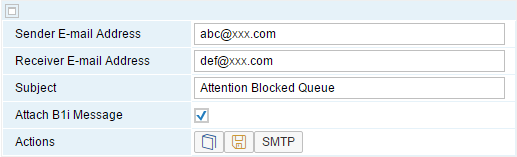
To receive e-mails if messages block an integration framework queue, select the checkbox.

QBlocker Alert Frequence

By default, the integration tries to process a message again after one minute. Define, how often you want to receive an e-mail notification. In the example above, the integration framework sends a notification after the first, the second and after 60 minutes.

[Configure]

To configure e-mail settings for notifications, click the button.



Sender E-mail Address

Enter the e-mail address of the sender of the queue blocker alert.

Receiver E-Mail Address

Enter the e-mail address of one who receives the queue blocker alert notification.

Subject

Enter the e-mail subject.

Attach B1i Message

By default, the integration framework attaches the message that has caused the error in the outbound phase.

[SMTP]

To enter or display connection information in the *Configuration Connectivity* user interface, click the button.

### 1.12.4 Defining Error Actions for the Outbound Phase

For the default error handling of the outbound phase, you can define error actions. You have the following options:

* Keep messages in the inbound queue for outbound processing instead of sending them to the error inbox.
* Let the integration framework try to process messages again before sending them to the error inbox.
* Let the integration framework send an e-mail notification.
* Let the integration framework not send the message to the error inbox.
* Let the integration framework wait for some time and try to process the message several times again before handing it over to the error inbox.

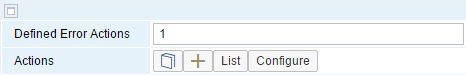
You can define the options above for the following:

* Define error actions for scenario steps. Additionally, you can limit the error actions to a specific sender and receiver system combination.
* Define error actions for scenario packages. The error actions are valid for all scenario steps of the package. You can limit error actions to a specific sender and receiver system combination.
* Define error actions for an outbound type, for example, file outbound. You can limit error actions to a specific sender and receiver system combination.

If you define several error actions, the integration framework uses the most specific one. First priority have scenario step-based error actions, followed by scenario package-based error actions, and finally the outbound-based error actions have lowest priority.

An error action for a specific sender and receiver combination has highest priority, followed by error actions for a specific sender system, then all error actions are considered for a specifc receiver system, and finally the ones without any sender or receiver assignment.

To define error actions, choose *Maintenance*→*Cfg Error Handling*→*[Outbound Error Actions]*



Defined Error Actions

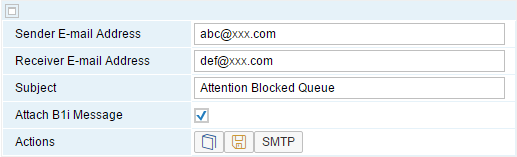
The integration framework displays the number of defined error actions for the outbound phase.

[Configure]

Some error actions require additional configuration settings. To provide configurations for sending e-mails and automatically resending messages, click the button.

**E-Mail**

If you want to receive e-mail notifications if errors occur in scenario packages, steps or outbound channels, select E-Mail. The integration framework opens the following user interfaces:



Sender E-mail Address

Enter the e-mail address of the sender of the error action information.

Receiver E-Mail Address

Enter the e-mail address of the one who receives the error action information. Note that you can only send the e-mail to one receiver.

Subject

Enter the e-mail subject.

Attach B1i Message

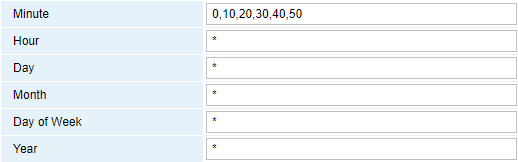
By default, the integration framework attaches the message that has caused the error in the outbound phase.

[SMTP]

To enter or display connection information in the *Configuration Connectivity* user interface, click the button.

**Automatic Resend**

If you want to automatically process messages again if errors occur in scenario packages, steps or outbound channels, select Automatic Resend. And provide timer settings. The integration framework opens the following user interface:

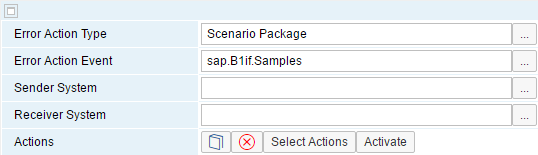


For more information, see the *Operations Guide Part One, section 1.1.4*



To add error actions, click the button.

The integration framework opens the following user interface:



Error Action Type

Select an error action type:

* Scenario Package
* Scenario Step
* Outbound channel

Error Action Event

Depending on the selected error action type, select a scenario package, a scenario step or an outbound type.

Sender System

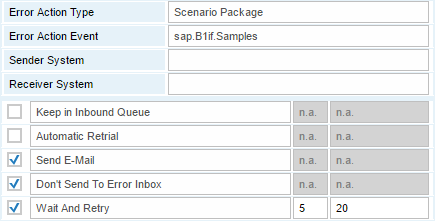
You have the option to select a sender system for the error action.

Receiver System

You have the option to select a receiver system for the error action.

[Select Actions]

Select error actions that you want to run for the error action type.



You can set the following if an error occurs in the outbound phase:

* Keep in Inbound Queue

Let the integration framework keep the message in the inbound queue for outbound processing.

* Automatic Retrial

If an error occurs, let the integration framework automatically try to process the message again.

Provide timer settings in the *Configure* function of the *Error Actions* user interface.

You cannot combine this action with the Keep in Inbound Queue action.

* E-Mail

If an error occurs, let the integration framework send an e-mail.

Provide e-mail settings in the *Configure* function of the *Error Actions* user interface.

* Don’t Send to Error Inbox

If an error occurs, do not let the integration framework send the message to the error inbox.

You cannot combine this action with the Automatic Retry action.

Use this option, if you do not want to use the error inbox. Together with the *Keep in Inbound* Queue option, you keep the message in the integration framework. If you do not use the Keep in Inbound Queue option, the integration framework removes the message from processing and writes it to a dedicated table.

* Wait and Retry

If an error occurs, let the integration framework wait for a defined period of time and try to process the message again for a defined number of times. Only after this time, the integration framework performs the error handling.

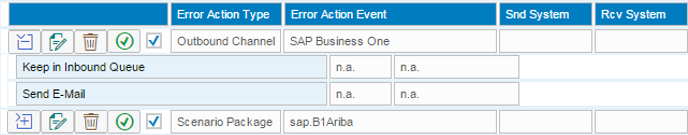
In the following fields, define the number of retry attemps and the waiting time in seconds before the next retry.

[Activate]

To activate the error actions for the error action type, click the [Activate] button. Active error actions have a green icon, inactive error actions have a red icon.

[List]

To display, change, activate or deactivate error actions, click the button.



* The list displays all error action events including type, event ID, sender and receiver filter.
* Collapse or expand each entry to display the assigned actions.
* To open the edit user interface for an error action event, click the pen icon.
* To delete an error action event, click the delete icon.
* To activate or deactivate an error action event, click the red or green icon. The green icon indicates active error action events, the red icon indicates inactive error action events.

### 1.12.5 Configuring the Garbage Collection for Error Information

The error handling stores information about the following:

* Messages with INCOMMIT status that the integration framework has set to FINAL for DI calls
* Message with ROLLBACK status that the integration framework has unsuccessfully tried to process
* Soft exceptions

Soft exceptions are exceptions that do not call the integration framework error handling. Usually, soft exceptions only occur temporarily and the integration framework processing resolves them after some time. If a soft exception occurs, the integration framework waits for 10 seconds and then tries to process the message again. At runtime, the integration framework displays soft execptions in the message log. For example, for SAP Business One DI inbound, the integration framework throws a soft exception, if the DI adapter is already busy and does not accept additional calls.

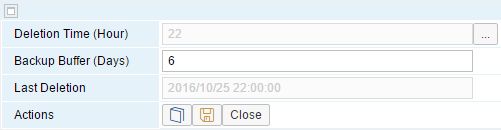
* Messages that block a queue together with the number of attempts to process them
* Conflicting settings
* Information about filtered events

You have, for example, imported a scenario package, have set it up and have activated it and now a step of the package is inactive and cannot process the event.

* Information about incoming events the integration framework cannot process, because the scenario step is not correct.
* If you have defined settings to remove messages from queues to enable further processing, the integration framework writes the deleted messages to a dedicated table.

If updated information is available for an already existing record, the integration framework does not create a new record, but updates the existing one.

To automatically delete old error information from the integration framework, choose *Maintenance* → *Cfg Error Handling* and click the *[Garbage Collection]* button.



Deletion Time (Hour)

Select the deletion time from the list. The integration framework deletes the log on the hour. By default, the integration framework deletes the message log at the 22nd hour.

Backup Buffer (Days)

Specify how many days you do not want any deletion. The default is 6 days.

Last Deletion

The integration framework displays the timestamp of the last automatic daily deletion.

[Save]

To save the configuration, click the button.

## 1.13 Configuring the Audit Control Function

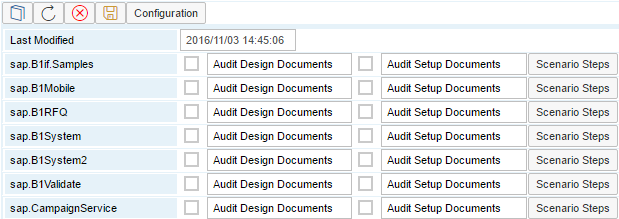
With the audit control monitor configuration you can create table entries to track changes in scenario design or scenario setup for all or for specific scenario packages or scenario steps. By default, audit control is not active after installation. Choose *Monitoring* → *Process Control* and expand the *Framework Processes* section. The *AuditControl* process is inactive.

You can create the AUDITCTRL table in a database. The table has the following fields:

* ts - timestamp
* usr – name of the admin user who has made the change
* id - name of the scenario package in which a document has been changed or name of the scenario step in which a document has been changed or the fixed value audit control, if the entry indicates that the audit control is switched on or off
* type – P, if the changed document belongs to a scenario package  
   S, if the changed document belongs to a scenario step  
   Y, if the entry indicates that the audit control is switched on or off
* doc – name of the changed document or start, if the entry indicates that the audit control has been switched on, or stop, if the entry indicates that the audit control has been switched off

Use the table content for auditing reports.

To open the audit control monitor configuration, choose *Maintenance*→*Cfg Audit Control*.



The audit control monitor displays scenario packages that are part of your integration framework.

Audit Design Documents

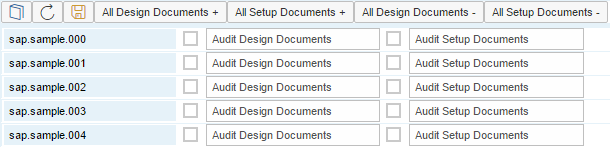
To deactivate audit control for the scenario package design documents, select the checkbox.

Audit Setup Documents

To deactivate audit control for the scenario package setup documents, select the checkbox.

[Scenario Steps]

To deactivate audit control for scenario steps of a scenario package, click the [Scenario Steps] button.



[All Design Documents+]

To select all scenario steps for deactivating the audit control for all design documents, click the button.

[All Setup Documents+]

To select all scenario steps for deactivating the audit control for all setup documents, click the button.

[All Design Documents-]

To deselect all scenario steps for deactivating the audit control for all design documents, click the button.

[All Setup Documents-]

To deselect all scenario steps for deactivating the audit control for all setup documents, click the button.

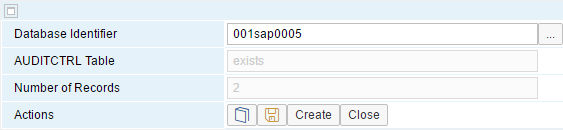
[Save]

To save your settings, click the button.

[Configuration]

To configure the database table that contains the audit control records, click the button.

The integration framework displays the following user interface:



Database Identifier

To select a database from SLD as the location for the AUDITCTRL table, click the […] button.

AUDITCTRL Table

The integration framework displays whether the table exists or does not exist in the database.

Number of Records

The integration framework displays the number of records in the AUDITCTRL table.

[Activate]

To create AUDITCTRL table in the database, click the button.

[Save]

To save your settings, click the button.

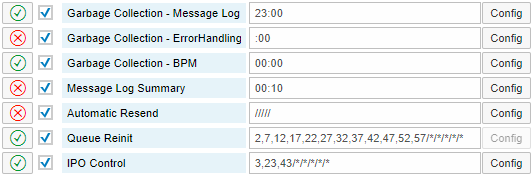
[Red button]

To activate audit control, click the [red button].

## 1.14 Configuring Daily Actions

Daily actions give you an overview of settings that you have defined in the integration framework.

To display daily actions, choose *Maintenance* → *Daily Actions*.



Icon

The green or red icon indicates whether you have configured the daily action or not.

Checkbox

To activate or deactivate a daily action, click the checkbox.

Daily Action Title

You can display or configure the following for daily actions:

* The garbage collection for the message log deletes old messages from the message log, if you have configured it.

For more information, see the section Configuring the Message Log

* The garbage collection for error handling deletes old error handling messages, if you have configured it.

For more information, see the section Configuring the Garbage Collection for Error Information

* The garbage collection for BPM-related information. For more information, see the Business Process Management guide
* The message log summary gives you an overview of transactions of one day. You can activate it and configure whether you want to receive a notification e-mail.
* With the automatic resend function you can set a timer that triggers a process to automatically resend messages in the error inbox. To enable the function, click Config and define a timer.
* The queue reinit function checks and reinitialzes the processing queues
* In the IPO control function, you can montitor scenario package processes and obtains an e-mail, if processes of a package fail repeatedly.

Field behind Title

The integration framework displays the last time it has performed the action, or the settings for the action.

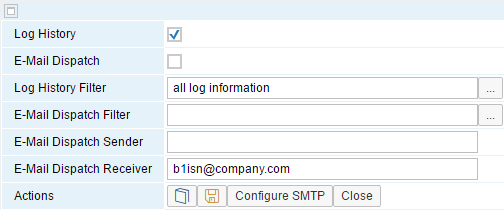
[Configure]

To configure the daily action, click the button.

### 1.14.1 Configuring the Log Summary

To receive a report of transactions of the previous day, activate the log summary. The report runs at hour 00:10. You can save the information in the message log history and you can receive an e-mail with the report.

To open the *Configuration of the Daily Action Log Summary* user interface, choose *Maintenance*→*Daily Actions* and for *LogSummary*, click the *Config* button.



Log History

To activate and define the log history, select the checkbox.

E-Mail Dispatch

To enable sending the message log history to an e-mail recipient, select the checkbox.

Log History Filter

To define, which messages you want to log, select the following:

* With all log information, you get a report about all messages.
* With cancelled logs only, you only get a report about the messages, which the integration framework could not process successfully.

E-Mail Dispatch Filter

To define, which messages you want to receive with an e-mail, select the following:

* With all log information, you get a report about all messages.
* With cancelled logs only, you only get a report about the messages, which the integration framework could not process successfully.

E-Mail Dispatch Sender

Enter the e-mail address of the message log sender.

E-Mail Dispatch Receiver

Enter the e-mail address of the message log receiver.

[Save]

To save your settings, click the button.

[Config SMTP]

For more information, see section *Configuring Connectivity to the Internet and E-Mail Server*

### 1.14.2 Configuring Message Log Deletion

To open the user interface, choose *Maintenance*→*Daily Actions* and for *LogGarbageCollection*, click the *Config* button.

For more information, see section *Configuring the Message Log*

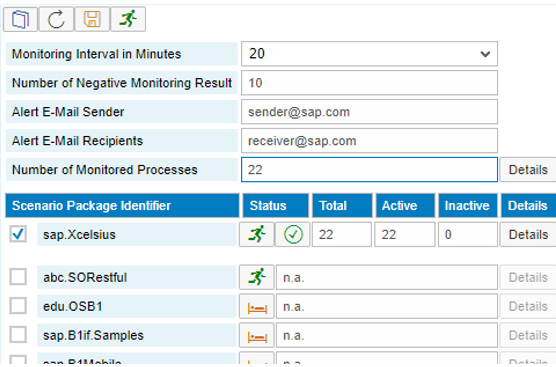
### 1.14.3 Monitoring Scenario Package Processes

The IPO control function offers the possibility to monitor processes of active scenario packages.

To open the user interface, choose *Maintenance*→*Daily Actions* and for *IPO Control*, click the *Config* button.

The monitor for scenario package processes displays scenario packages that are set up. You can select scenario packages that you want to monitor.

For selected scenario packages, you can display the runtime processes (IPO steps). The monitor displays the status of the scenario packages and errors that occur in scenario package processes, and you can display details and analyze the involved IPO logs.



Monitoring Interval in Minutes

Enter after how many minutes the monitor checks the processes

Number of Negative Monitoring Results

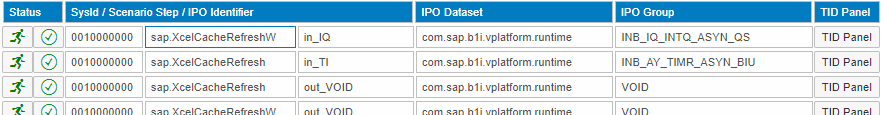
Enter after how many errors an e-mail recipient is notified.

Alert E-Mail Sender and Recipients

Enter the e-mail address of the sender and recipient email addresses separated by semicolon.

Number of Monitord Processes

The integration framework displays the number of monitored processes. To display process details, click Details.



Scenario Packages

For each selected scenario package, the monitor displays the status, the number of scenario package processes, the number of active and inactive scenario package processes. To display process details click Details.

The integration framework displays the following information:

* Status for each process (IPO)
* SysId, scenario step name and IPO name
* IPO dataset and group in BizStore
* TID Panel: Click the button to display the transactions of the process

The monitor allows selecting processes for scenario packages. If you only want to monitor specific processes (IPOs) of a package, provide the IPOControl.xml document in the vPac folder of the scenario package in the BizStore. The document has the following structure:

<IPOs>

<IPO>ipoStepUri </IPO>

<IPO>ipoStepUri </IPO>

…

</IPOs>

You can find the IPO step URIs in the transaction ID panel.

## 1.15 SAP Business One Offline Support

Documentation for the *B1 Offline Client* and *B1 Offline Server* functions is available in the *Configuring the Offline Support Server and Client* guide.

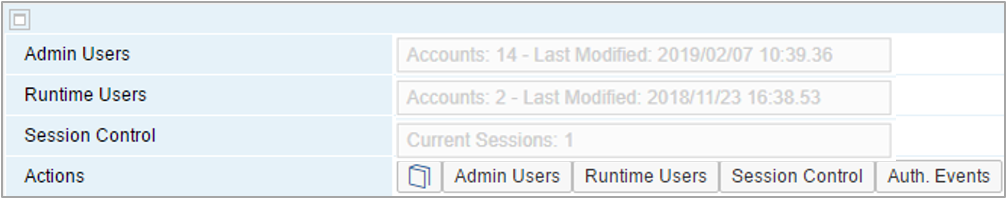
* The *B1 Offline Server* function is available in SAP Business One integration for SAP NetWeaver.
* The *B1 Offline Client* function is available in the integration framework for SAP Business One.

## 1.16 User and Session Administration

The integration framework supports a user and session concept. The session concept is relevant for incoming HTTP calls, such as:

* User administration of the integration framework
* Incoming HTTP calls for scenario packages
* Inbound channel for event sender from SAP Business One

To access the user interface, choose *Maintenance* → *User Administration*.



The integration framework supports administration and runtime users:

* Administration users set up systems, develop scenario packages, set up scenario packages and administer scenarios at runtime.
* Runtime users are technical users. They are event senders from SAP Business One and optional incoming HTTP calls for scenario packages that use basic authentication or a user authentication with special settings.

B1iadmin is the standard default administration and runtime user delivered with the installation.

Admin Users

The integration framework displays the number of administration users and the timestamp of the last change.

Runtime Users

The integration framework displays the number of runtime users and the timestamp of the last change.

[Admin User]

Add, change, delete and activate or deactivate user accounts for administrative tasks.

[Runtime User]

Add, change, delete and activate or deactivate user accounts for the integration processing runtime and the B1 event inbound channel.

[Session Control]

Display a list of currently running sessions. You can terminate a session.

[Auth. Events]

The integration framework displays the authentication event histroy for HTTP sessions of administration or runtime users.

### 1.16.1 User Administration

A user administration is available for administration and for runtime users. To open the user administration, click the according button.

Runtime users are event senders from SAP Business One and optional incoming HTTP calls for scenario package*s*, if the scenario package uses basic authentication or a user authentication with special settings. Event senders are only relevant, if you have installed the EventSender and DI Proxy.

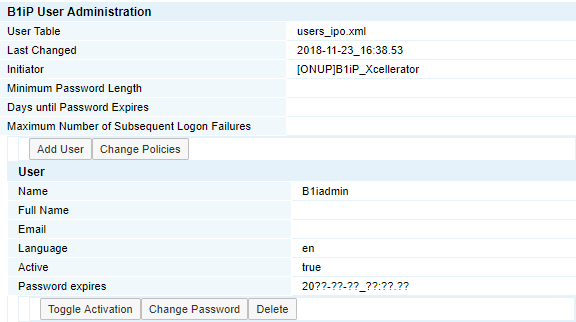
The following table gives you an overview of possible combinations:

| Scenario Package Design | Authorization Concept Definition | | | | Runtime | |
| --- | --- | --- | --- | --- | --- | --- |
| User/Password Handover | | Validation | |
| Authenti-cation | User/ Pass-word Hand-over | On\_Authen-ticate bfd | User List | Authentica-tion.bfd | Auth. Mode | Validation/  User List |
| No authentica-tion | - | - | - | - | none | - |
| Basic authentica-tion | - | - | - | - | basic | runtime user list |
| User authentica-tion () | basic | - | not defined | not defined | basic | runtime user list |
| basic | - | not defined | defined | basic | process step |
| userdef | not defined | not defined | not defined | basic | runtime user list |
| userdef | not defined | not defined | defined | basic | process step |
| userdef | not defined | defined | not defined | basic | special user list |
| userdef | not defined | defined | defined | basic | process step |
| userdef | defined | not defined | not defined | userdef | runtime user list |
| userdef | defined | not defined | defined | userdef | process step |
| userdef | defined | defined | not defined | userdef | special user list |
| userdef | defined | defined | defined | userdef | process step |

#### 1.16.1.1 Managing Runtime Users

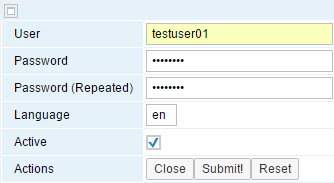
Runtime users are technical users. They are event senders of SAP Business One and optional incoming HTTP calls for scenario packages that use basic authentication or a user authentication with special settings. With the installation, the integration framework provides the B1iadmin default user.

To open the *User Administration* for runtime users and display the users, click [Runtime Users]:



[Add User]

To add a user, click the button. The following window opens:



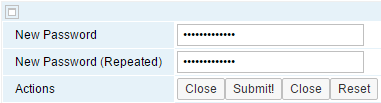
| **Field** | **Description** |
| --- | --- |
| User | Enter a unique user name |
| Password, Password (Repeated) | Enter the password for the user. The password must have eight or more characters.  Prior to B1iF version 1.17.7, the minimum password length is six characters. |
| Language | Enter the language for the user. The integration framework is currently available in English. The scenario setup user interface and some other related user interfaces are also available in German, French and Chinese |
| Active | This option allows you to enter future users for the integration framework and to set them to active later. To activate the user , select the checkbox. |
| Submit | To add a user, click the button. |

[Toggle Activation]

To set a user active or inactive, click the button.

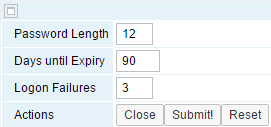
[Change Password]

To enter a new password for an existing user, click the button. Enter a password for the user. The password must have eight characters or more.



[Change Policy]

To change the policy for passwords, click the [Change Policy] button.



Password Length

Enter the length of the password that each user must set. The default in 8.

Days until Expiry

Enter the number of days until a password expires. The default is 100.

Logon Failures

Enter the maximum number of attempts, a user has to logon to the integration framework.

[Delete]

To delete the user, click the button.

#### 1.16.1.2 Managing Administration Users

Administration users set up systems, develop scenario packages, set up scenario packages and administer scenarios at runtime. They use the integration framework user interface. With the installation, the integration framework provides the B1iadmin default user.

To open the *User Administration* for administration users and display the users, click the [Admin User] button:

The framework displays the list of users.

[Add User]

To add a user, click the button. The following window opens:



| **Field** | **Description** |
| --- | --- |
| User | Enter a unique user name |
| Full Name | The framework uses the information when sending an e-mail after the user clicked the I have forgotten my password link on the login screen. |
| Email | The entry is required to display the I have forgotten my password link on the login screen |
| Password, Password (Repeated) | Enter the password for the user. The password must have eight or more characters.  Prior to B1iF version 1.17.7, the minimum password length is six characters. |
| Language | Enter the language for the user. The integration framework is currently available in English. The scenario setup user interface and some other related user interfaces are also available in German, French and Chinese |
| Active | This option allows you to enter future users for the integration framework and to set them to active later. To activate the user , select the checkbox. |
| Submit | To add a user, click the button. |

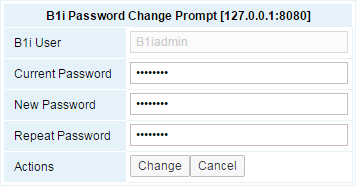
[Toggle Activation]

To set a user active or inactive, click the button.

[Reset Password]

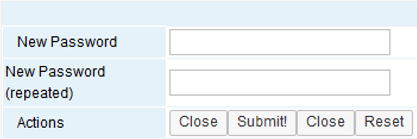
* To reset the password for a user, click the button.

If you log on for the first time after password reset, enter the current (old) password and enter the new password for further access to the integration framework. The new password must be different from the old password and must have at least eight characters.



* To reset the password for another user, click the [Reset Password] button.

The integration framework requires you to enter a new initial password for the user:



The password must have at least eight characters. Provide the initial password to the user.

If the user logs on for the first time after password reset, he or she enters the initial password in the *Current Password* field and enters the new password for further access to the integration framework. The new password must be different from the old password and must have at least eight characters.

**Password Expiration**

Administration user passwords expire after 100 days by default. You can change the default value in the following file:

.../B1iXcellerator/exec/webdav/com.sap.b1i.system.xc/xml.auth/users\_bfd.xml

Set the expiryDays attribute. The default is 100.

**Minimum Password Length**

Use the minLength attribute to increase the minimum length of the password. The default minimum length is eight characters.

**Maximal Number of Wrong Password Entries**

Use the maxFailures attribute to change the number of allowed wrong password entries. The default is 5.

[Change Policy]

To change the policy for passwords, click the button.



Password Length

Enter the length of the password that each user must set. The default in 8.

Days until Expiry

Enter the number of days until a password expires. The default is 100.

Logon Failures

Enter the maximum number of attempts, a user has to logon to the integration framework.

#### 1.16.1.3 Adding Views to Administration Users

As of integration framework version 1.22.0, you can add different types of views to administration users. The user views control access to integration framework functions on menu entry level. Already existing users continue to have access to all functions after upgrade. If you do not define views for new users, they do not have access to any functions.

The following user views are available:

**Administrator**

Users with the view can perform technical configuration, administration and content development. The view provides access to functions provided by the default B1iadmin user. The view allows access to all integration framework functions.

**Developer**

Users with the view can design and set up integration content, and they have access to monitoring and development-related functions.

**Configurator**

Users with the view can perform technical configuration and the configuration of integration content, and they have access to monitoring.

**Supervisor**

Users with the view can perform monitoring, value mapping, resend messages , and test connection.

The table below displays menu items of the integration framework, the delivered user views, and the functions they provide access to:

| **Menu** | **Administrator** | **Developer** | **Configurator** | **Supervisor** |
| --- | --- | --- | --- | --- |
| **Cockpit** | X | X | X | X |
| **SLD** | X |  | X | X |
| **Maintenance** |  |  |  |  |
| System Info | X | X | X | X |
| ZIP Import | X |  | X |  |
| Cfg Dev. Env | X | X |  |  |
| Cfg Runtime | X |  | X |  |
| Cfg Connectivity | X | X | X |  |
| Cfg Metadata | X |  | X |  |
| Cfg B1 Cloud | X |  | X |  |
| Cfg B1 Event Filter | X |  | X |  |
| Cfg B1 Event Subscriber | X |  | X |  |
| Cfg MsgLog | X | X | X |  |
| Cfg Error Handling | X | X | X |  |
| Cfg Audit Control | X |  | X |  |
| Daily Actions | X |  | X |  |
| B1 Offline Client | X |  | X |  |
| B1 Offline Server | X |  | X |  |
| User Administration | X |  | X |  |
| **Scenarios** |  |  |  |  |
| Package Design | X | X |  |  |
| Step Design | X | X |  |  |
| Setup | X | X | X | X |
| Control | X | X | X |  |
| Reports | X | X | X | X |
| Import | X | X | X |  |
| Export | X | X | X |  |
| Authentication | X | X |  |  |
| **Monitoring** |  |  |  |  |
| Message Log | X | X | X | X |
| Process Control | X | X | X | X |
| B1 Event Monitor | X | X | X | X |
| Queue Monitor | X | X | X | X |
| Authentication Monitor | X | X | X | X |
| Call Monitor | X | X | X | X |
| Audit Control Monitor | X |  | X | X |
| Message Log History | X |  | X | X |
| **Tools** |  |  |  |  |
| Control Center | X | X | X | X |
| Troubleshooting | X |  | X |  |
| Benchmarks | X |  | X |  |
| B1 Event Generator | X |  | X |  |
| B1 Event Filter Generation | X |  | X |  |
| XML Editor | X | X |  |  |
| Log Entries Mass Deletion | X | X |  |  |
| **Help** |  |  |  |  |
| XSLT Library | X | X |  |  |
| B1 Object Help | X | X |  |  |
| B1 Service Help | X | X |  |  |
| Online Help | X | X | X | X |
| Documents | X | X | X | X |
| B1 Landing Page | X | X | X | X |
| B1i Forum | X | X | X | X |

[Add User View]

To add a view to a user, click the button, select the view you want to assign to the user and click [Submit].

[Describe]

To display the description of the assigned user view, click the button.

[Remove]

To remove the view assignment from the user, click the button.

#### 1.16.1.4 Enabling the Password Reset Process

As an integration framework administrator, you can enable the I have forgotten my password link that triggers the password reset process in the integration framework login screen.

**Procedure**

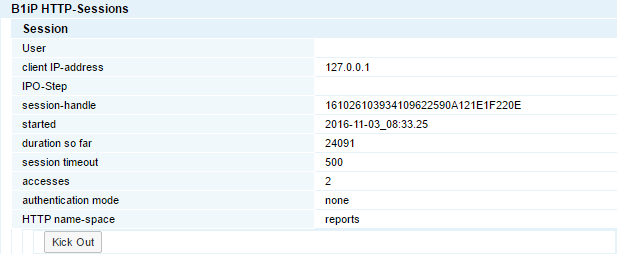
1. To enable the process to reset passwords for users, open the following document in the BizStore: com.sap.b1i.system.xc/xml.auth/sendEmailConnectionParams.xml.
2. Enter the following values:

| **Element** | **Description** |
| --- | --- |
| passwordResetEnabled | The parameter enables or disables the link on the login screen.  Set the value to true. The default is false. |
| smtpHost | Host name or IP address of the SMTP server. Together with the parameter above, the parameter is required for the process |
| smtpPort | Port of the SMTP server. Required for the process. |
| smtpUser | User name part of the credentials for the SMTP server.  If the server does not require authentication, leave the element empty. |
| smtpPassword | Password part of the credentials for the SMTP server.  If the server does not require authentication, leave the element empty. |
| fromMail | Sender e-mail address in the outgoing e-mail |
| useTSL | If the SMTP server uses TSL, set the value to true, otherwise to false. |
| useSSL | If the SMTP server uses SSL, set the value to true, otherwise to false. |

1. The integration framework delivers a predefined e-mail text. To change the text, open the following document in the BizStore: com.sap.b1i.system.xc/xsl/prepareEmail.xsl
2. In the document, adjust the text of the message variable.
3. To let integration framework users participate in the process, make sure that the Email field is filled with a valid e-mail address for each administration user in Maintenance → User Administration in the Admin Users function.
4. To make the E-mail message more personal, you can enter the first name and name of the user in the *Full Name* field. This is not required, if you do not want to store personal user data.

### 1.16.2 Session Control

With the session control monitor you can display currently running sessions. You also have the option to terminate (kick out) sessions.



The integration framework sorts the list by HTTP namespace, IPO step and user.

User

This is the user ID, the session runs for.

client IP-address

This is the IP address of the client.

IPO-Step

This is the name of the process step, if an inbound call of a scenario step initiates the session.

For more information about the process logic in the integration framework, see section *Process Control*

session-handle

This is the session identifier.

started

This is the timestamp of the session start.

duration so far

This field displays the session duration in seconds.

session timeout

This is the timeout setting for this session in seconds.

The session automatically expires when it is idle for the displayed period of time.

accesses

This is the number of calls in the session.

authentication mode

This is the authentication mode of this session. The following settings are available:

* none
* basic (user name, password)
* userdef (user-defined)

HTTP name-space

This is the namespace of the HTTP session. The namespace indicates the type of the incoming call.

* dummy

This is an administration session. This is typically a session triggered from the administration console.

* webdav

This is a session triggered by a WebDAV client

* basic

This is an incoming HTTP call, either by the EventSender or any incoming call for a scenario step.

* soap

This is an incoming SOAP call. This is any incoming call for a scenario step, triggered by a Web service.

[Kick Out]

To terminate a session, click the button. The session handling expires and the integration framework accepts no further calls.

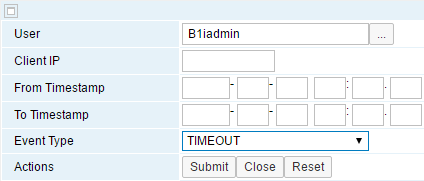
### 1.16.3 Authentication Events

Authentication events give you an overview of login information for HTTP sessions.

To generate a list of logins for all HTTP sessions, click the [Authentication Events] button. The history is a ring buffer and allows you displaying the last 500 entries.

Choose whether you want to display authentication events for administration or runtime users.

Enter your selection criteria or click [Submit!] to display the complete list.



User

Select a user from the list.

It depends on the authentication concept of a scenario package, if the incoming HTTP calls use the list, an individual list or even an individual validation process. If you want to select a user that is not part of the list, enter the user name.

For more information, see section *Authentication for Incoming HTTP Calls*

Client IP

To check if a specific machine triggers sessions, enter the IP address.

From Timestamp, To Timestamp

To select events for a specific time interval, enter the start and end time.

Event Type

The authorization events names end with a type. The following types are available:

* LOGON (

This is a successful logon.

* LOGOFF

This is a successful logoff.

* FAILURE

This logon has failed.

* TIMEOUT

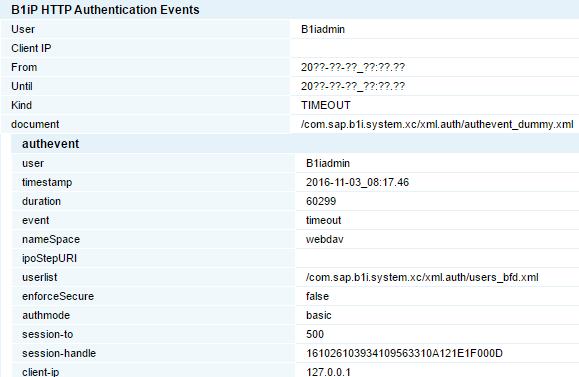
This logon has timed out.

* KICKOUT

The administration has kicked out this logon.

* DEACTIVATED

This is a logon, which has been deactivated after five failed attempts to log on.



# 2 Using Integration Framework Tools

## 2.1 Generating SAP Business One Events

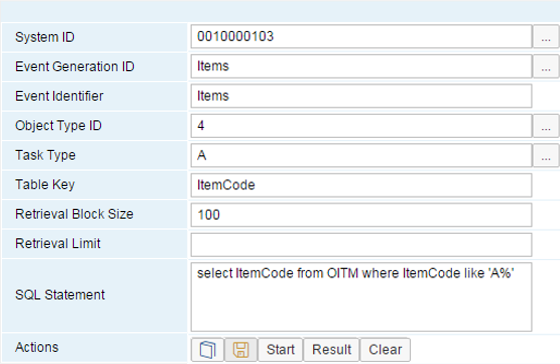
If an SAP Business One user creates, changes, or deletes data, SAP Business One creates events the integration framework picks up and processes, if a scenario step has subscribed to the events.

To create events for SAP Business One object types without changing anything in SAP Business One, use the SAP Business One event generator. Use it to initially load data from SAP Business One. For the selected object type, the event generator creates an event for each record of the SAP Business One table and places it in the integration framework internal queues. The entries in the queues trigger the import process from SAP Business One. You can create events for all records in a database table of an object type, or you can set a limit for event creation.

The event generator does not create events in the SAP Business One SEVT table, and it does not use the EventSender. It bypasses the mechanisms to avoid load on the components.

The integration framework stores the information for event generation in a profile. The user interface allows you to administer event generation profiles. The event generation ID and the system ID identify a profile.

To administer profiles and generate events, choose *Tools*→ B1 *Event Generator*.



System ID

Select a SAP Business One system from the System Landscape Directory (SLD).

Event Generation ID

Enter the identifier for the profile. To display a profile, select an identifier from the list.

Event Identifier

You have the option to enter an event identifier. The integration framework uses it as an attribute of the event.

Use the identifier, for example, to differentiate between initial load and delta processing. At runtime, you can access the value with the following XPath statement:

/vpf:Msg/vpf:Body/vpf:Payload[@Role=‘T‘]/Event/b1ie:B1IEvent/@Identifier

Object Type ID

Select an SAP Business One object type.

Task Type

Select the task type for event generation. The following options are available:

* A for Add or Insert. This is the default. Internally, the integration framework uses I.
* U for Update.
* D for Delete
* C for Cancel
* L for Close, for example, to set the status for a slaes order to closed.

Table Key

The integration framework automatically adds the primary key of the table for the selected object type.

Retrieval Block Size

Enter the number of events the integration framework generates in one pass. The default is 100.

Retrieval Limit

Enter the maximum number of events the integration framework generates in one pass.

Use the limit for testing to restrict the number of messages. For testing in scenario step development, you can use this function with limit = 1 instead of creating new test data in SAP Business One each time.

SQL Statement

The integration framework adds the SQL statement that selects records from the SAP Business One database table. You can use the {key} parameter to represent the key.

If the integration framework runs on SAP HANA, enter a valid SQL statement for SAP HANA.



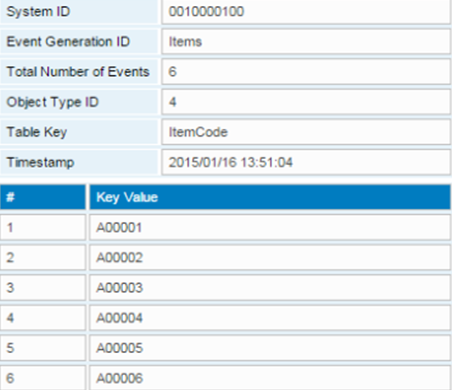
Save the generation profile.

[Start]

Trigger the event generation. Click the button only once.

[Result]

To display the result of the event generation, click the button.



The integration framework displays the events it has generated with the generation ID, the number of events and the timestamp.

To display the result in XML, click *Display result in XML*.

<?xml version="1.0" encoding="utf-8" ?>

<EventGenerator sysid="0010000100" genid="22" cnt="6" ts="2013/12/06 15:03:19">

<event no="1" object="2" key="CardCode" value="a" />

<event no="2" object="2" key="CardCode" value="a,bc" />

<event no="3" object="2" key="CardCode" value="a,bcd" />

<event no="4" object="2" key="CardCode" value="aaa" />

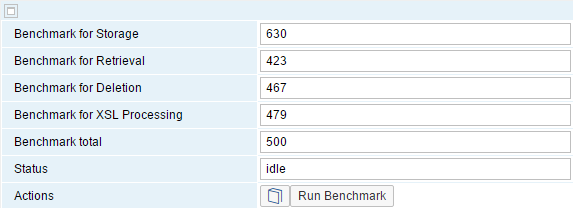
<event no="5" object="2" key="CardCode" value="aaasda" />

<event no="6" object="2" key="CardCode" value="c01" />

</EventGenerator>

## 2.2 Displaying Benchmarks

The benchmarks provide an initial indicator whether the integration framework is in healthy state. To displays benchmarks, choose *Tools* → Benchmarks.



To run calculations for benchmarks, click the [Run Benchmarks] button.

The integration framework displays the following:

* A benchmark for storing operations in the BizStore
* A benchmark for retrieval operations from the BizStore
* A benchmark for delete operations from the BizStore
* A benchmark for XSLT processing
* The total benchmark for all operations
* The benchmark processing status, either idle or busy

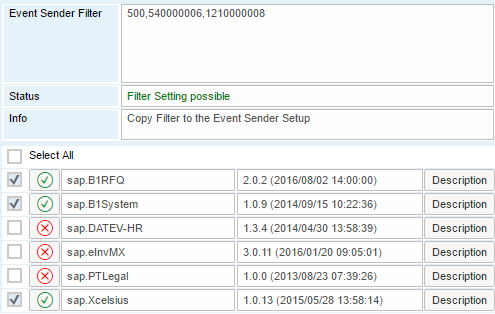
## 2.3 Using the SAP Business One Event Filter Generator

In the event sender setup, you can define filters that determine, for which company databases and objects events are created. If you enable event creation for the company database and do not define additional settings in the *Event Filter* section, you enable the creation of more events than you need for your integration scenarios. Such events remain in the SEVT table of the SBO-COMMON database and the table grows.

Using the SAP Business One event filter generator, you can generate filter settings based on the scenario packages in the integration framework. After filter settings generation, copy the settings and paste them to the *Include List B1 Object(s)* field in step 4/5 of the event sender setup.

As of integration framework version 1.22.19, the event filter generator is part of the event sender setup in the integration framework.

To generate filter settings, choose *Tools* → B1 *Event Filter Generator*.



List of Scenario Packages

The list displays available scenario packages triggered by SAP Business One events in the integration framework. The green or red icon indicates, whether the scenario package is active or inactive.

Select All, Deselect All

To select or deselect all scenario packages for event filter generation, click the checkbox.

Active scenarios and the SAP Business One system package (sap.B1System) are selected by default. You cannot deselect the system package, because the integration framework needs the notifications for the system package to keep the SAP Business One company database information synchronized SLD. To deselect an active scenario package, deactivte it first.

Checkbox for Each Scenario Package

To select or deselect a scenario package for event filter generation, click the checkbox.

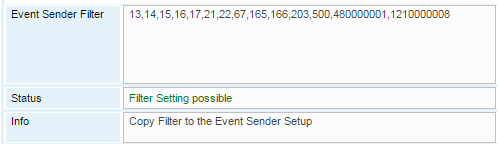
[Description]

To display the scenario package description, click the checkbox.

[Generate]

To generate the filter definitions for the selected scenario packages, click the button.

The integration framework displays the following information:



Event Sender Filter

The integration framework displays the object IDs required by the scenario packages. Copy the content and paste it to:

Event sender setup, step 4/5 *Choose the Company Databases*, click the *Filter* button, *Include List B1 Object(s)* field

Status

The integration framework displays, if the filter settings generation is possible or not. Filter setting generation is not possible, if a scenario step subscribes to all SAP Business One objects (\*).

**Reducing the Event Generation for a Generic SAP Business One Inbound Step**

If you design a scenario step using SAP Business One (B1) inbound that subscribes to all events entering an asterisk (\*) in the Identifier field and you want to use such a step in many packages, you can provide definitions to use the step for certain events.

* Add the vB1ObjList.xml file in the vPac.<your\_namespace>.<package\_name> folder of your scenario package in the BizStore.
* Define the events in the following way:

<vB1ObjList xmlns:bfa="urn:com.sap.b1i.bizprocessor:bizatoms">

<obj>2</obj>

<obj>3</obj>

<obj>4</obj>

</vB1ObjList>

The filter generator considers the definitions.

## 2.4 Displaying Documentation

The integration framework documentation is available in htm and pdf format. The integration framework displays the htm version in the user interfaces and in the online help. Use the pdf version for printing. The content is identical.

To access documentation, you have the following options:

**Integration framework User Interfaces**

In the integration framework user interfaces, click the  (book) icon. The integration framework opens the documentation for the user interface.

* If the book icon is light blue (), documentation is not yet available.
* If the documentation is available, but not yet loaded to the integration framework, the integration framework displays the following icon: 

**Online Help**

To get an overview of available documentation, choose Help → Online Help.

The integration framework displays documentation for the following areas.

* In the *Development Environment* guide, find information about how to set up the development environment and how to import and export documents.
* In the *Scenario Developemt* guide, find information about how to develop integration content in the integration framework.
* In the Business Process Managemant guide, find information about how to develop and manage business processes
* In the System Landscape Directory (SLD) guide, find information how to create system information
* *Operations Guide Part One* provides documentation about administering scenario packages, and monitoring.
* *Operations Guide Part Two* contains information about the technical configuration of the integration framework, the framework tools and additional configuration steps to ensure security.
* *Operations Guide Part Three* contains the security guide and performance information.
* The integration framework contains a *troubleshooting* framework that supports you in troubleshooting the following:
* SAP Business One event sender
* SAP Business One setup
* Mobile App for SAP Business One
* The *Schemas* guide provides information about the integration framework schemas.
* The *APIs* guide describes the integration framework APIs.
* With the integration framework, you can run connected SAP Business One systems in online (permanently connected) or in offline mode (occasionally connected). The *Offline Support* guide describes how to run SAP Business One in offline mode.

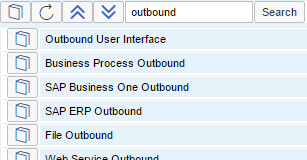


To expand or collapse all, click the icons.

/

To expand or collapse a node, click the icon.

Search



To search the headings of integration framework documentation, enter a term, or terms and click the search button.

The integration framework displays all headings containing the term or terms.



To display documentation, click the icon.

If the integration framework cannot find the heading in the document, it opens the document at the beginning.

If the integration framework cannot find the document, it displays the following icon: 

**Documentation for Printing in PDF Format**

To get an overview of available documentation, choose Help → Documents. The integration framework displays the guides available in PDF format.

To open the PDF document, click the button. The documentation content is identical with the one in the *Online Help* section, except that you can additionally find documentation assigned to scenario packages that are part of your integration framework and technical adapter documents. The scenario package documents either contain the configuration information for the scenario packages, or they point you to places, where you can find the configuration information.

## 2.5 Using the Embedded XML Editor in Scenario Design

In several places in scenario step design, you are required to edit documents:

* XSL documents of the xform and final atoms
* Regex and read file atoms for the format control document
* In flat file outbound for the format control document
* In file inbound retrieval for the format control document
* Process flow test environment for the inbound message
* Documents of the Key Exansion atom

You can use the internal embedded XML editor.

**Prerequisites**

To enable the XML editor, you have chosen *Maintenance* → *Dev. Environment* and you have selected the *Embedded XML Editor* checkbox.



The icon indicates that the XML editor is available. To edit the document, click the button. The document opens for editing.



To open the document using pretty print, select the checkbox.



To export a document to the xmledit.export.zip file, click the button.

 (Pretty Print)

To display the text in a structured way, click the button.

**XML Editor in the Tools Menu**

The XML editor is also available in the Tools menu.

* In the Document (BizStore URI) field, select the dataset, group and name of the document and click Open.

The XML editor opens displaying the document.

* Click Pretty Print to display the document in a structured way.
* Edit and save the document.

## 2.6 Performing Mass Deletion of Log Entries

When running the integration framework as a development system, the integration framework creates a high amount of log entries. The function displays the available message log, debug log and SAP Business One event log entries and enables you perform mass log deletion.

The following selection criteria are available:

Log Type

Select the log type you want to delete.

For the debug log type, you can choose the fast or slow deletion method. The fast deletion method makes the integration framework unresponsive. Before choosing the fast method, do the following:

* Choose Monitoring → Queue Monitor and clear the queues.
* Deactivate the scenario packages

The slow deletion method is significantly slower, however you can continue working in the integration framework and the function displays the progress of deletion.

Batch Size

The function deletes log entries in batches. Enter the batch size. The default is 1000.

Refresh Automatically

To automatically refresh the log entry display, select the checkbox.

Delete

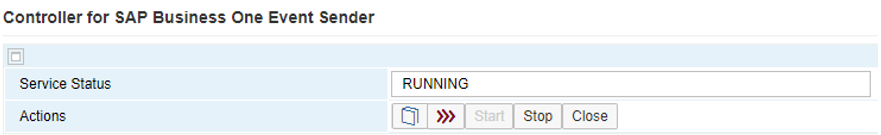
To delete log entries, click the icon.

The report displays the number log entries in the integration framework.

## 2.7 Stopping, Starting the Event Sender and Changing Settings

Note that the function only works, if the event sender is installed on the same machine as the integration framework.

SAP Business One writes events for new data, changes and deletions to the SEVT table of the SBO-COMMON database. Based on filter settings, the event sender accesses the table, retrieves data and hands over the events to the integration framework for further processing.



The function allows you to display the status of the SAP Business One event sender, start or stop the service and call the setup wizard to change event sender settings.

The installation program installs and sets up the event sender on the SAP Business One server. The following section describes event sender settings, although usually no further changes are required.

Only call the event sender setup in the following cases:

* You must change the password for database access.
* You have changed the B1iadmin password for the runtime user.
* You have moved to another server.
* To reduce the message load, you want to include or exclude some objects.
* You want to exclude users.

To check the settings for the event sender, use the integration framework troubleshooting function. In the integration framework, choose Tools → Troubleshooting, and in the Functional Group field, choose Event Sender.

**Procedure**

1. To call the SAP Business One event sender setup, choose Tools → Event Sender.
2. To stop the service, click Stop; to start the service, click Start.
3. To open the setup wizard, click Setup Wizard.
4. In step 1 (Connect to SAP Business One), in the Choose Database Type field, select the SAP Business One database type.
5. In the DB Connection Settings section, you can set the following:

* In the DB Server Name field, enter the computer name or IP address of the machine, where the database of the SAP Business One server is installed. Do not use localhost. We recommend using the host name of the server. Only if you have problems specifying the host name, use the IP address instead.
* In the Port field, enter the port number of the database server, where the SAP Business One server is installed.
* In the Setup DB Account and Password fields, the installation has set the database user name and password for database access during setup. This user must have access rights to create tables and store procedures.
* In the Running DB Account and Password fields, the installation has set the database user name and password for database access at runtime. This user must have access rights to the event log and event lock tables.
* To test the connection, click Test Connection.

1. Save your settings and click Next.
2. In step 2 (Configure Event Sender Parameters), the following settings are available in the Monitor Settings section.

* In the Idle Time (Millisecond) field, you can change the time period the event sender waits until it polls events from SAP Business One. The default is 3000 milliseconds.
* In the Batch Count field, you can set the number of events the event sender polls each time. The default is 10.
* Save your settings and click Next.

1. In step 3 (Configure Integration Framework Parameters), you can change general settings for the integration framework.

For the Distribute Sending Method, the event sender sends all events to the local server address and the event dispatcher takes over the task of distributing the events to other systems.

In the General Integration Framework Settings, you can configure the following:

* In the Protocol Type field, select the protocol for the connection between the event sender and the integration framework. To enable https, make settings in the Tomcat administration.
* In the Authentication Type field, always use the Basic option. This is the default.
* In the Framework Server Host field, enter the name or IP address of your integration framework or the SAP Business One integration for SAP NetWeaver server. Dor the Distribute sending method, the value is set to localhost.
* In the Framework Server Port field, enter the port number of your integration framework or the SAP Business One integration for SAP NetWeaver server.
* In the Username field, enter the user name for accessing the integration framework or SAP Business One integration for SAP NetWeaver server. The default is B1iadmin.
* n the Password field, enter the password for accessing the integration framework or SAP Business One integration for SAP NetWeaver server.
* To test the connection, choose the Test Connection button.

1. Save your settings and click Next.
2. In step 4 (Choose Company Databases), choose the company databases. The setup program displays the company databases in your SAP Business One system. For each company database, you can set up the following:

* Deselect the checkbox in front of the SAP Business One company database, if the company does not use the integration framework. If you deselect the checkbox, SAP Business One does not create events for the company database in the SEVT table.
* To determine the Include List B1 Object(s) settings based on the scenarios in the integration framework, click Generate. The SAP Business One event filter generator opens.
* Determine the objects for the include list and click Apply. If there are scenario steps subscribing to all obejcts (\*), see the status section in section 2.3.The wizard displays the list of company databases.
* Select the databases for which you want to set the include filter. Note that for databases with defined exclude filter settings, the checkbox is disabled.
* Click *OK* and the wizard writes the include filter settings to the selected databases.
* Alternatively, choose the Event Filter button for each company and enter the following:
* In the Include List B1 Object(s) field, enter the object identifier of the SAP Business One object or objects. Separate entries by comma. Use either the Include B1 Object(s) or the Exclude List B1 Object(s) function. Do not use the functions together.
* In the Exclude List B1 User field, enter SAP Business One users for which the event sender does not send events to the integration framework. Enter the SAP Business One user name, not the user code. Separate entries by comma.
* If you want the company database to create events based on indirect journal entries, select the Create Complete Journal Entry Events checkbox. Standard SAP Business One processing does not create events for indirect journal entries.
* Save your settings and click Next.

1. Step 5 (Summary Information) gives you a summary of the event sender settings. To save the settings, choose the Deploy button.
2. To restart the SAP Business One EventSender service, click Start.
3. Restart the SAP Business One client.

**Result**

The setup program stores the settings in the datasource.properties and eventsenderconfig.properties configuration files.

## 2.8 Configuring Garbage Collection in Control Center

The integration technology provides garbage collection jobs that run regularly.

* Queue garbage collection

The queue garbage collection removes messages that were processed in queues.

* Transaction log garbage collection
* BizStore garabge collection

Performs garbage collection of index headers without references to BizStore documents

The \_!!BSTgs(com\_sap\_b1i\_system\_xc) message put in an internal queue triggers the garbage collections. The integration technology performs garbage collections message block by message block. Triggered by the message, garbage collection works on the first block. After completing the block, the garbage collections push the message back to the first position of the queue. The message triggers garbage colletions again that start woking on the next block. You can observe the message in the queue monitor and have the impression that the message blocks the queue. This is not the case. The message changes each time the collectors push it back to the queue.

**Procedure**

To change the garbage collection timers, choose Tools → Control Center → Configuration → Deployment Panel.

1. For the first Default Deployment Document 'xcellerator.cfg', click the Cfg button to prepare the configuration.
2. Click the Cfg button again to display the configuration user interface.
3. Scroll down to find the configuratons transaction log garbage collection (TLogDelPrep), queue garbage collection (DBQgcPrep), and BizStore garbage collection (BSTgcPrep).
4. Adjust the setting in the Ip (inbound primary) section. The default settings are the following:

* The transcation log is deleted every three hours.
* The garbage collection for queue entries runs twice an hour.
* The garbage collection for BizStore documents runs twice a day.

1. To activate new settings, click Apply.

# 3 Further Configuration Tasks

## 3.1 Enabling Systems to Use HTTPS

For the system that accepts incoming calls using HTTPS, do the following:

**Procedure**

1. Open the administration user interface using https and port 8443.

The system displays a notification that there is a problem with this website’s security certificate.

1. Click the Continue to this website (not recommended) link.
2. Click the *Certificate Error* information next to the address field of the Microsoft Internet Explorer.
3. Click the *View Certificates* link.

The system displays that this CA Root certificate is not trusted.

1. To enable trust by installing this certificate in the Trusted Root Certification authority’s store, click the *Install Certificate…* button.
2. In the Certificate Import Wizard, click *Next*.
3. Select *Place all certificates in the following store* and click *Browse…* to select the **Trusted Root Certification Authorities**.
4. Click *Next* and *Finish*.
5. Close the browser and open the application using https and port 8443 again.
6. The system displays a lock icon, such as, for example: 
7. To export the root certificate, click the icon and click the *View Certificates* link.
8. Select the *Details* tab and click the *Copy to File* button.
9. Follow the instructions of the Certificate Export Wizard, select *DER encoded binary X.509 (.CER)* and save the certificate to your file system.

For the system that calls using HTTPS, do the following:

**Procedure**

1. Copy the server root certificate file to the local integration framework (B1if) system.
2. To open a DOS window on the local integration framework system, select Start → Run and enter CMD.
3. Navigate to the …\SAP Business One Integration\sapjre\_6\_64\jre\bin directory.
4. Run the following command:

keytool -import -file <path to cert> -keystore <path to the JRE cacerts file> -alias <name to store cert>

Where:

* <path to cert> is the path to the SSL certificate
* <path to the JRE cacerts file> is the path and name of the CACERT file of the JVM (the list of trusted certificates for the JVM)
* <name to store cert> is the name you want to use to store the certificate

1. The system requests a password. Enter **changeit**.
2. The system requests whether to trust this certificate. Enter **y**.

The system adds the certificate to the keystore.

**Result**

You can now configure HTTPS for the connection between your system that calls another system using HTTPS. In the configuration, use port 8443 for HTTPS.

If the systems send and receive messages, export and import the root certificate into the other system in both directions.

## 3.2 Exchanging a Certificate in the Tomcat Keystore

The installation program for the integration framework creates a self-signed certificate and stores it in the Tomcat keystore. The integration framework uses this certificate by default to enable incoming https calls. You can replace this certificate by a certificate signed by a Certification Authority (CA) of your choice.

First you delete the self-signed certificate from the keystore. Then you generate a new keystore and key pair and generate a certificate signing request you send to your CA. Once you have received the signing request response, import it into the keystore. Use Java keytool commands for your activities.

For the keytool commands, you need the following information:

* Keystore file: ./webapps/B1iXcellerator/.keystore (relative to the Tomcat base directory)
* Keystore password (<keystorepassword>): Find the default password in the ./Tomcat/conf/server.xml file in the keystorePass attribute.
* Key password (<keypassword>): The default key password is the same as the keystore password.
* Key alias: tomcat

**Procedure**

1. To delete the self-signed certificate from the keystore, enter keytool -delete -alias tomcat -keystore ./webapps/B1iXcellerator/.keystore -storepass <keystorepassword>.
2. To generate a key pair, enter keytool -genkeypair -validity 3650 -keyalg RSA -storepass <keystorepassword> -keypass <keypassword> -dname "CN=<machine name>" -keystore ./webapps/B1iXcellerator/.keystore.

<machine name> is the server/domain name

1. To generate a certificate signing request (CSR), enter keytool -certreq -keyalg RSA -file mycsr.csr -keystore ./webapps/B1iXcellerator/.keystore -storepass <keystorepassword> -keypass <keypassword>.
2. Send the CSR file to a CA.

The CA sends a certificate request response to you that contains the signed public-key certificate.

1. To import the certificate request response into the keystore, enter keytool -importcert -trustcacerts -alias tomcat -file mycsr.crt -keystore ./webapps/B1iXcellerator/.keystore -storepass <keystorepassword> -keypass <keypassword>.

mycsr.crt contains the certificate the CA issued to you.

## 3.3 Parameters of the Xcellerator File

Xcellerator.cfg is the central configuration file of the integration framework. You can find the file in the following directory:

..\SAP\SAP Business One Integration\B1iServer\tomcat\webapps\B1iXcellerator\Xcellerator.cfg

After installation, you may check the following parameters:

* xcl.webdav (disabled (default), readonly, full)

Controls the exposure of the WebDAV support in the integration framework

* xcl.safemode (true, false (default))

With this parameter, you can start the integration framework in regular or in safe mode. You can set no value or false (default) to start the integration framework in regular mode or you can set the value to true to start the integration framework in safe mode.

In safe mode the integration framework applications and adapter (IPO steps) are available and run, but you have only plain BizFlow and BizStore access available. HTTP access is limited to local without authentication.

* xcl.http.localOnly (true (default), false)

This parameter specifies the access to the administration user interfaces. If the parameter does not exist or is set to true, the access is limited to the local machine for the dummy and report namespaces. This is the default value. The installation or upgrade sets the parameter. If you set the value to false, access to remote machines is enabled. This parameter does not affect the ipo and soap namespaces.

* bpc.maxDumpSize=-1,0,positive integer

This parameter defines the maximum dump size of payload data on log level. If you set the value to -1, there is no constraint. If you set the value to 0, dumping is switched off. This is the default value. If you set the value to a positive integer, this value is the upper limit in kBytes for the dump size. Do not change this parameter in your productive environment.

* xcl.http.sessionTimeout (minutes, greater than 0, smaller than 1000)

This parameter specifies the timeout for http sessions. If it is set to a negative value or 0, the integration framework internally sets the value to 1. If no value is set, the default is 10. Do not set the value higher than 1000.

* xcl.http.xsrf (true,false)

This parameter specifies the protection against cross-site request forgery. If the parameter exists and is set to true, the protection is enabled for the dummy namespace. For backward compatibility the default is false.

To apply the changed settings, restart the integration framework service. To change the most important settings for development and production, choose *Maintenance → System Info* and click the  (*Define Profile for Production and Development*) button.

**Xcellerator-Parameters**

xcl.adapterclass.<jarfile>=<classname>, ...

This parameter registers an external, loadable adapter.

<jarfile> is name of the entry jar file of the adapter without extension,

<classname> is the class that implements the adapter. There can be multiple adapters, separated by comma.

The installation or upgrade sets the parameters. Do not change the settings unless you develop your own adapter.

xcl.threads=-1,0,1

This is the maximum number of internal worker threads required for the internal scheduler. The default value is -1. If you set the value to 0, there is no limit. A negative value indicates the number of threads per available processor.

xcl.dbcretries=<number>

This is the maximum number of attempts to connect to the RDBMS when the integration framework starts. If the connection to the database has failed, the integration framework waits one second and then tries again to connect to the database. If the parameter does not exist or has a negative value, there are endless connection retries. The default value is 120.

xcl.webdav=disabled,readonly,full

Enables or disables the WebDAV support in the integration framework. The default value is disabled. In a productive system set the value to disabled. Use full only for the development environment.

xcl.recovery=enabled,disabled

This parameter determines, whether recovery activation adjustments happen. The default value is enabled. Do not change this parameter.

xcl.safemode=true,false

With this parameter, you can start the integration framework in regular or in safe mode. You can set no value or false (default) to start the integration framework in regular mode or you can set the value to true to start the integration framework in safe mode.

In safe mode the integration framework applications and adapter (IPO steps) are available and run, but you have only plain BizFlow and BizStore access available. HTTP access is limited to local without authentication. For more information when to change this parameter, see section *Working in Safe Made*

xcl.cancelPeriod=<seconds>

This parameter specifies how long in seconds the integration framework waits before it cancels BizFlows that are subject to cancellation. If the time expires, the integration framework attempts to actively cancel the BizFlow. This can lead to a RetryableException. If the parameter does not exist, the default is 30 seconds. Do not change this parameter.

xcl.singledumps=true,false

This parameter specifies, whether the integration framework puts BizProcessor inter-atom message dumps in a single BizStore document or whether the integration framework puts message dumps as data in the IPO logs. If the parameter does not exist or the value is set to true, the message dumps are in a single Bizstore document. If the value is set to false, the message dumps are put as data to the IPO-Logs. Do not change this parameter.

xcl.reporting=true,false

This parameter enables or disables the Crystal Report runtime and the reporting functions for processing. The default it true. If the parameter does not exist or is set to false, the integration framework disables the reporting functions. The installation sets this parameter. Do not change this parameter.

xcl.http.sessionTimeout=<minutes, greater than 0>

This parameter specifies the timeout for http sessions. If it is set to a negative value or 0, the integration framework internally sets the value to 1. If no value is set, the default is 10. Do not set the value higher than 1000.

xcl.http.localOnly=true,false

This parameter specifies the access to the administration user interfaces. If the parameter does not exist or is set to true, the access is limited to the local machine for the dummy and report namespaces. This is the default value. The installation or upgrade sets the parameter. If you set the value to false, access to remote machines is enabled. This parameter does not affect the ipo and soap namespaces.

xcl.http.xsrf=true,false

This parameter specifies the protection against cross-site request forgery. If the parameter exists and is set to true, the protection is enabled for the dummy namespace. For backward compatibility the default is false.

**BizProcessor Parameters**

bpc.pltconvclass.<jarfile>=<classname>, ...

With this parameter you can register external, loadable payload type converters.

<jarfile> Enter the name of the entry jar file of the converter without extension.

<classname> Enter the class that implements the converter. You can enter more than one converter, separated by comma.

The installation or upgrade sets the parameter. Do not change the settings unless you develop your own converter.

bpc.jdbc\_url=jdbc:sqlserver://<localhost>;<further parameter>;<further parameter>

This parameter defines the connection URL for JDBC-based database access. The database vendor describes the required parameters. the installation sets the parameter. Do not change this parameter, unless you need to exchange the database.

bpc.jdbc\_dbtype=5

This parameter defines the database type and version.

1: Microsoft SQL Server 2000

2: IBM DB 2

3: Sybase ASE

4: Microsoft SQL Server 2005

5: SAP MaxDB

6: Microsoft SQL Server 2008

7: Microsoft SQL Server 2012

9: SAP HANA

bpc.jdbc\_owner=dbo

This parameter defines the owner of the tables accessed for JDBC-based database access. Do not change this parameter.

bpc.jdbc\_user=sa

This parameter defines the user for the JDBC-based database access. The installation sets this parameter. The installation sets this parameter.

bpc.jdbc\_password=

This parameter defines the plain text password for the JDBC-based database access. If at all, only use this parameter in a demonstration or test environment.

bpc.jdbc\_encpassword={{0...}}

This parameter defines the password for the JDBC-based database access. If this parameter exists and the value is not empty, this parameter supersedes the bpc.jdbc\_password parameter. The installation sets this parameter.

#bpc.jdbc\_altpassword=

This parameter is deprecated and no longer supported as of BPC 0.31.0 / XCL 0.37.0.

bpc.jdbc\_driver=com.sap.dbtech.jdbc.DriverSapDB

#bpc.jdbc\_driver=com.microsoft.sqlserver.jdbc.SQLServerDriver

#bpc.jdbc\_driver=com.mysql.jdbc.Driver

This parameter specifies the driver for the JDBC-based database access. The installation sets this parameter. Do not change this parameter.

bpc.threads=<integer>

This parameter defines the thread constraints for the BizProcessor. Do not change this parameter.

bpc.reuseLimit=1

This parameter is deprecated as of BPC 0.21.0 onward.

bpc.maxDumpSize=-1,0,positive integer

This parameter defines the maximum dump size of payload data on log level. If you set the value to -1, there is no constraint. If you set the value to 0, dumping is switched off. This is the default value. If you set the value to a positive integer, this value is the upper limit in kBytes for the dump size. Do not change this parameter in your productive environment.

bpc.allowBestXslProfile=true,false

This parameter defines the best possible XSL profile for transformations. If the parameter does not exist, it is set to true. This is the default value. Do not change this parameter.

bpc.historyDepth=0

This parameter defines the global depth of history for BizStore documents. It is possible to set an individual depth of history for each document storage; this must be between the globally set depth of history and the maximum possible depth of history. If the parameter does not exist it is set to 0. 0 is the default value. The maximum value is 36^4. Do not change this parameter.

**CoordService Parameters**

cos.registryport=6099

This is the registry port for the CoordServer in case of Outproc Client access. Do not change this parameter.

cos.hostname=localhost

This parameter defines where the Outproc CoordServer resides. In case of Inproc client usage, the value must be empty. Do not change this parameter.

cos.operationmode=-3,2,3,4

This parameter defines the COS operation mode.

2: INPROC\_SERVER (This is the default value.)

3: OUTPROC\_SERVER

4: OUTPROC\_CLIENT

-3: The current integration framework node works as Coordination Service only. It does not accept or perform other tasks.

Do not change this parameter.

cos.cleanupinterval=<seconds>

This parameter defines the time in seconds, after which the integration framework searches for orphaned sessions. Do not change this parameter.

cos.validperiod=<minutes>

This parameter is deprecated as of V 0.12.0.

cos.acquiretimeout=<seconds>

This parameter defines the global timeout for lock acquiries instead of immediate failing. The default value is 60.

cos.rctimeout=<seconds>

This parameter defines how long the integration framework tries to reconnect to a lost connection. The default is 600 seconds. Do not change this parameter.

**Logging Parameters**

The following parameters are Java logging parameters.

#handlers= java.util.logging.ConsoleHandler,java.util.logging.FileHandler

#handlers= java.util.logging.ConsoleHandler

handlers= java.util.logging.FileHandler

java.util.logging.FileHandler.pattern = %t/b1i\_%g.log

java.util.logging.FileHandler.limit = 10485760

java.util.logging.FileHandler.count = 10

java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter

#java.util.logging.FileHandler.formatter = java.util.logging.XMLFormatter

#java.util.logging.FileHandler.formatter = com.sap.b1i.utilities.NiceTextFormatter

#java.util.logging.ConsoleHandler.level = FINEST

#java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter

#java.util.logging.ConsoleHandler.formatter = com.sap.b1i.utilities.NiceTextFormatter

.level= SEVERE

com.sap.b1i.bizprocessor.level = SEVERE

com.sap.b1i.coordservice.level = SEVERE

com.sap.b1i.utilities.level = SEVERE

com.sap.b1i.dblayer.level = SEVERE

com.sap.b1i.xcellerator.level = SEVERE

In a productive integration framework the SEVERE level is recommended and the default. To set a higher level is not advisable. In a development environment use the CONFIG level. This level is required for creating debugging information.

## 3.4 Creating Keystores and Truststores in the BizStore

To administer private keys and certificates for scenario packages, create keystores and truststores in the BizStore. Keystores and truststores are technically identical. They differ in the way they are used.

Keystore

A keystore is a file that contains private keys and their certificates with the corresponding public key. You need a keystore, for example, to authenticate at a server using an X.509 client certificate when communicating using HTTPS.

Truststore

A truststore contains certificates from other parties you communicate with, or from Certificate Authorities (CA) that you trust to identify other parties. You need a truststore, for example, to establish HTTPS communication with another server.

If you do not provide a keystore or truststore in the BizStore, the integration framework accesses the configured Java runtime environment keystore and truststore by default. For a keystore, there is no out-of-the-box default configuration available on Java level. A default configuration exists for a truststore.

recommendation.gifRECOMMENDATION

We recommend creating a keystore or truststore or both for each scenario package, if you require HTTPS connections and authentication using a certificate.

If you only need a truststore, you can also consider using a central truststore for all scenarios. For a truststore, consider importing only the root certificate, not the complete chain, since the certificate at the end of the chain can change.

If you only need a truststore with well known and preshipped root certificates of the Java Virtual Machine, you can also consider using the Java default truststore.

Secure the access to keystores and truststores with passwords.

* Protect the access with a password for content changes, and for retrieval of confidential entries (private or secret keys).
* To provide a password for access to non-confidential entries (public certificates) is not required. If you secure access, it serves to checking the integrity of the store.
* In addition to the password for global access, you can provide an individual password for each confidential entry. If such a password is not in place, the integration framework uses the global access password instead.

recommendation.gif RECOMMENDATION

It is a convention of the SSL (secure socket layer) subsystem that access passwords for confidential entries must be identical with the global store access password. We recommend keeping the passwords identical, if you use store entries for SSL communication, for example, for establishing an HTTPS connection.

The BizStore supports for keystore files the \*.jks, \*.pfx , \*.pkcs12 and \*.p12 formats.

**Procedure**

1. Log on to the integration framework and enter the user name and password.
2. To import a certificate, choose Tools → Control Center → Configuration → Certificate Admin.

The function allows administering keystore and truststore documents in the BizStore.

You must provide a password for keystore document access. If the specified document does not yet exist and you add an entry, the platform creates the store.

1. To create a keystore or a truststore, in the *Administration of Keystores and Truststores in BizStore* user interface, enter the following information:

| **Field Name** | **Field Value** |
| --- | --- |
| Biz Store URI | Choose the *Ellipsis* button to select the BizStore URI, and then enter the name of the file.   * Select the BizStore dataset * Select the BizStore group.   Select a place in the BizStore that an upgrade of the integration framework does not overwrite. Use, for example, a directory in your scenario package folder structure.   * Select the BizStore unique alias, for example, unified. * Enter the name of the \*.jks file. |
| Store Password | Enter a password to access the store file. |

1. Click *Submit*.
2. To import a X.509 certificate, in the Certificate Administration for store <your chosen path for the key store file> user interface, click Add Entry.
3. In the Imports certificates to a key- or trust store within the Biz Store user interface, enter the following:

|  |  |
| --- | --- |
| **Field Name** | **Field Value** |
| Certificate | Use the *Browse* button to select the X.509 certificate from the local file system, for example, VLxxxx.cert. |
| Alias | Enter an alias you want to use for your certificate. |
| Store Password | For a keystore, enter the password already defined for your keystore. |

1. To upload your certificate, click *Submit*.

**Result**

To verify the successful import of the certificate, check the summary user interface. You can also check, whether the certificate has been added to your key store file.

The installation of the integration framework provides the .keystore keystore file in the …\IntegrationServer\Tomcat\webapps\B1iXcellerator folder. Consider uploading the file as a jks file to the BizStore. Use the keystore to upload additional certificates. Note that the password of the keystore and of each certificate that you add to the keystore must be identical.

## 3.5 Setting Up HTTPS Between Integration Framework Servers

Integration frameworks communicate with each other using the HTTP protocol. In such a scenario, the integration framework that initiates the connection is the client, the other integration framework is the server. To secure the connection using HTTPS, export the certificate from the Tomcat key store of the integration framework server and import it into the trust store of the integration framework client. The trust store is part of the BizStore.

note.gif NOTE

As of integration framework version 1.19.3, you can find the server certificate in the following folder: <integration framework installation path>\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\tomcat.cer

Omit steps 1 to 3, and start with step 4.

**Procedure**

1. On the integration framework server, navigate to the following directory: …\IntegrationServer\Tomcat\webapps\B1iXcellerator.
2. To export a certificate from the key store, enter the following command: <absolute path to keytool>\keytool -export –alias tomcat –keystore .keystore –file tomcat.cer
3. The program requests you to enter the keystore password. Press enter.

Keytool creates the tomcat.cer file in the directory.

1. Copy the tomcat.cer file to a directory on the integration framework client.
2. On the integration framework client, logon to the integration framework, and choose *Tools* *→* *Control Center* *→* *Configuration* *→* *Certificate Admin*.

This function allows to administer keystore and truststore documents in the BizStore.

1. To create a truststore, in the *Administrate key- and trust stores of Biz Store* user interface, enter the following information:

| **Field Name** | **Field Value** |
| --- | --- |
| Biz Store URI | To create the truststore, choose the *Ellipsis* button to select the BizStore URI, and then enter the name of the file.  Select the BizStore dataset  Select the BizStore group.  Select a place in the BizStore that an upgrade of the integration framework does not overwrite. Use, for example, a directory in your scenario package folder structure.  Select the BizStore unique alias, for example, unified.  Enter the name of the \*.jks file. |
| Store Password | Define a password for the store. |

1. Click *Submit*.
2. To import the certificate, in the Certificate Administration for store <your chosen path for the key store file> user interface, click Add Entry.
3. In the Imports certificates to a key- or trust store within the Biz Store user interface, enter the following:

| **Field Name** | **Field Value** |
| --- | --- |
| Certificate | Use the *Browse* button to select the certificate from the local file system. |
| Alias | Enter an alias you want to use for your certificate. |
| Store Password | Enter the password to the store. |

1. To upload your certificate, click *Submit*.

**Result**

You have fulfilled the prerequisites to connect from an integration framework to another integration framework using HTTPS. This is, for example, relevant, if you want to connect to a remote integration framework in the *B1 Event Subscriber* function. In the integration framework, choose *Maintenance → B1 Event Subscriber*, choose the *Create* button, in the *Protocol* field, enter https, in the Authentication field, enter basic, and in the *Trust Store URI* field, enter the path and name of the trust store.

## 3.6 Setting Up JDBC Connections with SSL between Framework and SAP HANA

To set up a JDBC connection with SSL settings from the integration framework to the SAP HANA server follow the steps in the procedure below. SAP HANA is the server and the integration framework the client. The user view of the integration framework is a Java application that uses JDBC connections with SSL settings to connect to the SAP HANA server.

**Prerequisites**

SSL settings are already established on the SAP HANA server using the commoncrypto option.

**Procedure**

1. To obtain the SAP HANA server trust store, logon to SUSE Linux with the <sid>adm account.
2. Open the terminal and go to the $SECUDIR directory.
3. Enter sapgenpse export\_own\_cert -f x509 -o sapsrv.cer -p sapsrv.pse
4. Copy sapsrv.cer to the integration framework server, for example to c:\temp\sapsrv.cer
5. On the integration framework server, logon to Microsoft Windows with the administrator account.
6. Run cmd as administrator and go to the $JAVA\_HOME directory.
7. To generate a trust store using the SAP HANA server certificate, enter the following:

keytool -importcert -keystore C:\temp\sapsrv.keystore -alias HANServer -file c:\temp\sapsrv.cer

1. Enter the password to the trust store and enter yes to add the certificate to the trust store.

The sapsrv.keystore file is the trust store with the HANServer alias and the password that you entered. It is the trust store for the JDBC connection with SSL settings.

## 3.7 Enabling a Secure Connection between Framework and SAP HANA

To secure the JDBC connection between the integration framework and the SAP HANA database that the integration framework uses, perform the steps below.

**Procedure**

1. On the server where the integration framework database is installed, logon to Windows with the administrator account.
2. Go to <Your B1i installation folder>\Tomcat\webapps\B1iXcellerator\ and open the xcellerator.cfg file for editing.
3. Change the value of the bpc.jdbc\_url property in the following way:

bpc.jdbc\_url=jdbc:sap://<server>:<port>?currentschema\=IFSERV&autocommit\=false&encrypt\=true&validateCertificate\=true&trustStore\=.\/..\/sapsrv.keystore

\=.\/..\/sapsrv.keystore: Example trust store file provided by SAP HANA server

If IFSERV is not the database name of the integration framework, change the name in the URL.

1. To restart the SAP Business One integration service, open the Services window, select SAP Business One Integration Service, click Stop and then click Start.

## 3.8 Enabling Secure Connections between Framework and Company Databases

**Procedure**

1. In the integration framework, choose SLD and in the navigation, open the entry for an SAP Business One company database and click Edit Entry.
2. Scroll down to the JDBC section and edit the url parameter value in the following way:

jdbc:sap://<server>:30115?currentschema=TESTDEMOVN&autocommit=false&encrypt=true&validateCertificate=true&trustStore=./../sapsrv.keystore

1. Save and test the connection.

## 3.9 Database Maintenance Tasks

Database activities depend on the nature of your organization's day-to-day work. There are many factors influencing system performance, such as disk space availability, the number of transactions occurring each day, and so on. It is essential to perform daily and regular checks to ensure the efficient operation of the integration framework. System performance depends on the correct administration of the database.

Find references to the following information in the sections below:

* Starting and stopping database services
* Performing weekly tasks
* Performing regular tasks
* Performing backups
* Performing restoration

**Database Maintenance Tasks for the Microsoft SQL Server**

For more information, see the SAP Help Portal, SAP NetWeaver → SAP NetWeaver Platform → SAP NetWeaver 7.4 → Application Help → Function-Oriented View → Database Administration → Database Administration for the Microsoft SQL Server.

**Database Maintenance Tasks for the SAP HANA Database**

For more information, see the SAP Help Portal, SAP NetWeaver → SAP NetWeaver Platform → SAP NetWeaver 7.4 → Application Help → Function-Oriented View → Database Administration → Database Administration for SAP HANA.

**Database Maintenance Tasks for SAP MaxDB**

For more information, see the SAP Help Portal, SAP NetWeaver → SAP NetWeaver Platform → SAP NetWeaver 7.4 → Application Help → Function-Oriented View → Database Administration → Database Administration for SAP MaxDB.

**Database Maintenance Tasks for MySQL**

For more information, see http://dev.mysql.com/doc/refman/5.5/en/sql-syntax-server-administration.html

## 3.10 Working in Safe Mode

Similar to an operating system, the integration framework supports a safe mode. If normal restart does not solve problems, you can restart the integration framework in safe mode. This can happen in the following cases:

* You have locked your user by wrong actions in the user administration.
* Erroneous processing always starts and blocks the integration framework, even after restart.
* The integration framework no longer starts, probably caused by application deployment problems.

In safe mode, the integration framework only provides limited functions. Run scenario packages only in regular mode. We recommend deactivating scenario packages for safe mode. Switch off safe mode as soon as you have solved the problem. Then activate your scenario packages again. For more information, see *Operations Guide, Part One*, section *Activation and Deactivation*

**Procedure**

1. You cannot enable safe mode in the administration user interface. The safe mode setting is a low level configuration of the integration framework in the xcellerator.cfg document. The document is available in the base directory of the integration framework:

..\SAP\<SAP Business One integration solution>\B1iServer\tomcat\webapps\B1iXcellerator\xcellerator.cfg

1. To enable safe mode, set the parameter: xcl.safemode=true

* Consider security aspects and be very careful with access rights to the document. For more information, see section *Securing xcellerator.cfg*
* If the safemode parameter does not existent in xcellerator.cfg, or is set to false, the integration platform starts in regular mode. If the parameter is set to true, the integration platform starts in safe mode.

1. If you change xcellerator.cfg, restart the integration service. To restart the service *SAP Business One Integration Service*, use the Microsoft Windows Service Panel.

**Result**

If the integration framework runs in safe mode:

* No integration framework applications or adapters (IPO steps) are available.
* The user authentication is disabled.
* Access is only possible from the local machine, regardless of settings in xcellerator.cfg.
* Only plain BizFlow and BizStore access is possible.
* The relevant administration tools still work, and in turn, allow the assignment of a new password or unlocking the account.

## 3.11 Options for Calling Framework Functions

To call integration framework functions, you can enhance the framework URL by adding the menu and menu item path. Additionally, you have the option to shorten the standard integration framework URLs. You can combine both options.

### 3.11.1 Enhancing the Framework URL

To open a function directly after login, add the following to the integration framework URL after the XML file that defines the integration framework menu:

&start=<main menu>/<menu\_item>

**Examples**

* http://127.0.01:8080/B1iXcellerator/exec/dummy/com.sap.b1ip.system.cc/bfd/AdminConsole.bfd?!defdoc=/com.sap.b1i.common/menu/opdev.xml**&start=Maintenance/Customer%20Administration**

After login, the framework directly opens the customer administration function of the maintenance menu.

* http://127.0.01:8080/B1iXcellerator/exec/dummy/com.sap.b1ip.system.cc/bfd/AdminConsole.bfd?!defdoc=/com.sap.b1i.vplatform.ide/ui/vIDE.xml**&start=Maintenance/Cfg%20Metadata**

After login, the framework directly opens the configuration of metadata function of the maintenance menu.

### 3.11.2 Using Short URLs

The integration framework offers the option to shorten URLs by defining a URL mapping. A valid URL mapping consists of a shortcut key followed by the equals sign followed by the replacement string:

<key>=<replacement>

The framework supports the following shortcut types:

* Go shortcuts let the user directly access an integration framework function in the user interface with a Web browser. Go shortcuts work with HTTP redirect.

For the shortcuts, disable the URL-immanent cross-site scripting protection of the integration framework.

* Jump shortcuts are available for machine to machine communication. The shortcuts work with internal URL mapping and avoid the extra roundtrip of an HTTP redirect. Jump shortcuts work with and without the enablement of URL-immanent cross-site scripting protection of the integration framework

**Prerequistes for Go Shortcuts**

* Using go shortcuts, change the following setting in the xcellerator.cfg file:

xcl.http.xsrf=false

* Save xcellerator.cfg and restart the integration service.

The setting disables the URL-immanent cross-site scripting protection of the integration framework. In a productive and in particular in a public cloud environment, do not open less trustworthy Web sites in the same browser together with the integration framework at the same time.

**Procedure**

1. To define shortcuts, choose Tools → Control Center → Configuration → Short URLs and click Add Shortcuts.
2. In the Shortcut field, enter the shortcut name. Only use one word.
3. In the URL Extension field, enter the part of the URL that is replaced by the shortcut.

Start with the part behind B1iXcellerator. In most cases, the extension starts with exec/dummy/ followed by the rest of the URL.

**Results**

The settings are saved to the urlshortcuts.properties file in the \IntegrationServer\Tomcat\webapps\B1iXcellerator folder.

You can use the definitions for go and jump shortcuts.

**Example**

Shortcut: dev

URL Extension: exec/dummy/com.sap.b1ip.system.cc/bfd/AdminConsole.bfd?!defdoc=/com.sap.b1i.common/menu/opdev.xml

Enter: https://<hostname>:<port>/B1iXcellerator/go/dev in your browser for UI access or https://<hostname>:<port>/B1iXcellerator/jump/dev for access using non-interactive HTTP clients.

# Copyrights, Trademarks, and Disclaimers

© Copyright 2022 SAP SE. All rights reserved.

The current version of the copyrights, trademarks, and disclaimers at <https://www.sap.com/about/legal/copyright.html> is valid for this document.