**Integration Framework**

**Operations**

**System Configuration and Monitoring**

**Last Modified: December 8, 2022**

[1 Getting Started with Operations 4](#_Toc121408562)

[2 Integration Framework Configuration 5](#_Toc121408563)

[2.1 Displaying System Information and Setting Profiles 5](#_Toc121408564)

[2.2 Importing BizStore Content 6](#_Toc121408565)

[2.3 Changing Technical Default Settings 8](#_Toc121408566)

[2.4 User and Session Administration 9](#_Toc121408567)

[2.4.1 User and Session Concepts 9](#_Toc121408568)

[2.4.2 Managing Administration Users 10](#_Toc121408569)

[2.4.3 Changing Your Administration User Entry and Password 13](#_Toc121408570)

[2.4.4 Managing Runtime Users 14](#_Toc121408571)

[2.4.5 Monitoring HTTP Sessions 16](#_Toc121408572)

[2.4.6 Analysing Authentication Events 17](#_Toc121408573)

[2.4.7 Enabling the Password Reset Process 19](#_Toc121408574)

[2.4.8 Viewing the Personal Data Change Log 20](#_Toc121408575)

[2.5 Creating Customer Information for Deployments 20](#_Toc121408576)

[3 Further Configuration Tasks 21](#_Toc121408577)

[3.1 Enabling Systems to Use HTTPS 21](#_Toc121408578)

[3.2 Exchanging a Certificate in the Tomcat Keystore 22](#_Toc121408579)

[3.3 Parameters of the Xcellerator File 23](#_Toc121408580)

[3.4 Creating Keystores and Truststores in the BizStore 31](#_Toc121408581)

[3.5 Setting Up HTTPS Between Integration Framework Servers 33](#_Toc121408582)

[3.6 Setting Up JDBC Connections with SSL between Service and SAP HANA 35](#_Toc121408583)

[3.7 Enabling a Secure Connection between Framework and SAP HANA 35](#_Toc121408584)

[3.8 Enabling Secure Connections between Framework and Company Databases 36](#_Toc121408585)

[3.9 Database Maintenance Tasks 36](#_Toc121408586)

[3.10 Options for Calling Framework Functions 37](#_Toc121408587)

[3.10.1 Enhancing the Framework URL 37](#_Toc121408588)

[3.10.2 Using Short URLs 38](#_Toc121408589)

[4 Creating and Activating Deployments 39](#_Toc121408590)

[4.1 Introduction to Deployment Panel 39](#_Toc121408591)

[4.2 Creating Deployments 41](#_Toc121408592)

[4.3 Entering Deployment-Specific Properties (Optional) 42](#_Toc121408593)

[4.4 Entering Values for Value Mapping Definitions (Optional) 43](#_Toc121408594)

[4.5 Adding Values in the Scenario Package Configuration (Optional) 44](#_Toc121408595)

[4.6 Assigning SLD Entries, Setting Filters and Deployment Activation 45](#_Toc121408596)

[4.7 Working with Runtime Artefacts 46](#_Toc121408597)

[4.8 Deployment Panel in the Step Modeler 48](#_Toc121408598)

[4.9 Using the Validation Result to Resolve Inconsistencies 49](#_Toc121408599)

[4.10 Configuring and Using Scenario Step Triggers 50](#_Toc121408600)

[4.11 Deactivation and Regeneration of Active Deployments 50](#_Toc121408601)

[4.12 Detecting Outdated Runtime Artefacts 50](#_Toc121408602)

[5 Monitoring 51](#_Toc121408603)

[5.1 Monitoring Transactions 51](#_Toc121408604)

[5.1.1 Defining Filter Settings and Displaying Logs 52](#_Toc121408605)

[5.1.2 Performing Transaction Log Operations 54](#_Toc121408606)

[5.2 Error Inbox Monitor 54](#_Toc121408607)

[5.3 Activating and Monitoring Integration Services 55](#_Toc121408608)

[5.3.1 SAP Business One Event Inbound Service 55](#_Toc121408609)

[5.3.2 SAP ERP IDoc Inbound Service 56](#_Toc121408610)

[5.3.3 Business Process Services 56](#_Toc121408611)

[5.3.4 SAP Business One Asynchronous Outbound Service 56](#_Toc121408612)

[5.3.5 System Services 57](#_Toc121408613)

[5.4 Monitoring Scenario Queues 57](#_Toc121408614)

[5.4.1 Introduction to Scenario Queues 57](#_Toc121408615)

[5.4.2 Defining QInfo and Trace ID for the Scenario Queue Monitor 58](#_Toc121408616)

[5.4.2.1 Using QInfo 58](#_Toc121408617)

[5.4.2.2 Using the Trace ID 58](#_Toc121408618)

[5.4.3 Using Filter Criteria for the Queue List 60](#_Toc121408619)

[5.4.4 Sorting the Queue List 61](#_Toc121408620)

[5.4.5 Working with the Queue List 62](#_Toc121408621)

[5.4.6 Working with Messages in the Queue and Stream 63](#_Toc121408622)

[5.5 Monitoring Technical Queues 63](#_Toc121408623)

[6 Tools and Help Functions 65](#_Toc121408624)

[6.1 Displaying Benchmarks 65](#_Toc121408625)

[6.2 Using the Embedded Internal XML Editor 65](#_Toc121408626)

[6.3 Displaying XSLT Libraries 66](#_Toc121408627)

[6.4 Displaying Documentation 67](#_Toc121408628)

[6.4.1 Displaying Online Help 67](#_Toc121408629)

[6.4.2 Displaying Documents for Prining 67](#_Toc121408630)

[6.5 Displaying and Using the Training Material 68](#_Toc121408631)

[Copyrights, Trademarks, and Disclaimers 69](#_Toc121408632)

# 1 Getting Started with Operations

The operations guide contains sections that are relevant for administrators of the integration framework and administrators of scenario packages for customers. Additionally, there are settings that become revevant, if you want to use the integration framework as a development environment for integration content.

**Functions for the Integration Framework Administrator**

|  |  |
| --- | --- |
| **Function** | **What you can do** |
| System Information | Look up the integration framework version |
| ZIP Import | Use the import function to update BizStore content |
| Configuration | Adjust the default integration framework ports and set internet proxies |
| User Administration | Add integration framework administration and runtime users  Unlock users  Reset passwords  Adjust views for administration users  Monitor session information and authentication events  Enable the I have forgotten my password process |

**Functions for the Scenario Package Administrator**

|  |  |
| --- | --- |
| **Function** | **What you can do** |
| Customer Administration | Create and administer customers. You can assign customers to deployments and use the information for monitoring |
| Deployment Panel | Set up new deployments for customers for scenario packages |
| SLD | Create systems for customers in the System Landscape Directory  For more information, see the SLD Guide |

**Functions for Integration Content Developer**

|  |  |
| --- | --- |
| **Function** | **What you can do** |
| System Information | Change the profile to development system |

# 2 Integration Framework Configuration

After installation, the integration framework is configured for a productive system environment. The following sections provide information about how to change the system defaut settings. This is relevant, if you want to use the integration framework as a development environment or you need to define ports for the integration framework that differ from the default ports.

## 2.1 Displaying System Information and Setting Profiles

System information provides details about the integration framework version and available functions. Additionally, you can define and switch between system profiles.

The integration framework offers a system profile for a productive environment and development environment. After installation or deployment, the service is configured for a productive environment. To use the service as a development environment, change the profile to development environment. Some profile setting changes affect the central xcellerator.cfg configuration file and require a restart of the service.

**Procedure**

1. To display system information, choose *Maintenance* → *System Info*.

The integration framework displays the following information:

| **Field** | **Description** |
| --- | --- |
| Version and BPM Version | Useful information for support |
| Server Timestamp | Timestamp of the integration framework server |
| Deployment | On premise or cloud deployment |

1. To change the system profile, click Browse in the System Profile field.

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

1. To change default settings of your production and development system profiles, click  (Define Profiles for Production and Development).

Profiles make the definition of relevant settings available in one place.

| **Parameter** | **Description** |
| --- | --- |
| Session Timeout | xcl.http.sessionTimeout of xcellerator.cfg  The parameter defines the timeout for http sessions of the user interface. The default is 10. Do not set the value higher than 1000. |
| WebDAV Support | xcl.webdav of xcellerator.cfg  Controls the exposure of WebDAV support in the integration framework  The following options are available:   * disabled (default) * readonly * full |
| Internal Worker Threads | bcp.threads of xcellerator.cfg  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. |
| Local Access Only | xcl.http.localOnly of xcellerator.cfg (true (default), false)  The parameter defines 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 value.  To allow access from a remote machine, set value to false. The parameter does not affect the ipo and soap namespaces. |
| Mode | In a productive environment, the mode is Customer, in a development environment, the mode is Vendor. |
| Development Prefix | 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 Prefix Description | Enter a description for the development prefix. |
| B1 Event Monitor | Switches the production of SAP Business One event logs on or off |
| xcellerator.cfg Log Level | The CONFIG log level is responsible for the production of detailed debugging information that is relevant for a development system. |

1. To display the functions available with the integration framework version, click Version and BPM Version. The integration framework opens the user interface.
2. In the Filter Text field, you can enter a search term and click Enter.
3. In the Filter Version field, you can select a version and display the added features of the version.

## 2.2 Importing BizStore Content

The function allows you to import documents 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. Use the function to initially import scenario packages provided by SAP or a partner.

**Prerequisites**

* You have added all documents including subfolders you want to import to one ZIP file.
* You have ensured that the ZIP application supports relative path and you have enable the function. The relative path function is usually enabled by default.

**Procedure**

1. To import an archive to the BizStore, choose Maintenance → Zip Import.
2. In the Choose Archive field, click Choose File and select the archive from the file system.
3. To keep existing documents in the dataset during import, select Keep Existing Documents.
4. To prevent the import of erroneous XSL stylesheets, select Prevent Erroneous Import.

An erroneous XSL stylesheet contains namespace declarations in the root element that the stylesheet does not use explicitly. Such namespace declarations are not visible on XML level. When extracting the archive, the XML processor is not aware of the namespace declarations and it does not supply them to the target documents. If the integration framework uses such namespaces at runtime, for example, in XPath expressions, it throws a runtime error, because the XSLT processor cannot resolve the namespace. To enforce the XML processor to include such implicitly used namespace declarations, provide an empty attribute within the root element that is bound to the namespace.

1. To enable file system compliant naming, select File System Compliant Naming.

The integration framework supports file system friendly naming for upgrade and patch import by default. It assumes that the encoding of the entry names is file system-compliant in the archive. It allows omitting file name extensions without losing payload type information and supplying distinct alias information without sacrificing the usability of the document in the file system. Compose the file names in the following way to achieve the particular result in the BizStore:

| **BizStore** | **File System** |
| --- | --- |
| hugo | hugo..ext |
| hugo(alias) | hugo(alias)..ext |
| hugo.ext | hugo.ext |
| hugo.ext(alias) | hugo(alias).ext |

1. To unescape unsafe URL characters, select Unescape Unsafe URL Characters.

The integration framework unescapes unsafe URL characters encoded in the components of the entry name. This can happen, if the integration framework has created the archive and if the entry names of the archive have originally contained such unsafe characters.

1. To import the archive, click Submit.
2. To control the import, you can add processing instructions to a document. Include the instructions on the hierarchy level below the root element. Note that the integration framework only considers the first instruction of each type.

The following instructions are available:

* <?com.sap.b1i.system\_import protect?>

Add the statement to the document you want to import. Use the statement to protect an already existing document. The integration framework does not overwrite it with the imported version.

* <?com.sap.b1i.system\_import protected?>

Alternatively, you can add the statement to the already existing document.

* <?com.sap.b1i.system\_import force?>

Add the statement to the document you want to import. The integration framework overwrites the already existing document, not matter whether there is a statement in the already existing document.

* <?com.sap.b1i.system\_autorun <URI>?>

Add the statement to the document you want to import. You can enter URIs that auto run in a browser window after import of the archive. You can enter many processing instructions. If you enter relative URIs, the integration framework resolves them to HTTP URIs relative to the HTTP-exposed BizStore URI of the document. If you enter absolute URIs, the integration framework invokes them as they are.

## 2.3 Changing Technical Default Settings

After installation, you can use the integration framework immediately as a productive environment. To use the integration framework for scenario package development, change settings for the development environment. Additionally, you have the option to change the integration framework default port settings, if there are already applications running with the integration framework default port settings.

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

**Procedure**

1. To change technical default settings, choose *Maintenance* → *Configuration*.
2. In the *Mode* field, enter Vendor if you are a vendor of scenario packages, or select Customer if you develop individual packages.
3. If you are a vendor, enter the development prefix in the Development Prefix field.

Use 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.

1. In the Development Prefix Description field, enter a description.
2. To change the default 8080 and 8443 ports, navigate to the server.xml Tomcat file. Goto the integration framework installation folder, choose /Tomcat/conf, open the file and change the settings in the first two connector port tags.

caution.gif CAUTION

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

1. Change the ports in the HTTP Port and HTTPS Port fields of the integration framework function.
2. Additionally, you can change the server address in the *Server Address* field. The installation sets the computer name by default. You can set it, for example to localhost.
3. Restart the SAP Business One integration service.
4. Change the properties for the menu entry, using the correct port number: Start → All Programs → Integration Framework → Integration Framework.
5. If there is a firewall between the integration framework and the internet, enter the proxy host name in the Internet Proxy Host field, and the proxy port in the Internet Proxy Port field.
6. For queue-triggered steps, enter the number of step instances that run in parallel.
7. To exclude dedicated steps from parallel processing, click Filter.

The framework displays all scenario steps. For steps that are excluded from parallel processing in design, the checkbox is disabled.

1. Select steps that you want to exclude from parallel processing.

## 2.4 User and Session Administration

### 2.4.1 User and Session Concepts

The integration framework has a user and session concept. The integration framework distinguishes between administration users and runtime users.

* Administration users access the integration framework user interface, set up systems, develop scenario packages, set up scenario packages and administer scenarios at runtime.
* 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.

B1iadmin is the default administration and the default runtime user delivered with the installation. We recommend changing the default users for productive systems. For access to the administration user interface, create dedicated administration users.

The session concept is relevant for incoming HTTP calls, such as:

* Administration users working with the user interface of the integration framework
* Incoming HTTP calls of scenario packages
* The inbound channel for event senders of SAP Business One

You can monitor the sessions using the HTTP session monitor.

### 2.4.2 Managing Administration Users

Administration users work with the integration framework user interface. They set up systems in SLD, develop scenario packages, set up or deploy scenario packages and administer scenarios at runtime. With the installation, the integration framework provides the B1iadmin default administration user. We recommend changing the default user and defining dedicated users that work with the user interface.

Administration users with the Administrator view assigned can change the general settings relevant for all users, can add and change user entries, can change their password and can reset passwords for other users.

**Procedure**

1. To open the administration for administration users, choose Maintenance → User Administration, and click Admin Users.

The user interface displays the timestamp of the last change caused by an administration user and the change initiator.

1. In the header, adjust general settings that are relevant for all users:

| **Field** | **Description** |
| --- | --- |
| Minimum Password Length | The default minimum password length is eight. Enter or select the password length. |
| Days Until Password Expires | Enter or select the number of days until passwords expire. The default is 100 days. |
| Maximum Number of Logon Failures | Enter or select the number of unsuccessful logon attempts users have before they are locked. The default is 5. |

1. To add a user, click Add User and enter the following information:

| **Field** | **Description** |
| --- | --- |
| User | Enter a unique user name. |
| Password, Password (Repeated) | Enter and repeat the password for the user. The password must have eight or more characters. |
| Language | Enter the language for the user. The integration framework is available in English.  SAP Business One integration for SAP NetWeaver offers some user interfaces in additional languages. |
| Main User View | Select the main user view that you want to assign to the user.  User views control access to integration framework functions on menu entry level. If you do not define views for new users, they do not have access to any functions.  For more information about user views and their access to integration framework functions, see the Views for Administration Users section. |
| Email | Enter the e-mail address of the user. In cloud environments, it enables the user to request a password reset when the user is locked. |
| Full Name | Enter the full name of the user. The procedure for a new password request uses the full name in the e-mail. |
| Active | To activate the user, select the checkbox. The function allows you to enter users and activate them later. |

1. Save your settings and close the window.
2. Provide the intial password to the user.

During the first log on, the user must enter the intial password and then enter and repeat a new password.

1. You can change settings for other users. The user interface displays all users below your user entry. For each user, you can assign user views, adjust the password expiry date, select the language, add or change the e-mail address, and add or change the full name.

After changing an entry, click the Refresh button. Changes are saved automatically.

1. To change your password, click Change Password and enter and repeat the password, save your settings and close the window.

Use the new password at the next log on.

1. To reset a password for another user, click Reset Password, enter and repeat a new initial password, save your settings and close the window.
2. Provide the new password to the user.

During first log on after password reset, the user enters the provided password, and then enters and repeats a new password. The new password must be different from the old password and must have at eight characters.

1. To delete a user, click Delete.

**Views for Administration Users**

User Views control access to integration framework functions on menu entry level. If you do not define views for new users, they do not have access to any functions.

To display available user views and their descriptions, click the Maintain User Views button in the Admin User Administration user interface.

| **Menu** | **Administrator** | **Developer** | **Configurator** | **Supervisor** |
| --- | --- | --- | --- | --- |
| **SLD** | X |  | X | X |
| **Maintenance** |  |  |  |  |
| System Info | X | X | X | X |
| ZIP Import | X |  | X |  |
| Configuration | X | X |  |  |
| Deployment Panel | X |  | X |  |
| Customers | X |  | X |  |
| User Administration | X | X | X | X |
| **Scenarios** | X |  |  |  |
| **Monitoring** |  |  |  |  |
| Transaction Monitor | X | X | X | X |
| Error Inbox | X | X | X | X |
| Service Monitor | X | X | X | X |
| Scenario Queue Monitor | X | X | X | X |
| Technical Queue Monitor | X | X | X | X |
| B1 Event Monitor | X | X | X | X |
| **Tools** |  |  |  |  |
| Control Center | X | X | X | X |
| Benchmarks | X |  | X |  |
| XML Editor | X | X |  |  |
| Certificate Tool | X |  | X |  |
| Mapping Tool | X |  | X |  |
| Transaction Report | X |  | X | X |
| DI Proxy Restart | X |  | X |  |
| **Help** |  |  |  |  |
| XSLT Library | X | X |  |  |
| B1 DI API Object | X | X |  |  |
| B1 DI API Service | X | X |  |  |
| Service Layer | X | X |  |  |
| Online Help | X | X | X | X |
| Documents | X | X | X | X |
| Training | X | X | X | X |
| SME Integration Forum | X | X | X | X |

### 2.4.3 Changing Your Administration User Entry and Password

Users without the Administrator user view assignment can change some fields for their user entry and they can change their password. If you locked your user or forgot your password, ask an administratior to reset your password or click the I have forgotten my password link in the logon screen.

**Procedure**

1. To open the *User Administration* for administration users, choose Maintenance → User Administration, and click Admin Users.

The user interface displays your entry.

1. Add or change the e-mail address and the full name and click the Refresh button. Changes are saved automatically.

Note that the e-mail address is required for the password reset request triggered on the login screen. Entering the full name is not required.

1. To change your password, click Change Password and enter and repeat the password, save your settings and close the window.

Use the new password at the next log on.

1. If the integration framework administrator enabled the password reset process, you can click the I have forgotten my password link on the login screen.

You get an e-mail with a temporary password.

1. Open the integration framework and enter your user name, the temporary password and enter and repeat the new password.

### 2.4.4 Managing Runtime Users

Runtime users are technical users. They send SAP Business One events and are optionally responsible for 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 runtime user. Administration users with the Administrator user view assigned can create, change and delete runtime users. Users with other user views can display the runtime users.

For more information about the authentication and involved BizFlows, see the table below:

| Scenario Package Design | Authorization Concept Definition | | | | Runtime | |
| --- | --- | --- | --- | --- | --- | --- |
| User/Password Handover | | Validation | |
| Authentication | User/ Password Handover | On\_Authen-ticate bfd | User List | Authentica-tion.bfd | Auth. Mode | Validation/  User List |
| No authentication | - | - | - | - | none | - |
| Basic authentication | - | - | - | - | basic | runtime user list |
| User authentication() | 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 |

**Prerequisites**

To create, change or delete runtime users, you must be an administration user with the Administrator user view assigned. Only an administrator can grant access rights to the API for the runtime user.

**Procedure**

1. To open the administration for runtime users choose Maintenance → User Administration, and click Runtime Users.
2. In the user interface header, adjust general settings that are relevant for all users:

| **Field** | **Description** |
| --- | --- |
| 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. To add a user, click Add User and enter the following information:

| **Field** | **Description** |
| --- | --- |
| User | Enter a unique user name. |
| Password, Password (Repeated) | Enter and repeat the password for the user. The password must have eight or more characters. |
| Language | Enter the language for the user. The default language is English. |
| Active | To activate the user , select the checkbox. The function allows you to enter users and to activate them later. |

1. After saving your settings, you can select the second checkbox to grant access rights to the API.
2. To change the password for a user, click Reset Password.
3. Enter and repeat the new password, save your settings and close the window.The password must have eight or more characters.
4. To delete a user, click Delete.

### 2.4.5 Monitoring HTTP Sessions

The http session control monitor allows you to display recently running HTTP sessions. You can terminate sessions.

The monitor displays the timestamp, user name that intitates the session, the channel and duration and the client IP address. You can display further details.

The following information is available in the details section:

| **Field** | **Description** |
| --- | --- |
| User | User ID, the session runs for |
| Session Start Time | Timestamp of session start |
| Session Channel |  |
| HTTP Namespace | Namespace of HTTP session. The namespace indicates the type of the incoming call.   * Browser (dummy)   This is an administration session invoked from the administration console.   * WebDAV   This is a session triggered by a WebDAV client   * basic   This is an incoming HTTP call, either by the event sender or by any incoming http call of a scenario step.   * soap   This is an incoming SOAP call. This is any incoming call of scenario step, triggered by a Web service. |
| Duration | Session duration in seconds |
| IPO Step | Name of the process step, if an inbound call of a scenario step initiates the session. |
| Client IP Address | IP address of the client |
| Session Handle | Session identifier |
| Session Timeout | Timeout setting for session in seconds. The session automatically expires when it is idle for the displayed period of time. |
| Accesses | Number of calls in the session |
| Authentication Mode | Authentication mode of session. The following settings are available:   * none * basic (user name, password) * userdef (user-defined) |

**Procedure**

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

### 2.4.6 Analysing Authentication Events

Authentication events provide you with information about login information for HTTP sessions.

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

**Procedure**

1. Enter your selection criteria or click Submit to display the complete list.

Selection Criteria for Authentication Events

| **Selection Criterion** | **Description** |
| --- | --- |
| Authentication Event Type | You can set a filter on administration or runtime user authentication events. |
| User | Select a user from the list.  Depending on the authentication concept of a scenario package, the incoming HTTP calls uses 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. |
| IP Address | To check if a specific machine triggers sessions, enter the IP address. |
| From Timestamp, To Timestamp | To select events for a specific time interval, select or enter the start and end time. |
| Event Type | The authorization events names end with a type. The following types are available:   * LOGON: For a successful logon * LOGOFF: For a successful logoff * FAILURE: For a failed logon * TIMEOUT: For a timed out logon * KICKOUT: An administration kicked out the logon. * DEACTIVATED: The logon is deactivated after failed logon attempts. |

The integration framework displays a list with login information. The list displays the latest login information first.

1. To display further details, click Details.

| **Field** | **Description** |
| --- | --- |
| User | User ID of logged-in user |
| Event Timestamp | Timestamp of session start |
| Event Channel | Displays the location where the event happened, for example, browser or WebDAV |
| HTTP Namespace | Namespace of HTTP session. The namespace indicates the type of the incoming call.   * dummy   This is an administration session invoked from the administration console.   * WebDAV   This is a session triggered by a WebDAV client   * basic   This is an incoming HTTP call, either by the event sender or by any incoming http call of a scenario step.   * soap   This is an incoming SOAP call. This is any incoming call of scenario step, triggered by a Web service. |
| Duration | Session duration in seconds |
| Client IP Address | IP address of the client |
| IPO Step | Name of the process step, if an inbound call of a scenario step initiates the authentication event |
| Session Handle | Session identifier |
| Session Timeout | Timeout setting for session in seconds. The session automatically expires when it is idle for the displayed period of time. |
| Secure Login (https) | Set to true or false |
| Authentication Mode | Authentication mode of session. The following settings are available:   * none * basic (user name, password) * userdef (user-defined) |
| System Information | For some authentication events, the integration framework displays system information. For example, for the failure event category, the integration framework provides the following information: XCL219 User is unknown |

### 2.4.7 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.

### 2.4.8 Viewing the Personal Data Change Log

Personal data change log provides you with information about which personal data have been changed.

To view the change log of personal data, click Personal Data Change Log. In the pop-up window, the log is displayed with the user who changed the data, the date and time of the change, and the new value of any attribute changed.

## 2.5 Creating Customer Information for Deployments

A deployment is a customer-specific setup and activation of a scenario package. To enable the assignment of a customer to a deployment, create customer information.

**Procedure**

1. To create customer information, choose Maintenance → Customer Administration.
2. To enter customer information, click the Create Customer button and enter a company name.

For internal purposes, the integration framework adds a company ID.

1. Enter the address and contact information and save your settings. This setting is optional.
2. To display the picture loaded by the customer API, click the Open Attachment button.
3. To display scenario packages deployed for the customer, click .

The customer scenario information displays package information and the number of messages in package-related queues.

**Results**

In the deployment panel, you can assign a customer to a deployment. In the transaction monitor, you can select transactions processed for a customer.

# 3 Further Configuration Tasks

## 3.1 Enabling Systems to Use HTTPS

The procedure below uses the Microsoft Internet Explorer as the Web browser. The procedure differs for other Web browser, however the general steps are the same.

**Procedure**

1. From the Web browser, 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 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.

**Results**

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 for 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 check the following parameters in particular:

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

Controls the exposure of WebDAV support in the integration framework

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

With the 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)

The 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. The parameter does not affect the ipo and soap namespaces.

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

The 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 the parameter in your productive environment.

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

The 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)

The 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 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>, ...

The 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

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

xcl.safemode=true,false

With the 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 the parameter, see section *Working in Safe Made*

xcl.cancelPeriod=<seconds>

The 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 the parameter.

xcl.singledumps=true,false

The 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 the parameter.

xcl.reporting=true,false

The 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 the parameter. Do not change the parameter.

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

The 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

The 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. The parameter does not affect the ipo and soap namespaces.

xcl.http.xsrf=true,false

The 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 the 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>

The 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 the parameter, unless you need to exchange the database.

bpc.jdbc\_dbtype=5

The 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

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

bpc.jdbc\_user=sa

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

bpc.jdbc\_password=

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

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

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

#bpc.jdbc\_altpassword=

The 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

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

bpc.threads=<integer>

The parameter defines the thread constraints for the BizProcessor. Do not change the parameter.

bpc.reuseLimit=1

The parameter is deprecated as of BPC 0.21.0 onward.

bpc.maxDumpSize=-1,0,positive integer

The 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 the parameter in your productive environment.

bpc.allowBestXslProfile=true,false

The 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 the parameter.

bpc.historyDepth=0

The 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 the parameter.

**CoordService Parameters**

cos.registryport=6099

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

cos.hostname=localhost

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

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

The 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 the parameter.

cos.cleanupinterval=<seconds>

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

cos.validperiod=<minutes>

The parameter is deprecated as of V 0.12.0.

cos.acquiretimeout=<seconds>

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

cos.rctimeout=<seconds>

The parameter defines how long the integration framework tries to reconnect to a lost connection. The default is 600 seconds. Do not change the 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, do not set a higer level. In a development environment use the CONFIG level. This level is required to display debug 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.

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 the \*.jks, \*.pfx and \*.p12 formats.

**Procedure**

1. Log on to the integration framework.
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 Importing Certificates to a Keystore or Truststore in BizStore user interface, enter the following:

|  |  |
| --- | --- |
| **Field Name** | **Field Value** |
| Certificate | Click *Browse* 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.

## 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.

**Procedure**

1. Copy the tomcat.cer file of the integration framework server 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*.

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

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

| **Field Name** | **Field Value** |
| --- | --- |
| Biz Store URI | To create the truststore, choose Browse 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 Control Center Certificate Import user interface, enter the following:

| **Field Name** | **Field Value** |
| --- | --- |
| Certificate | Click *Browse* 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 the certificate, click *Submit*.

**Result**

You have fulfilled the prerequisites to connect from an integration framework to another integration framework using HTTPS.

## 3.6 Setting Up JDBC Connections with SSL between Service 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 framework, click Stop and then click Start.

## 3.8 Enabling Secure Connections between Framework and Company Databases

**Procedure**

1. In the 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 7.5 → 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 7.5 → 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 7.5 → 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 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.

### 3.10.1 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.

### 3.10.2 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

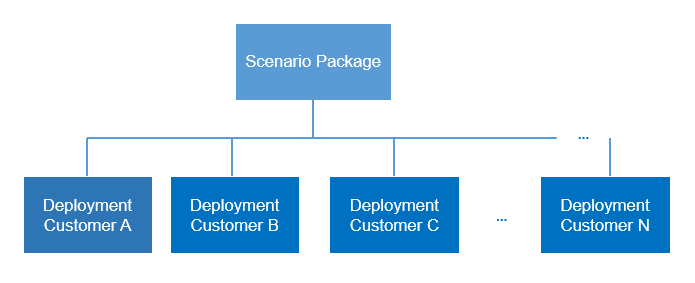
URL Extension: exec/dummy/com.sap.b1ip.system.cc/bfd/AdminConsole.bfd?!defdoc=/com.sap.b1i.common/menu/opdev.xml

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.

# 4 Creating and Activating Deployments

## 4.1 Introduction to Deployment Panel

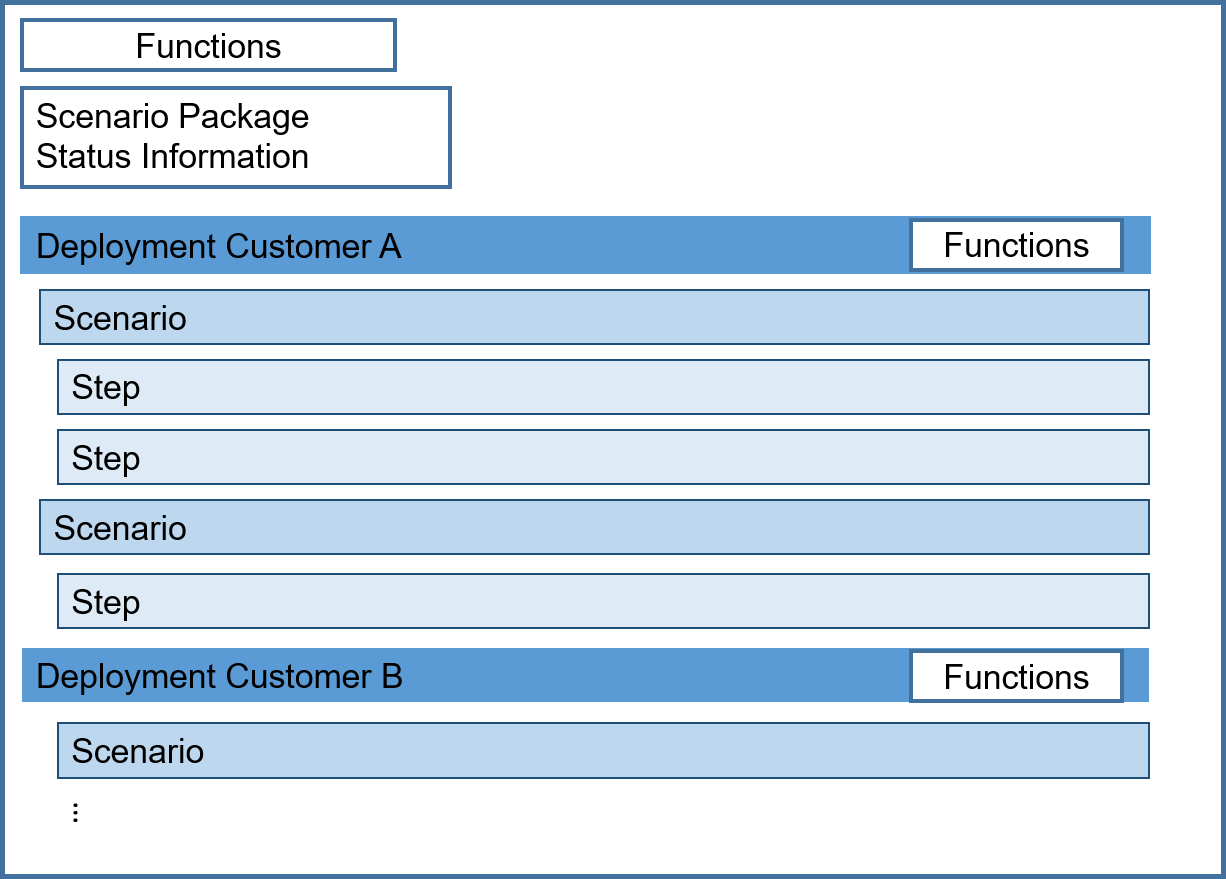
In the on premise use case, you set up and activate a scenario package for one customer. In the cloud use case, you can set up and activate a scenario package for many customers. A deployment is the customer-specific setup and activation of a scenario package. The deployments are strictly separated.



Deployment for Many Customers in Cloud Use Case

**Deployment Panel Overview**

The deployment panel provides functions to add and activate deployments for scenario packages.

  
Deployment Panel

In the **functions** area, you can display the documentation for the deployment panel, display documentation for the selected scenario package and a scenario design concept, refresh the user interface, add a deployment to the selected scenario package, regenerate active deployments for a scenario package, deactivate deployments, display the validation result status and remove all deployments from the scenario package.

In the functions area for each deployment, define value mapping pairs and deployment-specific property values.

In the **Scenario Package and Status Information** area, you can select a scenario package for deployment, displays the number of scenarios in scenario package and display the development, deployment and activation status for the package.

For a selected scenario package, expand the customer-specific deployment, the scenarios and steps. For synchronous steps (HTTP and Web Service), click the URL button to display the URL that you need to call the integration framework from the outside.

**Steps for Deployment Creation and Activation**

| **Step** | **Activity** | **Function in Integration Framework** |
| --- | --- | --- |
| 1 | Create customer systems | SLD |
| 2 | Create customer information | Maintenance → Customer Administration |
| 3 | Select package, add deployment and assign customer record | Maintenance → Deployment Panel |
| 4 | If required, enter deployment-specific property values |
| 5 | If required, enter value pairs for value mapping definitions |
| 5 | If required, enter values in the scenario package administration |
| 6 | Select scenarios and steps for activation |
| 7 | Assign SLD systems to deployment |
| 8 | If required, set up filter definitions based on criteria fields |
| 9 | Activate deployment |

## 4.2 Creating Deployments

To set up and activate a scenario package for a specific customer, add a deployment to the deployment panel.

**Prerequisites**

* You created the systems in SLD that the customer wants to connect through the scenario package.
* You created a customer record for the deployment in Customer Administration for the multi-tenancy mode.

**Procedure**

1. To open the deployment panel, choose Maintenance → Deployment Panel.
2. To create a deployment for a customer, select a scenario package in the Scenario Package field, and click the Add Deployment button.

The integration framework adds a line to the deployment panel.

1. In the red field, enter the deployment name.
2. Go to the next field and select a customer.

The deployment panel creates the new deployment and adds the scenarios and steps to the deployment.

1. If you are in the design phase in the step modeler, or you are a system administrator and want to troubleshoot the deployment, you have the option to click the  (Detailed Logging) button for each scenario to enable the production of detailed debugging information.

The detailed debugging information enables the red arrows in the test environment and in monitoring.

**Results**

The new deployment is available. The deployment is inactive. Deployments are sorted by deployment name.

## 4.3 Entering Deployment-Specific Properties (Optional)

If the scenario package requires settings that are different for each deployment, enter the property values. The user interface automatically saves your entries, a save function is not available.

**Prerequisites**

To enter or change values, deactivate the deployment.

**Procedure**

1. In the deployment panel, click the  (Deployment-Specific Properties) icon for the deployment.
2. Enter or select values for the deployment.
3. For an array of strings, click *Expand* and then the *Add* button.

The function adds an element record.

1. Enter a value.
2. Add further element records as required.

## 4.4 Entering Values for Value Mapping Definitions (Optional)

At design time, the value mapping function allows the integration developer to define fields and attributes of the XML message for which the mapping of values take place between sender and receiver systems. If the scenario package contains value mapping definitions, the  (Value Mappings) icon is enabled for each deployment. You can enter value pairs for active deployments.

Instead of entering value pairs, you can use the import and export functions:

* ZIP import and export

The ZIP import function allows importing value mappings in an XML document. For each sender and receiver system combination and mapping definition, the document contains value pairs. The document is available in the BizStore in the following place:

com.sap.b1i.dev.scenarios.setup/<package\_name>/vm.<deployment\_name>.xml

The export function exports the XML document.

* Import and export per sender, receiver and value definition combination

For each sender and receiver combination and value mapping definition, you can import and export value pairs in an Excel file with comma-separated value (CSV) format.

**Procedure**

1. To add value mapping settings, in the deployment panel, click the  (Value Mappings) icon and in the Value Mapping Setup, click the + (Add Value Mapping Field) icon.
2. Select a value mapping definition and the function adds the definition to the table.
3. In the definition line, click + (Add Value Mapping Combination of Sender and Receiver) and in the added line, select a sender and a receiver system combination.

If value pairs are valid for all sender and receiver sytem combinations, selet all or enter \*.

1. To define sender values that are mapped to the receiver values, click + (Add Value Mapping) or, if there are many values, click Add 10.
2. Enter the value pairs. The function detects duplicate entries and highlights the fields in red.
3. Sort and invert the value pairs.
4. To export all value mapping definitions and settings to an XML file that is part of a ZIP, click ZIP Export.

The value mapping definitions, sender receiver combinations and value pairs are part of the com.sap.b1i.dev.scenarios.setup/<package\_name>/vm.<deployment\_name>.xml document.

1. To export mapped values for a sender and receiver system combination and value mapping definition, click Export. The function creates a comma-separated values (CSV) file that you can open in Microsoft Excel.
2. To create the CSV file, select the character encoding ( default is ISO-8839-1), delimiter (default is ;) a character wrapper, if your values contain the delimiter and click Export.

The function creates a CSV file. The file name consists of the development namespace, valmap, the deployment name and the SysIds of the sender and receiver system.

1. To import mapped value pairs to a sender and receiver system combination, click Import and select a CSV file from the file system.

**Results**

* At runtime, the framework maps the values. If you defined a value pair for the all senders and all receivers combination, but added a value pair for a specific sender and all receivers or even a value pair for a specific sender and receiver combination, the runtime uses the value pair of the most specific combination.
* Value mapping detects the sender and receiver systems, if the information is available at runtime.
* If you added processing instructions to the inbound XML message that determine a sender and a receiver system combination, the value mapping only considers the sender and receiver system combination.

## 4.5 Adding Values in the Scenario Package Configuration (Optional)

If the scenario package provides a scenario administration, the  (Scenario Package Configuration) button is enabled.

**Procedure**

In the deployment panel, click the  (Scenario Package Configuration) icon and enter the required values.

## 4.6 Assigning SLD Entries, Setting Filters and Deployment Activation

Select the scenarios and scenario steps that you want to activate for the deployment. If scenarios and steps require the assignment of SLD entries, assign the systems, set filters defined by criteria fields and add further setup configuration. Then, you are ready to activate the deployment.

**Prerequisites**

You created SLD entries for the customer in SLD. To simplify the selection of SLD entries in the deployment panel, you created an SLD category for the customer and assigned all customer-related systems to the category.

**Procedure**

1. Expand scenarios and steps of the scenario package.
2. Select the scenario or scenarios you want to activate.

The integration framework displays a green or red flag. A green flag indicates that all information for activation is available. A red flag indicates that information is missing and you need to assign SLD entries.

To select dedicated steps of a scenario, select the scenario first and then deselect the steps that you do not want to activate.

1. If the deployment panel displays a red flag, click the Systems button in the the deployment line to assign SLD systems to the scenario. The integration framework displays SLD assignments for senders, receivers and flow calls.

Alternatively, you can click Systems on scenario or scenario step level.

1. In the header of the Deployments – SLD Assignments user interface, in the SLD Category field, select the category that you created for the customer.
2. In each line that displays a red flag, click the Assignment button and select a system or systems from SLD.
3. If the package definition requires the setup of filters for senders or receivers defined by criteria fields in package design, click the  (Filters Configuration) button.

If the button is disabled, there are no filter definitions.

* To configure filter definitions, click Add. The framework displays the first criterial field of the package definition. The filter is active by default. You can select another criteria field.
* Define the filter definition and to add aonther filter definition click Add.

The framework adds another line.

* In the new line, you can select whether the new difínition is related to the existing one with a logical OR or AND.
* After defining all filers, close the window. The green filter icon indicates that filters are avaible.

1. For some inbound channels that are generic, for example, B1EV (SAP Business One), a developer can define selection options for inbound. If you select a system and the Setup button is enabled, click the button to display the selection options.
2. For the predefined properties, you can select values and close the window. With a green Setup button, the framework indicates that properties are selected.
3. Once the validation flag color is green, click the  (Activate) button in the deployment line.
4. For some inbounds, for example, Incoming B1 Event and Incoming IDocs, the framework provides integration services that perform certain tasks for the inbound. If a step uses such an inbound, the related services must be active. The thumb up or down icons indicate that a step uses the service and whether it is active or not.

Note that if you deactivate or delete a deployment, the services, for example, the SAP Business One event subscription, are not deactivated automatically. To deactivate the subscription, click the thumb up icon.

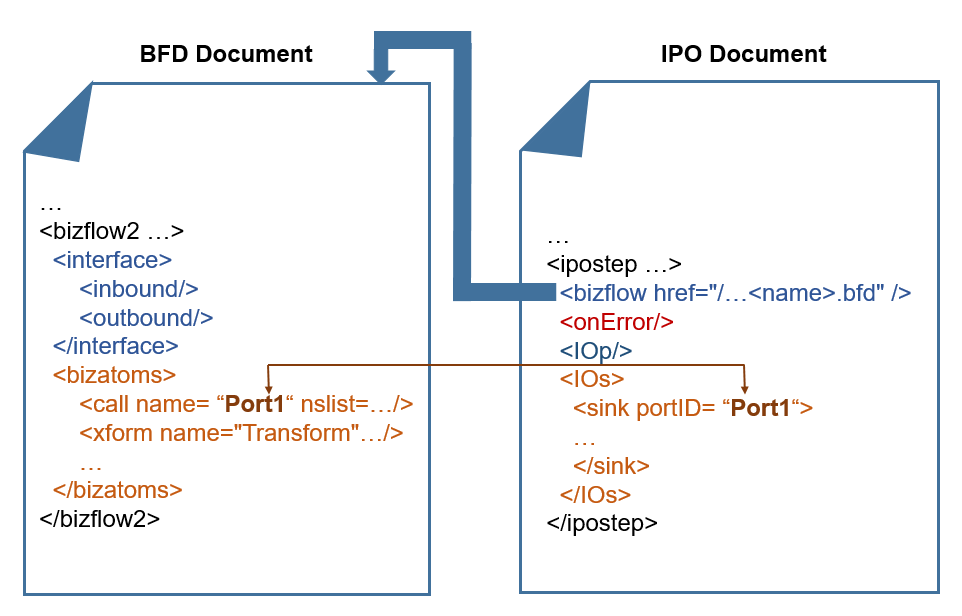
**Results**

The *Activate* button changes to  (Deployment Active).

If the deployment panel still displays red flags, activation is not possible, because there is something wrong in the design. Use the status report to analyse inconsistences.

## 4.7 Working with Runtime Artefacts

The activation of a deployment generates runtime artefacts that the integration platform (B1iP) requires to process the scenario step. Runtime artefacts are the BFD document, the IPO document, and the deployment document.

  
BFD and IPO Documents

**BFD Document**

The BizFlow definition (BFD) document describes the processing phase of a scenario step. The activation of a deployment generates the document.

In the <interface> section, you find the <inbound> tag that contains the general flow properties that are handed over to the flow. In the <outbound> tag, you define properties you want to hand over to the outbound phase.

In the <bizatoms> tag, you find the definition of all atoms of the BizFlow. If an atom is a call, the value of the name attribute corresponds to the portID in the associated IPO document.

After initial activation, the document is still available after deactivation. A further activation updates the document.

**IPO Document**

The activation of a deployment generates the IPO document. The document defines the inbound, processing and outbound (IPO) of a scenario step.

* in the <bizflow> tag, the document references the associated BizFlow document.
* In the <IOp> (inbound outbound primary) tag, the document defines the inbound and outbound of the scenario step.
* In the <IOs> (inbound, outbound secondary) tag, the document defines the properties of all adapter calls that happen in the processing phase of the scenario step. The portid attribute contains the name of the adapter call atom and lists all properties that are already defined in the design phase. If the adapter properties are obtained through the assignment of an SLD entry, the activation already writes the values to the document. If the properties are obtained at runtime through an XPath statement, it is noted in the document. The generation aims to provide as many properties as possible in the IPO document to ensure a good performance.

If you assign more than one SLD entry to a scenario step, you find the <Multiple> root element that contains the <ipostep> elements, one for each SLD system.

If you deactivate a deployment, the integration framework deletes the IPO document.

**Deployment Document**

For an active deployment, you can display the deployment document. The deployment document contains information about the activation and whether detailed logging is enabled for the step.

**Procedure**

1. To display runtime artefacts for an active deployment, click the Runtime Artefacts button for a scenario step. A window opens with tabs for the BFD, IPO, deployment and property sources.
2. Click the Property Sources tab to display all adapter properties and values of the scenario step. You get information about the source of the property value, for example, set to a fixed values in the step design, or obtained from an assigned SLD entry.

## 4.8 Deployment Panel in the Step Modeler

Use the deployment panel in the step modeler to test your scenario package in the system landscape. The deployment panel test includes the inbound and outbound phase of scenario steps and checks the consistency of all adapter calls or port definitions. Create a test deployment (test customer) that uses the scenario package to integrate systems with each other.

To open the deployment panel, click Deployment Panel for the scenario package in the package explorer.

## 4.9 Using the Validation Result to Resolve Inconsistencies

To indicate that a scenario or a scenario step is ready for deployment, the deployment panel displays flags on scenario package, scenario and scenario step level. A green flag indicates that all required properties are available. A red flag indicates that there is something wrong with the ports or adapter calls of the scenario.

The flag color depends only on selected scenario steps. If a selected scenario step displays a red flag, the related scenario also displays a red flag. A scenario can only have a green flag, if all selected scenario steps belonging to the scenario have a green flag, too.

If the integration framework displays a red flag, click the icon and display further information:

* There are inconsistencies in adapter call definitions in design
* You have defined a group port ID for adapter calls of different connectivity type
* You have used the same port ID more than once in a scenario step.
* Information required for the deployment is not available:
* Assignments to SLD systems are missing
* Mandatory adapter property values are missing

**Procedure**

1. If the deployment panel displays a red flag for a scenario, expand the scenario to display the steps.
2. Deselect steps with a green flag and select the first scenario step with a red flag, close the user interface, and in the deployment panel, click Status.

The status report displays errors for selected scenarios and scenario steps. For scenarios and steps that have a green flag, the status report does not display detailed information.

1. Analyze the scenario error information to determine the root cause.

* If you are using the deployment panel in the step modeler, change the design accordingly.
* If you are using the deployment panel in the Maintenance menu, notify the development team to solve the problem.

1. For a selected scenario step, you can display the properties and the source of the property values.

## 4.10 Configuring and Using Scenario Step Triggers

Configure the trigger of a scenario step and trigger the step for further testing.

**Procedure**

1. For the scenario step that you want to trigger, click the  (Configure Trigger) button. The development environment opens the *Test Trigger Configuration* user interface.

If the integration framework runs for a single tenant on premise, the Deployment Name value is ST for single tenant.

1. The Inbound Message checkbox indicates whether an inbound message is available or not.

If an inbound message is missing but required, provide the message in the scenario step folder in the com.sap.b1i.dev.scenarios.setup dataset in the BizStore. Use the trigger.msg.xml name for the inbound message.

1. The user interface displays further required entries in red. Select or enter values and close the user interface.
2. To trigger the step, click the Trigger button.

The deployment panel displays the single transaction monitor with the transaction status and the duration of the transaction in milliseconds.

1. For further investigation, click the buttons.

For more information, see section 2.1.2 Performing Transaction Log Operations

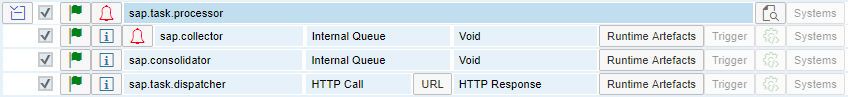
## 4.11 Deactivation and Regeneration of Active Deployments

The functions for the deactivation of all deployments and regeneration of active deployments are particularly important in scenario step development.

Changes in XSL and JavaScript documents do not require a redeployment. However, changes in the process flow require a redeployment to create the related runtime artefacts. To regenerate active deployments, click the  button.

## 4.12 Detecting Outdated Runtime Artefacts

The integration framework generates internal version numbers for scenario steps. Each time, a developer saves the step in step design, the framework sets a higher internal version number. The activation of a deployment generates the required runtime artefacts for the currently available internal version. If the integration framework detects that the internal version of the runtime artefacts differs from the internal version of step design, the deployment panel displays the  icon.

  
Scenario and Scenario Step with Outdated Runtime Artefacts

The sap.collector scenario step runs with artefacts that differ from the step design. This is not an error. It only indicates that un updated design version is available. You can click the  regeneration function to synchronize the runtime artefacts with the design.

# 5 Monitoring

To analyse the runtime, integration framework provides monitoring of messages and processes. You have various options to analyze even the smallest details.

note.gif NOTE

All time-related information with regards to setup, processing and monitoring of the integration framework messages; such as timestamps or scheduler timer setting, comes from the integration framework server and its local time zone.

**BPM Monitor**

For more information about the BPM monitor, see the Business Process Management Guide

**Cockpit**

The integration framework offers a cockpit that displays information about integration scenarios, system information and system resource information.

## 5.1 Monitoring Transactions

The transaction monitor displays transactions that the system performs for scenario steps and deployments. A transaction is the processing of a scenario step. To open the transaction monitor, choose Monitoring → Transaction Monitor.

### 5.1.1 Defining Filter Settings and Displaying Logs

**Procedure**

Use the following filter criteria:

| **Field** | **Description** |
| --- | --- |
| Scenario Package | Allows you to filter transactions of a scenario package. Select a package from the list. |
| Deployment | Select a deployment for a scenario package |
| Scenario | Select a scenario for a scenario package |
| Scenario Step | Select a step for a package and scenario |
| From Timestamp, To Timestamp | Allows you to set time intervals |
| Maximum Number of Results | Allows you to limit the number of transactions for display |
| Transaction Status | Allows you to filter messages according to their status.  In the dropdown list you can select one of the following values:   * STARTED   The integration framework started the transaction.   * COMPLETED   The integration framework successfully completed the transaction.   * CANCELLED   The integration framework finished the transaction with an exception.   * INCOMMIT   The integration framework finished the transaction and waits for commitment.   * INROLLBACK   The transaction failed and is in the roll back phase. |

The transaction logs are displayed in a table.

| **Field** | **Description** |
| --- | --- |
| Number | Number of displayed messages |
| Transaction URI Pattern | Displays the URI pattern for further investigation |
| Actions – Open Flow Debugger | Display the fllow debugger for the step. If debugging information is available, the debugger displays red arrows that you can click to display the inbound messages at each point of the flow.  A red icon indicates, that errors occurred in a logical inbound or outbound, for example, in B1AO.1. The logical B1AO.1 outbound, for example, is implemented as an include into your step processing. You can do the following:   * Open the flow debugger and click the Include element. The framework displays the included logical outbound. * Clicking the call atom displays the Transaction Monitor – Logical Adapter. The monitor displays transactions handed over in the call with their status. In the monitor, you can open the flow debugger and display the inbound and outbound message. |
| Actions – Open Inbound Document | Displays the inbound document of the scenario step |
| Actions – Open Outbound Document | Displays the outbound document of the scenario step |
| Status | - Transaction Canceled  – Transaction Finished Successfully  – Transaction in Incommit Phase, or Transaction in Rollback, or Transaction Started |
| Start Timestamp | Timestamp of transaction start |
| Duration | Displays the processing time in milliseconds |
| Deployment | Displays the deployment, for the in premise verison, the monitor displays ST for single tenant. |
| Scenario | Displays the scenario |
| Scenario Step | Displays the step |
| Sender | Displays the sender SLD system ID |
| Trigger/Object | Displays the trigger and object of step, for example, B1EV [2], SAP Business One inbound for the business partner object |
| Info | Click the button to display further trigger information |
| Arrow | Click the arrow to display the transaction ID. |

The Single Transaction Monitor displays the following information. For more information, see the table above:

* Scenario package
* Deployment name
* Scenario
* Scenario step
* Inbound
* Outbound
* Timestamp
* Duration
* Status

### 5.1.2 Performing Transaction Log Operations

**Procedure**

1. To display detailed processing information of a transaction, click [IPO Log].

The integration framework displays detailed inbound, processing and outbound information of the transaction, if the production of detailed logging information is enabled. If an error or exception occurrs, the integration framework displays error information and the call stack at the end of the list.

1. To display the message flow inquiry, click [MsgFlow Inq.].

The message flow inquiry displays on low level, how the message is processed by the integration framework.

1. To display the processing time and the differents steps the message runs through, click [MsgProcTime].
2. To display step execution details in one document, click [ExecDetails].

You can look up steps; display inbound parameters, and the inbound message for all steps. You can access the information in a graphical representation clicking the [Debug] button.

1. To display the debug information for the setp, click [DEBUG].
2. To analyse potential performance issues, click [Profiler].

The integration framework displays all process steps with processing details sorted by duration, internal database interactions sorted by duration, and the size of the inbound message sorted by size for all process steps.

## 5.2 Error Inbox Monitor

The error inbox monitor displays messages that the integration framework cannot hand over to the receiver system. After handing over the message to an error inbox for the receiver system, the integration framework continues processing the next message to avoid blocked queues. From the error inbox, an administrator can display, debug, resend or delete the error messages.

**Procedure**

1. To display the error inbox per receiver system, choose Monitoring → Error Inbox and click the receiver system with messages in the error inbox.
2. In the Error Inbox Filter section, define filter criteria for display and click Display/Refresh.
3. The monitor displays messages per package and deployment with the timestamp and result message.
4. Use the functions in the Actions column to display, debug or resend the message.
5. To delete messages, click the checkbox in front of the row and click Delete.

## 5.3 Activating and Monitoring Integration Services

The integration framework offers application-specific and general integration services. You can use the specific integration services in your scenario packages. Additionally, the monitor displays the services of business process management. To display integration services, choose Monitoring → Service Monitor.

### 5.3.1 SAP Business One Event Inbound Service

For SAP Business One inbound, the service picks up events and requests the according sender information from the SAP Business One system. You need the service for the B1EV logical inbound adapter.

**Activation and Monitoring**

1. Choose Monitoring → Service Monitor, and for the SAP Business One Event Inbound Service, click  (Configure Integration Service) and in the setup user interface, click the  (Activate Service) button.
2. Once the service is active, click the  (Display Available Transactions) button to display the transaction ID panel for the activated service.
3. To display the subscribers of the integration service, click  (Display Subscribers of Service).

The framework displays the scenario package identifier, deployment and the number of steps that use the service.

### 5.3.2 SAP ERP IDoc Inbound Service

For incoming IDocs from SAP ERP systems, the service obtains the IDocs and looks up the systems that are subscribed to the IDocs. You need the service for the IDOC logical inbound adapter.

**Activation and Monitoring**

1. Choose Monitoring → Service Monitor, and for the SAP Business One Event Inbound Service, click  (Configure Integration Service) and in the setup user interface, select the sub services for SAP ERP systems defined in SLD, and click the  (Activate Service) button.
2. Once the service is active, click the  (Display Available Transactions) button to display the transaction ID panel for the activates integration services.
3. To display the subscribers of the integration service, click  (Display Subscribers of Service).

The framework displays the scenario package identifier, deployment and in number of steps that use the service.

### 5.3.3 Business Process Services

If you use business process management, display and monitor the related services and activate the *BPMN Engine - Timeout Controller* service.

### 5.3.4 SAP Business One Asynchronous Outbound Service

Using the SAP Business One Asynchronous outbound service, you have various options to hand over data to SAP Business One.

**Activation and Monitoring**

1. Choose Monitoring → Service Monitor, and for the SAP Business One Event Inbound Service, click  (Configure Integration Service) and in the setup user interface, select the sub services for SAP ERP systems defined in SLD, and click the  (Activate Service) button.
2. Once the service is active, click the  (Display Available Transactions) button to display the transaction ID panel for the activates integration services.
3. To display the subscribers of the integration service, click  (Display Subscribers of Service).

### 5.3.5 System Services

The monitor additionally displays services running in the background for several use cases:

* iPaaS client services for the cloud landscape
* SAP Business One Event Handler Service (iPaaS Version) in the cloud landscape
* API service to approach the integration framework through the API
* Scenario queue monitor services
* Mapping tool: XSD To XML generator services
* Common services

## 5.4 Monitoring Scenario Queues

### 5.4.1 Introduction to Scenario Queues

Unlike the B1iP-based technical queue monitor that potentially displays all queues and messages used in the integration framework, the scenario queue monitor offers a **scenario view** on queues and messages in queues. Based on scenario packages, scenarios, scenario steps, deployments, sender systems and (or) customer, you can control the status of and administer the related queues.

**Scenario Package-Related Queues**

The following inbound types use queues:

* DBQI Internal Queue Trigger
* ENQI Successor
* B1EV SAP Business One Inbound by Events
* IDOC SAP ERP - Incoming IDOC
* BPMI Business Process Inbound
* BYDI SAP Business ByDesign Inbound
* MQIN Multiple Queue Inbound

### 5.4.2 Defining QInfo and Trace ID for the Scenario Queue Monitor

In scenario design, you have the following options to define search settings for the scenario queue monitor:

* QInfo
* Trace ID

#### 5.4.2.1 Using QInfo

In scenario design, you can define the QInfo property for the above inbound types. Set a fixed value, this is usually the business object identifier. In the Business Object filter field of the monitor, you can select the value.

#### 5.4.2.2 Using the Trace ID

Messages are put to queues either through a logical inbound adapter or throughby another scenario step. Functions that put messages in queues, can define a trace ID. The trace ID is saved with the message, and you can use the ID to identify queue messages. The scenario queue monitor offers the option to set a filter to trace IDs.

**Logical Inbound Adapters**

The following logical inbound adapters are technically triggered by internal queue:

* B1EV SAP Business One Inbound by Events
* IDOC SAP ERP - Incoming IDOC
* BYDI SAP Business ByDesign Inbound
* BPMI Business Process Inbound

The internal queues trigger subscribed scenario steps. The integration framework evaluates the trace ID and hands over the trace ID value to the queue.

For the B1EV, IDOC and BYDI logical inbound adapters, you can define the trace ID in scenario design using the Trace ID property. You can set a fixed value or you can define an XPath statement. The XPath statement runs against the inbound message. If the logical inbound adapter includes data retrieval, like for B1EV, the integration framework determines the trace ID after data retrieval. The mechanism allows you to define the XPath statement running against the retrieved data.

If you do not set the trace ID for B1EV and IDOC, the integration framework sets a default value. The default value for B1EV is the business object identifier, for example, 2 for Business Partner and for IDOC the default value is the root tag name of the incoming IDoc that is the IDoc type, for example, DEBMAS05.

For BPMI (business process management inbound), define the trace ID in the business process modeler. Define the trace ID for a service task, a send task and a message end task. If you start the trace ID with /, the framework assumes that the entry is an XPath statement. The framework evaluates against the inbound message of the scenario step. A trace ID without / at the beginning is a fixe value.

**Examples**

* B1EV

In the Trace ID field, set the value, for example, to //b1e:b1event/b1e:objecttype to save the SAP Business One object ID to the trace ID.

* BPM Service Task

In the Trace ID field, set the value, for example, to //inbound/bpm.start/@step.ident to pick up the step identifier.

**Steps Based on Internal Queues**

For the following inbound types, scenario steps are triggered by messages in inbound queues that are put to queue usually by other scenario steps:

* DBQI Internal Queue Trigger
* ENQI Predecessor Trigger
* MQIN Multiple Queue Inbound

You can use the following atoms in scenario step processing to trigger other queue-triggered scenario steps:

* DBQO Call in the flow
* DBQO.1 Call in the flow based on B1if 1.x atom
* DBQO Outbound to a queue
* ENQO Outbound to call a successor

The atoms support the Trace ID property. You can set a fixed value, you can set a value by using a flow property or you can define an XPath statement that is evaluated against the incoming message of the call atom.

### 5.4.3 Using Filter Criteria for the Queue List

You can define the following filter criteria for the display of queues:

**Filter Critera**

| **Field** | **Description** |
| --- | --- |
| Scenario Package | Allows you to filter queues of a scenario package. Select a package from the list. In the queue list, the scenario package column is not displayed. |
| Scenario | Select a scenario for a scenario package. The scenario column is not displayed in the queue list |
| Business Object | With a selected scenario package, select a business object of the scenario package to filter the queue list by a business object of the package. The business object column is not displayed in the queue list. In scenario step design, define the business object value by using the QInfo property |
| Deployment | With a selected scenario package, you can select a deployment of the package to filter the queue list by a deployment of the selected package. The deployment column is not be displayed in the queue list. |
| Scenario Step | With a selected scenario package and a scenario, you can select a scenario step of the package and scenario to filter the queue list by a scenario step. The scenario step column is not displayed in the queue list. |
| Display Mode | Select to either display all queues that are related to scenarios or to only display queues contain at least one message. |
| Customer | If you defined customers in the Customer Administration function of the Maintenance menu and assignd deployments to customers, you can select a customer to filter the queue list by a customer. The customer column is not displayed in the queue list. |
| Inbound Adapter Type | The scenario queue monitor displays all scenario steps that are technically triggered by internal queue. The following inboudn adapters use internal queue:   * DBQI Internal Queue Trigger * ENQI Successor * B1EV SAP Business One Inbound by Events * IDOC SAP ERP - Incoming IDOC * BPMI Business Process Inbound * BYDI SAP Business ByDesign Inbound * MQIN Multiple Queue Inbound |
| Sender System | Scenario steps that are triggered by the B1EV, IDOC or MQIN inbound types support multiple sender systems. Filter the queue list to a sender system. The sender column is not displayed in the queue list. |

### 5.4.4 Sorting the Queue List

To sort the queue list, click the header field.

| **Field** | **Sort List by** |
| --- | --- |
| St. (Status) | Status, lists IPOs with an exception first, then active IPOs and then inactive IPOs |
| Cnt (Count)  Number of messges in the queue | Number of messages in the queue in descending order |
| Scenario Package | Scenario package, in alphabetical and ascending order |
| Scenario | Scenario, in alphabetical and ascending order |
| Scenario Step | Scenario step, in alphabetical and ascending order |
| Sender | Sender system identifier, in numerical and ascending order |
| Customer | Customer, in alphabetical and ascending order |
| Business Object | Business object, in alphabetical and ascending order |
| Adapter | Adapter, in alphabetical and ascending order |
| Queue | Queue name, in alphabetical and ascending order |
| Stream | Stream name, in alphabetical and ascending order |

### 5.4.5 Working with the Queue List

The queue list displays one line for each scenario step with queue inbound that meets the filter critera. The scenario step is either active or inactive. If the step is inactive, there are either messages in the queue, because you set the step inactive during processing.

The first columns of the queue list displays the control information.

| **Control Information** | **Description** |
| --- | --- |
|  | The scenario step is active and there are no messages in the queue. |
|  | You deactivated the scenario step in the deployment panel. There are no messages in the queue |
|  | You deactivated the scenario step in the deployment panel. There are 4 messages in the queue. You can display the messages and you can delete the messages from the queue.  For more information, see section Working with Messages in the Queue and Stream |
|  | The scenario step is active. However, currently the step is inactive due to an exception that happenend in the last processing. There are 41 messages in the queue. You can display the messages and you can delete the messages from the queue.  For more information, see section Working with Messages in the Queue and Stream |

The last illustration in the table above informs you that the step is active, however currently deactivated due to an exception in the last processing. There are already 41 messages waiting in the queue. It is obvious that the first message potentially blocks the queue by causing an exception.

**Procedure**

1. To investigate the message, click the red icon in the first column to open the exception user interface.

* In the Iteration Count field, the function displays the number of attempts to process the message again.
* Click the [Debug] button to display the debugging user interface.

1. If there is no error in the coding, but the inbound message is the root cause, open the Queue Message List and delete the first message in the queue to allow the message processing to continue.

### 5.4.6 Working with Messages in the Queue and Stream

Use the queue message list monitor to display messages in a queue and stream. The monitor reads messages block by block with 50 messages per block. You can navigate forward and backward between blocks. Filter messages by trace ID. You can delete a single message in the queue and you have multiple options for batch deletion.

**Procedure**

1. To display messages in a queue, click  (Queue Message List).
2. You can browse messages block by block.
3. Sort the message list by message or by trace ID.
4. To delete messages, you have the following options:

* Delete all Messages in this List
* Delete All Messages in this List that are selected
* Delete All Messages in Queue/Stream with selected Trace ID
* Delete All Messages in Queue/Stream

## 5.5 Monitoring Technical Queues

You can hand over messages from one scenario step to another by using internal queues. The queue monitor allows you to monitor the message queues, streams (sub-queues) and messages in streams. The queue monitor allows you to check the current status in internal queues.

**Procedure**

1. To display or delete messages messages in a queue or stream choose *Monitoring*→ Technical *Queue Monitor*.

The integration framework displays queues, streams that contains at least one message. Due to fast processing, you typically cannot display messages waiting in an internal queue.

1. To display a message, click Display.
2. To check the process that created the message in the queue, click [MsgFlowInq.].
3. To delete a message from the stream, click [Delete].
4. To delete the messages from the stream, click [Clear].

# 6 Tools and Help Functions

## 6.1 Displaying Benchmarks

The benchmarks provide an initial indicator whether the integration framework is in a healthy state.

**Procedure**

1. To displays benchmarks, choose *Tools* → Benchmarks.
2. To start calculations for benchmarks, click Run Benchmarks.

**Result**

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

A value of 300 or higher indicates a good average performance

## 6.2 Using the Embedded Internal XML Editor

The integration framework provides an embedded internal XML Editor you can use to access BizStore documents.

**Procedure**

1. To select a document and open it for editing, choose *Tools* → XML Editor.
2. Select the dataset, group and document from the BizStore and click Open.

The integration framework displays the document.

1. To display the text in a structured way, click Pretty Print.
2. To automatically pretty print a document, click Settings and select Perform Pretty Print.

## 6.3 Displaying XSLT Libraries

For frequently used tasks in the transformation area, the integration framework provides libraries that you can use in the XSL documents. The following library functions are available:

* String operations

String operations provide functions to manipulate strings, respectively to retrieve some information from them. You can use string operations to delete leading zeros in a string, for example.

* Date/Time functions

The date/time operations provide functions around date and time. You can retrieve the current date and time. You can calculate some special dates or provide formatted output.

* System functions

The system functions are more technical, for example, to generate a globally unique identifier (GUID).

* Crypt

Functions to crypt and decrypt content

* Memory Variables

Functions are available to initialize or set a memory variable, and to obtain the current value.

**Procedure**

1. To display available library functions, select *Tools/Help* → *XSLT Library*.
2. Select a library.

The documentation displays available templates with a short description. The templates names start with the b1ilib*.* abbreviation, followed by the name.

1. To display a function, click the name, and the integration framework displays the information. For example, to display detailed information about the b1ilib.today\_minus template, click the name. it provides information about how to call the function, a detailed description, the parameters, the default settings and an example how to use it. You can copy the example and paste it to your XSL stylesheet.

## 6.4 Displaying Documentation

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

**Procedure**

Click the  (book) icon in user interfaces.

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 red book icon.

### 6.4.1 Displaying Online Help

The online help displays available documentation of the integration framework.

* Information about setting up the development environment for interaction with the BizStore
* Scenario development information
* Using the System Landscape Directory (SLD)
* Operations
* Available adapter request and response documents for scenario development

**Searching in Online Help**

The function provides a simple search tool. Enter a term in the search field, click Search, and the integration framework displays headings that contain the term.

### 6.4.2 Displaying Documents for Prining

The documents function provides documentation in PDF format. The content is identical with the one in the *Online Help* section. Additionally, find documentation assigned to scenario packages that are part of your integration framework. The documents contain the configuration information for scenario packages.

## 6.5 Displaying and Using the Training Material

The integration framework contains the sap.dev.training scenario package. The package contains steps that help you getting started with the integration framework version 2.

In the training function, you can display the objectives of each section, open the slides for each subsection and click the scenario steps described in the slides. The training package uses the technical adapters and the framework message is in the hand of the integration developer.

## 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.