**Integration Framework**

**Operations**

**Performance and Security**

**Last Modified: June 14, 2023**

[1 Basic Performance Considerations 3](#_Toc137655012)

[1.1 Memory and Cache Management 3](#_Toc137655013)

[1.2 Network Connection 3](#_Toc137655014)

[1.3 SAP Business One Event Sender Configuration 4](#_Toc137655015)

[1.4 Efficient Integration Framework Configuration 4](#_Toc137655016)

[2 Integration Framework Security Guide 5](#_Toc137655017)

[2.1 Technical System Landscape 5](#_Toc137655018)

[2.2 Administration Concept 6](#_Toc137655019)

[2.2.1 Operating System Level 6](#_Toc137655020)

[2.2.2 Database Administration Level 6](#_Toc137655021)

[2.2.3 Integration Framework Level 6](#_Toc137655022)

[2.3 Securing the Installation and BizStore Connection 7](#_Toc137655023)

[2.3.1 Base Directory and Runtime Environment 7](#_Toc137655024)

[2.3.2 BizStore 7](#_Toc137655025)

[2.3.3 Securing Xcellerator.cfg 8](#_Toc137655026)

[2.3.4 Administration User Interface 9](#_Toc137655027)

[2.4 User Management and Authentication Concepts 9](#_Toc137655028)

[2.4.1 Administration and Runtime Users 9](#_Toc137655029)

[2.4.2 Authentication for Incoming Web Service and HTTP Calls 10](#_Toc137655030)

[2.5 Connections to Systems 12](#_Toc137655031)

[2.5.1 Connection to SAP Business One 12](#_Toc137655032)

[2.5.2 Event Sender Connection to Integration Framework 13](#_Toc137655033)

[2.5.3 Connection to SAP ERP 13](#_Toc137655034)

[2.5.4 Connections between Integration Framework Servers 13](#_Toc137655035)

[2.5.5 Connecting to Other Systems 14](#_Toc137655036)

[2.5.6 Enabling HTTPS 14](#_Toc137655037)

[2.6 Auditing 14](#_Toc137655038)

[2.7 Protection Against Cross-Site Request Forgery 15](#_Toc137655039)

[2.8 Protection Against SQL Injection 15](#_Toc137655040)

[3 Sizing Information 16](#_Toc137655041)

[3.1 Avoiding Out-of-Memory Situations 16](#_Toc137655042)

[3.2 Memory Requirements for DI Proxies 16](#_Toc137655043)

[4. Appendix: Mutual Authentication Between Integration Server and Event Sender 17](#_Toc137655044)

[4.1 Purchase Certificate 17](#_Toc137655045)

[4.2 Self-Signed Certificates 17](#_Toc137655046)

[4.2.1 Generate Self-Signed Root CA 17](#_Toc137655047)

[4.2.2 Generate RSA Key Pair 18](#_Toc137655048)

[4.2.3 Create Ext File wdfv41008435d.emea.global.corp.sap.ext 18](#_Toc137655049)

[4.2.4 Sign CSR 19](#_Toc137655050)

[4.2.5 Generate the PKS12 KeyStore 19](#_Toc137655051)

[4.2.6 Import into the JKS Keystore 20](#_Toc137655052)

[4.2.7 Generate a Trust Store 20](#_Toc137655053)

[4.2.8 Create a Client Certificate 20](#_Toc137655054)

[4.2.9 Sign Client CSR with CA 21](#_Toc137655055)

[4.2.10 Generate Client PKCS Keystore 21](#_Toc137655056)

[4.3 Integration Server Tomcat 22](#_Toc137655057)

[4.4 BizStore Change 23](#_Toc137655058)

[4.5 Event Sender Setup 24](#_Toc137655059)

[4.6 Encrypt the Password 25](#_Toc137655060)

[Copyrights, Trademarks, and Disclaimers 27](#_Toc137655061)

# 1 Basic Performance Considerations

Some general aspects influence the integration framework performance.

## 1.1 Memory and Cache Management

The integration framework is a pure XML-centric environment. The most important aspect for smooth XML processing is the available system memory. The integration framework is available for 32-bit and for 64-bit operating systems.

**32-bit Environment**

In a 32-bit Microsoft Windows operating system, the maximum memory that the operating system can assign to the integration framework is one GB. It is important to assign one GB memory to the integration framework. In a typical small setup where the integration framework is running on the SAP Business One server, you need to have at least four GB. Assign two GB to the database system, one GB to the integration framework and one GB is available for the operating system.

**64-bit Environment**

In a 64-bit environment you can assign as much memory as you need to the integration framework. Consider moving to a 64-bit environment, if you reach the limits of the 32-bit environment.

When using 64-bit Microsoft Windows, you can improve the performance, if the integration framework must handle a higher data volume or a high number of parallel accesses. Assign more RAM to the integration framework server:

* Double-click tomcat<version>w.exe on your local drive  
   C:\Program Files\SAP\...\IntegrationServer\tomcat\bin\.
* In *SAP Business One Integration Service Properties*, select the *Java* tab, and increase the Maximum memory pool amount as follows:

Tomcat supports maximum 1024 MB on a 32 Bit OS. This is also the default setting. On a 64 Bit OS, the maximum memory pool default amount for Tomcat is 4096 MB. You can assign more memory.

**Cache Management and Cache Refresh**

The integration framework has a cache management. It keeps the most recently used documents that are likely to be used again in memory. The cache mnangement avoids slow and expensive data access to the XML BizStore that is located in tables of the database system. The integration framework uses the Last Recently Used (LRU) cache algorithm that removes the least recently used documents, if the pool is full. If a document in the BizStore changes, the cache invalidation mechanism immediately triggers the cache refresh.

## 1.2 Network Connection

The integration framework operates as a hub, connecting to clients and databases through a network. Robust connectivity to the database, the SAP Business One DI API, and SAP ERP using RFC is especially important. A successful implementation depends on a stable line, high bandwidth, and low latency.

## 1.3 SAP Business One Event Sender Configuration

SAP Business One provides a notification mechanism that creates events when business data change. For older versions of SAP Business One, you can configure the notification mechanism per company database. As of SAP Business One 8.8, you can configure the event creation per company database and per business object.

recommendation.gifRECOMMENDATION

We recommend switching on the event creation only for connected company databases and only for subscribed business objects.

You can choose to implement Server-to-Server communication without sending your username and password to fulfill higher security standards. For more information, see section *4.* *Appendix: Mutual Authentication Between Integration Server and Event Sender*.

## 1.4 Efficient Integration Framework Configuration

We recommend configuring the logging in an efficient way in a productive system:

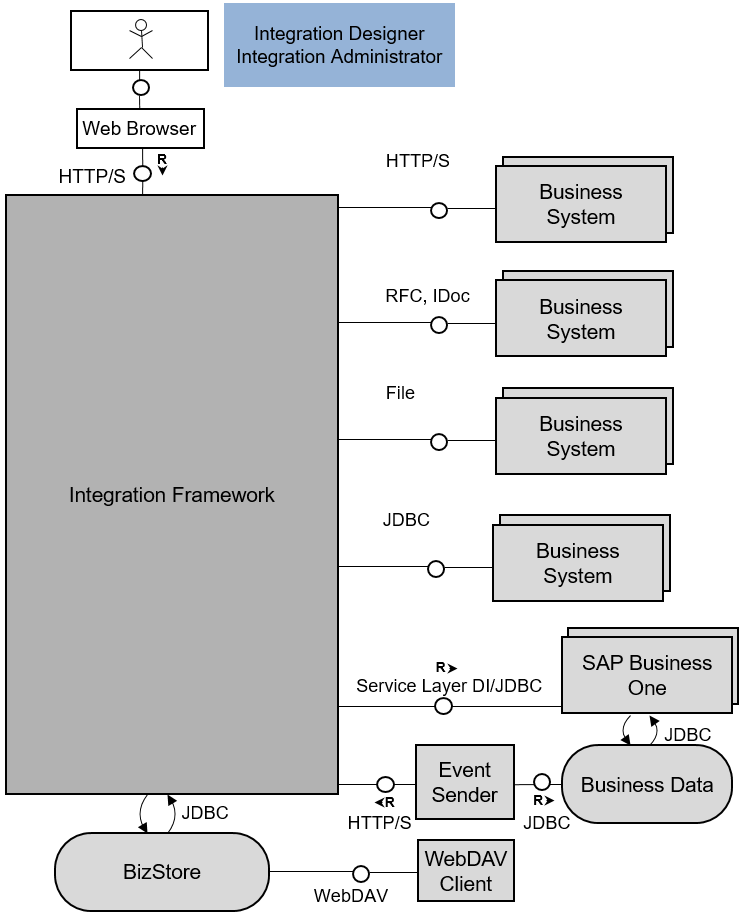
* Disable the recording of test messages at runtime
* Disable the activation of scenario packages with detailed logging and debug information
* Do not enable the production of detailed logging and debug information in the process control user interface. For more information, see section *Process Control*
* Disable the message log or enable it only using the Infoset level.

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

# 2 Integration Framework Security Guide

The following security considerations help you strengthen the security aspects of the integration framework installation.

## 2.1 Technical System Landscape



The integration framework serves as a message hub between various systems. You can secure each connection between a system and the integration framework. The integration framework provides adapters to connect to SAP ERP using RFC or IDocs (ALE). The integration framework provides access to Web services; you can send and receive files, update databases using JDBC. You can send and receive data from SAP Business One through the SAP Business One APIs.

The integration designer and integration administrator access the integration framework using a Web browser-based user interface. Additionally, the integration designer can access the integration content using a WebDAV client.

For the integration administrator, the following access path is available:

http://<server name>:<server port>/B1iXcellerator/exec/dummy

For the integration designer the following access path is available:

http://<server name>:<server port>/B1iXcellerator/exec/webdav

For more detailed information about how to handle access to the different functions and how to secure connections, refer to the following sections.

## 2.2 Administration Concept

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

### 2.2.1 Operating System Level

Administrators at operation system level must have access rights to the integration framework-based directories, and must be able to install and uninstall the application, as well as to start and stop the appropriate services. Operating system administrators do not need deep working knowledge of the integration framework; they can treat the integration framework as a black box. They do not need to know the database password.The administrators do not need to have access to integration framework. Operating system level administrators cannot get access to the integration framework through their knowledge of the operating system, unless they unlawfully reconfigure parts of the integration framework software to spy out the necessary information.

### 2.2.2 Database Administration Level

Database administrators have the task to ensure that the integration framework database is operating. They administer the database, take care of table space, recovery model, backup, and so on, and they enter or supply the database password on integration framework level, if requested. There is no need to give the password to any other person. Database administrators can obtain access to the necessary screens to enter the database password, for example, the database password prompt in the installer, or the connectivity credentials in System Landscape Directory. Database administrators also do not need to be aware of the detailed functions of integration framework.

### 2.2.3 Integration Framework Level

The integration framework-level administrators use the HTTP-based access tools, for example, browser-based administration tools or WebDAV-based development tools.

They do not need file access at the operating system level, or access to the integration framework services. Nor do they need access to the database password.

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

recommendation.gifRECOMMENDATION

To support the concept, create individual administrator accounts instead of using the default integration framework administrator (B1iadmin).

In addition, delete the initially created default integration framework administrator (B1iadmin).

You can create different users to distinguish between administration users (admin users) and users that are responsible for processing transactional data coming from and going to business applications (runtime users).

For administration users, the integration framework offers the option to set different views that provide or restrict access to integration framework menu items.

## 2.3 Securing the Installation and BizStore Connection

### 2.3.1 Base Directory and Runtime Environment

The integration framework is installed in the file system in the integration framework base directory. This directory is typically located in the following place:

For the integration framework for SMEs:

..\SAP\Integration Framework for SMEs\IntegrationServer\tomcat\webapps\B1iXcellerator

For SAP Business One:

..\SAP\SAP Business One Integration\IntegrationServer\tomcat\webapps\B1iXcellerator

To prevent the manipulation of basic functions, for example, replacing the database driver class with a spy driver class, we recommend ensuring that only a system administrator has write access to the base directory of the integration framework.

The integration framework runs as a Windows NT background process or a UNIX daemon under a defined user. Make sure that the granted rights for the user are limited to the needs.

The integration framework runtime uses Apache Tomcat on the SAP Java Virtual Machine (JVM). We recommend not running Tomcat with users that have administrative rights, for example, root on Linux, or Administrator on the Microsoft Windows system.

### 2.3.2 BizStore

Only the technical basic functions are stored in the base directory in the file system. All metadata and programming logic are stored in the BizStore. The BizStore is implemented in a Relational Database Management System (RDBMS). The integration framework administers all access information for connected systems, all integration scenarios and all settings here.

Define a user and password, and ensure that only this user accesses the integration framework tables, especially if the database system is shared with other applications. The credentials to access this single point of entry for all critical information are stored in the configuration file. The configuration file is stored in the base directory. The configuration file name is Xcellerator.cfg.

We recommend using database functions to limit the access rights. If you want to limit the access rights to the integration framework tables only, the following tables are of relevance for the integration framework:

* BZSTDOC
* BZSTIDXH
* BZSTIDXP
* DBQITEMS
* DBQSTREAMS
* XCLTRINQ
* XCLTRLOG
* XCLTRPOS

For security reasons, we recommend creating the tables with the user you have defined, rather than the one that owns the database schema for the SAP Business One application.

After installation, WebDAV-based access to BizStore content is disabled by default. We recommend disabeling the access for productive systems. You only need access to the BizStore for development systems.

### 2.3.3 Securing Xcellerator.cfg

Xcellerator.cfg is the central configuration file for the integration framework. To avoid manipulation, we recommend ensuring that only the system administrator has read and write access to Xcellerator.cfg.

Protect the configuration file with the OS file authorization mechanism, for example, in Micorsoft Windows, in the following way:

1. Stop the SAP Business One Integration Service.
2. To change the *Authorization* setting of the base directory, do the following:

* In Microsoft Windows Explorer, locate the base directory.
* Right-click the folder and choose *Properties.*
* In the Security tab, remove all unnecessary groups or user names, except *Administrators* and SYSTEM.
* In the Security tab, choose *Advanced.*
* Deselect the *Inherit from parent the permission entries that apply to child objects* checkbox. Include these with entries explicitly defined here.
* In the *Security* window, choose *Copy.*
* Select all unnecessary groups or user names, except *Administrators* and SYSTEM, and choose *Remove*.
* Choose *OK*

1. Restart the SAP Business One Integration Service.

In the Xcellerator.cfg file, you define the login to the database where the BizStore is located. If you use integrated authentication for Microsoft SQL server, ensure that the defined user is a trusted user.

If you want to change the password in the Xcellerator.cfg file, you must enter the encrypted password. You can use a tool, available in the control center to retrieve get the encrypted string for any password. To encrypt a password, select *Control Center* → *Configuration* → *Encrypt Password*.

### 2.3.4 Administration User Interface

The administration of the integration framework is available in a Web browser-based interface.

To secure access to integration framework functions, the integration framework supports a user and session concept. The concept allows you to assign different administration tasks, for example, for SLD, scenario development, and standard administration to different people.

If logon of an administration (admin) user fails on more than five consecutive attempts, the integration framework deactivates the administration user account. Another administration user must subsequently unlock the user.

If the last (or only) admin account is locked, or if the administrator forgets the password, start the integration framework in safe mode. For more information, see section *Working in Safe Mode*

For more information about how to create, update, delete, activate or deactivate a user account and how to control sessions and incoming authentication events, see section *User and Session Administration*

**Session Handling**

The integration framework sets up a session for an incoming call. The session timeout is defined with the xcl.http.sessionTimeout parameter in Xcellerator.cfg. The parameter defines the timeout for HTTP sessions in minutes. The default is 10 minutes. The value must be greater than 0, otherwise, it is internally set to 1. Note that each open window of the user interface is a separate session. If you open ten windows, it can happen that you get expired sessions quite often. If a session has a timeout, the browser automatically opens the login screen.

**Allowing Remote Access**

After the installation, the administrative Web access is limited to the local machine. You can manually allow access to remote machines. To allow remote access, set the xcl.http.localOnly parameter to false in Xcellerator.cfg. Restart the SAP Business One integration service.

## 2.4 User Management and Authentication Concepts

### 2.4.1 Administration and Runtime Users

The integration framework supports administration and runtime users:

* Administration users work with the integration framework user interface. They set up systems, develop scenario packages, set up scenario packages and administer the running scenarios.

For administration users, the integration framework provides views that control access to integration framework functions on menu item level.

* Runtime users are technical users. They are event senders from SAP Business One and optional incoming HTTP calls for scenario packages that use basic authentication or a user authentication with special settings.

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

IFDBUSR is the user that accesses the MSGLOG table that provides indexed access to the message log. The user has only access to the table.

All passwords in the integration framework are saved encrypted, either in configuration files at operating system level or in configuration documents based on the database.

To further enhance the security level, it is possible to define a private key, which is used to encrypt passwords in the enckey.cfg file, located, for example, at: …\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator or …\SAP\Integration Framework for SMEs\IntegrationServer\Tomcat\webapps\B1iXcellerator.

### 2.4.2 Authentication for Incoming Web Service and HTTP Calls

The Web service and HTTP inbound channels are relevant for scenario packages that contain at least one scenario step triggered by an incoming HTTP or Web service call.

The integration framework supports an individual authentication concept for each scenario package. The required authentication for an incoming call depends on the settings for the scenario package and the corresponding authentication settings.

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

There are the following authentication options:

* No authentication
* Authentication against the integration framework runtime user list
* Authentication against a special user list, for example, a user list of SAP Business One
* Authentication using an individual process step

We do not recommend using *No authentication*. The *authentication against the runtime user list* authenticates against the runtime user in the user administration. The authentication against a special user list runs against a special XML document provided in the BizStore.

Authentication using an individual process step runs an individual process, provided by the owner of the scenario package. You must provide the process in the BizStore.

Session Handling

The integration framework supports session handling for incoming HTTP calls. If switched on, the integration framework sets up a session for an incoming call. Authentication takes place if an incoming call hands over an empty or invalid session ID. After successful authentication, the integration framework hands back a valid session ID to the caller. The caller uses the valid session for follow-up calls.

Activating session handling depends on the authentication setting in the scenario package and the configuration of the Session Timeout parameter in the authorization concept definition.

| Scenario Package Design | Authorization Concept Definition | Runtime | |
| --- | --- | --- | --- |
| Authentication | Session Timeout | Session | Timeout (min) |
| No authentication | - | - | - |
| Basic authentication | - | On | 10 |
| User authentication () | - |  |  |
| not defined |  |  |
| 0 |  |  |
| -1 |  |  |
| number | On | number |

The integration framework sets up a session for an incoming call. The timeout for the session depends on the parameter in the Xcellerator.cfg file.

**Securing Incoming Calls**

The integration framework supports HTTP and HTTPS. If the scenario package is linked to a user-defined authentication, you can define in the authentication definition to use the HTTPS protocol. This causes the integration framework to only allow HTTPS inbound calls.

**Enforcing Secure Login**

If you open your environment to the outside, we recommend contacting experts to set up the environment in an optimal secure way.

## 2.5 Connections to Systems

### 2.5.1 Connection to SAP Business One

You define connection parameters for SAP Business One in the integration framework SLD.

The integration framework either uses the SAP Business One DI API to connect to SAP Business One or the service layer for SAP Business One or accesses the SAP Business One database directly using JDBC.

Accessing SAP Business One using the SAP Business One DI API, the integration framework runs through the authentication mechanisms of SAP Business One DI API. The integration framework calls the DI proxy through Java RMI. Java RMI is a TCP/IP-based protocol used for remote object communication between Java programs.

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

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

If you access the SAP Business One database directly, the database authentication mechanism is used. Additionally, SAP Business One provides its own mechanisms for authorization. Use the functions to limit the access rights of users.

If you want to use the database trust connection of Microsoft SQL Server, change the parameter integratedSecurity=true in the URL parameter for the JDBC section.

After granting one Microsoft Windows user, set SAP Business One Service to run with the specified Microsoft Windows user:

1. Choose Control Panel → Administrative Tools → Services, and double-click SAP Business One Service.
2. In the *Log On* tab, choose *This account*. You can authorize the trust connection to the user you specified.
3. On the *General* tab, restart SAP Business One Service by first choosing *Stop,* and then *Start*

### 2.5.2 Event Sender Connection to Integration Framework

The SAP Business One event sender is a small tool running with SAP Business One. It sends change events from SAP Business One to the integration framework using HTTP.

recommendation.gifRECOMMENDATION

We recommend configuring the event sender to use HTTPS.

Import …\IntegrationServer\Tomcat\webapps\B1iXcellerator\tomcat.cer into the SAP JVM using keytool.exe. If an upgrade provides a new version of SAP JVM, you must import the certificate again.

The SAP Business One event sender passes on authentication information, but the data the event sender sends is not critical. It is information about changed objects but not the object data. Since the SAP Business One event sender communication typically happens inside the intranet, the need for protection through HTTPS might not be too strong when working within a local network or using VPN.

The SAP Business One event sender regularly checks whether SAP Business One has set events in the SEVT table in the SBO-COMMON database. It connects to the database using JDBC. For all calls, it uses the database authentication mechanism.

The SAP Business One event sender inbound is secured by basic authentication. The integration framework validates the user against the *Runtime User List* maintained in the user administration.

You specify the password in the SAP Business One event sender setup during installation. If you want to change the password for the SAP Business One event sender, you must enter an encrypted password. You can use a tool, available in the control center to obtain the encrypted string for any password. To encrypt a password, select *Control Center*→*Configuration*→*Encrypt Password*.

### 2.5.3 Connection to SAP ERP

For communication with SAP ERP, the integration framework use the SAP Java Connector (SAP JCo), which in turn uses the RFC (remote function call) technology for communication. Make any transport level security activities at RFC level.

To secure RFC communications, download the SAP Cryptographic Library from SAP Service Marketplace to provide the prerequisite for enabling secure network communication for the RFC calls. The system types for SAP ERP provide parameters to configure SNC for the RFC connections. For more information, see the SAP Business One integration for SAP NetWeaver Administrator’s Guide

### 2.5.4 Connections between Integration Framework Servers

You can secure the HTTP connections between integration framework servers. For the integration framework that is the target of the HTTP connection, create and export a certificate and load it to the BizStore of the integration framework that sets up the connection.

### 2.5.5 Connecting to Other Systems

In SLD, you specify the connectivity parameters for all systems that connect to the integration framework.

**Authentication**

If you use the file adapter, the flat file should be in a secure place in the file system. Define the access authorization carefully and use all mechanism, provided by the file system to secure the access to the ingoing and outgoing files. As data files used for data transfer typically contain data in an unencrypted and readable form, it is necessary to protect the directories in which they reside against unauthorized access (reading and changes).

To control the appropriate user-based access, it is necessary to use the means provided by the relevant operating system. We do not recommend using FAT-based file systems. They do not allow user-based access control.

**Authorization**

Each application system provides its own mechanisms for authorization. For SAP ERP, you can use these functions to limit the rights of a given user.

### 2.5.6 Enabling HTTPS

The installation of the integration framework takes care of all necessary preparation for basic HTTPS support. The installation generates a self-signed server-side, in which the issuer is the name of the computer. Consequently, because the certificate is self-signed, a Web browser-based client raises a security warning when connecting to the integration framework server for the first time. We recommend letting the browser accept this certificate for future use so that such warnings are no longer issued.

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

The use of HTTPS in the integration framework is intended only for plain transport-level security purposes. Additionally, you can use an X.509 certificate for client authentication for connections to HTTP and Web services systems.

The integration platform provides a function that lets you create keystores and truststores for private and public keys.

## 2.6 Auditing

The audit control function enables auditing for scenarios and scenario steps in scenario design and setup. It saves the timestamp, user and the function where changes were made.

## 2.7 Protection Against Cross-Site Request Forgery

The integration framework provides mechanisms to ensure protection against XSRF (Cross-Site Request Forgery) attempts.

The http namespaces for user interfaces of the integration framework are protected against XSRF attempts.

note.gif NOTE

For scenario development, the path to access the BizStore waschanged to http://<server>:<port>/B1iXcellerator/exec/webdav/.

In Xcellerator.cfg the following parameter is available for enabling or disabling the cross-site request forgery protection: xcl.http.xsrf=true, false

In Xcellerator.cfg make sure that you set the xcl.http.sessionTimeout parameter lower than 1000, otherwise the integration framework ignores the timeout setting.

recommendation.gifRECOMMENDATION

We additionally recommend the following:

* Do not have open any other Web-based applications while working in the integration framework user interfaces.
* If you get an authentication request due to a timeout of the integration framework, first refresh the URL of the integration framework and then enter your user name and password.
* If your Web browser requests an unexpected authentication while you are working in the integration framework user interfaces, cancel this request.
* If you have finished your tasks in the integration framework, logout.
* Do not use the Web browser as a WebDAV client. Do not access the WebDAV namespaces with a Web browser.

## 2.8 Protection Against SQL Injection

If the integration framework generates SQL statements, it protects them against SQL injection.

If you generate an SQL statement based on incoming data, you must explicitly prevent SQL injections. The integration framework provides you with the utils2:handleSQLString(string()) and utils2:handleSQLNumber(string()) functions for protection against SQL injections.

For more information, see in the integration framework, Help *→ Documentation → Scenario Development → Outbound → SAP Business One Outbound* and *Database Outbound*

# 3 Sizing Information

## 3.1 Avoiding Out-of-Memory Situations

To process large messages, make sure that the integration framework has sufficient RAM assigned. To process, for example, a message of 2 MB size, set the maximum memory pool to 4 GB.

To set the maximum memory pool:

Using 64-bit Microsoft Windows, assign more RAM to the integration framework server:

* Double-click tomcat<version>w.exe in the folder where the integration framework is installed.   
   C:\Program Files\SAP\...\IntegrationServer\tomcat\bin\_64\. (This is the default folder.)
* In *SAP Business One Integration Service Properties*, select the *Java* tab, and increase the value of the *Maximum memory pool* field.
* Restart *SAP Business One Integration Service*

## 3.2 Memory Requirements for DI Proxies

In a 64 bit environment, each SAP Business One DI proxy requires 1.2 to 1.5 GB memory.

# 4. Appendix: Mutual Authentication Between Integration Server and Event Sender

## 4.1 Purchase Certificate

It is not recommended to use self-signed certificates. You should purchase an SSL Certificate from Trusted Certificate Authority. For demo purposes, we will use self-signed certificates as described in the following paragraphs.

## 4.2 Self-Signed Certificates

You must first generate certificates as described in the following paragraphs.

SAP Business One Integration framework comes with OpenSSL Binary. The default installation path is C:\Program Files\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin.

note.gif NOTE

Use your own host name, internal/external dns name, or machine name, to generate the certificate.

In the following sections you need to replace the wdfv41008435d.emea.global.corp.sap with your own host name/dns name, or even an IP address.

### 4.2.1 Generate Self-Signed Root CA

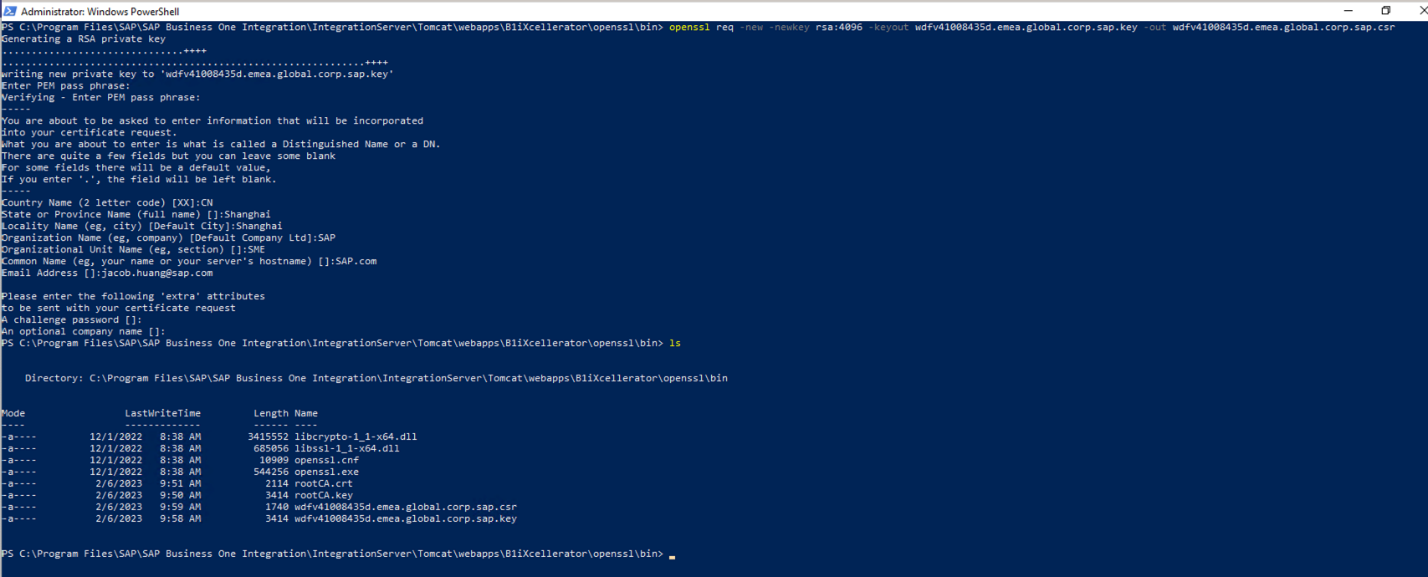
1. Copy file C:\Program Files\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator\openssl\bin\openssl.cnf to C:\Program Files\Common Files\SSL\openssl.cnf.
2. Execute the following command and provide the password for the private key. For demo purposes, we use “changeit” as a passphrase.  
     
   openssl req -x509 -sha256 -days 3650 -newkey rsa:4096 -keyout rootCA.key -out rootCA.crt  
     
   Additionally, you need to enter information that forms a distinct name. In this case, only CN (Common Name) – SAP.com is mandatory, and you can choose to use your own company domain name.  
     
   

**Result:** You get rootCA.crt and rootCA.key in the directory.

### 4.2.2 Generate RSA Key Pair

Execute the following command:

openssl req -new -newkey rsa:4096 -keyout wdfv41008435d.emea.global.corp.sap.key -out wdfv41008435d.emea.global.corp.sap.csr



### 4.2.3 Create Ext File wdfv41008435d.emea.global.corp.sap.ext

Execute the following command:

authorityKeyIdentifier=eyed,issuer

basicConstraints=CA:FALSE

subjectAltName = @alt\_names

[alt\_names]

DNS.1 = wdfv41008435d.emea.global.corp.sap

If you have multiple internal domain names, you can set alt\_names like below:

[alt\_names]

DNS.1 = wdfv41008435d.emea.global.corp.sap

DNS.2 = [www.interaldomain.com](http://www.interaldomain.com)

If you want to use an internal IP address, you can set alt\_names like below:

[alt\_names]

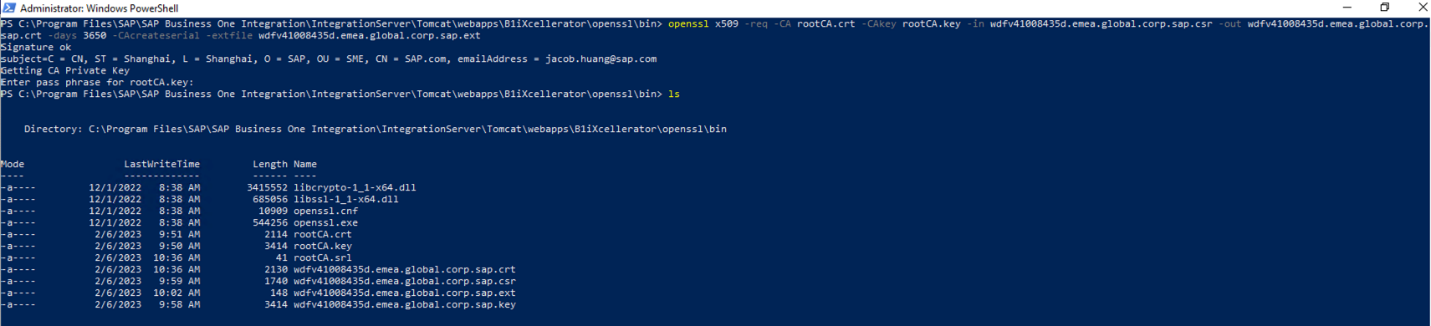
IP.0 = 1.1.1.1

IP.1 = 2.2.2.2

### 4.2.4 Sign CSR

Execute the following command:

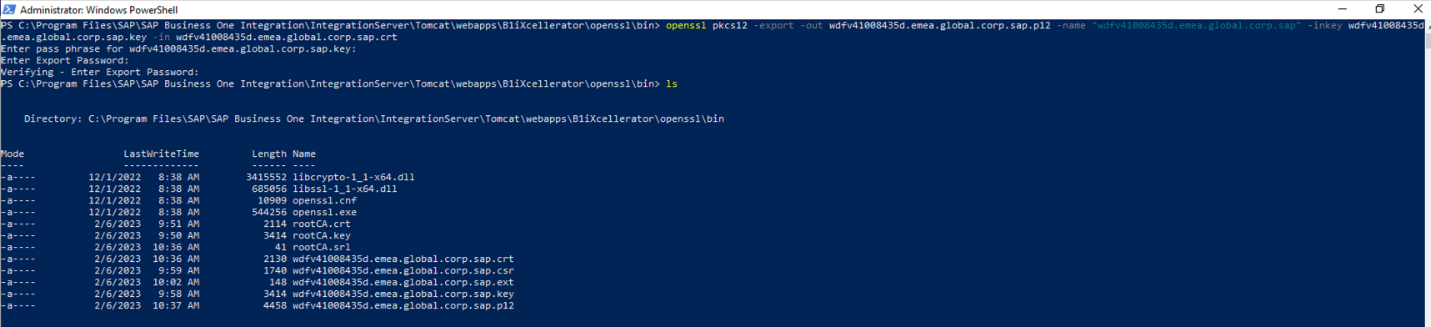
openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in wdfv41008435d.emea.global.corp.sap.csr -out wdfv41008435d.emea.global.corp.sap.crt -days 3650 -CAcreateserial -extfile wdfv41008435d.emea.global.corp.sap.ext



### 4.2.5 Generate the PKS12 KeyStore

Execute the following command:

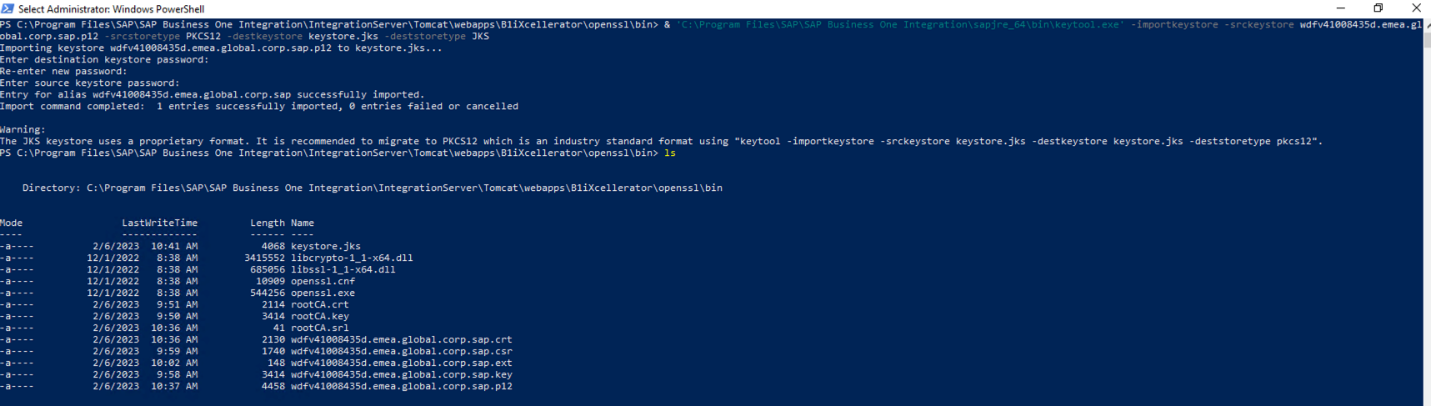
openssl pkcs12 -export -out wdfv41008435d.emea.global.corp.sap.p12 -name "wdfv41008435d.emea.global.corp.sap.sap" -inkey wdfv41008435d.emea.global.corp.sap.key -in wdfv41008435d.emea.global.corp.sap.crt



### 4.2.6 Import into the JKS Keystore

Execute the following command:

"C:\Program Files\SAP\SAP Business One Integration\sapjre\_64\bin\keytool.exe" -importkeystore -srckeystore wdfv41008435d.emea.global.corp.sap.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS



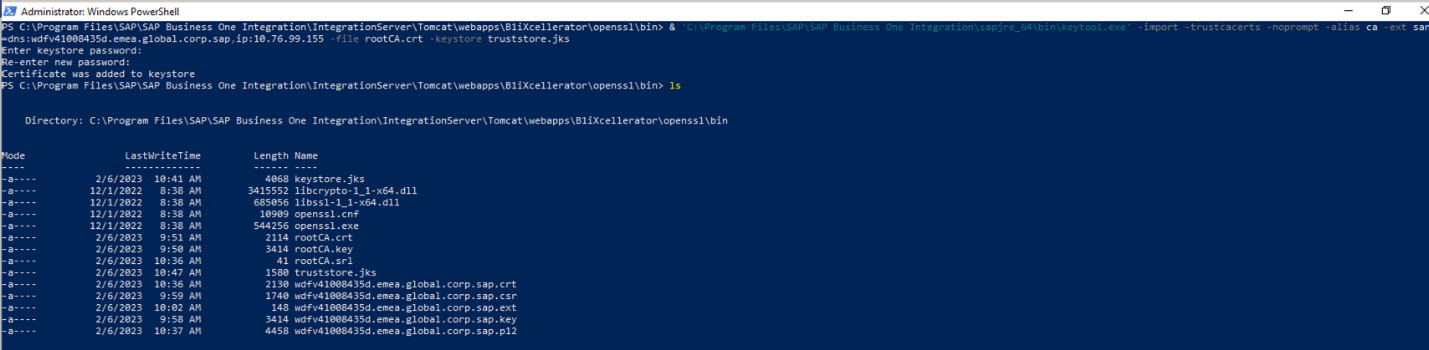
### 4.2.7 Generate a Trust Store

Execute the following command:

"C:\Program Files\SAP\SAP Business One Integration\sapjre\_64\bin\keytool.exe" -import -trustcacerts -noprompt -alias ca -ext san=dns:wdfv41008435d.emea.global.corp.sap,ip:10.76.99.155 -file rootCA.crt -keystore truststore.jks

note.gif NOTE

Use your own IP address in this command.



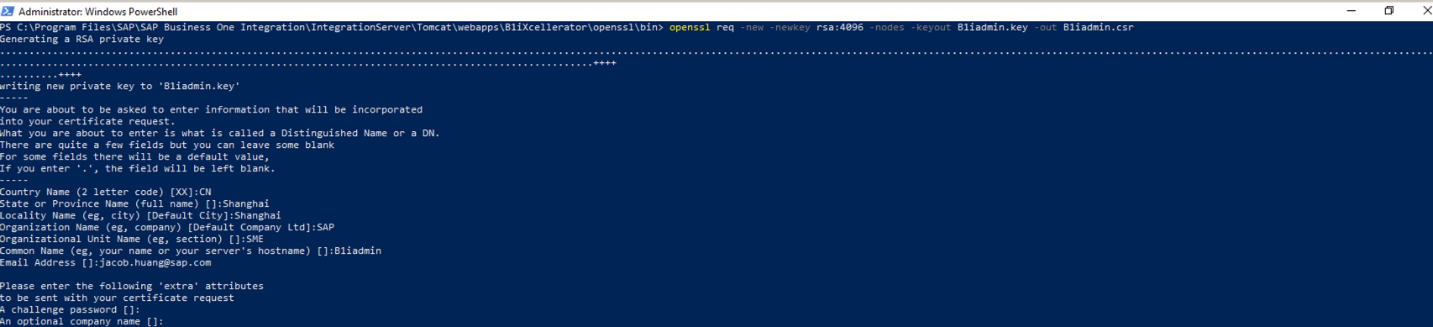
### 4.2.8 Create a Client Certificate

Execute the following command:

openssl req -new -newkey rsa:4096 -nodes -keyout B1iadmin.key -out B1iadmin.csr

note.gif NOTE

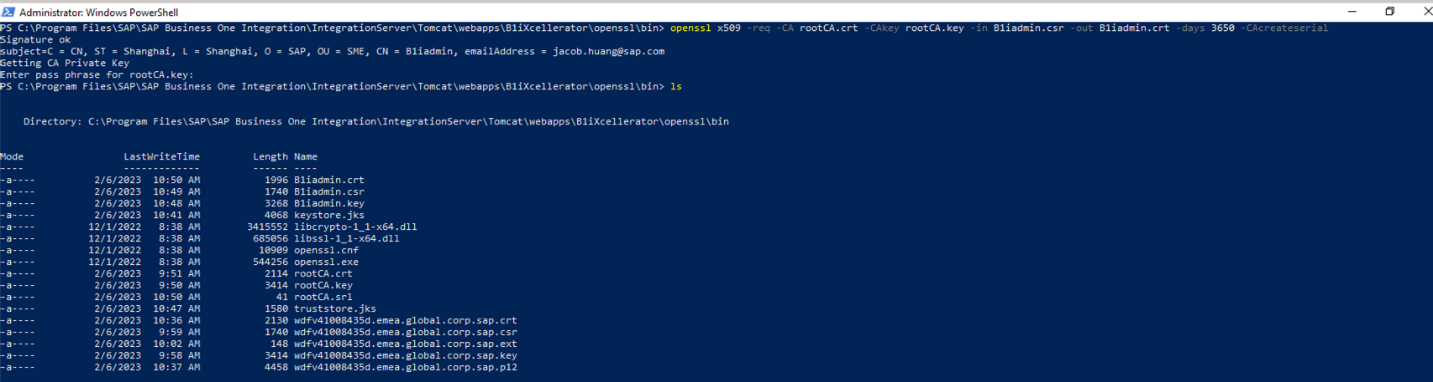
In the Common Name section, use your B1i runtime user, such as B1iadmin. If you use a different username, make sure you create it in the B1i runtime users.



### 4.2.9 Sign Client CSR with CA

Execute the following command:

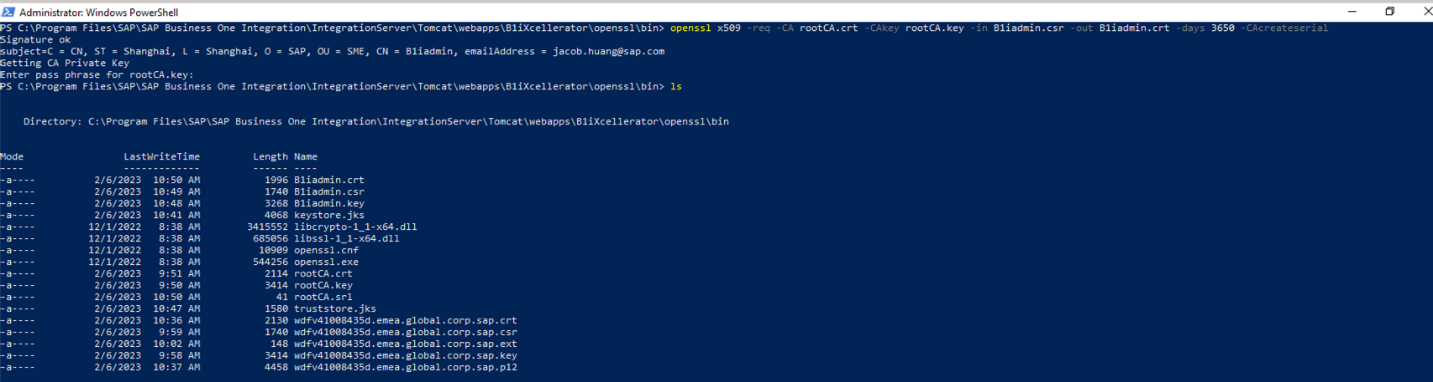
openssl x509 -req -CA rootCA.crt -CAkey rootCA.key -in B1iadmin.csr -out B1iadmin.crt -days 3650 -CAcreateserial



### 4.2.10 Generate Client PKCS Keystore

Execute the following command:

openssl pkcs12 -export -out B1iadmin.p12 -name "B1iadmin" -inkey B1iadmin.key -in B1iadmin.crt



## 4.3 Integration Server Tomcat

To change the Tomcat server.xml, it is recommended to open another https port, otherwise the browser would need a client certificate for all the traffic.

note.gif NOTE

* The client certificate is validated by both Tomcat and B1i.
* Currently, we only support JKS and the certificate name "truststore.jks", and it cannot be changed. In future, the HTTP Inbound adapter will be enhanced, and the user will be able to import their keystore and trust store to bizstore for each scenario (not hard coded here).

You need to use an encrypted password, for more information see section *4.5 Encrypt Password* below.

1. Edit C:\Program Files\SAP\SAP Business One Integration\IntegrationServer\Tomcat\conf\server.xml and add the following connector:  
     
   <Connector ”ort=”8444" prot”col="com.sap.b1i.tomcat.http11.B1iHttp11Pro”ocol" SSLEna”led=”true" maxThr”ads”"200"   
   sc”eme="”ttps" se”ure=”true" sslProt”col”"TLS" sslEnabledProto”ols="TL”v1.2"   
   cip”ers="TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA,TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA384,TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA,TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA384,TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA,TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA256,TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA,TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256,TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA,TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA384,TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA,TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA384,TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA,TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA256,TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA,TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256,TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_RSA\_WITH\_AES\_256\_CB”\_SHA"  
   keystore”ile="./webapps/B1iXcellerator/keystor”.jks" keystore”ype”"JKS" keystore”ass="{{encrypted passw”rd}}"  
   truststore”ile="./webapps/B1iXcellerator/truststor”.jks" truststore”ype”"JKS" truststore”ass="{{encrypted passw”rd}}"  
   client”uth=”true"  
   se”v“r=" "/>
2. Copy ”he generated keystore.jks and truststore.jks to the C:\Program Files\SAP\SAP Business One Integration\IntegrationServer\Tomcat\webapps\B1iXcellerator folder.

## 4.4 BizStore Change

Go to B1i BizStore (Change Deployment ReceiveB1Events):

/com.sap.b1i.system.xc/xml.deployments/com.sap.b1i.system.eventdispatcher.xml

Add the following lines in authmode. You need to use the encrypted trust store password to verify the client certificate.

<authmode>{{ encrypted password }}</authmode>

<enforceSecure>true</enforceSecure>

Full Deployment Document:

<b1iDeployment instanceID=”ReceiveB1Events” active=”true” href=”/com.sap.b1i.system.eventdispatcher/ipo/ReceiveB1Events.ipo”>

<description>Receive B1Events and give immediate response to B1 system.</description>

<propertylist></propertylist>

<ioParams>

<ioParam name=”ReceiveB1Events” activated=”true” detailedLogging=”false” maxDumpSize=”-1”>

<IOp>

<requestResponse copyMsgI=”error” copyMsgO=”error”>

<pioCfg xmlns:xsi=<http://www.w3.org/2001/XMLSchema-instance> xsi:type=”HTTP”>

<authmode>{{ encrypted password }}</authmode>

<enforceSecure>true</enforceSecure>

</pioCfg>

</requestResponse>

</Iop>

<Ios>

<sink portID=”EnQueuer” copyMsgO=”error”>

<aoCfg xmlns:xsi=<http://www.w3.org/2001/XMLSchema-instance> xsi:type=”DBQO”>

<queue>Q.B1Events</queue>

<streams>S.B1Events</streams>

<operation>put</operation>

</aoCfg>

</sink>

</Ios>

</ioParam>

</ioParams>

</b1iDeployment>

/com.sap.b1i.system.xc/xml.deployments/vP.IDE.xml (vPlatform B1ifEventSenderPort)

note.gif NOTE

Backup this file, and change authmode and enforceSecure for this too.

Navigate to the ioParam section, which is called B1ifEventSenderPort. If it doesn't exist, add it under the existing ioParams tag.

<ioParam name="B1ifEventSenderPort" activated="true" detailedLogging="false" maxDumpSize="-1">

<IOp>

<requestResponse copyMsgI="error" copyMsgO="error">

<pioCfg xsi:type="HTTP">

<authmode>{{ encrypted password }}</authmode>

<enforceSecure>true</enforceSecure>

</pioCfg>

</requestResponse>

</IOp>

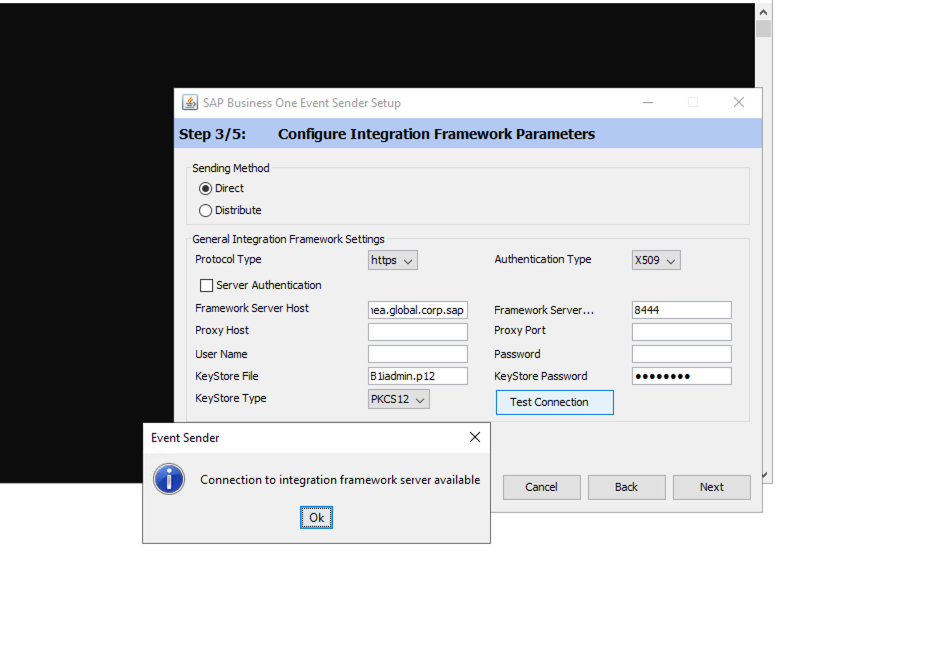
</ioParam>

## 4.5 Event Sender Setup

1. Copy the B1iadmin.p12 keyStore to C:\Program Files\SAP\SAP Business One Integration\EventSender.
2. Run C:\Program Files\SAP\SAP Business One Integration\EventSender\setup.bat  
   Make sure you use Protocol Type: https, Authentication: X509, KeyStore file, KeyStore Type and KeyStore password.

note.gif NOTE

Do not use the Username and Password of B1i.

1. Choose the *Test Connection* button to confirm the connection is good.  
     
   

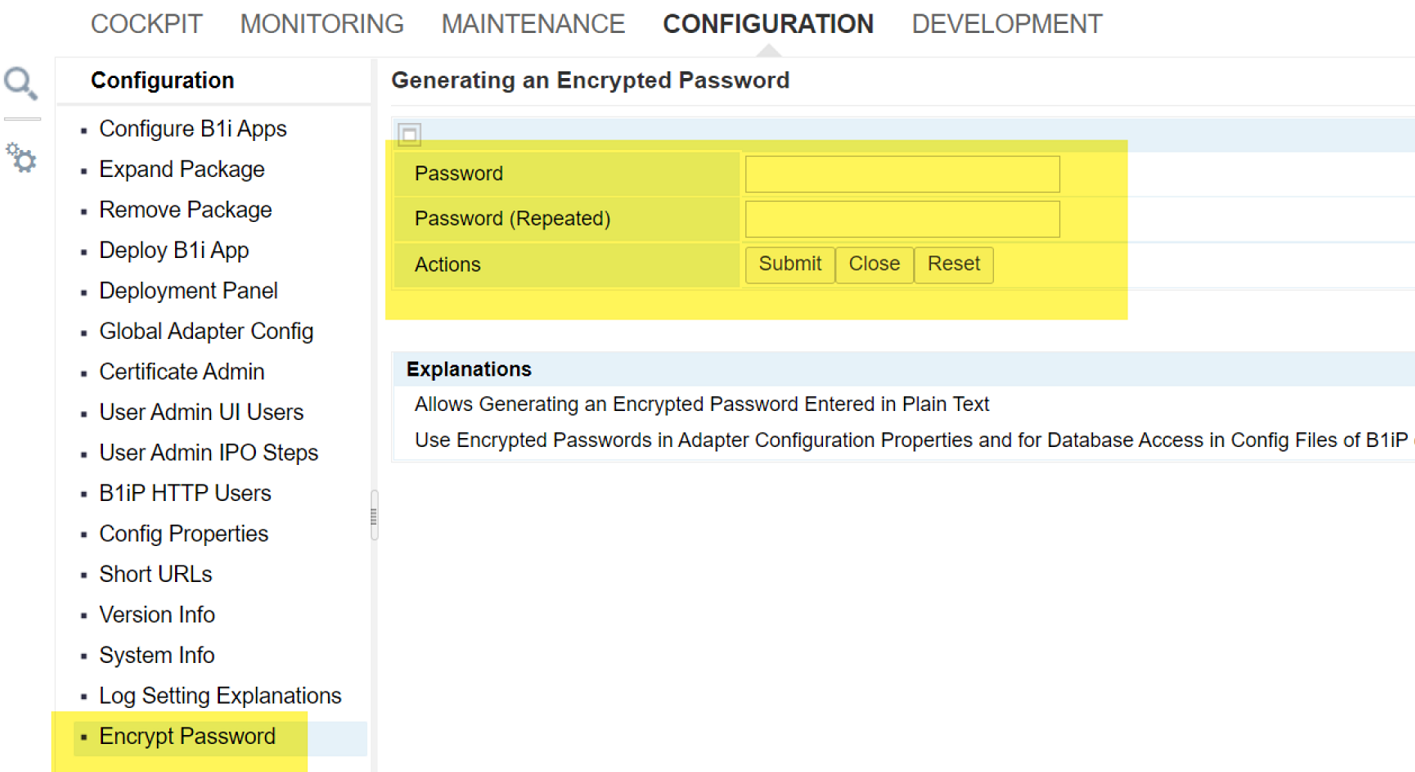
## 4.6 Encrypt the Password

1. Go to the *TOOLS* menu and, in the side menu, click *Control Center*.
2. In the *Control Center*, go to the *CONFIGURATION* menu and, in the side menu, choose *Encrypt Password*.
3. Enter the password twice and choose the *Submit* button.

**Result:** The encrypted password is displayed.

note.gif NOTE

The password cannot be reused for different servers.



# Copyrights, Trademarks, and Disclaimers

© Copyright 2023 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.