opentext™

ALM Solutions Connector

Software version: 6.2.2 and later

Configuration Guide

Document release date: June 2023

Send Us Feedback

Let us know how we can improve your experience with the Configuration Guide.

Send your email to: docteam@microfocus.com

Legal Notices

Contents

Overview

OpenText™ ALM Solutions Connector (ALM SC) is a flexible set of services and programs for Windows or UNIX/Linux platforms that enables you to deploy to IBM z/OS through OpenText ChangeMan ZMF.

ALM SC can be used to retrieve a list of change packages for selection from ChangeMan ZMF that are suitable for deployment, and then perform a number of potential actions using the default ChangeMan ZMF functionality. ALM SC uses web services and passes predefined credentials and selection information for ChangeMan ZMF applications and change packages of various types.

This guide covers the integration between Release Control and ALM Solutions Connector. Along with the Release Control help, it explains how to configure the integration with ChangeMan ZMF. ALM SC works with Release Control through the Release Control ChangeMan ZMF plugin.

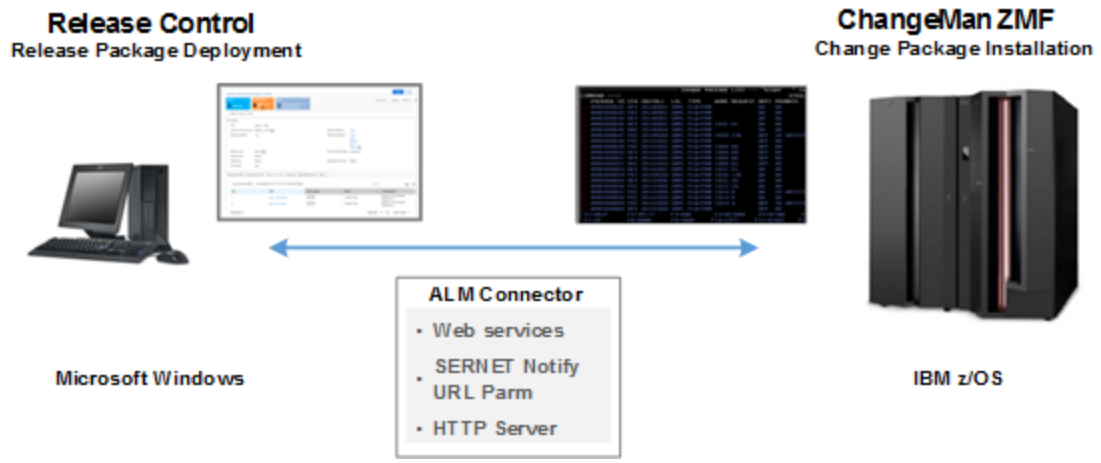
For supported configurations of Release Control, ChangeMan ZMF, and ALM Solutions Connector, see the ALM Solutions Connector Readme.

Note:
- To deploy to z/OS using ChangeMan ZMF with Deployment Automation, see the Deployment Automation help. ALM Solutions Connector works with Deployment Automation through the Deployment Automation ChangeMan ZMF plugin. For version support, see the Deployment Automation Integrations Matrix.
- **Custom integrations:** Use this guide to understand the integration and make necessary adjustments for your implementation.

ChangeMan ZMF communication configuration overview

To activate the integration, configure ChangeMan ZMF communication on the z/OS mainframe and on the integrating product's server.

The following image provides an overview of the Release Control / ChangeMan ZMF integration through ALM Solutions Connector:



Next steps:

- "Configure ALM Solutions Connector on the mainframe" on the next page
- "Configuration in ChangeMan ZMF" on page 10
- "Install and configure the ALM Solutions Connector services" on page 13

Configure ALM Solutions Connector on the mainframe

To configure the ALM Solutions Connector support on the z/OS mainframe:

- Configure a proxy user ID for each mainframe host, or LPAR, that the integrating product uses to log in to ChangeMan ZMF. See "Configure ChangeMan ZMF proxy user ID" below.
- Configure matching user IDs in TSO and SBM so that you can use Single Sign-On (SSO). See "Configure TSO user IDs and permissions" on the next page.

Configure ChangeMan ZMF proxy user ID

For each ChangeMan ZMF host server, or LPAR, you must set up a proxy user ID, or trusted user ID.

You specify these in the **zmf.properties** configuration file when you configure ChangeMan ZMF communication on the Release Control integrating server.

A proxy user ID grants you automatic access to ChangeMan ZMF through the integration without logging in. The proxy ChangeMan ZMF user ID connects to the host server on your behalf.

> **Example:** Suppose you want to freeze a release unit. The orchestration invoked for the Freeze function requires access to the ChangeMan ZMF host server. Your TSO user ID is on your SBM contact record and is associated with the proxy user ID. However, there is no password stored in your contact record.
>
> The proxy user ID, which does have a password, logs in to the ChangeMan ZMF host server on your behalf. The proxy user ID impersonates you, but it does not have access to other resources, such as performing ChangeMan ZMF functions. Your authority levels are in effect for the transaction.

The proxy user ID can be any SAF-defined user ID. It doesn't require any specific attributes or TSO access. This user ID must be given READ or higher access to the **trusted resource**. The trusted resource is a SAF resource, by default **SERENA.SERNET.AUTHUSR** in the **FACILITY** class. You can modify the resource and class by changing the names in the **SERLCSEC** module, which is delivered as source code with ChangeMan ZMF. This module is used for customizing security-related functions.

> **Note:** You don't need to alter **SERLCSEC** to support the integration, as it is already coded for the preceding resource name and class. Be sure to use the version of **SERLCSEC** that is appropriate to your version of ChangeMan ZMF, including customizations.
>
> The **trusted resource** is not related to the **RACF** user ID **TRUSTED** attribute.

Configure TSO user IDs and permissions

TSO IDs for accessing ChangeMan ZMF from Release Control must have permission to access every resource required by ChangeMan ZMF functions that Release Control uses.

You may need to configure matching user IDs in SBM and TSO depending on your Single Sign-On (SSO) settings:

- **If SSO is set to true in the Release Control ZMF plugin configuration**, configure matching user IDs in TSO and SBM for each Release Control user who runs the processes enabled by the Release Control ZMF plugin, such as configuring and deploying ZMF deployment tasks. ALM Solutions Connector uses the proxy user name and password specified in the `almsernet` service resource properties to access ChangeMan ZMF on behalf of the currently logged on SBM user.

  In this case, the user ID for logging in to SBM is the user ID that shows in the history as having carried out the ChangeMan ZMF actions.
- **If SSO is set to false in the Release Control ZMF plugin configuration**, ALM SC logs in to ChangeMan ZMF with the user name and password specified in the

plugin configuration, which are the actual TSO ID and password. You do not need to have matching user IDs.

In this case, the TSO user ID in the plugin configuration is the user ID that shows in the history as having carried out the ChangeMan ZMF actions, even if different SBM users performed the deployment tasks.

For details about setting Single Sign-On (SSO) and adding the user ID and password in the plugin configuration, see the ChangeMan ZMF Plugin section in the Release Control Plugin help.

Next steps:

- "Configuration in ChangeMan ZMF" on the next page

Configuration in ChangeMan ZMF

For ALM Solutions Connector to work, you need to configure ChangeMan ZMF:

- **Specify startup parameters**. For details, see "Add ChangeMan ZMF startup parameters" below and "Startup parameters example " on the next page.
- **Configure change packages**. For details, see "Configure change packages" on page 12.

Add ChangeMan ZMF startup parameters

To enable access to ALM Solutions Connector services, update the ChangeMan ZMF server with required startup parameters. These parameters are keyword options used with the SERNET started task.

You can pass the parameters to SERNET in different ways. For details on setting SERNET parameters, see the ChangeMan ZMF help.

To set the startup parameters:

1. Add the **CMN=(,XXXX)** parameter to the ChangeMan ZMF startup, where **XXXX** is the SERNET TCP/IP port that processes SERNET requests.
2. Add the SERNET **NTFYURL** parameter. This parameter is required for notifying your integration when an ALF event is emitted from ChangeMan ZMF, which indicates that ChangeMan ZMF has completed a requested task. Specify the parameter as follows:

   ```
   NTFYURL='<connectorHostName>:<port>/almzmfalf/services/ZMFALFEve
   ntRouter'
   ```

   where:

   - **<connectorHostName>** is the server name where your ALM SC services are installed.
   - **<port>** is the port number for ALM SC server.

> **Caution:** The **NTFYURL** parameter is case-sensitive. Enter the non-variable text exactly as displayed, and make sure to include single quotation marks around the variable string.

3. To enable the changes, restart ChangeMan ZMF. Then verify that the `CMN` port has been started in the SERPRINT listing data set.

Startup parameters example

The following example demonstrates the configuration of the ChangeMan ZMF startup parameters:

```
*******************************************************************
****
*                      MY SERNET MODULE
*                 SUBSYSTEM ID 'A' (ALL SITE)
* Please only activate (1)EventRouter at a time..Comment out the
* ones not in use. SERNET can only handle EventRouter.03/19/09 - JN

*******************************************************************
****
STAX=YES                          /* DO NOT DISCONNECT ISPF
APPLICATION
ESTAE=NO                          /* ESTAE RECOVERY
CMN=(,5314)                       /* CHANGE MAN TCP/IP PORT NUMBER
SUBSYS=I                          /* CHANGE MAN SUBSYS ID
SDNOTIFY=H8                       /* WATCH-DOG TIMER
EX003=N                           /* SERJES exit for security
AUTOMESSENGER=NOTIFY              /* ZDD, RLC notify
*TRACE=(SER,1,3)
*TRACE=(CMN,1,3)
TCPIP=TCPIP
XML=YES
XCH=6124,XCHMSG=6177              /* ZDD, RLC
NTFYURL='connectorHostName:8080/almzmfalf/services/ZMFALFEventRoute
r'
```

> **Caution:** If your site is a DP site, you must set the same hostname and port in the **NTFYURL** parameter specified for the DP site and the P site. Otherwise, the P site continues to wake up looking for work and fill up the **JESMSGLG** (JES message log).

For details on passing parameters to SERNET, see the section about passing parameters to SERNET in the ChangeMan ZMF Installation Guide.

Configure change packages

Change packages and their related ChangeMan ZMF entities are accessed through the integration.

As part of your ongoing administration and use of ChangeMan ZMF, you need to configure the following:

- Applications
- Sites
- Change packages
- Approver lists
- Promotion levels

For details, see the ChangeMan ZMF help.

Install and configure the ALM Solutions Connector services

To set up ALM Solutions Connector, install and configure the ALM Solutions Connector services:

1. Install a supported version of Common Tomcat.
2. Install the services provided with ALM Solutions Connector.
3. Configure ALF properties to connect distributed products to ChangeMan ZMF on the mainframe. This functionality is implemented through the **almzmfalf** services.
4. Configure the login details to enable a proxy user login on the mainframe on behalf of the SBM user. This functionality is implemented on the distributed side through HTTP Server (**almsernet** services), on the mainframe side through the proxy user ID and individual TSO IDs, and through SBM using Single Sign-On (SSO).

To install and configure the ALM Solutions Connector services, see the following topics:

- "Install Common Tomcat" on the next page
- "Install the ALM Solutions Connector services" on page 15
- "Configure ALF properties" on page 16
- "Configure the login for SSO" on page 18
- "Configure the default login for ZMF services" on page 22
- "Configure one-way SSL" on page 24
- "Configure two-way SSL" on page 25
- "Enable SSL on ChangeMan ZMF" on page 28

Install Common Tomcat

The ChangeMan ZMF plugin runs under OpenText Common Tomcat, which is supplied as part of OpenText Common Tools.

Required Common Tools versions:

ALM SC 6.2.5 and later	• Common Tomcat 9.0 • Java Runtime Environment 11.0
ALM SC 6.2.2–6.2.4	• Common Tomcat 8.5 • Java Runtime Environment 8.0

Default installation directories:

ALM SC 6.3.1 and later	OpenText Common Tomcat: **C:\Program Files\OpenText\common\tomcat\<version>**
	OpenText Common JRE: **C:\Program Files\OpenText\common\jre\<version>**
ALM SC 6.3.0.1 and earlier	Micro Focus Common Tomcat: **C:\Program Files\Micro Focus\common\tomcat\<version>**
	Micro Focus Common JRE: **C:\Program Files\Micro Focus\common\jre\<version>**

To install Common Tomcat:

1. Download the Common Tools installer from the Software Licenses and Downloads (SLD) portal. Make sure the Common Tools version is compatible with your version of ALM Solutions Connector.
2. Run the installer.

When the installation is complete, Common Tomcat is ready to host the ALM Solutions Connector services.

Next, install the ALM Solutions Connector services.

Install the ALM Solutions Connector services

To install the ALM Solutions Connector services:

1. (Optional) If you don't have Common Tomcat, download and install it as described in the previous section.
2. Download the ALM Solutions Connector files from the Software Licenses and Downloads (SLD) portal.
3. Extract the following **war** files from the installation package:
   - **almzmfalf.war**
   - **almsernet.war**
   - **almzmf.war**
   - **zmfws.war**

   > **ALM Solutions Connector 6.2.2 and earlier:** The **zmfws** services were named the **almzmfws** services.

4. Copy the **war** files to the Common Tomcat **<tomcat-install-dir>\webapps** directory.
5. Restart Common Tomcat. When running, the server automatically unpacks and deploys the **war** files.

After installing the ALM Solutions Connector services, configure resource properties for the following services:

- **almzmfalf**

  For details, see "Configure ALF properties" on the next page.
- **almsernet**

For details, see "Configure the login for SSO" on page 18.

- **almzmf**

  For details, see "Configure the default login for ZMF services" on page 22.

> **Note:** Although the **zmfws** services need no additional configuration, they are used when deployment tasks run.

The host and port information for ChangeMan ZMF as well as the URL for ALM Solutions Connector are specified in the ZMF plugin configuration. You can define multiple plugin configurations that point to different ChangeMan ZMF systems and ALM Solutions Connector configurations.

Configure ALF properties

To use the integration, you must configure the ChangeMan ZMF integration ALF properties.

To configure the ALF properties:

1. Edit the **zmfalf_resource.properties** file in your ALM services installation. By default, this file is in the Common Tomcat **WEB-INF\conf** directory, for example:

   <tomcat-install-dir>\webapps\almzmfalf\WEB-INF\conf\zmfalf_resource.properties

2. Specify the following properties:

Property	Description
SBM_ALF_EVENTMANAGER URL	The URL that points to the SBM ALF event manager, for example: **http://SBMserver:8085/eventmanager/services/ALFEventManager**
SBM_USERID	The user ID for the SBM ALF event manager (SBM application environment user ID).

Property	Description
SBM_PASSWORD	The password for the user ID.
SBM_VERSION	The SBM version. This is informational only.
RLC_ NOTIFICATION_ URL	The URL that points to the Release Control services that are waiting for a notification on whether a task has completed or failed, for example: **http://SBMserver:8085/rlc/notification/zmf** **Note:** In a multiple-machine SBM configuration, this URL should point to the Release Control server where SBM common services are running.

Here's an example of the ALF properties:

```
# Property resource bundle file for Axis2 ZMF Service
# Used to configure Axis2 ZMF Service system properties.
# SBM_ALF_
EVENTMANAGERURL=http://SBMhostname:8085/eventmanager/services/AL
FEventManager

# The SBM userid must have access to the appropriate SBM
projects/tables and it
must also have access to ZMF applications controlled by RLM.
SBM_USERID = admin
SBM_PASSWORD = admin
SBM_VERSION = 11.1

RLC_NOTIFICATION_
URL=http://RLChostname:8085/rlc/notification/zmf
```

3. Restart Common Tomcat.

> **Tip:** If you are configuring properties for other services, wait to restart until you have configured them all.

After you have validated the configuration, encrypt the credentials in the resource properties file by running the provided encryption script, **encrypt.cmd**.

Run the version of the encryption script located in the same directory as the file with the credentials you want to encrypt, for example:

<tomcat-install-dir>\webapps\almzmfalf\WEB-INF\conf\encrypt.cmd

> **Note:** Because this is a Java script, **java.exe** must be resolved in your path to run the script.
> For example, **JAVA_HOME** can be set in system variables, and the Java path, such as **C:\Program Files\OpenText\common\jre\<version>\bin**, can be set in the system path. You can open a command prompt and navigate to the Java path, or modify the script file to have the full path.

Configure the login for SSO

If you set up your Release Control ZMF plugin configurations to use SSO, you must configure the proxy login for the HTTP Server in the **almsernet** service properties.

For details, see the following documentation:

- To configure and use SSO with the Release Control ZMF plugin, see the Release Control Plugin help.
- To ensure secure login and to enable SSO, the plugin uses the SBM security token together with the Proxy ID and TSO IDs configured on the mainframe. See "Configure ChangeMan ZMF proxy user ID" on page 7 and "Configure TSO user IDs and permissions" on page 8.

To configure the almsernet properties:

1. Edit the **sernet_resource.properties** file in your ALM Solutions Connector services installation. By default, this file is in the Common Tomcat **WEB-INF** directory, for example:

   <tomcat-install-dir>\webapps\almsernet\WEB-INF\sernet_resource.properties

2. Specify the following properties for accessing SERNET and ChangeMan ZMF:

Property	Description
DEFAULT_HOST_USE_SSL = false	If ChangeMan ZMF is configured to use SSL, set this option to **true**. For details, see "Enable SSL on ChangeMan ZMF" on page 28.
DEFAULT_HOST_ADDRESS	The host name or IP address for the ChangeMan ZMF host (LPAR) to use as the default. For the Release Control ZMF plugin, you can find this information in the plugin configuration.
DEFAULT_HOST_PORTID	The port number for the default ChangeMan ZMF host. For the Release Control ZMF plugin, you can find this information in the plugin configuration.
DEFAULT_HOST_PROXYID	The proxy ID for the default mainframe host. If this property is set up correctly, the plugin uses the SBM security token and login on behalf of the user ID represented by the security token using the given proxy ID. The value of this property is case-sensitive.
DEFAULT_HOST_PROXYID_PSWD	The password for the proxy ID. The value of this property is case-sensitive.
ZMF_HOST_VERSION	The version of ChangeMan ZMF for which this configuration was set up. This is informational only.
ALM_CONNECTOR_VERSION	The version of ALM Solutions Connector for which this configuration was set up. This is informational only.
USE_SSO_USER	This property enables you to use the ZMF View widget in Release Control when SSO is disabled. By default, it is set to **true**. If you are not using SSO in Release Control for ZMF plugin configuration, set the property to **false**. **Note:** Do not use the **$HOST_PROXYID** and **$HOST_PROXYID_PSWD** variables. To use the ZMF View widget with SSO disabled, provide a valid ZMF user and password.

For example:

```
# Property resource bundle file for the ALMSERNET
#
TRACE = NO
DEFAULT_POUND = #
DEFAULT_HOST_ADDRESS = $HOST_ADDRESS
DEFAULT_HOST_PORTID = $HOST_PORTID
DEFAULT_HOST_USE_SSL = false
DEFAULT_USER = IBMUSER
DEFAULT_MSGLOG_PATH = /u/sernet/serservd
DEFAULT_HOST_PROXYID = $HOST_PROXYID
DEFAULT_HOST_PROXYID_PSWD = $HOST_PROXYID_PSWD
USE_SSO_USER = true
ZMF_HOST_VERSION = ZMF 8.2
ALM_CONNECTOR_VERSION = ALM Connector 6.3
```

3. **ALM Solutions Connector 6.3.0.1 and later:** To enable the ZMF View widget in Release Control to display information from multiple ChangeMan ZMF hosts, add the following properties for each host:

Property	Description
<CUSTOM_ID>_ HOST_ADDRESS	The host name or IP address for the ChangeMan ZMF host, for example: **SERVER1_HOST_ADDRESS = myZMFhost.com**
<CUSTOM_ID>_ HOST_PORTID	The port number for the ChangeMan ZMF host.
<CUSTOM_ID>_ HOST_PROXYID	The proxy ID for the ChangeMan ZMF host. If this property is set up correctly, the plugin uses the SBM security token and login on behalf of the user ID represented by the security token using the given proxy ID. **Caution:** The value of this property is case-sensitive.
<CUSTOM_ID>_ HOST_PROXYID_ PSWD	The password for the proxy ID. **Caution:** The value of this property is case-sensitive.

> **Note: <CUSTOM_ID>** cannot contain spaces, equals signs (**=**), and colons (**:**).

You can have different ChangeMan ZMF hosts with the same user credentials and port number.

For example:

```
SERVER1_HOST_ADDRESS = 000.000.000.001
SERVER1_HOST_PORTID = <port_1>
SERVER1_HOST_PROXYID = <ZMF_proxy_ID_1>
SERVER1_HOST_PROXYID_PSWD = <ZMF_proxy_password_1>
SERVER2_HOST_ADDRESS = 000.000.000.002
SERVER2_HOST_PORTID = <port_2>
SERVER2_HOST_PROXYID = <ZMF_proxy_ID_2>
SERVER2_HOST_PROXYID_PSWD = <ZMF_proxy_password_2>
SERVER3_HOST_ADDRESS = myZMFhost.com
SERVER3_HOST_PORTID = <port_2>
SERVER3_HOST_PROXYID = <ZMF_proxy_ID_2>
SERVER3_HOST_PROXYID_PSWD = <ZMF_proxy_password_2>
```

When attempting to get the details of a change package, the widget compares the host and port values in the **sernet_resource.properties** file against those in the Release Control Deployment Unit properties. If the widget finds a matching host and port combination, it uses these credentials. If no host and port combinations match, the default host name and port number are used.

4. Restart Common Tomcat.

> **Tip:** If you are configuring properties for other services, wait to restart until you have configured them all.

After you have validated the configuration, encrypt the credentials in the resource properties file by running the provided encryption script, **encrypt.cmd**.

Run the version of the encryption script located in the same directory as the file with the credentials you want to encrypt, for example:

<tomcat-install-dir>\webapps\almsernet\WEB-INF\encrypt.cmd

> **Note:** Because this is a Java script, **java.exe** must be resolved in your path to run the script.
> For example, **JAVA_HOME** can be set in system variables, and the Java path, such as
> **C:\Program Files\OpenText\common\jre\<version>\bin**, can be set in the system path. You can open a command prompt and navigate to the Java path, or modify the script file to have the full path.

Configure the default login for ZMF services

If you use the **almzmf** services resource properties in your implementation, you need to configure them.

These properties are meant to be overridden by Release Control **almsernet** properties. But they are used if the Release Control **almsernet** properties do not include the proxy connection details. These are also used for a direct integration through SBM.

To ensure secure login and enable SSO, the plugin uses the SBM security token together with the Proxy ID and TSO IDs configured on the mainframe. See "Configure ChangeMan ZMF proxy user ID" on page 7 and "Configure TSO user IDs and permissions" on page 8.

To configure the almzmf properties:

1. Edit the **zmf_resource.properties** file in your ALM Solutions Connector services installation. By default, this file is in the Common Tomcat **WEB-INF\conf** directory, for example:

   <tomcat-install-dir>\webapps\almzmf\WEB-INF\conf

2. Specify the following properties for accessing ChangeMan ZMF through the ZMF services.

Property	Description
DEFAULT_HOST_ ADDRESS	The host name or address for the ChangeMan ZMF host.
DEFAULT_HOST_ PORTID	The port number for the ChangeMan ZMF host.
DEFAULT_HOST_ PROXYID	The proxy ID for the mainframe host. If this property is set up correctly, the plugin uses the SBM security token and login on behalf of the user ID represented by the security token using the given proxy ID.
DEFAULT_HOST_ PROXYID_PSWD	The password for the proxy ID.
ZMF_HOST_ VERSION	The version of ChangeMan ZMF for which this configuration is set up. This is informational only.

Here is an example of the **almzmf** properties:

```
DEFAULT_HOST_ADDRESS = myZMFhost.com
DEFAULT_HOST_PORTID = 3434
DEFAULT_HOST_PROXYID = <ZMF_proxy_ID>
DEFAULT_HOST_PROXYID_PSWD = <ZMF_proxy_password>
ZMF_HOST_VERSION = ZMF 8.2
ALM_CONNECTOR_VERSION = ALM Connector 6.3
```

Caution: The **DEFAULT_HOST_PROXYID** and **DEFAULT_HOST_ PROXYID_PSWD** properties are case-sensitive.

3. Restart Common Tomcat.

Tip: If you are configuring properties for other services, wait to restart until you have configured them all.

After you have validated the configuration, encrypt the credentials in the resource properties file by running the provided encryption script, **encrypt.cmd**.

Run the version of the encryption script located in the same directory as the file with the credentials you want to encrypt, for example:

<tomcat-install-dir>\webapps\almzmf\WEB-INF\conf\encrypt.cmd

> **Note:** Because this is a Java script, **java.exe** must be resolved in your path to run the script.
> For example, **JAVA_HOME** can be set in system variables, and the Java path, such as
> **C:\Program Files\OpenText\common\jre\<version>\bin**, can be set in the system path. You can open a command prompt and navigate to the Java path, or modify the script file to have the full path.

Configure one-way SSL

This section explains how to configure one-way SSL for communication between Release Control (SBM) and ALM Solutions Connector.

The following ports are default for one-way SSL:

- **Port 8243** for connecting to SBM services.
- **Port 8443** for connecting to ALM Solutions Connector services.

To configure one-way SSL:

1. Obtain a Certificate Authority (CA) root certificate and generated keypair certificates for the SBM hostname and the ALM Solutions Connector hostname, signed by the CA root certificate. SBM should be configured to use one-way SSL with these certificates. See the SBM Configurator Help.
2. Configure the Common Tomcat server that serves ALM Solutions Connector to use one-way SSL. Open the **server.xml** file in the Common Tomcat **<tomcat-install-dir>\conf** directory and edit the settings in **server.xml**:
   - Use port 8443.
   - Provide a valid path and password to the keystore/truststore file.
   - Set **clientAuth** to **false** (to indicate one-way SSL).

   Here is an example of the server settings:

   ```
   <Connector port="8443" SSLEnabled="true"
   scheme="https" secure="true" sslProtocol="TLS"
   ```

```
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"
maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100"
keystoreFile="conf/sample-ssl.jks" keystorePass="serena"
keyAlias="connectorHostName"
truststoreFile="conf/sample-ssl.jks" truststorePass="serena"
clientAuth="false" />
```

3. Import the CA root certificate and key pair for the ALM Solutions Connector hostname into your **.jks** file and into the **cacerts** file in the Common JRE **security** directory, for example:

   <java-install-dir>\bin\lib\security

   The default password is **changeit**.

4. Edit the SBM links in the **zmfalf_resource.properties** file in the Common Tomcat **WEB-INF\conf** directory, for example:

   <tomcat-install-dir>\webapps\almzmfalf\WEB-INF\conf\zmfalf_resource.properties

   Change them to receive ALF Events on the secure SBM port, for example:

   https://sbmhostname:8243

5. Restart the Common Tomcat service to apply the changes.
6. On the Release Control Providers administrator page, change the link in the **Mainframe Connector** field to use the secure port, for example:

   https://connectorHostName:8443

Configure two-way SSL

This section explains how to configure two-way SSL, or mutual authentication, for communication between Release Control (SBM) and ALM Solutions Connector.

The following ports are default for two-way SSL:

- **Port 8443** for connecting to SBM services

- **Port 8543** for connecting to ALM Solutions Connector services

To configure two-way SSL:

1. Obtain a Certificate Authority (CA) root certificate and generated keypair certificates for the SBM hostname and the ALM Solutions Connector hostname, signed by the CA root certificate. SBM should be configured to use two-way SSL with these certificates. See the SBM Configurator Help.
2. Configure the Common Tomcat server that serves ALM Solutions Connector to use two-way SSL. Open the the **server.xml** file in the Common Tomcat **<tomcat-install-dir>\conf** directory and edit the settings in **server.xml**:
   - Use port 8543.
   - Provide a valid path and password to the keystore/truststore file.
   - Set **clientAuth** to **true** (to indicate two-way SSL).

   Here is an example of the server settings:

   ```
   <Connector port="8543" SSLEnabled="true"
   scheme="https" secure="true" sslProtocol="TLS"
   sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"
   maxHttpHeaderSize="8192"
   maxThreads="150" minSpareThreads="25"
   enableLookups="false" disableUploadTimeout="true"
   acceptCount="100"
   keystoreFile="conf/sample-ssl.jks" keystorePass="serena"
   keyAlias="connectorHostName"
   truststoreFile="conf/sample-ssl.jks" truststorePass="serena"
   clientAuth="true" />
   ```

3. Import the CA root certificate and keypair for the ALM Solutions Connector hostname into your **.jks** file and into the **cacerts** file in the Common JRE **security** directory, for example:

   <java-install-dir>\bin\lib\security

   The default password is **changeit**.
4. Edit the SBM links in the **zmfalf_resource.properties** file in the Common Tomcat **WEB-INF\conf** directory, for example:

<tomcat-install-dir>\webapps\almzmfalf\WEB-INF\conf\zmfalf_resource.properties

Change them to receive ALF Events on the secure SBM port, for example: **https://sbmhostname:8443**.

5. Change the Common Tomcat service to run with parameters.
   a. Stop the Common Tomcat service.
   b. Open a command prompt.
   c. In the command window, change location to the Common Tomcat **<tomcat-install-dir>\bin** directory.
   d. Run the following command:

ALM SC 6.3.1	`tomcat9w.exe //ES//OpenTextTomcat`
ALM SC 6.2.5–6.3.0.1	`tomcat9w.exe //ES//MicroFocusTomcat`
ALM SC 6.2.4 and earlier	`tomcat8w.exe //ES//MicroFocusTomcat`

   e. In the resulting window, in the **Java** tab in **Java Options**, add your **keystore** and **truststore** parameters, for example:

```
-Djavax.net.ssl.keyStoreType=JKS
-Djavax.net.ssl.keyStore=C:\Program Files
(x86)\OpenText\common\tomcat\9.0\conf\sample-ssl.jks
-Djavax.net.ssl.keyStorePassword=serena
-Djavax.net.ssl.trustStoreType=JKS
-Djavax.net.ssl.trustStore=C:\Program Files
(x86)\OpenText\common\jre\11.0\lib\security\cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

6. Apply the changes.
7. Start the Common Tomcat service.
8. In the Release Control Providers administrator page, change the link in the **Mainframe Connector** field to use the secure port, for example, **https://connectorHostName:8543**.
9. **SBM 10.1.5.x:** Use override values in the SBM **config.properties** file:

<SBM-install-dir>\Common\tomcat\server\default\webapps\rlc\WEB-INF\classes\config.properties

For example:

```
server.url.override=https://sbmhostname:8443
oe.eventmanager.ws.url.override=https://sbmhostname:8443
```

Enable SSL on ChangeMan ZMF

To enable SSL on ChangeMan ZMF:

1. Import a server certificate issued by a trusted CA into ZMF. For details on how to configure your ZMF environment to use SSL, see the ChangeMan ZMF help.
2. Import a trusted CA certificate into the Connector **keystore** and **truststore** files:
   - Import the CA root certificate into your **.jks** and **cacerts** files in the Common JRE **security** directory, for example:

     <java-install-dir>\bin\lib\security

     The default password is **changeit**.
   - Edit the **sernet_resource.properties** file in the Common Tomcat **WEB-INF\conf** directory:

     <tomcat-install-dir>\webapps\almsernet\WEB-INF\conf\sernet_resource.properties

     Set this property: **DEFAULT_HOST_USE_SSL = true**
   - Restart the Common Tomcat service.
3. If you are using the ChangeMan ZMF plugin, make sure that the plugin version is supported.
4. In the Base Plugin Configuration, set the property **Use ChangeMan SSL** to **true**.