



CHAPTER 16

Enabling Resource Manager to Use Secure Sockets Layer Connections on a JBoss Application Server

- [Component Identity via SSL, page 16-1](#)
- [How to Generate Certificates, page 16-1](#)

Component Identity via SSL

Secure Sockets Layer (SSL) connections rely on the existence of digital certificates. A digital certificate reveals information about its owner, including the owner's identity.

During the initialization of an SSL connection, the server must present its certificate to the client for the client to determine the server identity. The client can also present the server with its own certificate for the server to determine the client identity. SSL is therefore, a means of propagating identity between components.

How to Generate Certificates

- [Methods for Creating a New Certificate, page 16-2](#)
- [Prerequisites, page 16-2](#)
- [Using Keytool to Generate a Certificate, page 16-2](#)
- [Configuring JBoss to Use SSL, page 16-4](#)
- [Accessing Resource Manager via HTTPS, page 16-5](#)

Methods for Creating a New Certificate

A client can trust the contents of a certificate if that certificate is digitally signed by a trusted third party. A Certificate Authority (CA) acts as a trusted third party and signs certificates on the basis of its knowledge of the certificate requestor.

There are two methods for creating a new certificate.

- Request that a CA generates the certificate on your behalf.

The CA creates a new certificate, digitally signs it, and delivers it to the requester. Popular web browsers are preconfigured to trust certificates that are signed by certain CAs. No further client configuration is necessary for a client to connect to the server through an SSL connection.

Therefore, CA signed certificates are useful where configuration for each and every client that accesses the server is impractical.

- Generate a self-signed certificate.

This option is quicker and requires fewer details to create the certificate, but the certificate is not signed by a CA. Any client that connects to this server over an SSL connection needs configuration to trust the signer of this certificate. Therefore, self-signed certificates are only useful when you can configure each of the clients to trust the certificate. It is possible in some cases to present a self-signed certificate to an untrusting client. In some web browsers, when the certificate is received and does not match any of those listed in the client trust file, a prompt appears asking if the certificate should be trusted for the connection and added to the trust file.

Prerequisites

Cisco Unified Videoconferencing Manager uses the JBoss application server platform. The JBoss application server installs with Cisco Unified Videoconferencing Manager automatically.

To use SSL with JBoss, the following conditions must be met:

- You have a certificate.
- You configure JBoss to use this certificate.
- You store the certificate in a JKS keystore.

Using Keytool to Generate a Certificate

Keytool is the command line Java utility. This section describes how to use keytool to create a private and public self-signed certificate key pair.

Procedure

Step 1 Open a DOS window and set the path to point to the JDK or JRE *bin* directory. For example

```
D:\>set path= D:\jdk1.5.0\bin
```

Step 2 Create a self-signed certificate key pair. For example

```
D:\>keytool -genkey -keyalg RSA
-dname "cn=scheduler,ou=users,ou=yourcountry,
DC=yourcompany,DC=com"
```

```
-alias scheduler -keypass yourcompany -keystore
scheduler.keystore
-storepass yourcompany
```

- Step 3** Specify RSA as the private key to ensure that the MD5 with RSA signature algorithm is used. Not all web browsers support the DSA cryptograph algorithm, which is the default when RSA is not specified.
- Step 4** Set a password of at least six characters to protect the private key.
- Step 5** Specify the keystore file and keystore password (the option is storepass). Type each string on a single line.
- Step 6** If you do not wish to send a certificate signing request, skip to [“Configuring JBoss to Use SSL” section on page 16-4](#).

- Step 7** Generate the certificate signing request. For example
- D:\>keytool -certreq -v -alias scheduler -file scheduler.csr -keypass yourcompany
 - -keystore scheduler.keystore -storepass yourcompany

This request generates the following output:

Certification request stored in file <scheduler.csr>

Submit this to your CA

- Step 8** Send the scheduler.csr file to your selected CA for signing.
- Step 9** Save the content of the signed certificate to a file. For example, scheduler.cer.
- Step 10** Import the CA trusted root certificate into the keystore. For example

```
D:\>keytool -import -alias "Provider Test CA Root" -file "Provider Test Root.cer"
-keystore sceduler.keystore -storepass yourcompany
```

where

- Provider Test CA Root is the directory containing the test CA root binary and text files.
- Provider Test Root.cer is the test CA root binary file.

When the command is successfully executed, the following output displays:

```
Certificate was added to keystore
```

- Step 11** Import the certificate responses from the CA into the keystore file using the same alias name that was first given to the self-signed certificates.

In this example, the alias name is scheduler. Using an alternative alias name generates a new signed certificate and not a personal certificate chain.

```
D:\>keytool -import -trustcacerts -alias scheduler -file scheduler.cer
-keystore scheduler.keystore -storepass yourcompany
```

When the command is successfully executed, the following output displays:

```
Certificate reply was installed in keystore
```

You have now created a keystore file that stores a valid certificate for use.

Configuring JBoss to Use SSL

Configure the JBoss application server for use with SSL.

Procedure

-
- Step 1** Copy the scheduler.keystore file to
<Resource Manager installation directory>\jboss\server\default\conf
- Step 2** Open the server.xml file located in jboss\server\default\deploy\jbossweb-tomcat50.sar
- Step 3** Locate the section beginning with the line
 <!-- SSL/TLS Connector configuration using the admin devl guide keystore
- Step 4** Remove the comment indicators and make the following changes:
- Uncomment out the SSL/TLS connector.
 - Change the keystore file from **chap8.keystore** to **scheduler.keystore**.
 - Change the keystorePass from **rmi+ssi** to **yourcompany**.
 - We recommend that you change the port from 8443 to 443 so that the user does not need to type the port when accessing Resource Manager. Like port 80, port 443 is a known HTTPS port.

The amended text appears as follows:

```
<!-- A HTTP/1.1 Connector on port 8080 or 80 -->
<Connector port="8080" address="{jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>

<!-- A AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="{jboss.bind.address}"
enableLookups="false" redirectPort="443" debug="0"
protocol="AJP/1.3"/>

<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="{jboss.server.home.dir}/conf/
scheduler.keystore"
keystorePass="yourcompany" sslProtocol = "TLS" />
<!-- -->
```

- Step 5** Restart JBoss.
-

Accessing Resource Manager via HTTPS

Procedure

- Step 1** Type a URL of the format `https://localhost`, or `https://localhost:8443` (if port 8443 is used instead of 443). If the certificate in use is a test root certificate or a self-signed certificate that is not trusted by Internet Explorer, a security alert appears.
- Step 2** Click **Yes** to access Resource Manager.
- Step 3** To avoid this message in future logins, click **View Certificate**:
- Step 4** Click **Install Certificate**.
- Step 5** After the certificate is installed, the user will not see the security alert on subsequent logins.
-

