TLS Configuration for Jetty and Tomcat Server

This section details steps to perform the following:

Enable Minimum TLS Version for Cisco Prime Collaboration Assurance Client Connections

Follow are the steps for Minimum TLS configuration for Cisco Prime Collaboration Assurance Client interfaces.

Before you begin

Note All HTTPS connections from Cisco Prime Collaboration Assurance to VOS based devices are controlled by the below settings.

Procedure

Step 1 Login as *root* user to edit the following file:

```
/opt/emms/conf/connector.xml
```

Step 2 Edit <minTLSProtocol>TLSv1</minTLSProtocol> for particular connection type (HTTPS).

TLSv1 configured, TLSv1, TLSv1.1, TLSv1.2 enabled

TLSv1.1 configured, TLSv1.1, TLSv1.2 enabled

TLSv1.2 configured, TLSv1.2 enabled

Step 3 Restart all Cisco Prime Collaboration Assurance services.

Enable TLS Protocol for Jetty Server

Note

1. Jetty server is configured to enable all the 3 protocols, by default.
2. For example, to disable TLS v1 protocol and have only TLS v1.1 and TLS v1.2 enabled. Follow these steps:

Procedure

Step 1 Edit the following file:

```
/opt/jetty/etc/jetty-ssl.xml
```

Step 2 Add the below entries under **sslContextFactory** tag. For example,

```
<Set name="IncludeProtocols">
    <Array type="String">
    <Item>TLSv1.1</Item>
    <Item>TLSv1.2</Item>
    </Array>
</Set>
<Set name="ExcludeProtocols">
   <Array type="String">
   <Item>TLSv1</Item>
   </Array>
</Set>
```

Step 3 Restart the Jetty server using the following command:

```
systemctl restart jetty
```

Enable TLS Protocol for Tomcat Server

Note

1. Tomcat server is configured to enable all the 3 protocols, by default.
2. For example, to disable TLS v1 protocol and have only TLS v1.1 and TLS v1.2 enabled. Follow these steps:

Procedure

Step 1 Edit the following file:

```
/opt/emms/apache-tomcat-8.5.11/conf/server.xml
```

Step 2 Replace **sslProtocols** parameter in **port 8443** connector tag with **protocols** parameter and mention the required protocols to be enabled.

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" **sslProtocols="TLSv1,TLSv1.1,TLSv1.2"**

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" **protocols="TLSv1.1,TLSv1.2"**

Step 3 Restart all processes on Cisco Prime Collaboration Assurance when the above configuration is complete.