Enhancing Security for Web UI

This appendix contains the following section:

Enhancing Security for Web UI

When connected through the Secured Socket Layer (SSL) protocol using HTTPS, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These ciphers usually include weak cipher session keys and can affect system security. In case you want to harden the system, adjust the ciphers as below:

Note The default installation of Cisco Prime Network Registrar 10.1 works with Transport Layer Security (TLS) 1.2. You can change the configuration to make it work with the older TLS versions, if needed.

Step 1 Open the **server.xml** file in the *install-path*/tomcat/conf folder in your Cisco Prime Network Registrar installation folder.

Step 2 Add a ciphers statement to the HTTPS connector statement and list down the allowed ciphers as described in the following example:

Note The values for **port**, **keystoreFile**, and **keystorePass** must match the values that you have configured in your system.

```
<Connector port="8443"

maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

maxHttpHeaderSize="8192"

enableLookups="false"

disableUploadTimeout="true"

acceptCount="100" scheme="https" secure="true"

clientAuth="false"

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
```

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA"

keystoreFile="conf/.keystore"

sslProtocol="TLSv1.2"

sslEnabledProtocols="TLSv1.2"/>
```

Step 3 Restart Cisco Prime Network Registrar for the changes to take effect.