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 11.1 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 /var/nwreg2/{local | regional}/tomcat/conf folder.

Step 2 Use the below recommended sslEnabledProtocols and ciphers, or configure it as per your security requirement. For more details, refer the tomcat SSL/TLS Configuration document available online.

```
<Connector port="${cnrui.https.port}" protocol="com.cisco.cnr.webui.tomcat.SecureHTTP"

relaxedQueryChars='[]'

maxConnections="1024" maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false"

keystoreFile="..."

keystorePass="..."

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"

compression="on"

compressionMinSize="2048"

noCompressionUserAgents="gozilla, traviata"

URIEncoding="UTF-8"

compressableMimeType="text/html,text/xml,text/plain, text/css,text/javascript,
application/x-javascript,application/javascript"

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

Note The **keystoreFile** and **keystorePass** values are specific to your installation. You should not change these values as it will be overwritten each time Cisco Prime Network Registrar is started.

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

Note Cisco Prime Network Registrar 11.1 supports TLS 1.3 with below ciphers:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

If you want to leverage TLS 1.3, you need to update the server.xml file appropriately and restart Cisco Prime Network Registrar.