APPENDIX C

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. Therefore, you may want to adjust the ciphers to disable the use of weak ciphers in the web UI.

To adjust the ciphers:

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="SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
           keystoreFile="conf/.keystore"
           keystorePass="changeit"
           sslProtocol="TLS" />
```

The *ciphers* attribute can carry a comma-separated list of encryption ciphers that this socket is allowed to use. By default, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These contain the weak export-grade ciphers in the list of available ciphers. This results in the web UI supporting weak cipher session keys.

Note The ciphers are specified using the Java Secure Socket Extension (JSSE) cipher naming convention.

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