There are two forms of communication that exist between Cisco Unified MeetingPlace Video Integration and the Video Administration for Cisco Unified MeetingPlace. One uses SOAP over HTTP(s) and one uses a proprietary XML protocol over a persistent TCP socket. We recommend that you secure the communication between these two servers to guard against security attacks.

A set of server and client certificates are installed with Video Integration by default. These certificates are signed by using a Certificate Authority key that is generated by using OpenSSL. After installing Video Integration, SSL is turned off by default.

Contents

Configuring a Basic Level of Security by Using OpenSSL

To encrypt the communication between the Video Administration server and the Web Conferencing servers that have Video Integration installed, you can use the OpenSSL configuration files that are installed by default.

You must do both of the following procedures:

- To Configure Basic Security on the Video Administration Server
- To Configure Basic Security on the Cisco Unified MeetingPlace Video Integration Servers

Caution! It is important that you back up all files before editing. Restoring to a known working configuration can be difficult without backups of the default files.

To Configure Basic Security on the Video Administration Server For Release 6.0

1. Browse to a file named **vcs-core.properties**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss\bin.
2. Make a backup copy of the file.
3. Open the file with Notepad and search for a section beginning with **#for MCU proxy XML API**.

4. Confirm that the following six lines are in the vcs-core.properties file. If they are not, add them. If they begin with a **#**, remove the **#**.

```
com.radvision.icm.dciproxy.server.useSystemKeyStore=false
com.radvision.icm.mcuproxy.useSSL=true
com.radvision.icm.dciproxy.server.keystore=..\\server\\default\\conf\\i
com.radvision.icm.dciproxy.server.keystorePassword=radvision
com.radvision.icm.dciproxy.server.trustKeystore=..\\server\\default\\co
com.radvision.icm.dciproxy.server.trustKeystorePassword=radvision
```

   Note: You will probably need to modify the second line from com.radvision.icm.mcuproxy.useSSL=false to com.radvision.icm.mcuproxy.useSSL=true (This enables SSL.)
5. Browse to a file named **server.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss\server\default\deploy\jbossweb-tomcat55.sar.
6. Make a backup copy of the file.
7. Open the file for editing with Notepad and confirm that the following eight lines are in the server.xml file. If they are not, add them:

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
keystorePass="radvision"
truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
truststorePass="radvision"
sslProtocol = "TLS" />
```

   Note: You probably will not need to modify the server.xml file.
8. Browse to a file named **web.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss\server\default\deploy\vcs.ear\icmservice.war\WEB-INF.

   Note: If you find an icmservice.war file instead of an icmservice.war folder, you can use a zip/unzip program to open the .war file and edit the web.xml file. You do not need to unzip the .war file.
9. Make a backup copy of the file.
10. Open the file for editing with Notepad and confirm that the following lines are in the web.xml file. If they are not, add them:

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>ScheduleService</web-resource-name>
<description>ScheduleService</description>
<url-pattern>/1.0/ScheduleService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<security-constraint>
<web-resource-collection>
<web-resource-name>ResourceService</web-resource-name>
<description>ResourceService</description>
<url-pattern>/1.0/ResourceService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
```

```
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<security-constraint>
<web-resource-collection>
<web-resource-name>ControlService</web-resource-name>
<description>ControlService</description>
<url-pattern>/1.0/ControlService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<login-config>
<auth-method>CLIENT-CERT</auth-method>
<realm-name>icmservice</realm-name>
</login-config>
<security-role>
<role-name>SvrAdmin</role-name>
</security-role>
-->
```

11. Delete the first and last lines of this example ("<!--" and "-->") and save and close the file.
12. Browse to a file named **login-config.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss\server\default\conf.
13. Make a backup copy of the file.
14. Open the file for editing with Notepad and confirm that the following ten lines are in the login-config.xml file. If they are not, add them:

```
</application-policy>
<application-policy name="icmservice">
<authentication>
<login-module
code="com.radvision.icm.service.security.ICMServiceCertLoginModule"
flag="required">
<module-option
name="password-stacking">useFirstPass</module-option>
<module-option
name="securityDomain">java:/jaas/SecurityDomainICMService</module-optic
<module-option
name="rolesProperties">roles.properties</module-option>
</login-module>
</authentication>
</application-policy>
```

Note: You probably will not need to modify the login-config.xml file.

15. Browse to a file named **jboss-service.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss\server\default\conf.
16. Make a backup copy of the file.
17. Open the file for editing with Notepad and confirm that the following eight lines are in the jboss-server.xml file. If they are not, add them:

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.web:service=SecurityDomain">
<constructor>
```

```
<arg type="java.lang.String"
value="SecurityDomainICMService"/>
</constructor>
<attribute
name="KeyStoreURL">resource:icmservice.keystore</attribute>
<attribute name="KeyStorePass">radvision</attribute>
</mbean>
```

Note: You probably will not need to modify the jboss-service.xml file.

18. Reboot Video Admin server for changes to take effect

To Configure Basic Security on the Video Administration Server For Release 6.0

1. Browse to a file named **vcs-core.properties**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss-3.2.5\bin.
2. Make a backup copy of the file.
3. Open the file with Notepad and search for a section beginning with **#for MCU proxy XML API**.
4. Confirm that the following six lines are in the vcs-core.properties file. If they are not, add them. If they begin with a **#**, remove the **#**.

```
com.radvision.icm.dciproxy.server.useSystemKeyStore=false
com.radvision.icm.mcuproxy.useSSL=true
com.radvision.icm.dciproxy.server.keystore=..\\server\\all\\conf\\icmse
com.radvision.icm.dciproxy.server.keystorePassword=radvision
com.radvision.icm.dciproxy.server.trustKeystore=..\\server\\all\\conf\\
com.radvision.icm.dciproxy.server.trustKeystorePassword=radvision
```

   Note: You will probably need to modify the second line from com.radvision.icm.mcuproxy.useSSL=false to com.radvision.icm.mcuproxy.useSSL=true (This enables SSL.)
5. Browse to a file named **server.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\deploy\jbossweb-tomcat50.sar.
6. Make a backup copy of the file.
7. Open the file for editing with Notepad and confirm that the following eight lines are in the server.xml file. If they are not, add them:

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
keystorePass="radvision"
truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
truststorePass="radvision"
sslProtocol = "TLS" />
```

   Note: You probably will not need to modify the server.xml file.
8. Browse to a file named **web.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\deploy\icmservice.war\WEB-INF.

   Note: If you find an icmservice.war file instead of an icmservice.war folder, you can use a zip/unzip program to open the .war file and edit the web.xml file. You do not need to unzip the .war file.
9. Make a backup copy of the file.
10. Open the file for editing with Notepad and confirm that the following lines are in the web.xml file. If they are not, add them:

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>ScheduleService</web-resource-name>
```

```
<description>ScheduleService</description>
<url-pattern>/1.0/ScheduleService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<security-constraint>
<web-resource-collection>
<web-resource-name>ResourceService</web-resource-name>
<description>ResourceService</description>
<url-pattern>/1.0/ResourceService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<security-constraint>
<web-resource-collection>
<web-resource-name>ControlService</web-resource-name>
<description>ControlService</description>
<url-pattern>/1.0/ControlService/*</url-pattern>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>SvrAdmin</role-name>
</auth-constraint>
</security-constraint>
<login-config>
<auth-method>CLIENT-CERT</auth-method>
<realm-name>icmservice</realm-name>
</login-config>
<security-role>
<role-name>SvrAdmin</role-name>
</security-role>
-->
```

11. Delete the first and last lines of this example ("<!--" and "-->") and save and close the file.
12. Browse to a file named **login-config.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\conf.
13. Make a backup copy of the file.
14. Open the file for editing with Notepad and confirm that the following ten lines are in the login-config.xml file. If they are not, add them:

```
</application-policy>
<application-policy name="icmservice">
<authentication>
<login-module
code="com.radvision.icm.service.security.ICMServiceCertLoginModule"
flag="required">
<module-option
name="password-stacking">useFirstPass</module-option>
<module-option
```

```
name="securityDomain">java:/jaas/SecurityDomainICMService</module-optic
<module-option
name="rolesProperties">roles.properties</module-option>
</login-module>
</authentication>
</application-policy>
```

Note: You probably will not need to modify the login-config.xml file.

15. Browse to a file named **jboss-service.xml**, which can be found in \Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\conf.
16. Make a backup copy of the file.
17. Open the file for editing with Notepad and confirm that the following eight lines are in the jboss-server.xml file. If they are not, add them:

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.web:service=SecurityDomain">
<constructor>
<arg type="java.lang.String"
value="SecurityDomainICMService"/>
</constructor>
<attribute
name="KeyStoreURL">resource:icmservice.keystore</attribute>
<attribute name="KeyStorePass">radvision</attribute>
</mbean>
```

Note: You probably will not need to modify the jboss-service.xml file.

18. Reboot Video Admin server for changes to take effect

To Configure Basic Security on the Cisco Unified MeetingPlace Video Integration Servers

1. Stop the **Cisco Unified MeetingPlace Web Conferencing** master service. The Cisco Unified MeetingPlace Video service will automatically stop.
2. In the Windows Control Panel, double-click **MeetingPlace Gateways**.
3. Click the **Video Security** tab.
4. Check the **Encrypt Video Administration Communication** checkbox. Answer Yes to the question about changing the port to 8443. (This changes the Video Administration Port setting on the Video tab. You can also do it manually.)
5. Do not check the **Verify Server Certificates** check box.
6. Check the **Use Client Certificates** check box.
7. Click **OK**.
8. Restart the Cisco Unified MeetingPlace Web Conferencing master service. The Cisco Unified MeetingPlace Video service will automatically restart.
9. Repeat Step 2 through Step 8 on every server that has Cisco Unified MeetingPlace Video Integration installed.

Once security is configured on the Video Administration server and on all of the Web Conferencing servers that have Video Integration installed, any future changes to the security levels must be made on all servers, including the Video Administration server. In addition, services must be restarted whenever changes to security settings are made.