Disabling weak SSL cipher suites to improve security

On this page:

Target audience:

CAST AI Administrators

Summary: this page explains how to modify your Apache Tomcat web application server, Windows Operating System and Apache web server to **disable weak SSL cipher suites** to improve security when using the HTTPS protocol to access CAST web applications.

Introduction

As described in Configuring the use of secure https protocol with Tomcat for the CAST web applications, it is possible to configure Tomcat for **secure https** access to the CAST web applications (CAST AIC Portal/CAST Application Analytics Dashboard/CAST Engineering Dashboard). Apache recommends an SSL connector for you to use and by default this connector (whether APR or JSSE based) will include a list of Cipher Suites the client (i.e. the CAST web application) is permitted to negotiate in the SSL handshake phase. Unfortunately this list of Cipher Suites will include weak export grade ciphers that are insecure. As such CAST recommends actually specifying the Cipher Suites you wish to use, rather than relying on the default which includes many insecure ciphers that could pose a risk to your organization's security.

In addition, you may also want to disable weak cipher suites in the Windows Operating System and in Apache webserver if you are using them to host the Tomcat web application server.

Apache Tomcat changes

CAST recommends specifying making the following changes to disable weak cipher suites:

APR based SSL connector

If you are using an APR based SSL connector, CAST recommends specifying the following cipher suites:

```
HIGH:MEDIUM:!MD5!EXP:!NULL:!LOW:!ADH
```

You can add these cipher suites into your SSL connector using the SSLCipherSuite directive (listed at the end of the connector in the example below):

```
<Connector
        protocol="HTTP/1.1"
        port="443"
        scheme="https"
        secure="true"
        SSLEnabled="true"
        clientAuth="false"
        SSLProtocol="SSLv3+TLSv1"
        SSLCertificateFile="path/to/server.crt"
        SSLCertificateKeyFile="path/to/server.pem"/>
        SSLCipherSuite="HIGH:MEDIUM:!MD5!EXP:!NULL:!LOW:!ADH"
/>
```

Following any changes you make, **save the %CATALINA_HOME%\conf\server.xml** file and then **restart** your application server so that the changes are taken into account.

JSSE based SSL connector

If you are using a JSSE based SSL connector, CAST recommends specifying the following cipher suites:

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA
```

You can add these cipher suites into your SSL connector using the cipher attribute (listed at the end of the connector in the example below):

```
<Connector
        protocol="HTTP/1.1"
        port="443"
        scheme="https"
        secure="true"
        SSLEnabled="true"
        clientAuth="false"
        SSLProtocol="TSL"
        keystoreFile="path/to/keystore"
        keystorePass="passwordOfKeystore"
        ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
        TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,
        TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256,
        TLS_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA"
/>
```

Following any changes you make, **save the %CATALINA_HOME%\conf\server.xml** file and then **restart** your application server so that the changes are taken into account.

Disabling weak SSL ciphers in Windows Operating System

You may want to reconfigure your host Windows Operating System to avoid the use of weak SSL cipher suites. The configuration changes are OS specific:

- For Microsoft Windows XP and Microsoft Windows Server 2003, follow these instructions: http://support.microsoft.com/kb/245030
- For all other CAST supported Operating Systems, remove the cipher suites that you have identified as weak from the Supported Cipher Suite list by following these instructions: https://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx

Disabling weak ciphers in Apache server

You may want to reconfigure your Apache webserver (if you are using it in conjunction with Tomcat) to avoid the use of weak SSL cipher suites. Similar to the instructions given above for Tomcat, modify (or add) the SSLCipherSuite directive in the **httpd.conf** or **ssl.conf** file:

```
SSLCipherSuite="HIGH:MEDIUM:!MD5!EXP:!NULL:!LOW:!ADH"
```