

# HowTo SSLCiphers

## How do I restrict the list of SSL ciphers used by Connector

Firstly, the configuration attribute and its values depend on what HTTPS implementation you are using. You may be using either Java-based implementation aka JSSE — with BIO and NIO connectors, or OpenSSL-based implementation — with APR connector.

### Links:

- [HTTP Connector configuration reference \(Tomcat 7\)](#)

## Using Java implementation

For BIO and NIO connectors the attribute that specifies the list of ciphers is called **ciphers** and multiple values are separated by a comma (,). For the list of possible values see the list of cipher suite names for your version of Java, e.g.

- [Oracle Java 6](#)
- [Oracle Java 7](#)

See thread "Default SSL ciphers supported by Tomcat 6" from October 2009 [here](#) for a short program that displays available ciphers in your particular JVM.

### Sample configuration:

```
ciphers="SSL_RSA_WITH_RC4_128_MD5,
        SSL_RSA_WITH_RC4_128_SHA,
        TLS_ECDHE_ECDSA_WITH_RC4_128_SHA,
        TLS_ECDHE_RSA_WITH_RC4_128_SHA,
        TLS_ECDH_ECDSA_WITH_RC4_128_SHA,
        TLS_ECDH_RSA_WITH_RC4_128_SHA"
```

## Using OpenSSL implementation (APR connector)

For APR connector the attribute that specifies the list of ciphers is called **SSLCipherSuite** and multiple values are separated by a colon (:). Generally, it is configured in the same way as SSLCipherSuite directive of [mod\\_ssl](#) of Apache HTTPD server. For the list of possible values see [OpenSSL documentation](#), or run `openssl.exe ciphers -v`.

### Sample configurations:

a)

```
SSLCipherSuite="RSA:!EXP:!NULL:+HIGH:+MEDIUM:-LOW"
```

b)

```
SSLCipherSuite="RC4-SHA"
```