Ciphers

TLS Cipher suite choice

There is no right choice since there are always trade-offs to make between better security better interoperability, better performance etc.. Where you choose to draw that line is a choice you need to make. The following information is provided to help you make that choice. The ratings provided are those calculated by the excellent SSL Labs Test. Keep in mind that, as more vulnerabilities are discovered, these ratings are only ever going to get worse over time. The results shown on this page were correct at the time they were generated.

BIO/NIO/NIO2 with JSSE Results (Default)

	Java 6	Java 7	Java 8	Java 9	Java 10
Tomcat 7	C	B	A	A	A
Tomcat 8	N/A	B	A	A	A
Tomcat 8.5	N/A	B	A	A	A
Tomcat 9	N/A	N/A	A	A	A

Note: These results were obtained using the JCE Unlimited Strength Jurisdiction Policy Files

Note: The Java 6 results are capped at C because Java 6 does not support TLS 1.1 or 1.2.

Note: The Java 7 results are capped at B because Java 7 does not support AEAD ciphers.

The equivalent OpenSSL cipher configurations used to obtain the above results are:

Java 6	HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!DHE
Java 7	HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA:!DHE
Java 8	HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA
Java 9	HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA

Note: kRSA ciphers are not excluded in Java 6 since they are likely to be the only ones left

Note: In Java 7 and earlier DHE ciphers use insecure DH keys with no means to configure longer keys which is why DHE ciphers are excluded in those Java versions.

NIO/NIO2 with JSSE+OpenSSL Results (Default)

	Java 6	Java 7	Java 8	Java 9	Java 10
Tomcat 8.5	N/A	A	A	A	A
Tomcat 9	N/A	N/A	A	A	A

The OpenSSL cipher configuration used was **HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA**. Up-to-date selection of secure cipher suites in OpenSSL format is available at Mozilla wiki.

APR with OpenSSL Results (Default)

	Java 6	Java 7	Java 8	Java 9	Java 10
Tomcat 7	A	A	A	A	A
Tomcat 8	N/A	A	A	A	A
Tomcat 8.5	N/A	A	A	A	A
Tomcat 9	N/A	N/A	A	A	A

The OpenSSL cipher configuration used was **HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA**. Up-to-date selection of secure cipher suites in OpenSSL format is available at Mozilla wiki.

Environment

The results above were generated with:

- Java 6, 64-bit, update 45
- Java 7, 64-bit, update 80
- Java 8, 64-bit, update 172
- Java 9, 9.0.4
- Apache Tomcat 7.0.88-dev, r1737253.
- Apache Tomcat 8.0.53-dev, r1737224.
- Apache Tomcat 8.5.32-dev, r1737241.
- Apache Tomcat 9.0.9-dev, r1737193.
- tc-native 1.2.16