

# SSL 证书- Tomcat

优化加密算法

(cipher)



## 优化加密算法 (cipher)

( a ) 适用于 Tomcat 5, 6

Tomcat 目录下该文件 "Server.xml" 加入青色的字

```
<Connector port="443" maxHttpHeaderSize="8192" address="192.168.1.1"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true" clientAuth="false"
keystoreFile="SomeDir/SomeFile.key" keystorePass="Poodle"
truststoreFile="SomeDir/SomeFile.truststore" truststorePass="HomeRun"
```

```
sslProtocol="TLSv1, TLSv1.1, TLSv1.2"
SSL_RSA_WITH_RC4_128_MD5,
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,
SSL_RSA_WITH_DES_CBC_SHA,
SSL_DHE_RSA_WITH_DES_CBC_SHA,
SSL_DHE_DSS_WITH_DES_CBC_SHA,
SSL_RSA_EXPORT_WITH_RC4_40_MD5,
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
"/>
```

( b ) 适用于 Tomcat 7, 8

Tomcat 目录下该文件 "Server.xml" 加入青色的字

```
<Connector port="443" maxHttpHeaderSize="8192" address="192.168.1.1"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true" clientAuth="false"
keystoreFile="SomeDir/SomeFile.key" keystorePass="Poodle"
```

truststoreFile="SomeDir/SomeFile.truststore" truststorePass="HomeRun"

*sslProtocol="TLSv1, TLSv1.1, TLSv1.2"*  
*ciphers="TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,*  
*TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384,*  
*TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA,*  
*TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA,*  
*TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,*  
*TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256,*  
*TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA,*  
*TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA,*  
*TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA,*  
*TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA,*  
*TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA,*  
*TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_ECDH\_RSA\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384,*  
*TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,*  
*TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256,*  
*TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,*

*TLS\_ECDH\_RSA\_WITH\_AES\_128\_GCM\_SHA256,*  
*TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256,*  
*TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA,*  
*TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA,*  
*TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA,*  
*TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA,*  
*TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV*  
"/>