

Windows Tomcat 프로토콜 설정 가이드

본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다.

[고객센터]
한국기업보안. 유서트 기술팀
02-3442-7230



한국기업보안
Korea Corporation Security

1. Tomcat 기본 설정 파일을 수정합니다.(SSLProtocol)

설정 파일 경로 : <Tomcat 경로>/conf/server.xml

SSL 포트를 선언하는 Connector 속성 내부에 사용할 TLS 를 정의합니다.

버전 별 설정 방법에 차이가 있습니다.

TLS 1.2 & TLS 1.1프로토콜은 톰캣 버전 상관없이 JAVA 1.7.x 버전 이상이 필요합니다.

파란색으로 표시된 부분 외에는 버전 별로 상이할 수 있으며, 구문 위치 예시를 위해 포함한 사항입니다.

파란색 부분 외 다른 설정은 버전에 맞게 설정해 주시기 바랍니다.

Tomcat 7 버전 대까지 : SSL 포트 Connector 속성 내부

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true"
keystoreFile="<인증서 경로>" keystorePass="<인증서 패스워드>" clientAuth="false"
sslProtocol="TLSv1.2"
/>
```

Tomcat 8.5 버전 이후 : Connector 속성 내 SSLHostConfig 속성 내부

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true">
    <SSLHostConfig
protocols="TLSv1.2"
SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA">
        <Certificate certificateKeystoreFile="<인증서 경로>"
certificateKeystorePassword="<인증서 패스워드>" type="RSA" />
    </SSLHostConfig>
</Connector>
```

2. Tomcat 기본 설정 파일을 수정합니다.(SSLCipherSuite)

설정 파일 경로 : <Tomcat 경로>/conf/server.xml

SSL 포트를 선언하는 Connector 속성 영역 내

버전 별 설정 방법에 차이가 있습니다.

파란색으로 표시된 부분 외에는 버전 별로 상이할 수 있으며, 구문 위치 예시를 위해 포함한 사항입니다.
파란색 부분 외 다른 설정은 버전에 맞게 설정해 주시기 바랍니다.

Tomcat 7 버전 대까지 : SSL 포트 Connector 속성 내부

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true"
keystoreFile="<인증서 경로>" keystorePass="<인증서 패스워드>" clientAuth="false"
sslProtocol="TLS1.2"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WI
TH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SH
A, SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
/>
```

Tomcat 8.5 버전 이후 : Connector 속성 내 SSLHostConfig 속성 내부

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true">
<SSLHostConfig
protocols="TLSv1.2 "
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WI
TH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SH
A, SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA">
<Certificate certificateKeystoreFile="<인증서 경로>"
certificateKeystorePassword="<인증서 패스워드>" type="RSA" />
</SSLHostConfig>
</Connector>
```