

Tomcat 서버 Secure ID 인증서 설치 매뉴얼

1. 소개

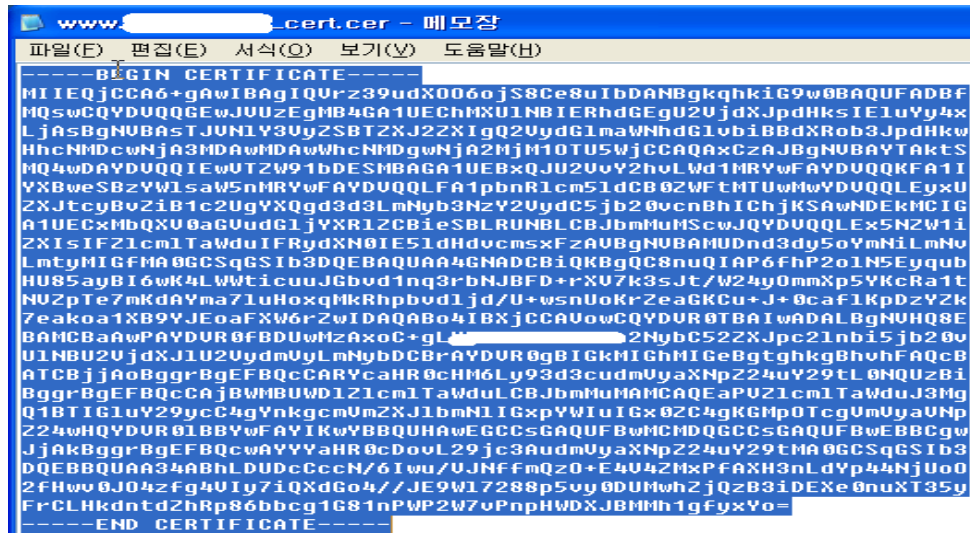
이 매뉴얼은 발급 받은 Verisign Secure ID 인증서를 단독적으로 운영되는 Tomcat 서버에 설치하는 방법에 대해서 설명합니다.

2. 인증서 파일의 저장

A. 인증서 복사

메일로 받은 인증서를 복사하여 메모장과 같은 ASCII 텍스트 편집기로 붙여넣기 하여 server.crt 와 같은 이름으로 저장합니다.

(---BEGIN CERTIFICATE ~ ---END CERTIFICATE--- 까지 모두 복사)



B. Keystore에 인증서의 설치

JDK에서 제공하는 keytool을 사용하여 메일로 수신한 인증서를 keystore에 설치한다.

```
$JAVA_HOME/bin/keytool -import -v -trustcacerts -alias [key name] -file [인증서 파일] -keystore [keystore file name]
```

```
[root@squid ssl]# $JAVA_HOME/bin/keytool -import -v -trustcacerts -alias tomcats -file icert.crt -keystore icert
Enter keystore password: █
```

개인키 생성시 입력한 패스워드를 입력하고 설치 과정 중 yes, no를 물어오면 y를 입력하여 설치를 완료한다.

3. 톰캣 서버 설정

A. \$CATALINA_HOME/conf/server.xml 파일의 편집

톰캣이 사용하는 기본 SSL 포트는 8443번으로서 톰캣 버전에 따라서 각기 다르게 설정된다. 이 매뉴얼에서는 기본 설정만을 다룬다.

i. Tomcat 4.x

[server.xml]

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="8443" enableLookups="true" scheme="https" secure="true"
    acceptCount="100"
    useURIVValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="$keystore_file_path"
    keystorePass="$keystore password"
    clientAuth="false" sslProtocol="TLS" />
</Connector>
```

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
I
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="8443" enableLookups="true" scheme="https" secure="true"
    acceptCount="100"
    useURIVValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="/opt/tomcat4/conf/ssl/icert"
    keystorePass="12345" clientAuth="false" sslProtocol="TLS" />
</Connector>
```

ii. Tomcat 5.x

[server.xml]

```
<Connector className="org.apache.coyote.tomcat5.CoyoteConnector"
    port="8443" enableLookups="true" scheme="https" secure="true"
    acceptCount="100"
    useURIVValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat5.CoyoteServerSocketFactory"
    keystoreFile="$keystore_file_path"
    keystorePass="$keystore password"
    clientAuth="false" sslProtocol="TLS" />
</Connector>
```

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat5.CoyoteConnector"
  port="8443" enableLookups="true" scheme="https" secure="true"
  acceptCount="100"
  useURIVValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat5.CoyoteServerSocketFactory"
    keystoreFile="/opt/tomcat5.0/conf/ssl/icert"
    keystorePass="12345" clientAuth="false" sslProtocol="TLS" />
</Connector>
```

iii. Tomcat 5.5.x

[server.xml]

```
<Connector
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true" disableUploadTimeout="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="$keystore_file_path"
  keystorePass="$keystore password" />
```

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true" disableUploadTimeout="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="/opt/tomcat5.5/conf/ssl/icert"
  keystorePass="12345" />
```

iv. Tomcat 6.x

[server.xml]

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
  port="8443" minSpareThreads="5" maxSpareThreads="75"
  enableLookups="true" disableUploadTimeout="true"
  acceptCount="100" maxThreads="200"
  scheme="https" secure="true" SSLEnabled="true"
  keystoreFile="$keystore_file_path"
  keystorePass="$keystore password"
  clientAuth="false" sslProtocol="TLS"/>
```

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/opt/tomcat/webapps/ssl/icert" keystorePass="dkldspdlawm"
clientAuth="false" sslProtocol="TLS"/>
```

B. 톰캣 서버 시작

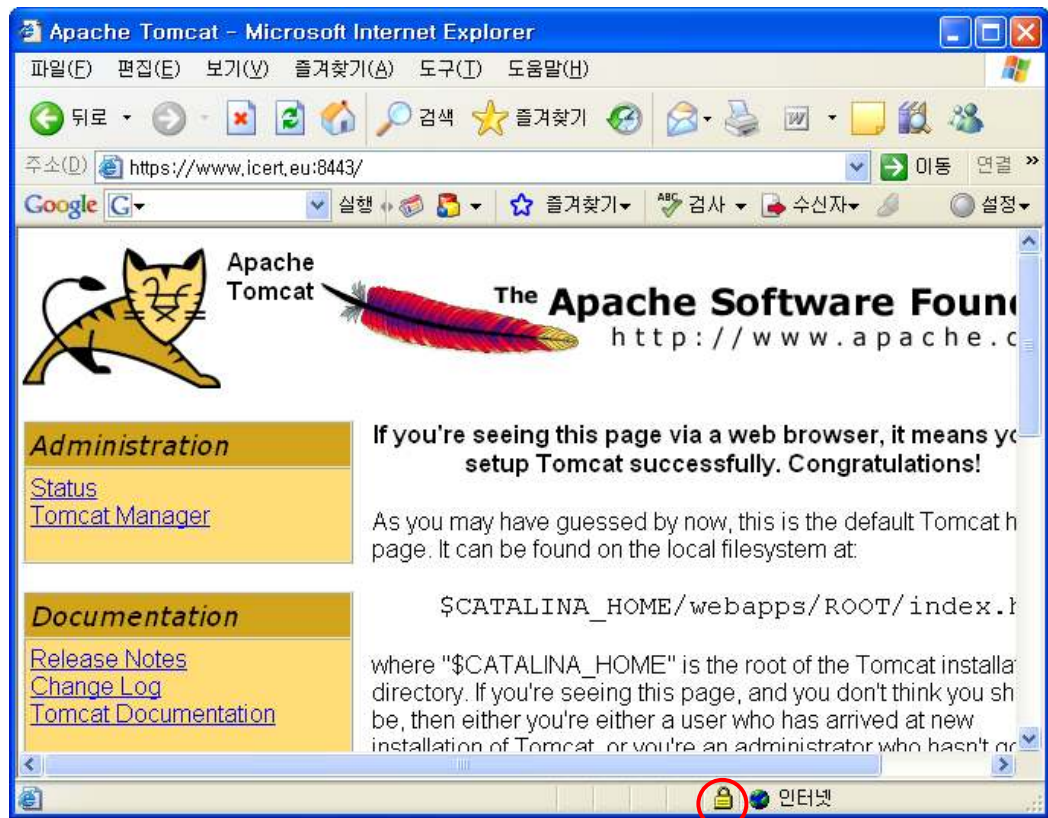
설정이 완료 되었다면 아래와 같은 명령으로 톰캣 서버를 실행 합니다.

```
# $CATALINA_HOME/bin/shutdown.sh
# $CATALINA_HOME/bin/startup.sh
```

C. SSL 설정 확인

아래와 같이 브라우저로 접속하여 IE 브라우저 하단에 자물쇠가 생성 되는지 확인하도록 합니다.

```
https://www.example.com:8443
```



끝.