Apache SSL 프로토콜 설정 가이드

[고객센터]
한국기업보안. 유서트 기술팀
02-512-5495

1. Apache SSL Protocol 및 cipher 설정

1) **($HOME_BASE/conf/httpd.conf** 를 열어 아래와 같이 설정 합니다.

- 아래값은 샘플 값입니다.

[샘플 값 1]

```
<VirtualHost *:443>
    ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot "/usr/local/apache2/home2/"
    ServerName  ucert.co.kr
ErrorLog "/usr/local/apache2/logs/ssl_error_log"
TransferLog "/usr/local/apache2/logs/ssl_access_log"

<Directory "/usr/local/apache2/home2">
    AllowOverride None
    Require all granted
</Directory>

SSLEngine on
SSLProtocol ALL -SSLv2 -SSLv3
SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES2
56-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES2
56-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DE
S-CBC3-SHA:!KRB5-DES-CBC3-SHA
```

SSLProtocol ALL -SSLv2 -SSLv3 +TLSv1.2 +TLSv1.1 +TLSv1

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

[샘플 값 2]

```
<VirtualHost *:443>
    ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot "/usr/local/apache2/home2/"
    ServerName  ucert.co.kr
ErrorLog "/usr/local/apache2/logs/ssl_error_log"
TransferLog "/usr/local/apache2/logs/ssl_access_log"

<Directory "/usr/local/apache2/home2">
    AllowOverride None
    Require all granted
</Directory>

SSLEngine on
SSLProtocol ALL -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-DSS-A
ES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-
SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA:AES128-GCM-SHA256:AES2
56-GCM-SHA384:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RS
A-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA:!DHE-RSA-AES128-GCM-SHA256:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES128-SHA256:!DHE-RSA-AES256-SHA:!DHE-RSA-
AES128-SHA:!DHE-RSA-AES256-SHA256:!DHE-RSA-CAMELLIA128-SHA:!DHE-RSA-CAMELLIA256-SHA
```

SSLProtocol ALL -SSLv2 -SSLv3 +TLSv1.2 +TLSv1.1 +TLSv1

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA:!DHE-RSA-AES128-GCM-SHA256:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES128-SHA256:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-SHA:!DHE-RSA-AES256-SHA256:!DHE-RSA-CAMELLIA128-SHA:!DHE-RSA-CAMELLIA256-SHA

2. Apache 를 재기동 합니다.

3. 서버 재구동 후 프로토콜 활성화를 확인 합니다.

-확인 명령어 (:443 외 다른 포트번호를 기입해도 됩니다. [SSL 적용 포트])

openssl s_client -connect [해당 IP 및 도메인]:443 -ssl3 -- sslv3 프로토콜 통신 확인

openssl s_client -connect [해당 IP 및 도메인]:443 –ssl2 -- sslv2 프로토콜 통신 확인

openssl s_client -connect [해당 IP 및 도메인]:443 –tls1 -- tls1.0 프로토콜 통신 확인

openssl s_client -connect [해당 IP 및 도메인]:443 –tls1_1 -- tls1.1 프로토콜 통신 확인

openssl s_client -connect [해당 IP 및 도메인]:443 –ssl2 --sslv2 프로토콜 통신 확인

```
C:₩Users₩ucert>openssl s_client -connect 192.168.0.85:4430 -ssl2
Loading 'screen' into random state - done
CONNECTED(000000E0)
6124:error:1407F0E5:SSL routines:SSL2_WRITE:ssl handshake failure:.₩ssl₩s2_pkt.c:429:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 48 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv2
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1427098342
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

openssl s_client -connect [해당 IP 및 도메인]:443 -ssl3 -- sslv3 프로토콜 통신 확인

```
C:₩Users₩ucert>openssl s_client -connect 192.168.0.85:4430 -ssl3
Loading 'screen' into random state - done
CONNECTED(000000E0)
3172:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:.₩ssl₩s3_pkt.c:615:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1427098422
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

openssl s_client -connect [해당 IP 및 도메인]:443 –tls1 --tls1.0 프로토콜 통신 확인

```
---
SSL handshake has read 4498 bytes and written 481 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES256-SHA
    Session-ID: A9048DF7D2A3CA5ACAB44072CC6A51324E18E88A9191BB602922744CB1B3E246
    Session-ID-ctx:
    Master-Key: 400E0FBBE053AEEE917155291764E0EFC5AA349481B44120C4651D46BBD3954D3CB90F323D6311ECFFD3A6ACF112B532
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1480034443
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

openssl s_client -connect [해당 IP 및 도메인]:443 –tls1.1 --tls1.1 프로토콜 통신 확인

```
---
SSL handshake has read 4514 bytes and written 497 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.1
    Cipher    : AES256-SHA
    Session-ID: 843931BDAA3B404C8602DC8446906689FBB06F99FFE4580C56E71ADAA1F3EB06
    Session-ID-ctx:
    Master-Key: 096694E257C05213037AE045E500C85AA9EC400A4AF3EF9404661CE458E224FDB3F8CF6F4B9AF57687AB3F05BE1F53A6
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1480034475
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```