

IHS SSL 프로토콜 설정 가이드

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

[고객센터]

한국기업보안. 유서트 기술팀

02-512-5495



1. IHS SSL Protocol 및 cipher 설정

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

- 아래값은 샘플 값입니다.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 4430
<VirtualHost *:4430>
SSLEnable
SSLProtocolDisable SSLv2 SSLv3
SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA
SSLCipherSpec SSL_RSA_WITH_RC4_128_SHA
SSLCipherSpec SSL_RSA_WITH_DES_CBC_SHA

</VirtualHost>
KeyFile /opt/IBM/HTTPServer/conf/test.co.kr.kdb
SSLDisable
# End of example SSL configuration
```

SSLEnable

SSLProtocolDisable SSLv2 SSLv3

SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA

SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA

SSLCipherSpec SSL_RSA_WITH_RC4_128_SHA

SSLCipherSpec SSL_RSA_WITH_DES_CBC_SHA

2. IHS 를 재기동 합니다.

3. 서버 재구동 후 프로토콜 활성화를 확인 합니다.

-확인 명령어

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 --ssl2 프로토콜 통신 확인

```
C:\Users\Wucert>openssl s_client -connect 192.168.0.85:4430 -ssl2
Loading 'screen' into random state - done
CONNECTED(00000000)
6124:error:1407F0E5:SSL routines:SSL2_WRITE:ssl handshake failure:.WsslWs2_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 --ssl3 프로토콜 통신 확인

```
C:\Users\Wucert>openssl s_client -connect 192.168.0.85:4430 -ssl3
Loading 'screen' into random state - done
CONNECTED(00000000)
3172:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:.WsslWs3_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)
---
```



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

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

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

```
---
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: 400E0FB8E053AE0EE917155291764E0EFC5AA349481B44120C4651D466B03954D3CB90F323D6311ECFFD3A6ACF112B532
    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)
---
```



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

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.