

Lighttpd

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. SSL 설정구문 내에 내용을 추가합니다.(SSLProtocol)

모든 버전을 사용하지 않고, TLSv1.2 만 사용(권장)

```
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-all, TLSv1.2",  
                           "Options" => "-ServerPreference")
```

설정 예시 :

```
server.modules += ( "mod_openssl" )  
$SERVER["socket"] = ":::::443" {  
    ssl.engine           = "enable"  
    ssl.privkey          = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/KeyFile_sslinstall.ucert.co.kr crt.key"  
    ssl.pemfile          = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/File_sslinstall.ucert.co.kr crt.crt"  
    ssl.openssl.ssl-conf-cmd = ("Protocol" => "-all, TLSv1.2",  
                               "Options" => "-ServerPreference")  
}
```

가능한 모든 버전을 사용하되 SSLv2, SSLv3, TLSv1.0, TLSv1.1 버전은 사용하지 않음.

```
ssl.openssl.ssl-conf-cmd = ("Protocol" => "all, -SSLv2, -SSLv3, -TLSv1, -TLSv1.1",  
                           "Options" => "-ServerPreference")
```

설정 예시 :

```
server.modules += ( "mod_openssl" )  
$SERVER["socket"] = ":::::443" {  
    ssl.engine           = "enable"  
    ssl.privkey          = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/KeyFile_sslinstall.ucert.co.kr crt.key"  
    ssl.pemfile          = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/File_sslinstall.ucert.co.kr crt.crt"  
    ssl.openssl.ssl-conf-cmd = ("Protocol" => "all, -SSLv2, -SSLv3, -TLSv1, -TLSv1.1",  
                               "Options" => "-ServerPreference")  
}
```

2. SSL 설정구문 내에 내용을 추가합니다. (SSLCipherSuite)

ssl.openssl.ssl-conf-cmd 설정 내부에 추가합니다.

설정 내용은 Lighttpd 공식 보안 설정 가이드 내용을 기반으로 합니다.

권장 알고리즘 사용(권장)

해당 설정 시 구버전 브라우저 호환성 이슈 가능성 있습니다.

"CipherString" => "EECDH+AESGCM:AES256+EECDH:CHACHA20:!SHA1:!SHA256:!SHA384"

설정 예시 :

```
server.modules += ( "mod_openssl" )
$SERVER["socket"] == "ssl:443" {
    ssl.engine           = "enable"
    ssl.privkey           = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/KeyFile_sslinstall.ucert.co.kr crt.key"
    ssl.pemfile           = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/File_sslinstall.ucert.co.kr crt.crt"

    ssl.openssl.ssl-conf-cmd = ( "Protocol" => "all, -SSLv2, -SSLv3, -TLSv1, -TLSv1.1",
                                "Options"  => "-ServerPreference",
                                "CipherString" => "EECDH+AESGCM:AES256+EECDH:CHACHA20:!SHA1:!SHA256:!SHA384" )
}
```

범용 알고리즘 사용

TLSv1.0, TLSv1.1 알고리즘까지 지원되어 보안 상 취약점으로 작용할 수 있습니다.

"CipherString" => "EECDH+AESGCM:AES256+EECDH:CHACHA20"

설정 예시 :

```
server.modules += ( "mod_openssl" )
$SERVER["socket"] == "ssl:443" {
    ssl.engine           = "enable"
    ssl.privkey           = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/KeyFile_sslinstall.ucert.co.kr crt.key"
    ssl.pemfile           = "/etc/lighttpd/ssl/sslinstall.ucert.co.kr crt/File_sslinstall.ucert.co.kr crt.crt"

    ssl.openssl.ssl-conf-cmd = ( "Protocol" => "all, -SSLv2, -SSLv3, -TLSv1, -TLSv1.1",
                                "Options"  => "-ServerPreference",
                                "CipherString" => "EECDH+AESGCM:AES256+EECDH:CHACHA20" )
}
```