Increasing FortiVoice Enterprise Encryption Level

This article examines how to increase your FVE encryption level on release 5.0.4 and above.

What does strong encryption do?

Enabling the use of strong encryption will:

- disable deprecated SSL versions: SSLv2, SSL v3
- enable TLS 1.0, 1.1, and 1.2 by default (you may choose to enable any of the TLS versions by using the ssl-versions CLI command. See below.)
- disable weak encryption and hash algorithm and only enable AES and SHA/SHA256
- generate key length of at least 128 bits
- provide HTTPS administration access
- support SIP over TLS.

How to enable strong encryption

To enable Strong Encryption, run the following CLI command:

```
config system global
        set strong-crypto enable
        end
```

To disable Strong Encryption, run the following CLI command:

```
config sys global
        set strong-crypto disable
        end
```

The default setting for strong-crypto is disabled.

To set SSL versions, run the following CLI command:

```
config system global
        set ssl-versions {ssl3|tls1_0|tls1_1|tls1_2}
        end
```

Note that when strong encryption is enabled, you cannot set SSL versions and

“system sip-setting/tls-client-protocol” to SSLv3, and vice versa.

Accepted ciphers with strong encryption enabled

Protocol	Key length	Cipher
TLSv1	**256 bits**	**ECDHE-RSA-AES256-SHA**
TLSv1	**256 bits**	**DHE-RSA-AES256-SHA**
TLSv1	**256 bits**	**AES256-SHA**
TLSv1	**128 bits**	**ECDHE-RSA-AES128-SHA**
TLSv1	**128 bits**	**DHE-RSA-AES128-SHA**
TLSv1	**128 bits**	**AES128-SHA**
TLS11	**256 bits**	**ECDHE-RSA-AES256-SHA**
TLS11	**256 bits**	**DHE-RSA-AES256-SHA**
TLS11	**256 bits**	**AES256-SHA**

TLS11	**128 bits**	**ECDHE-RSA-AES128-SHA**
TLS11	**128 bits**	**DHE-RSA-AES128-SHA**
TLS11	**128 bits**	**AES128-SHA**
TLS12	**256 bits**	**ECDHE-RSA-AES256-SHA**
TLS12	**256 bits**	**DHE-RSA-AES256-SHA256**
TLS12	**256 bits**	**DHE-RSA-AES256-SHA**
TLS12	**256 bits**	**AES256-SHA256**
TLS12	**256 bits**	**AES256-SHA**
TLS12	**128 bits**	**ECDHE-RSA-AES128-SHA**
TLS12	**128 bits**	**DHE-RSA-AES128-SHA256**

TLS12	**128 bits**	**DHE-RSA-AES128-SHA**
TLS12	**128 bits**	**AES128-SHA256**
TLS12	**128 bits**	**AES128-SHA**