Strength-Details für SSL-Chips

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die SSL-Chiffren anzeigen, die zur Verwendung und Unterstützung auf der Cisco E-Mail Security Appliance (ESA) verfügbar sind.

Strength-Details für SSL-Chips

Die SSL-Chiffren, die zur Verwendung und Unterstützung verfügbar sind, können jederzeit durch Ausführen der folgenden Aktionen in der CLI angezeigt werden: **sslconfig > überprüfen**

Wenn Sie gefragt werden "Geben Sie die SSL-Verschlüsselung ein, die Sie überprüfen möchten", klicken Sie auf Return (Zurück), um dieses Feld leer zu lassen und ALLE Verschlüsselungen anzuzeigen.

ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au = RSA	Enc=AESGCM(256)	Mac = AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(256)	Mac = AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au = RSA	Enc=AES(256)	Mac = SHA3
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac = SHA3
ECDHE-RSA-AES256-SHA	SSLv3	Kx=ECDH	Au = RSA	Enc=AES(256)	Mac = SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac = SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac = SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au = RSA	Enc=AES(256)	Mac = SHA1
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac = SHA1
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx = DH	Au=DSS	Enc=AESGCM(256)	Mac = AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx = DH	Au = RSA	Enc=AESGCM(	Mac =

				256)	AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx = DH	Au = RSA	Enc=AES(256)	Mac = SHA2
DHE-DSS-AES256-SHA256	TLSv1.2	Kx = DH	Au=DSS	Enc=AES(256)	Mac = SHA2
DHE-RSA-AES256-SHA	SSLv3	Kx = DH	Au = RSA	Enc=AES(256)	Mac = SHA1
DHE-DSS-AES256-SHA	SSLv3	Kx = DH	Au=DSS	Enc=AES(256)	Mac = SHA1
DHE-RSA-CAMELLIA256-SHA	SSLv3	Kx = DH	Au = RSA	Enc=Kamelien(256)	Mac = SHA1
DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx = DH	Au=DSS	Enc=Kamelien(256)	Mac = SHA1
AES256-GCM-SHA384	TLSv1.2	Kx = RSA	Au = RSA	Enc=AESGCM(256)	Mac = AEAD
AES256-SHA256	TLSv1.2	Kx = RSA	Au = RSA	Enc=AES(256)	Mac = SHA2
AES256-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=AES(256)	Mac = SHA1
CAMELLIA256-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=Kamelien(256)	Mac = SHA1
PSK-AES256-CBC-SHA	SSLv3	Kx = PSK	Au=PSK	Enc=AES(256)	Mac = SHA1
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au = RSA	Enc=AESGCM(128)	Mac = AEAD
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(128)	Mac = AEAD
ECDHE-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au = RSA	Enc=AES(128)	Mac = SHA2
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac = SHA2
ECDHE-RSA-AES128-SHA	SSLv3	Kx=ECDH	Au = RSA	Enc=AES(128)	Mac = SHA1
ECDHE-ECDSA-AES128-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac = SHA1
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac = SHA1
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au = RSA	Enc=AES(128)	Mac = SHA1
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac = SHA1
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx = DH	Au=DSS	Enc=AESGCM(128)	Mac = AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx = DH	Au = RSA	Enc=AESGCM(128)	Mac = AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx = DH	Au = RSA	Enc=AES(128)	Mac = SHA2
DHE-DSS-AES128-SHA256	TLSv1.2	Kx = DH	Au=DSS	Enc=AES(128)	Mac = SHA2
DHE-RSA-AES128-SHA	SSLv3	Kx = DH	Au = RSA	Enc=AES(128)	Mac = SHA1
DHE-DSS-AES128-SHA	SSLv3	Kx = DH	Au=DSS	Enc=AES(128)	Mac = SHA1

DHE-RSA-SEED-SHA	SSLv3	Kx = DH	Au = RSA	Enc=SEED(128)	Mac = SHA1
DHE-DSS-SEED-SHA	SSLv3	Kx = DH	Au=DSS	Enc=SEED(128)	Mac = SHA1
DHE-RSA-CAMELLIA128-SHA	SSLv3	Kx = DH	Au = RSA	Enc=Kamelien(128)	Mac = SHA1
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx = DH	Au=DSS	Enc=Kamelien(128)	Mac = SHA1
AES128-GCM-SHA256	TLSv1.2	Kx = RSA	Au = RSA	Enc=AESGCM(128)	Mac = AEAD
AES128-SHA256	TLSv1.2	Kx = RSA	Au = RSA	Enc=AES(128)	Mac = SHA2
AES128-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=AES(128)	Mac = SHA1
SAATGUT	SSLv3	Kx = RSA	Au = RSA	Enc=SEED(128)	Mac = SHA1
CAMELLIA128-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=Kamelien(128)	Mac = SHA1
IDEA-CBC-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=IDEA(128)	Mac = SHA1
PSK-AES128-CBC-SHA	SSLv3	Kx = PSK	Au=PSK	Enc=AES(128)	Mac = SHA1
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	Au = RSA	Enc=RC4(128)	Mac = SHA1
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=RC4(128)	Mac = SHA1
RC4-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=RC4(128)	Mac = SHA1
RC4-MD5	SSLv3	Kx = RSA	Au = RSA	Enc=RC4(128)	Mac=
PSK-RC4-SHA	SSLv3	Kx = PSK	Au=PSK	Enc=RC4(128)	Mac = SHA1
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au = RSA	Enc=3DES(168)	Mac = SHA1
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=ECDSA	Enc=3DES(168)	Mac = SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac = SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au = RSA	Enc=3DES(168)	Mac = SHA1
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac = SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx = DH	Au = RSA	Enc=3DES(168)	Mac = SHA1
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx = DH	Au=DSS	Enc=3DES(168)	Mac = SHA1
DES-CBC3-SHA	SSLv3	Kx = RSA	Au = RSA	Enc=3DES(168)	Mac = SHA1
PSK-3DES-EDE-CBC-SHA	SSLv3	Kx = PSK	Au=PSK	Enc=3DES(168)	Mac = SHA1
EDH-RSA-DES-CBC-SHA	SSLv3	Kx = DH	Au = RSA	Enc=DES(56)	Mac = SHA1
EDH-DSS-DES-CBC-SHA	SSLv3	Kx = DH	Au=DSS	Enc=DES(56)	Mac = SHA1

```
DES-CBC-SHA                    SSLv3    Kx = RSA  Au = RSA  Enc=DES(56)   Mac =
                                                                          SHA1
```

Überprüfen von TLSv1.2-Chiffren

Von der **sslconfig > überprüfen** CLI bei der Frage "TLSv1.2" verwenden, SSL Verschlüsselung zur Überprüfung:

```
Enter the ssl cipher you want to verify.
[]> TLSv1.2

ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
ADH-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=None Enc=AESGCM(256) Mac=AEAD
ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(256) Mac=SHA256
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
ADH-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=None Enc=AESGCM(128) Mac=AEAD
ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(128) Mac=SHA256
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
NULL-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=None Mac=SHA256
```

Überprüfen von SSLv3-Chiffren

Von der **sslconfig > überprüfen** CLI auf "SSLv3" klicken, wenn Sie gefragt werden, SSL Verschlüsselung zur Überprüfung:

```
Enter the ssl cipher you want to verify.
[]> SSLv3

ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
SRP-DSS-AES-256-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(256) Mac=SHA1
SRP-RSA-AES-256-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(256) Mac=SHA1
SRP-AES-256-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
```

```
PSK-AES256-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
SRP-DSS-AES-128-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(128) Mac=SHA1
SRP-RSA-AES-128-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(128) Mac=SHA1
SRP-AES-128-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
DHE-RSA-SEED-SHA SSLv3 Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1
DHE-DSS-SEED-SHA SSLv3 Kx=DH Au=DSS Enc=SEED(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
ADH-SEED-SHA SSLv3 Kx=DH Au=None Enc=SEED(128) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
PSK-AES128-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA1
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=3DES(168) Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=3DES(168) Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=3DES(168) Mac=SHA1
SRP-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
PSK-3DES-EDE-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
ADH-DES-CBC-SHA SSLv3 Kx=DH Au=None Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
EXP-EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH(512) Au=DSS Enc=DES(40) Mac=SHA1 export
EXP-ADH-DES-CBC-SHA SSLv3 Kx=DH(512) Au=None Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA SSLv3 Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
ECDHE-RSA-NULL-SHA SSLv3 Kx=ECDH Au=RSA Enc=None Mac=SHA1
ECDHE-ECDSA-NULL-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=None Mac=SHA1
NULL-SHA SSLv3 Kx=RSA Au=RSA Enc=None Mac=SHA1
NULL-MD5 SSLv3 Kx=RSA Au=RSA Enc=None Mac=MD5
```

Überprüfen von niedrigen Chiffren

Verwenden Sie im Menü **sslconfig >** CLI **überprüfen** die Option LOW, wenn Sie gefragt werden, welche SSL-Verschlüsselung überprüft werden soll:

```
Enter the ssl cipher you want to verify.
[]> LOW

EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56) Mac=SHA1
```

```
ADH-DES-CBC-SHA SSLv3 Kx=DH Au=None Enc=DES(56) Mac=SHA1
DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
```

Überprüfen von mittleren Chiffern

Von der **sslconfig > überprüfen** Wählen Sie im CLI-Menü die Option "MEDIUM" aus, wenn Sie gefragt werden, welcher SSL-Verschlüsseler Sie überprüfen soll:

```
Enter the ssl cipher you want to verify.
[]> MEDIUM

DHE-RSA-SEED-SHA SSLv3 Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1
DHE-DSS-SEED-SHA SSLv3 Kx=DH Au=DSS Enc=SEED(128) Mac=SHA1
ADH-SEED-SHA SSLv3 Kx=DH Au=None Enc=SEED(128) Mac=SHA1
SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1
IDEA-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=IDEA(128) Mac=SHA1
IDEA-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=IDEA(128) Mac=MD5
RC2-CBC-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-MD5 SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
```

Überprüfen von hohen Chiffren

Von der **sslconfig > überprüfen** Wählen Sie im CLI-Menü die Option "HIGH" aus, wenn Sie gefragt werden, welcher SSL-Verschlüsseler Sie überprüfen soll:

```
Enter the ssl cipher you want to verify.
[]> HIGH

ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES256-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
SRP-DSS-AES-256-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(256) Mac=SHA1
SRP-RSA-AES-256-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(256) Mac=SHA1
SRP-AES-256-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
ADH-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=None Enc=AESGCM(256) Mac=AEAD
ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(256) Mac=SHA256
ADH-AES256-SHA SSLv3 Kx=DH Au=None Enc=AES(256) Mac=SHA1
ADH-CAMELLIA256-SHA SSLv3 Kx=DH Au=None Enc=Camellia(256) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
```

```
PSK-AES256-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES128-SHA SSLv3 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
SRP-DSS-AES-128-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=AES(128) Mac=SHA1
SRP-RSA-AES-128-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(128) Mac=SHA1
SRP-AES-128-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
ADH-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=None Enc=AESGCM(128) Mac=AEAD
ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(128) Mac=SHA256
ADH-AES128-SHA SSLv3 Kx=DH Au=None Enc=AES(128) Mac=SHA1
ADH-CAMELLIA128-SHA SSLv3 Kx=DH Au=None Enc=Camellia(128) Mac=SHA1
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1
PSK-AES128-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=3DES(168) Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=DSS Enc=3DES(168) Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=3DES(168) Mac=SHA1
SRP-3DES-EDE-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA SSLv3 Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA SSLv3 Kx=DH Au=DSS Enc=3DES(168) Mac=SHA1
ADH-DES-CBC3-SHA SSLv3 Kx=DH Au=None Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-MD5 SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5
PSK-3DES-EDE-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=3DES(168) Mac=SHA1
```

Zugehörige Informationen

- Verhindern von Verhandlungen für Null- oder Anonyme Chiffren auf der ESA und SMA
- Ändern der mit SSL/TLS auf der ESA verwendeten Methoden und Chiffren