

SSL 암호 강도 세부 정보

목차

[소개](#)

[SSL 암호 강도 세부 정보](#)

[TLSv1.2 암호를 확인하는 방법](#)

[SSLv3 암호를 확인하는 방법](#)

[낮은 암호를 확인하는 방법](#)

[중간 암호를 확인하는 방법](#)

[높은 암호를 확인하는 방법](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 사용 가능하며 지원되는 SSL 암호를 보는 방법에 대해 설명합니다.

SSL 암호 강도 세부 정보

사용 가능하며 지원되는 SSL 암호는 CLI에서 다음을 실행하여 언제든지 확인할 수 있습니다
`.sslconfig > 확인`

"Enter the ssl cipher you want to verify(확인하려는 SSL 암호 입력)"라는 메시지가 나타나면 return 키를 눌러 이 필드를 비워 두고 모든 암호를 표시합니다.

ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(256)	Mac=D
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	AU=ECDSA	Enc=AESGCM(256)	Mac=D
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=84
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	AU=ECDSA	Enc=AES(256)	Mac=84
ECDHE-RSA-AES256-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=
ECDHE-ECDSA-AES256-SHA	SSLv3	Kx=ECDH	AU=ECDSA	Enc=AES(256)	Mac=
SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)	Mac=
SRP-RSA-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(256)	Mac=
SRP-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(256)	Mac=
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=D
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=D
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=56
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=56

DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(256)	Mac=
DHE-DSS-AES256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(256)	Mac=
DHE-RSA-CAMELOPE256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=동백(256)	Mac=
DHE-DSS-CAMELOPE256-SHA	SSLv3	Kx=DH	Au=DSS	Enc=동백(256)	Mac=
AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=D
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=56
AES256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=
카멜리아256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=동백(256)	Mac=
PSK-AES256-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(256)	Mac=
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(128)	Mac=D
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	AU=ECDSA	Enc=AESGCM(128)	Mac=D
ECDHE-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=56
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	AU=ECDSA	Enc=AES(128)	Mac=56
ECDHE-RSA-AES128-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=
ECDHE-ECDSA-AES128-SHA	SSLv3	Kx=ECDH	AU=ECDSA	Enc=AES(128)	Mac=
SRP-DSS-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(128)	Mac=
SRP-RSA-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=AES(128)	Mac=
SRP-AES-128-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=AES(128)	Mac=
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=D
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=D
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=56
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=56
DHE-RSA-AES128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=AES(128)	Mac=
DHE-DSS-AES128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=AES(128)	Mac=
DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)	Mac=)
DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)	Mac=)
DHE-RSA-CAMELOPE128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=동백(128)	Mac=
DHE-DSS-CAMELOPE128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=동백(128)	Mac=
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=D
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=56
AES128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=
시드-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=)
카멜리아128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=동백(128)	Mac=
아이디어-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=IDEA(128)	Mac=
PSK-AES128-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=AES(128)	Mac=
ECDHE-RSA-RC4-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=RC4(128)	Mac=
ECDHE-ECDSA-RC4-SHA	SSLv3	Kx=ECDH	AU=ECDSA	Enc=RC4(128)	Mac=

RC4-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=
RC4-MD5	SSLv3	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=
PSK-RC4-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=RC4(128)	Mac=
ECDHE-RSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	Au=RSA	Enc=3DES(168)	Mac=
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	Kx=ECDH	AU=ECD SA	Enc=3DES(168)	Mac=
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=3DES(168)	Mac=
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=RSA	Enc=3DES(168)	Mac=
SRP-3DES-EDE-CBC-SHA	SSLv3	Kx=SRP	Au=SRP	Enc=3DES(168)	Mac=
EDH-RSA-DES-CBC3-SHA	SSLv3	Kx=DH	Au=RSA	Enc=3DES(168)	Mac=
EDH-DSS-DES-CBC3-SHA	SSLv3	Kx=DH	Au=DSS	Enc=3DES(168)	Mac=
DES-CBC3-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=3DES(168)	Mac=
PSK-3DES-EDE-CBC-SHA	SSLv3	Kx=PSK	Au=PSK	Enc=3DES(168)	Mac=
EDH-RSA-DES-CBC-SHA	SSLv3	Kx=DH	Au=RSA	Enc=DES(56)	Mac=
EDH-DSS-DES-CBC-SHA	SSLv3	Kx=DH	Au=DSS	Enc=DES(56)	Mac=
DES-CBC-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=DES(56)	Mac=

TLSv1.2 암호를 확인하는 방법

에서 `sslconfig > 확인` CLI 메뉴에서 "TLSv1.2"를 사용할 수 있는 항목을 SSL 확인할 암호:

```
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

SSLv3 암호를 확인하는 방법

에서 `sslconfig > 확인` CLI 메뉴에서 "SSLv3"을 사용할 때 SSL 확인할 암호:

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
```

낮은 암호를 확인하는 방법

sslconfig > verify CLI 메뉴에서 확인할 SSL 암호를 묻는 메시지가 나타나면 "LOW"를 사용합니다.

```
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
```

중간 암호를 확인하는 방법

에서 sslconfig > 확인 확인할 SSL 암호를 묻는 메시지가 나타나면 CLI 메뉴에서 "MEDIUM"을 사용합니다.

```
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
```

높은 암호를 확인하는 방법

에서 sslconfig > 확인 확인할 SSL 암호를 묻는 메시지가 나타나면 CLI 메뉴에서 "HIGH"를 사용합니다.

```
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

관련 정보

- ESA 및 SMA에서 Null 또는 익명 압호에 대한 협상 방지
- ESA에서 SSL/TLS와 함께 사용되는 방법 및 압호 변경