

SSL密码器优点详细信息

目录

[简介](#)

[SSL密码器优点详细信息](#)

[如何验证TLSv1.2密码器](#)

[如何验证SSLv3密码器](#)

[如何验证低密码器](#)

[如何验证中等密码器](#)

[如何验证高密码器](#)

[相关信息](#)

简介

本文描述如何查看是可用的为使用并且思科电子邮件安全工具的SSL密码器(ESA)支持。

SSL密码器优点详细信息

是可用为使用的SSL密码器和支持能通过运行以下在任何时间看到从CLI：`sslconfig >验证`

当被提示的“回车您要验证”的ssl密码器，请按下返回留出此字段空白和显示所有密码器。

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-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(Mac=

DHE-DSS-CAMELLIA256-SHA	SSLv3	Kx=DH	Au=DSS	256) Enc=Camellia(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=
CAMELLIA256-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(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-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=RSA	Enc=Camellia(128)	Mac=
DHE-DSS-CAMELLIA128-SHA	SSLv3	Kx=DH	Au=DSS	Enc=Camellia(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=
SEED-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=SEED(128)	Mac=)
CAMELLIA128-SHA	SSLv3	Kx=RSA	Au=RSA	Enc=Camellia(128)	Mac=
IDEA-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=ECDSA	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=

如何验证TLSv1.2密码器

从sslconfig >config CLI菜单，请使用"TLSv1.2"，当询问验证的SSL密码器：

```
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
```

如何验证SSLv3密码器

从sslconfig >config CLI菜单，请使用"SSLv3"，当询问验证的SSL密码器：

```
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
```

如何验证低密码器

从`sslconfig >config` CLI菜单，请使用“LOW”，当询问验证的SSL密码器：

```
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
```

如何验证中等密码器

从`sslconfig >config` CLI菜单，请使用“介质”，当询问验证的SSL密码器：

```
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
```

如何验证高密码器

从`sslconfig >config` CLI菜单，请使用“HIGH”，当询问验证的SSL密码器：

```
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

相关信息

- [防止空或匿名密码器的协商在ESA和SMA](#)
- [修改方法和密码器与在ESA的SSL/TLS一起使用](#)