

# رؤآت م و 3.3 ISE ف ر ف ش ت ت لك ش

## ت ا و ت ح م ل ا

[ق م د ق م ل ا](#)

[ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[م د خ ت س م ل ا ن و ك م ل ا](#)

[ق م و ع د م ل ا ر ي ف ش ت ل ا ت ا ع و م ح م](#)

## ق م د ق م ل ا

ق م د خ ي ف د ع ب ا م ي ف و 3.3 ISE ب ل م ع ت س ي ف ل ت خ م ق ر ف ش ل ل ا ل د ع ي ن ا ف ي ك ق ي ث و ا ذ ه ف ص ي ق م ل ا ا ذ ه ل ع ق ر ط ي س ل ل ا ل م ع ت س م ك ل ل ذ ل ف ل ت خ م .

## ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

### ت ا ب ل ط ت م ل ا

د ن ت س م ل ا ا ذ ه ل ق ص ا خ ت ا ب ل ط ت م د ج و ت ال .

### م د خ ت س م ل ا ن و ك م ل ا

ق ي ل ا ت ل ل ا ق ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ل ا د ن ت س م ل ا ا ذ ه ي ف ق ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت :

- Cisco ن م 3.3 ر ا د ص ا ل ا ISE .

ق ص ا خ ق ي ل م ع م ق ي ب ي ف ق د و ج و م ل ا ق ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ق ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت ت ن ا ك ا ذ ا . ( ي ض ا ر ت ف ا ) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ق م د خ ت س م ل ا ق ز ه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش .

## ق م و ع د م ل ا ر ي ف ش ت ل ا ت ا ع و م ح م

TLS ن م 1.0 و 1.1 و 1.2 ت ا ر ا د ص ا ل ا Cisco ISE م ع د ي .

ل و و س م ل ل (GUI) ق ي م و س ر ل ا م د خ ت س م ل ا ق ه ج ا و ل TLS 1.3 م ي د ق ت م ت ، Cisco ISE ن م 3.3 ر ا د ص ا ل ا ن م ف : 1.3 TL ر ب ع HTTPS ل و و س م ل ل ل و و س و ل ر ي ف ش ت ل ا ه ذ ه م ع د م ت ي . ط ق ف :

- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256

ق م و ع د م ق ي و ا ض ي ب ل ل ت ا ي ن ح ن م ل ا ه ذ ه RSA و ECDSA م د ا خ ت ا د ا ه ش Cisco ISE م ع د ي :

- secp256r1
- SECP384r1
- SECP521r1

ةوموعدملا ريفش تاللا تاومجم لودجلا اذه درسي

ةرفش	EAP/DTLS RADIUS ةقداصم	أو HTTPS نم CRL لي زنت LDAP/Syslog لاصتا نم آلا/DTLS CoA
ecdhe-ecdsa-aes256-gcm-sha384	TLS 1.1 ب حامسلا دنع ،معن	TLS 1.1 ب حامسلا دنع ،معن
ecdhe-ecdsa-aes128-gcm-sha256	TLS 1.1 ب حامسلا دنع ،معن	TLS 1.1 ب حامسلا دنع ،معن
ECDHE-ECDSA-AES256-SHA384	TLS 1.1 ب حامسلا دنع ،معن	TLS 1.1 ب حامسلا دنع ،معن
ecdhe-ecdsa-aes128-sha256	TLS 1.1 ب حامسلا دنع ،معن	TLS 1.1 ب حامسلا دنع ،معن
ECDHE-ECDSA-AES256-SHA	SHA-1 حمسي ام دنع ،معن	SHA-1 حمسي ام دنع ،معن
ECDHE-ECDSA-AES128-SHA	SHA-1 حمسي ام دنع ،معن	SHA-1 حمسي ام دنع ،معن
ecdhe-rsa-aes256-gcm-sha384	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت
ECDHE-RSA-AES128-GCM-SHA256	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت
ECDHE-RSA-AES256-SHA384	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت
ECDHE-RSA-AES128-SHA256	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت	مادختساب حامسلا دنع ،معن ECDHE-RSA ةينقت

ECDHE-RSA-AES256-SHA	مادختساب حامسلا دن ع ،معن ECDHE-RSA/SHA-1.	مادختساب حامسلا دن ع ،معن ECDHE-RSA/SHA-1.
ECDHE-RSA-AES128-SHA	مادختساب حامسلا دن ع ،معن ECDHE-RSA/SHA-1.	مادختساب حامسلا دن ع ،معن ECDHE-RSA/SHA-1.
DHE-RSA-AES256-SHA256	ال	معن
DHE-RSA-AES128-SHA256	ال	معن
DHE-RSA-AES256-SHA	ال	SHA-1 حمسي ام دن ع ،معن
DHE-RSA-AES128-SHA	ال	SHA-1 حمسي ام دن ع ،معن
AES256-SHA256 زارطال	معن	معن
AES128-SHA256 زارطال	معن	معن
AES256-SHA زارطال	SHA-1 حمسي ام دن ع ،معن	SHA-1 حمسي ام دن ع ،معن
AES128-SHA زارطال	SHA-1 حمسي ام دن ع ،معن	SHA-1 حمسي ام دن ع ،معن
DES-CBC3-SHA	ب حامسلا دن ع ،معن 3DES/SHA-1.	ب حامسلا دن ع ،معن 3DES/SHA-1.
DHE-DSS-AES256-SHA	ال	و 3DES/DSS ني كمت دن ع ،معن SHA-1.
DHE-DSS-AES128-SHA	ال	و 3DES/DSS ني كمت دن ع ،معن SHA-1.
EDH-DSS-DES-CBC3-SHA	ال	و 3DES/DSS ني كمت دن ع ،معن SHA-1.
واش-4 يميلق ال انواعتال	رايخ ني كمت متي ام دن ع ة في عضلا ةرفشلاب حامسلا تال و كوت و ربلال ةحفص ي ف	ال

	م تي ام دن ع و اه ب حوم س م ل ا SHA-1. ة ر ف ش ب ح ا م س ل ا	
RC4-MD5	رايخ ني ك م ت م تي ام دن ع ة في ع ض ل ا ة ر ف ش ل ا ب ح ا م س ل ا ت ا ل و ك و ت و ر ب ل ا ة ح ف ص ي ف م تي ام دن ع و اه ب حوم س م ل ا SHA-1. ة ر ف ش ب ح ا م س ل ا	ال
طوق ف ل و ه ج م ل ا AP-FAST داد م ا ADH-AES-128-SHA	م ع ن	ال
ح ا ت ف م ل ا م ا د خ ت س ا ن م ق ق ح ت ل ا	ة د ا ه ش ي و ت ح ت ن ا ن ك م ي KeyUsage=Key Agreement و ExtendedKeyUsage=Client Authentication ه ذ ه ل : <ul style="list-style-type: none"> <li>• ecdhe-ecdsa-aes128-gcm-sha256</li> <li>• ecdhe-ecdsa-aes256-gcm-sha384</li> <li>• ecdhe-ecdsa-aes128-sha256</li> <li>• ECDHE-ECDSA-AES256-SHA384</li> </ul>	
ة ح ص ن م ق ق ح ت ل ا ExtendedKeyUse	ل م ل ا ة د ا ه ش ي و ت ح ت ن ا ب ج ي ر ي ف ش ت =KeyUsage ة ق د ا ص م و ح ي ت ا ف م ل ا ExtendedKeyUsage=Client ة ل ل ا ت ل ا ت ا ر ف ش ل ل : <ul style="list-style-type: none"> <li>• AES256-SHA256 ز ا ر ط ل ا</li> <li>• AES128-SHA256 ز ا ر ط ل ا</li> <li>• AES256-SHA ز ا ر ط ل ا</li> <li>• AES128-SHA ز ا ر ط ل ا</li> <li>• DHE-RSA-AES128-SHA</li> </ul>	م د ا خ ل ا ة د ا ه ش ي و ت ح ت ن ا ب ج ي ل م ل ا ة ق د ا ص م =ExtendedKeyUsage م د ا خ ل ا .

## ت ا ن ي و ك ت ل ا

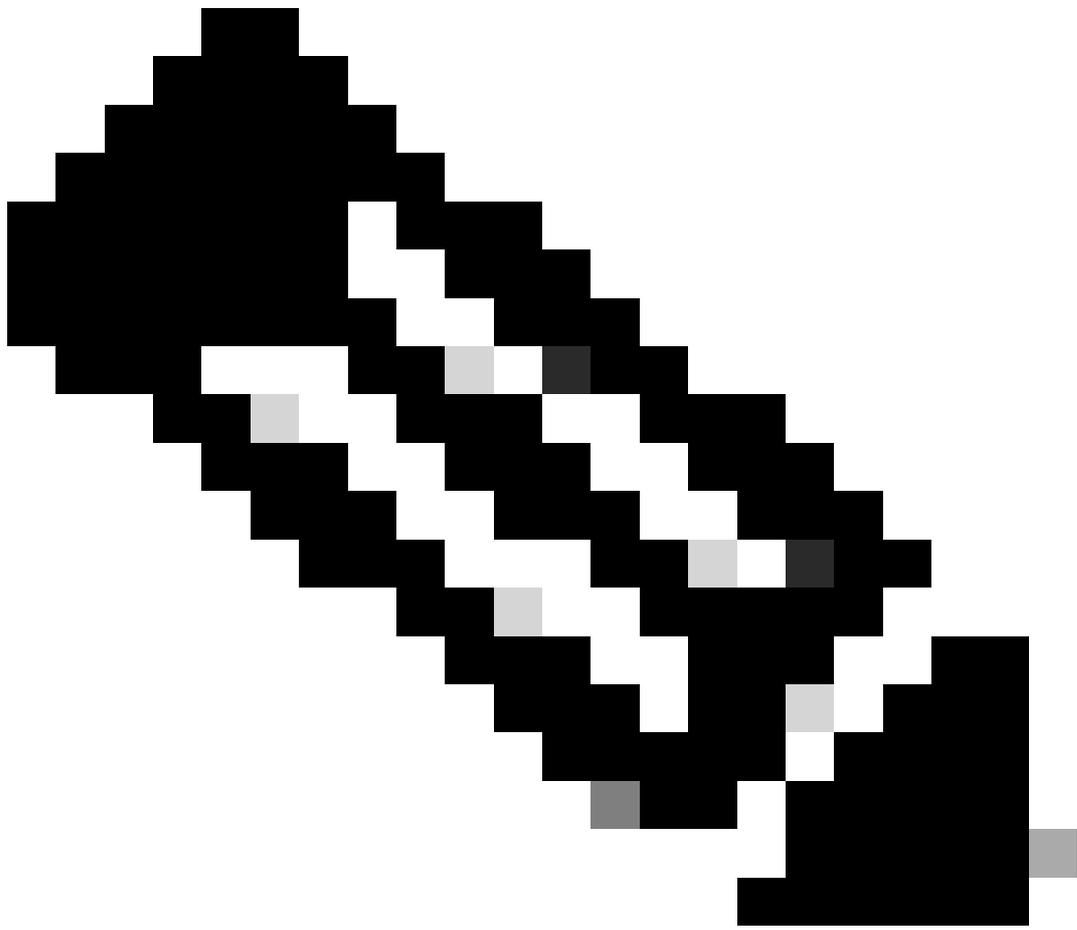
ن ي م ا ت ل ا ت ا د ا ع ا ن ي و ك ت

نېمأتلل تادادعإ نېوكتل ءارجإل اذھ ءارجإب مق



1. ءمئاقلا ءنوقئأ قوف رقنا، Cisco ISE ءيموسرلا مدختسملا ءهجاو ئف ( نېمأتلل تادادعإ>تادادعإل>مإظنل > ءرادإ رتخاو )

2. ءناخ ددح. ءئلالتملا TLS تارادصلإ نم قاطن وأ دحاو رتخأ، TLS تارادصلإ تادادعإ مسق ئف. اهنئكمت دئرت ئتلل TLS تارادصلإ ءرواوملا رايئخالل



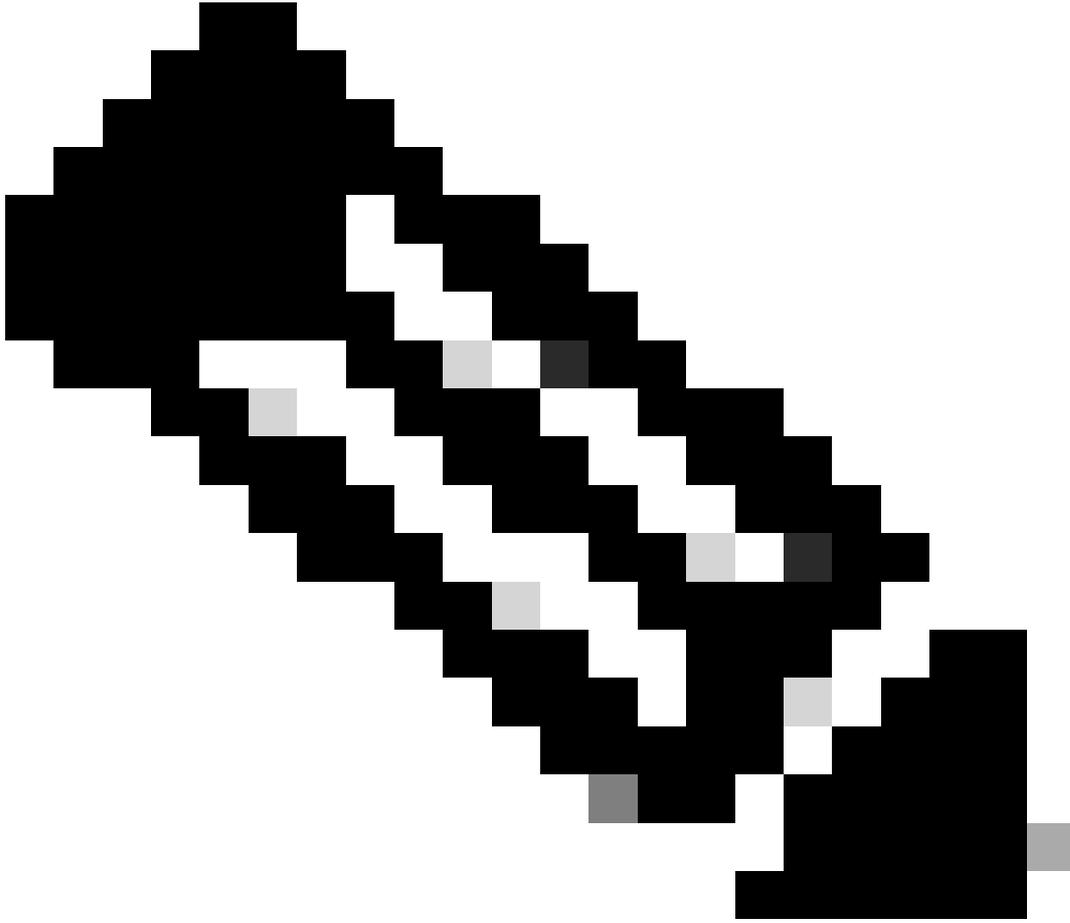
نم رثكأ ترتخأ اذإ. هلئطعت نكمئ الوئضارتفلا لكشب TLS 1.2 نئكمت متئ: ءظحال م TLS ترتخأ اذإ، لاثملا لئبس ىلع. ءئلالتم تارادصلإ رايئخالل ءئلع بئئ، TLS رادصلإ لئغشت ءءاعإ ىلإ انه تارفشملا رئئغئ دؤئ دق. ائئاقلت TLS 1.1 نئكمت متئ، 1.0، ISE.

حمسا، اضيأ. ةيلالتل تامدخ لل 1.2 و 1.1 و 1.0 TLS نيكمت : 1.2 و 1.1 و 1.0 TLS ب حامسلا  
هذه لمعل ريسل ءارظنلل عم لصاوتلاب SHA-1 ريفشتل حمسي : SHA-1 ريفشت

- ةقداصم EAP.
- مداخل نم CRL لي زنت
- يجراخل syslog مداخلو ISE ني ب نم آل Syslog لاصتا
- نم آ LDAP لي مءك ISE
- نم آ ODBC لي مءك ISE
- ERS تامدخ
- pxGrid تامدخ
- (ب ةصاخلا ةزهجال ةبوابو لي مءل دادم ةبوابو فيضلا لخدم لثم) ISE تابواب عي مء
- MDM لاصتا
- PassiveID لي ءك و لاصتا
- قءصملا عءرملا ءوزم
- لوؤسملل (GUI) ةيموسرلا مءختسملا ةءءاولا لوصولا

لاصتاللى لءال ي ةءرءملا تانوكملا ةطساوب ءفانملا هذه مءءتسا مءي:

- 443: لوؤسملا لوصولو
- تابوابل امنيوءك مء ءفانم ي أ و 8449 و 8445 و 8444 و 8443 و 9002 Cisco ISE تابواب ISE.
- 9063 و 9061 و 9060: ءءال ربياعم
- pxGrid: 8910



يصوصون. يضا رتفا لكش ب SHA-1 ةرفش ب حامسلا راخ لي طعت متي: ةظحال م  
نامألا زيزعتل SHA-384 و SHA-256 تارفش مادختساب

حامسلا راخ لي طعت وأ ني كمت دع ب رشن ةي لمع يف دقعلا ةفاك لي غشت ةداع| بجي  
تاريي غت قي بطت متي نلف، ةحجان لي غشتلا ةداع ةي لمع نكت مل اذا. SHA-1 تارفش لاب  
ني وكتلا

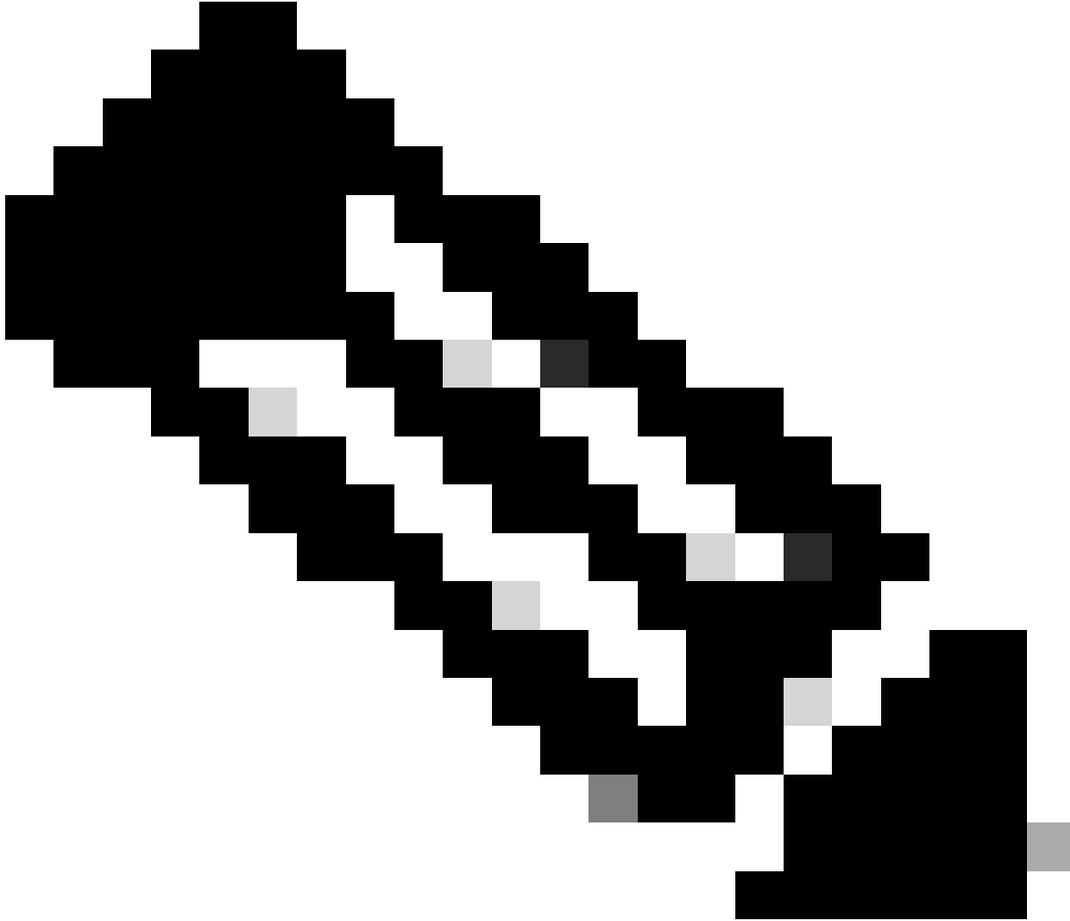
طقف SHA-1 تارفش ب دوزم لي مع لواح اذا، SHA-1 ةرفش ب حامسلا راخ لي طعت متي ام دنع  
لي معلا ضرعتسم يلع أطخ ةلاسر ةي وركنكم يو، ةحفاصملا لشف ي، Cisco ISE ب لاصتالا

ي مادقلا ءارظنلا عم ل صاوتلاب SHA-1 تارفش ل حامسلا عم تاراخلا دحأ رتخأ:

- ءارظنلا عم ل صاوتلاب SHA-1 تارفش عي معجل حامسلا: SHA-1 تارفش عي معجل حامسلا  
ي مادقلا
- ل حامسلا: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA ل طقف حامسلا  
ي مادقلا ءارظنلا عم ل صاوتلاب TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA Cipher

ل: 443 ذفنملا ربع لوصولاب HTTPS لوؤسملل TLS 1.3 حمسي: TLS 1.3 ب حامسلا

- Cisco ISE ةرادال (GUI) ةيموسرلا مدختسملا ةهجاو
- ةحوتفملا تاقيبطتلا ةجرمب ةهجاو) 443 ذفنملل تاقيبطتلا ةجرمب تاهجاو نيكمتمت (ERS، MnT).



مق TLS 1.3 دقعلا نيبتالاصتالا عاونأ عيجمو AAA تالاصتالا معدتال: ةظحالم ربع لوؤسملا لوصول ةلصللا تاذا مداوخلالو ةالمعلالو Cisco ISE ل TLS 1.3 نيكمتمب TLS 1.3.

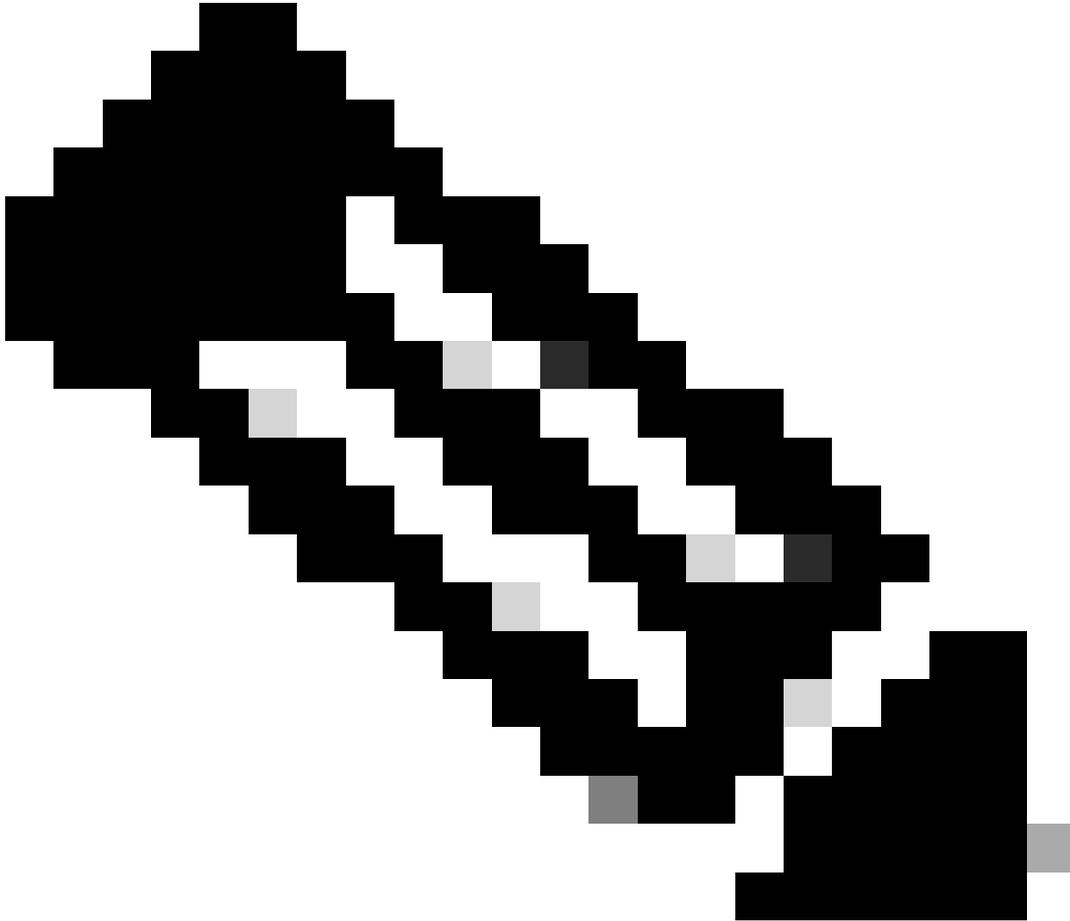
عم لصالولاب ECDHE-RSA ريفشتل حمسي: 3DES و ECDHE-RSA ريفشتب حامسلا هذه لمعلال ريسل ءارظنلا

- EAP مداخك Cisco ISE نيوكتمتي
- RADIUS DTLS مداخك Cisco ISE نيوكتمتي



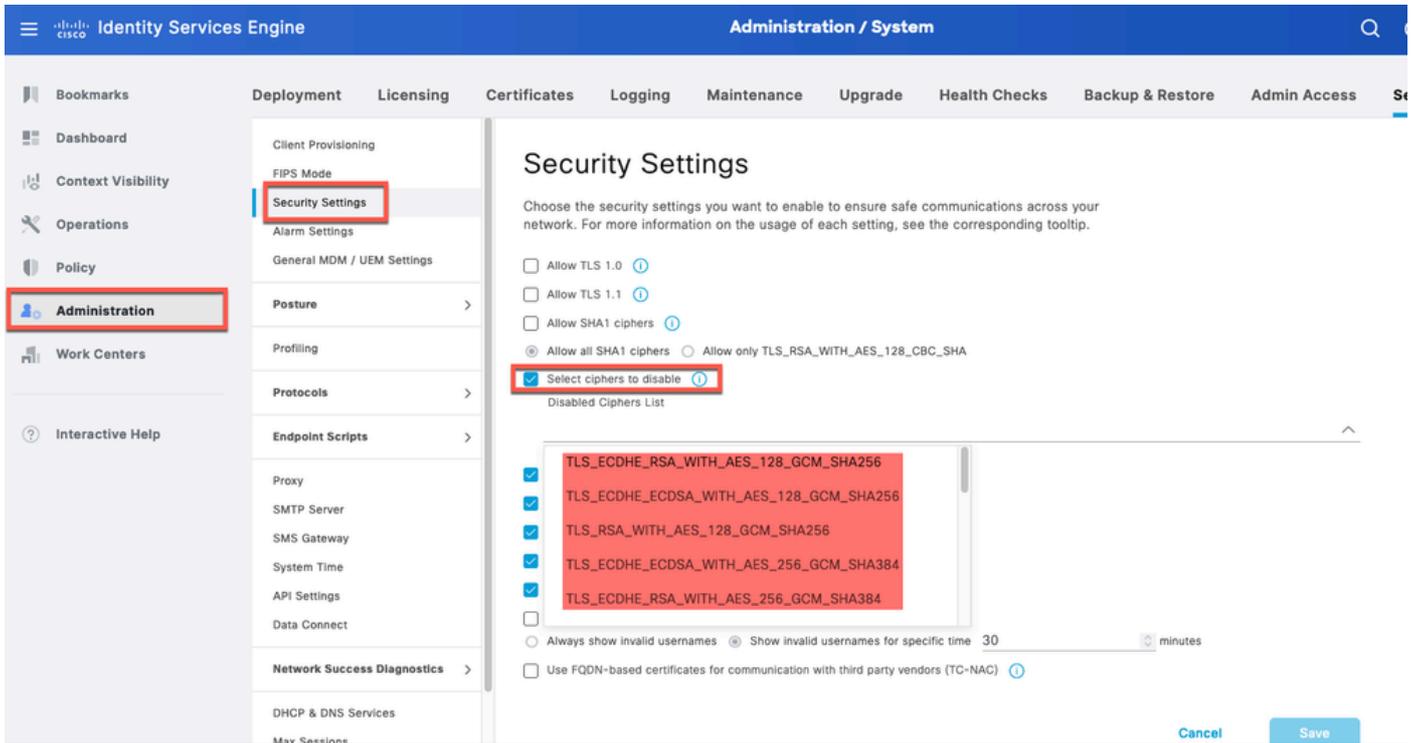
SHA1 تارفش نيكمت متيسف، SHA1 ةرفش ب حامسلا راخ نيكمت مت اذا، لاثملا لپس  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA، ب طقف حامسلا راخ ديدحت ةلاح يف. ةمئاقلا هذه يف  
ةرفش ب حامسلا راخ ليطعت مت اذا. ةمئاقلا هذه يف طقف اذ SHA1 ريفشت نيكمت متي  
اذه يف SHA1 ريفشت يا نيكمت كنكمي الف، SHA1

---



مداخ ليغشت ةداع متت، اهلطعت دارملا تارفشملا ةمئاق ريرحت دنع: ةظحالم  
ةداع متت، اهلطعت وأ FIPS عضو نيكمت دنع Cisco ISE دقع عيمج ىلع قيبتل  
نع ريبك فقوت تقوى لىل يدوى امم دقعلا عيمج ىلع تاقيبطتلا مداوخ ليغشت  
ةمئاق نيوكت راخ مادختساب ريفشت يا ليطعت ب تمق اذا. ماظنلل لمعلا  
مداوخ ليغشت ةداع دع ب لطملا ريفشتلا ةمئاق نم ققحتف، ايودي ريفشتلا  
FIPS عضو لاقتنا ب بسب لطملا ريفشتلا ةمئاق ريفشت متي ال. قيبتل

---



إرفش زجعي نأ رايخ ISE 3.3

- زربم ل، 37 رايخ ل مادخت ساو application configure ise رم أ ل لي غشت كن كم ي ISE (CLI) رم او أ رطس ة ه جاو نم م حي حصت فرعم وه ة لصل ل يذ أ طخ ل. EAP-TLS ل RSA\_PSS ل عي قوت نم /disable/current\_status ن ي كم ت. هذ ة شاش ل ة طق ل ي ف ل عا طخ ل ل Cisco [CSCwb77915](https://www.cisco.com/c/en/us/td/docs/configuration/guide/rsa_pss_eap_tls.html).

```

isedemo-33/admin#application configure ise
Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLUGINS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[0]Exit
  
```

إرفش زجعي نأ رايخ ISE 3.3 عي قوت نم /disable/current\_status ن ي كم ت ل RSA\_PSS ل عي قوت نم ل عا طخ ل ل

ة لصل ل تاذ تام ول عم

•

[Cisco نيم تاليزنت لايون فلما معدليا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا