Cijfers in ISE 3.3 en hoger configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de verschillende door ISE 3.3 gebruikte algoritmen kunt wijzigen, zodat de gebruiker controle over deze mechanismen heeft.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.3.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Ondersteunde cipher Suites

Cisco ISE ondersteunt TLS-versies 1.0,1.1 en 1.2.

Van Cisco ISE-softwarerelease 3.3 is TLS 1.3 alleen voor Admin GUI geïntroduceerd. Deze algoritmen worden ondersteund voor admin HTTPS-toegang via TL 1.3 :

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE ondersteunt RSA- en ECDSA-servercertificaten. Deze elliptische krommen worden ondersteund:

- sec256r1
- sec384r1
- sec521r1

Deze tabel geeft een overzicht van de ondersteunde Cipher Suites:

Cryptor Suite	EAP-verificatie/RADIUS DTLS	CRL-download via HTTPS of Secure LDAP/Secure Syslog-communicatie/DTLS CoA
ECDHE-ECDSA-AES256-GCM-SHA384	Ja, als TLS 1.1 is toegestaan.	Ja, als TLS 1.1 is toegestaan.
ECDHE-ECDSA-AES128-GCM-SHA256 router	Ja, als TLS 1.1 is toegestaan.	Ja, als TLS 1.1 is toegestaan.
ECDHE-ECDSA-AES256-SHA384 router	Ja, als TLS 1.1 is toegestaan.	Ja, als TLS 1.1 is toegestaan.
ECDHE-ECDSA-AES128-SHA256 router	Ja, als TLS 1.1 is toegestaan.	Ja, als TLS 1.1 is toegestaan.
ECDHE-ECDSA-AES256-SHA	Ja, als SHA-1 is toegestaan.	Ja, als SHA-1 is toegestaan.
ECDHE-ECDSA-AES128-SHA	Ja, als SHA-1 is toegestaan.	Ja, wanneer SHA-1 is toegestaan.
ECDHE-RSA-AES256-GCM-SHA384	Ja, als ECDHE-RSA is toegestaan.	Ja als ECDHE-RSA is toegestaan.
ECDHE-RSA-AES128-GCM-SHA256 router	Ja, als ECDHE-RSA is toegestaan.	Ja, als ECDHE-RSA is toegestaan.
ECDHE-RSA-AES256-SHA384 router	Ja, als ECDHE-RSA is toegestaan.	Ja, als ECDHE-RSA is toegestaan.

ECDHE-RSA-AES128-SHA256 router	Ja, als ECDHE-RSA is toegestaan.	Ja, als ECDHE-RSA is toegestaan.
ECDHE-RSA-AES256-SHA	Ja, als ECDHE-RSA/SHA-1 is toegestaan.	Ja, als ECDHE-RSA/SHA-1 is toegestaan.
ECDHE-RSA-AES128-SHA router	Ja, als ECDHE-RSA/SHA-1 is toegestaan.	Ja, als ECDHE-RSA/SHA-1 is toegestaan.
DHE-RSA-AES256-SHA256 router	Nee	Ja
DHE-RSA-AES128-SHA256 router	Nee	Ja
DHE-RSA-AES256-SHA	Nee	Ja, wanneer SHA-1 is toegestaan.
DHE-RSA-AES128-SHA	Nee	Ja, wanneer SHA-1 is toegestaan.
AES256-SHA256 router	Ja	Ja
AES128-SHA256 router	Ja	Ja
AES256-SHA switch	Ja, als SHA-1 is toegestaan.	Ja, als SHA-1 is toegestaan.
AES128-SHA switch	Ja, als SHA-1 is toegestaan.	Ja, als SHA-1 is toegestaan.
DES-CBC3-SHA	Ja, wanneer 3DES/SHA-1 is toegestaan.	Ja, wanneer 3DES/SHA-1 is toegestaan.
DHE-DS-AES256-SHA	Nee	Ja, wanneer 3DES/DS en SHA-1 zijn ingeschakeld.
DHE-DS-AES128-SHA	Nee	Ja, wanneer 3DES/DS en SHA-1 zijn ingeschakeld.

EDH-DS-DES-CBC3-SHA	Nee	Ja, wanneer 3DES/DS en SHA-1 zijn ingeschakeld.
RC4-SHA	Wanneer de optie zwakke algoritmen toestaan op de pagina Toegestane protocollen is ingeschakeld en wanneer SHA-1 is toegestaan.	Nee
RC4-MD5	Wanneer de optie zwakke algoritmen toestaan op de pagina Toegestane protocollen is ingeschakeld en wanneer SHA-1 is toegestaan.	Nee
AP-FAST anonieme levering alleen: ADH-AES-128-SHA	Ja	Nee
Belangrijke toepassingen valideren	Het clientcertificaat kan de KeyUsage=Key-overeenkomst en de ExtendedKeyUsage=Client-verificatie voor deze algoritmen hebben: • ECDHE-ECDSA-AES128-GCM-SHA256 router • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 router • ECDHE-ECDSA-AES256-SHA384 router	
Uitgebreid sleutelgebruik valideren	Clientcertificaat moet beschikken over KeyUsage=Key Encipherment en ExtendedKeyUsage=Client-verificatie voor deze algoritmen: • AES256-SHA256 router • AES128-SHA256 router • AES256-SHA switch	Servercertificaat moet ExtendedKeyUsage=Server-verificatie hebben.

	• AES128-SHA switch • DHE-RSA-AES128-SHA	

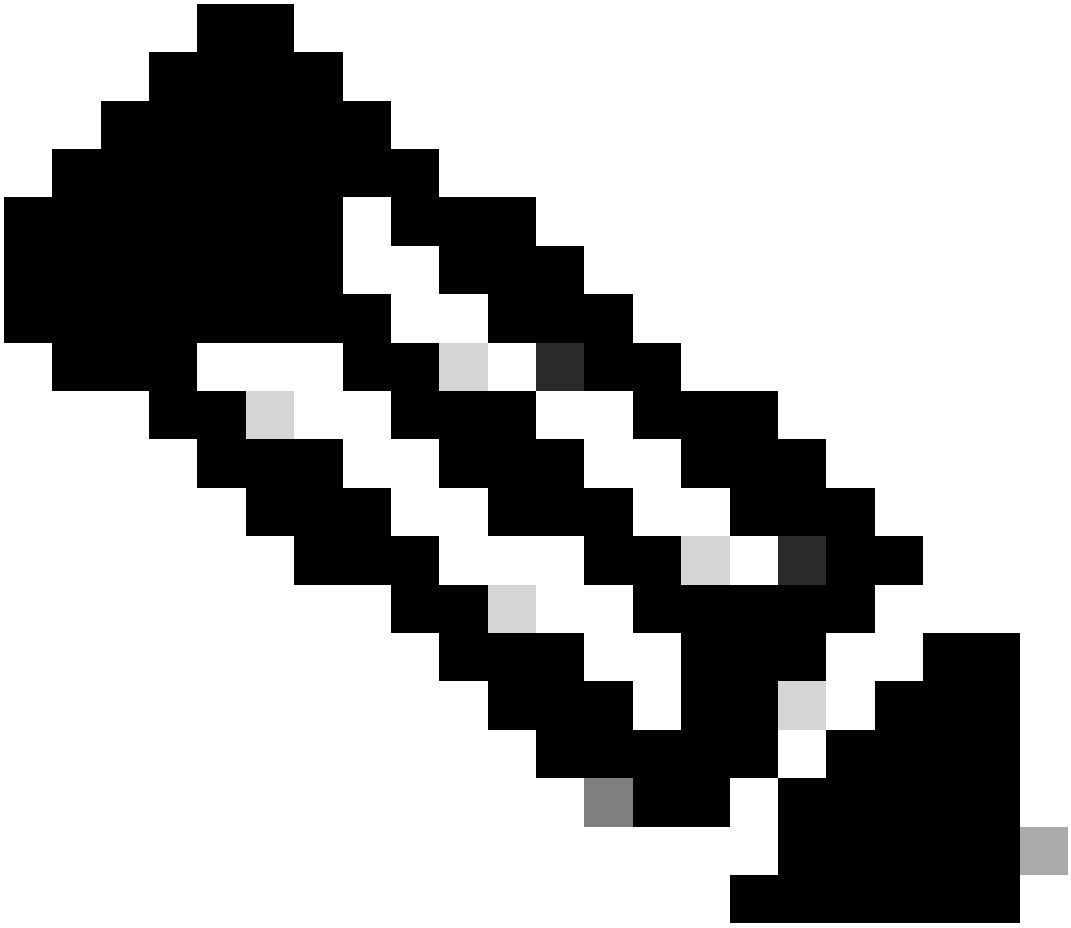
Configuraties

Beveiligingsinstellingen configureren

Voer deze procedure uit om de beveiligingsinstellingen te configureren:

1. Klik in de Cisco ISE GUI op het menupictogram () en kies Beheer > Systeem > Instellingen > Beveiligingsinstellingen.

2. Kies in het gedeelte TLS-instellingen een of een reeks opeenvolgende TLS-versies. Schakel het aankruisvakje in naast de TLS-versies die u wilt inschakelen.



Opmerking: TLS 1.2 is standaard ingeschakeld en kan niet worden uitgeschakeld. Als u meer dan één TLS-versie kiest, moet u achtereenvolgende versies kiezen. Als u bijvoorbeeld TLS 1.0 kiest, wordt TLS 1.1 automatisch ingeschakeld. Het veranderen van de algoritmen kan hier opnieuw beginnen van ISE veroorzaken.

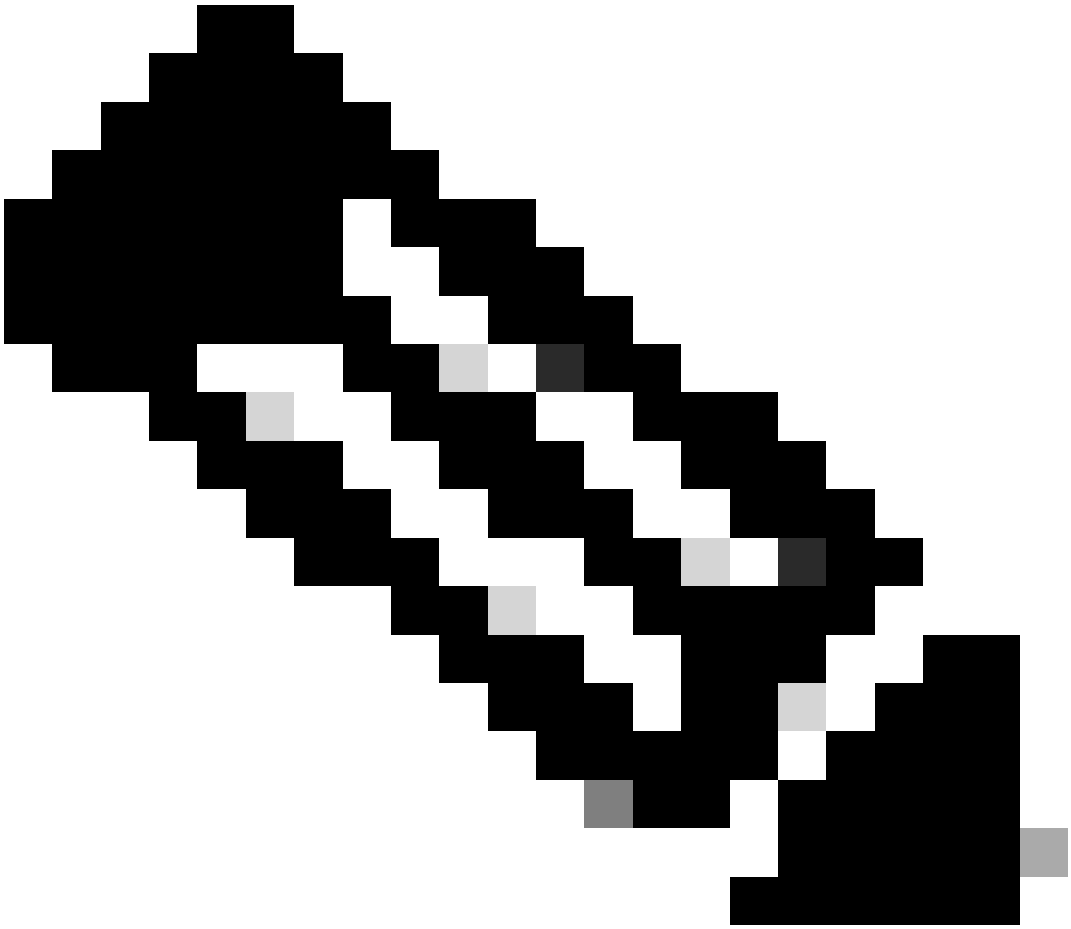
Sta TLS 1.0, 1.1 en 1.2 toe: Schakelt TLS 1.0, 1.1 en 1.2 in voor de volgende services. Laat ook SHA-1-algoritmen toe: hiermee kunnen SHA-1-algoritmen met peers communiceren voor deze werkstromen:

- EAP-verificatie.
- CRL-download via HTTPS-server.
- Beveiligde Syslog communicatie tussen ISE en externe syslog server.
- ISE als een beveiligde LDAP-client.
- ISE als een beveiligde ODBC-client.
- ERS-diensten.
- pxGrid-services.
- Alle ISE-portalen (bijv. Guest Portal, client provisioningportal, MyDevices Portal).

- MDM-communicatie.
- Communicatie met Passive ID Agent.
- Bepaling van de certificeringsinstantie.
- Beheerderstoegang via GUI.

Deze poorten worden gebruikt door de componenten die bovenaan worden vermeld voor communicatie:

- Admin Access: 443
- Cisco ISE-poorten: 9002, 8443, 8444, 8445, 8449 of elke poort die voor ISE-poorten is geconfigureerd.
- ERS: 9060, 9061, 9063
- PxGrid: 8910



Opmerking: de optie Sha-1-coderingen toestaan is standaard uitgeschakeld. We raden u aan om SHA-256 of SHA-384-algoritmen te gebruiken voor verbeterde beveiliging.

U moet alle knooppunten in een plaatsing opnieuw opstarten na het toelaten of onbruikbaar maken van de optie Allow SHA-1 Cypers. Als het opnieuw opstarten niet succesvol is, worden de configuratiewijzigingen niet toegepast.

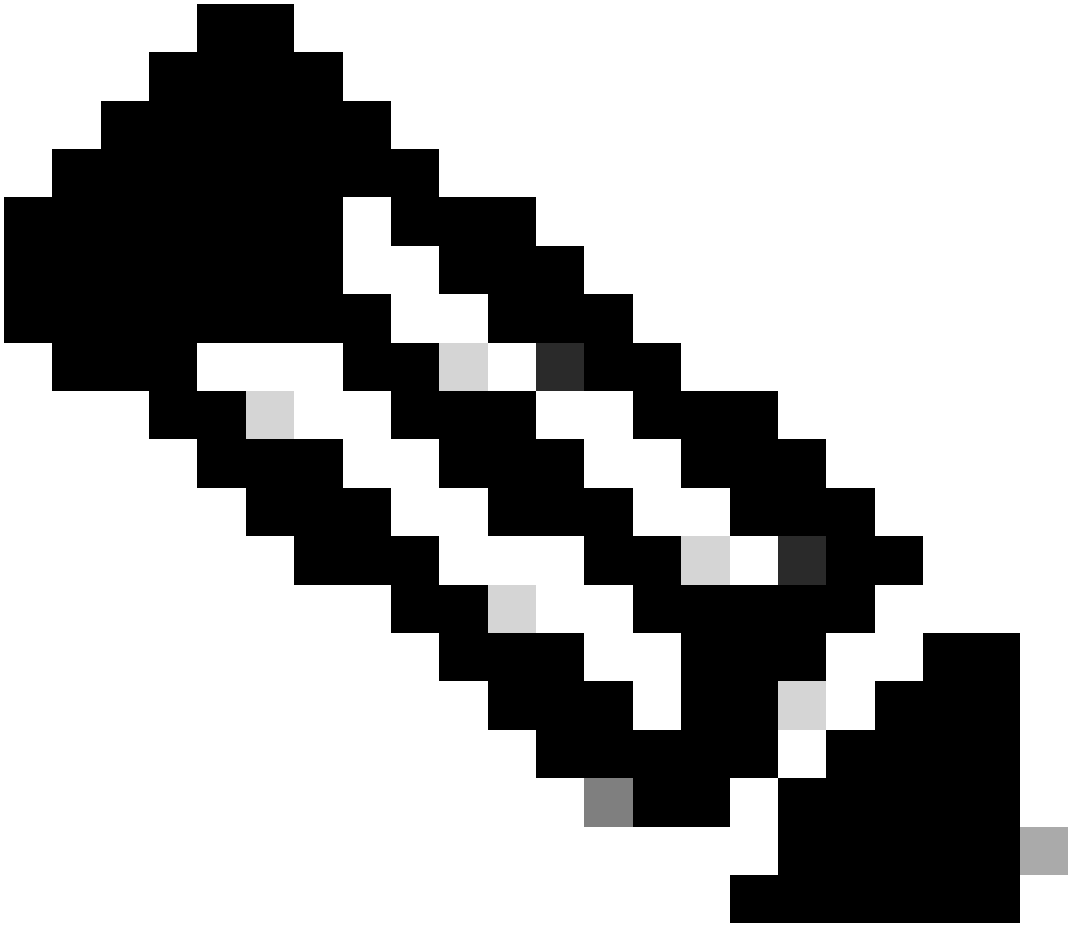
Wanneer de optie Sha-1-algoritmen toestaan is uitgeschakeld en als een client met alleen SHA-1-algoritmen probeert verbinding te maken met Cisco ISE, mislukt de handdruk en ziet u een foutmelding in de clientbrowser.

Kies een van de opties terwijl u SHA-1-algoritmen toestaat om te communiceren met oudere peers:

- Alle SHA-1-algoritmen toestaan: hiermee kunnen alle SHA-1-algoritmen communiceren met oudere peers.
- Sta alleen TLS_RSA_WITH_AES_128_CBC_SHA toe: Stelt alleen TLS_RSA_WITH_AES_128_CBC_SHA-algoritme in staat om te communiceren met bestaande peers.

Toestaan van TLS 1.3: Maakt TLS 1.3 voor beheerder HTTPS-toegang via poort 443 mogelijk voor:

- Cisco ISE-beheerGUI
- API's ingeschakeld voor poort 443 (Open API, ERS, MnT).



Opmerking: AAA-communicatie en alle soorten internodencommunicatie ondersteunen TLS 1.3 niet. Schakel TLS 1.3 in op Cisco ISE en de relevante clients en servers voor beheertoegang via TLS 1.3.

ECDHE-RSA- en 3DES-algoritmen toestaan: hiermee kunnen ECDHE-RSA-algoritmen voor deze werkstromen communiceren met peers:

- Cisco ISE wordt geconfigureerd als een EAP-server
- Cisco ISE wordt geconfigureerd als een RADIUS DTLS-server
- Cisco ISE wordt geconfigureerd als een RADIUS DTLS-client
- Cisco ISE-downloads met CRL van HTTPS of een beveiligde LDAP-server
- Cisco ISE wordt geconfigureerd als een beveiligde syslogclient
- Cisco ISE wordt geconfigureerd als een beveiligde LDAP-client

DSS-algoritmen voor ISE als client toestaan: wanneer Cisco ISE als client fungeert, kunnen DSS-algoritmen voor deze werkstromen met een server communiceren:

- Cisco ISE wordt geconfigureerd als een RADIUS DTLS-client
- Cisco ISE-downloads met CRL van HTTPS of een beveiligde LDAP-server
- Cisco ISE wordt geconfigureerd als een beveiligde syslogclient
- Cisco ISE wordt geconfigureerd als een beveiligde LDAP-client

Verouderde onveilige TLS-heronderhandeling voor ISE als client toestaan: maakt communicatie mogelijk met oudere TLS-servers die geen veilige TLS-heronderhandeling voor deze werkstromen ondersteunen:

- Cisco ISE-downloads met CRL van HTTPS of een beveiligde LDAP-server
- Cisco ISE wordt geconfigureerd als een beveiligde syslogclient
- Cisco ISE wordt geconfigureerd als een beveiligde LDAP-client

Ongeldige gebruikersnamen weergeven: standaard geeft Cisco ISE het ongeldige bericht weer voor verificatiefouten vanwege onjuiste gebruikersnamen. Voor een betere debugging dwingt deze optie Cisco ISE om gebruikersnamen in rapporten weer te geven, in plaats van het ongeldige bericht. Bericht dat de gebruikersnamen altijd voor ontbroken authentificaties worden getoond die niet wegens onjuiste gebruikersnamen zijn.

Deze functie wordt ondersteund voor Active Directory, Interne Gebruikers, LDAP en ODBC-identiteitsbronnen. Het wordt niet ondersteund voor andere identiteitsbronnen, zoals RADIUS-token, RSA of SAML.

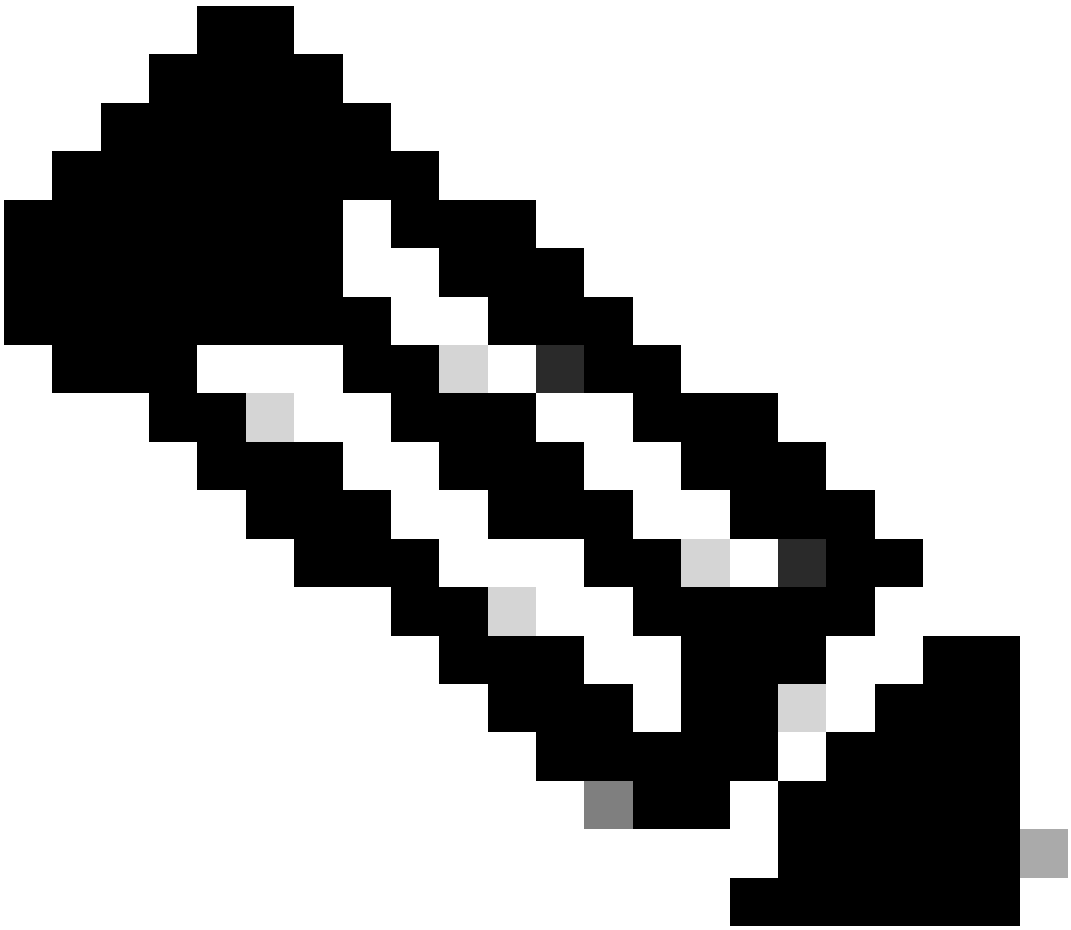
Gebruik op FQDN gebaseerde certificaten voor communicatie met externe leveranciers (TC-NAC): op FQDN gebaseerde certificaten moeten aan deze regels voldoen:

- De SAN- en GN-velden in het certificaat moeten FQDN-waarden bevatten. Hostnamen en IP-adressen worden niet ondersteund.
- De certificaten van de vervanging moeten het vervangingskarakter slechts in het uiterst linkse fragment bevatten.
- FQDN die in een certificaat wordt verstrekt moet DNS oplosbaar zijn.

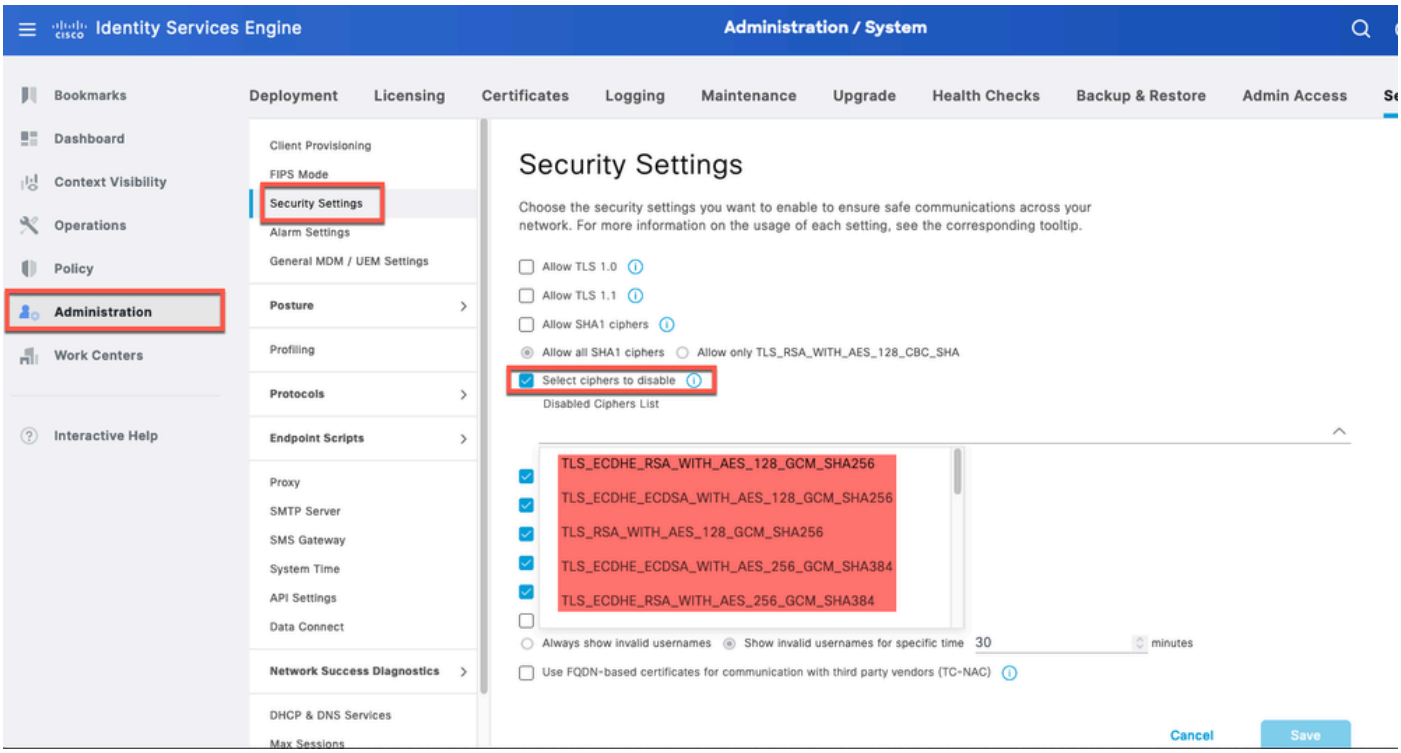
Specifieke grafieken uitschakelen

Controleer de optie Programmeerlijst handmatig configureren als u algoritmen handmatig wilt configureren om te communiceren met deze Cisco ISE-componenten: admin UI, ERS, OpenAPI, beveiligde ODBC, portals en pxGrid. Er wordt een lijst met algoritmen weergegeven met toegestane algoritmen die al zijn geselecteerd. Als bijvoorbeeld de optie Allow SHA1 Cyphers is ingeschakeld, worden SHA1-algoritmen in deze lijst ingeschakeld. Als de optie Alleen TLS_RSA_WITH_AES_128_CBC_SHA toestaan is geselecteerd, wordt alleen dit SHA1-algoritme in deze lijst ingeschakeld. Als de optie Sha1-algoritmen toestaan is uitgeschakeld, kunt u in dit

geval geen SHA1-algoritme inschakelen



Opmerking: wanneer u de lijst met uit te schakelen algoritmen bewerkt, wordt de toepassingsserver opnieuw gestart op alle Cisco ISE-knooppunten. Wanneer de FIPS-modus is in- of uitgeschakeld, worden de toepassingsservers op alle knooppunten opnieuw opgestart, wat resulteert in aanzienlijke systeemdowntime. Als u algoritmen hebt uitgeschakeld met de optie Lijst met lettertypen handmatig configureren, controleert u de lijst met uitgeschakelde algoritmen nadat de toepassingsservers opnieuw zijn opgestart. De lijst met uitgeschakelde algoritmen wordt niet gewijzigd vanwege de overgang naar de FIPS-modus.



Optie om Cryptors ISE 3.3 uit te schakelen

- Van ISE CLI kunt u de opdracht uitvoeren application configure iseen Optie 37 gebruiken, die in deze screenshot is gemarkeerd, **Enable/Disable/Current_status of RSA_PSS-handtekening voor EAP-TLS**. De verwante bug is Cisco bug-id CSCwb7915.

```
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 REPLOGNS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
```

Optie om RSA_PSS voor EAP-TLS uit te schakelen/in te schakelen

Gerelateerde informatie

-

Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.