

Integreer ISE 3.3 met Stealthwatch 7.5.1 met behulp van externe CA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Configureren](#)

[Deel A: Certificaatconfiguratie voor Secure Network Analytics \(Stealthwatch\)](#)

[Deel I - MVO genereren voor het Secure Network Analytics pxGrid-clientcertificaat](#)

[Deel II - Een Secure Network Analysis MaxGrid-clientcertificaat maken met een externe CA](#)

[DEEL III - Het Clientcertificaat voor Secure Network Analytics \(PxGrid\) aan de Manager toevoegen](#)

[DEEL IV - Het CA Root Certificaat importeren in de Manager Trust Store](#)

[Deel B: Cisco Identity Services Engine 3.3 certificaatconfiguratie](#)

[DEEL I - Een ISE-servercertificaat met xGrid genereren](#)

[DEEL II - Een ISE-serverpakketcertificaat maken met een externe CA](#)

[DEEL III - Het CA Root Certificate importeren in de ISE Trust Store](#)

[DEEL IV - Binding van het ISE-certificaat aan het verzoek tot ondertekening van het certificaat \(CSR\)](#)

[integreren](#)

[Verifiëren](#)

[Probleemoplossing](#)

[Probleem met DNS-oplossing](#)

[Oplossing](#)

[Onbekende CA-fout of betrouwbaar certificaat ontbreekt](#)

[Oplossing](#)

[Bekende gebreken](#)

Inleiding

In dit document worden procedures beschreven om ISE 3.3 te integreren met Secure Network Analytics (Stealthwatch) via pxGrid-verbindingen.

Voorwaarden

Cisco raadt kennis over deze onderwerpen aan:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Secure Network Analytics (Stealthwatch)
- TLS-/SSL-certificaten.
- PKI op Windows-server 2016

Gebruikte componenten

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

- Identity Services Engine (ISE) versie 3.3 patch 4
- Secure Network Analytics (Stealthwatch) 7.5.1
- Windows-server 2016 als een externe certificeringsinstantie (CA)-server.

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.

Configureren

Deel A: Certificaatconfiguratie voor Secure Network Analytics (Stealthwatch)

Deel I - MVO genereren voor het Secure Network Analytics pxGrid-clientcertificaat

1. Log in op Stealthwatch Management Console (SMC).
2. Selecteer in het hoofdmenu de optie Configureren > Wereldwijd > Centraal beheer.



Risk



Monitor



Investigate



Report



Configure

Configure

X

Detection

Host Group Management

Alarm Severity

Policy Management

Response Management

Network Scanners

Analytics

Alerts

Global

Central Management

User Management

Manager

UDP Director

External Lookup

System

Voor het gebruik van certificaatsjabloon pxGrid zijn zowel clientverificatie als serververificatie in het veld "Uitgebreid gebruik van sleutel" nodig.

6. Download een gegenereerd certificaat in Base-64 formaat en sla het op als pxGrid_client.cer.

Microsoft Active Directory Certificate Services – Avaste-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

DEEL III - Het Clientcertificaat voor Secure Network Analytics (PxGrid) aan de Manager toevoegen

1. Navigeer naar het gedeelte Aanvullende SSL/TLS-clientidentiteiten van de Manager Configuration in Central Management.

2. De sectie Aanvullende SSL/TLS-clientidentiteiten bevat een formulier om het gemaakte clientcertificaat te importeren.

3. Geef het certificaat een vriendelijke naam, klik vervolgens op Select File om het certificaatbestand te vinden.

4. Selecteer de root of emittent CA .cer bestand of het certificaat ketting bestand (.pem / .cer / .crt) onder de Chain Certificate file sectie.

5. Klik op Add Client Identity (Clientidentiteit toevoegen) om het certificaat aan het systeem toe te voegen.

6. Klik op Instellingen toepassen om de wijzigingen op te slaan.

DEEL IV - Het CA Root Certificaat importeren in de Manager Trust Store

1. Navigeer naar de MS Active Directory Certificate Service startpagina en selecteer Download een CA-certificaat, certificaatketen of CRL.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:[Request a certificate](#)[View the status of a pending certificate request](#)[Download a CA certificate, certificate chain, or CRL](#)

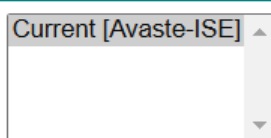
2. Selecteer Base-64-formaat en klik vervolgens op CA-certificaat downloaden.

3. Sla het certificaat op als CA_Root.cer.

Microsoft Active Directory Certificate Services -- Avaste-ISE**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:**Encoding method:**☐ DER☒ Base 64[Install CA certificate](#)[Download CA certificate](#)[Download CA certificate chain](#)[Download latest base CRL](#)[Download latest delta CRL](#)

4. Log in op de Stealthwatch Management Console (SMC).

5. Selecteer in het hoofdmenu de optie Configureren > Wereldwijd > Centraal beheer.

6. Klik op de pagina Inventaris op het (ellips)-pictogram voor de Manager.

7. Kies Applicatie configuratie bewerken.

8. Selecteer het tabblad Algemeen.

9. Navigeer naar het gedeelte Trust Store en importeer eerder geëxporteerd CA_Root.cer certificaat.

10. Klik op Nieuw toevoegen.

Central Management Inventory Data Store Update Manager App Manager Smart Licensing Database

Inventory / Appliance Configuration

Appliance Configuration - Manager

smcrrc (10.106.127.50) / Last Updated: 2/8/2025, 5:30:58 PM by admin

Appliance Network Services **General**

☐ Enable FIPS Encryption Libraries

☐ Enable Common Criteria Encryption Libraries

SMTP Configuration

SMTP Server

Port

From Email

User Name

Password

Encryption Type

☒ SMTPS ☐ STARTTLS ☐ Un-Encrypted

Backup Configuration Encryption

Make sure you save your password. If you lose your password, you can change it. However, you will not be able to restore a backup configuration file without the password.

☐ Enable Encryption

Backup Configuration Password

Confirm Password

External Services

If you enable a service, make sure you enable it on the other required appliances. Refer to the tooltip for requirements.

☒ Enable Cisco Security Cloud Control

☒ Enable Customer Success Metrics

☒ Enable Threat Feed

Feed Confidence Level

7

DoDIN Notifications

☐ Enable

To Email

Trust Store

Add New

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
yy1nde2owmzmdu5ndc2m2rzm...	Secure Network Analytics	Secure Network Analytics	2024-06-20 20:17:15	2029-06-21 20:17:15	403c0116b1af4d3b71e9060afdb...	4096	Delete
fc751new.www.cisco.com	Secure Network Analytics	Secure Network Analytics	2024-06-23 12:14:09	2029-06-24 12:14:09	14e60739401a8e204c7f03b12279...	4096	Delete
AWS	Amazon	Amazon	2015-05-26 05:30:00	2038-01-17 05:30:00	66c9cf99bfb0a39e2f0788a43e69...	2048	Delete

5 items per page 1 - 3 of 3 items Page 1 of 1

11. Geef het certificaat een vriendelijke naam en klik vervolgens op Select File... om het eerder geëxporteerde ISE CA-certificaat te selecteren.

12. Klik op Certificaat toevoegen om de wijzigingen op te slaan.

Add Certification Authority Certificate

Friendly Name *

AVASTEROOTCA

Certificate File *

AVASTE_ROOT.cer

Select file...

Cancel Add Certificate

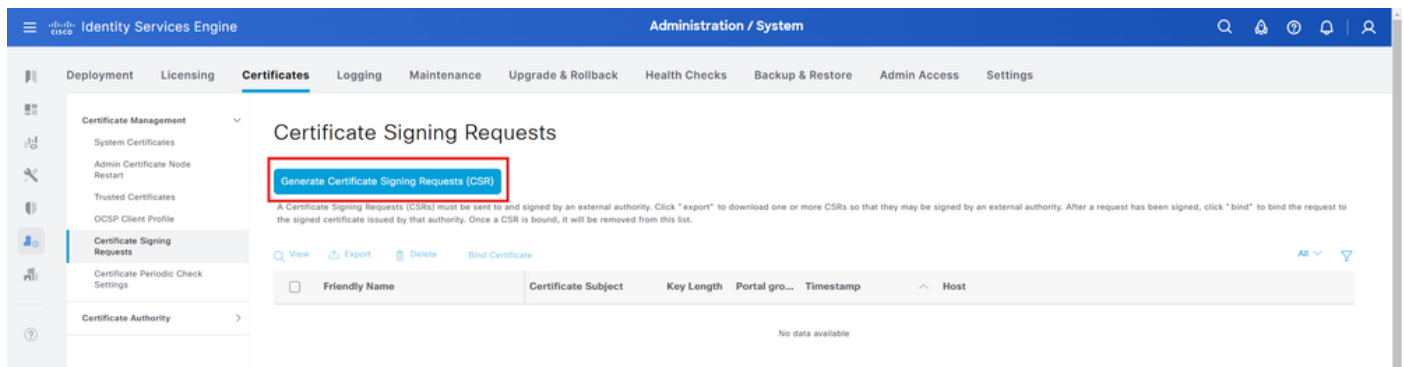
13. Klik op Instellingen toepassen om de wijzigingen op te slaan.

Deel B: Cisco Identity Services Engine 3.3 certificaatconfiguratie

DEEL I - Een ISE-server-pxGrid-certificaat genereren

Een CSR genereren voor een ISE-server pxGrid-certificaat:

1. Log in op Cisco Identity Services Engine (ISE) GUI.
2. Navigeer naar Administratie > Systeem > Certificaten > Certificaatbeheer > Certificaatondertekeningsaanvragen.
3. Selecteer Generate Certificate Signing Verzoek (CSR).



4. Selecteer pxGrid in het veld Certificaat(s) wordt gebruikt voor.
5. Selecteer ISE-knooppunt waarvoor het certificaat wordt gegenereerd.
6. Vul zo nodig andere gegevens van het certificaat in.
7. Klik op Generate.

Usage

Certificate(s) will be used forpxGrid

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ avasteise271	avasteise271#pxGrid

Subject

Common Name (CN)
SFQDNS

Organizational Unit (OU)
AAA

Organization (O)
Cisco

City (L)
Bangalore

State (ST)
KA

Country (C)
IN

Subject Alternative Name (SAN)

DNS Name

avasteise271.avaste.local

IP Address

10.127.197.128

* Key type

RSA

* Key Length

4096

* Digest to Sign With

SHA-384

Certificate Policies

Generate

Cancel

8. Klik op Exporteren en lokaal opslaan van het bestand.

×

Successfully generated CSR(s)

Certificate Signing request(s) generated:

avasteise271#pxGrid

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

DEEL II - Een ISE-serverpakketcertificaat maken met een externe CA

1. Ga naar MS Active Directory Certificate Service, <https://server/certsrv/>, waar de server IP of DNS van uw MS-server is.
2. Klik op Certificaat aanvragen.

Microsoft Active Directory Certificate Services — Avastis RSE [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

3. Kies om een geavanceerde certificaataanvraag in te dienen.

Microsoft Active Directory Certificate Services -- Avasto-ISE

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

4. Kopieert de inhoud van de SR die in de vorige sectie is gegenereerd naar het veld Opgeslagen aanvraag.
5. Selecteer pxGrid als certificaatsjabloon en klik vervolgens op Indienen.

Microsoft Active Directory Certificate Services — Avastc-ISE

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

```
MQZJZG0RPOC2007/SUZYTHPPARTWVXWCYKSGMqgEATF0HqEVEtBg
wB9BEswkHQCFZj4wKCCKpmouZsgskZ1S5BK1KgPps9zD2XrFuCR
qFzbekMl1wRFIF18XH/tkeJAbLXSg04MosEvXCHIGINPRsWawje/A
EWIh3cedSKd/BwFEJqLpxmKbs27ux7oKTPTfTh8+ovKguPn4TmU7C
T1uoQ3i7UL1pnZLsgHQh2owQpkd7CXITiFoYLcWASAM/gvP/yHqn5
664io9JF/8dJpmPw028pUSF6inS8HIFZrUd8MCAwEAABMEoGCsGs
MDswEwYDVRO81BAwCkgYIKwYBBQUHAwIwJAAYDRORBBowGAITc21jc
2NivlmVybYCEmp/MjANBgkqhkiG9w0BAQsFAAOCAgEANSQ90dwe
eFZCS+wghwahe8bzzyGD2NDSeeeddzlykhsafJOMQBQRuRidV6
oolkc3TIDyr8rScdioz0XPukZQARPAKL/PxM4Z1ShSV58HR4VKSw
Se3nz2HA+3q01XBdt8q9o2rNl7MoUs43VCjHAGKM2B1CYQy2oLdCX
y/VIZHo4PrvLL22GXZkuQCwJUDB/GGrYtAfUfd2K0mh/Raxdn29
XJCWaqcn4j2T4eUJDQz1Da368KVXL4ATXP31Ayfs9f9qTjJPXBEB4
Sq4ZQvw2d9TpKRvNlo1a3QygnCqFXiqZSkB11JFDIXvZKTD3wc3
1XHU5jr6v0zyjAeyGwukaACRSAm1Ww3Bm08uTMq1UIQMj4hKKOS
TF175msAq7paasT2GpdgXyby2wQB4hhJgrQYGQWSxh3acq+XuCoPG
1rksdntUfRAc10y5dhSp7bcnsXgmBC35xU6sr+legGFaxgN1o
0MGIS9/ywFbaSP0s8NmX457GG9BM275VCAKKEaL4fb+dybtbSiX58
WySCDYotX97VvsNCXC/mjk=
-----END CERTIFICATE REQUEST-----
```

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7).

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >



Opmerking: Voor het gebruik van certificaatsjabloon pxGrid zijn zowel clientverificatie als serververificatie in het veld "Uitgebreid gebruik van sleutel" nodig.

6. Download het gegenereerde certificaat in Base-64-formaat en sla het op als ISE_pxGrid.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

DEEL III - Het CA Root Certificate importeren in de ISE Trust Store

1. Navigeer naar MS Active Directory Certificate Service startpagina en selecteer Download een CA-certificaat, certificaatketen of CRL.

Microsoft Active Directory Certificate Services -- Avaste-ISE Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

2. Selecteer Base-64 formaat en klik vervolgens op CA-certificaat downloaden.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Avaste-ISE] ▲

▼

Encoding method:

☐ DER

☒ Base 64

[Install CA certificate](#)

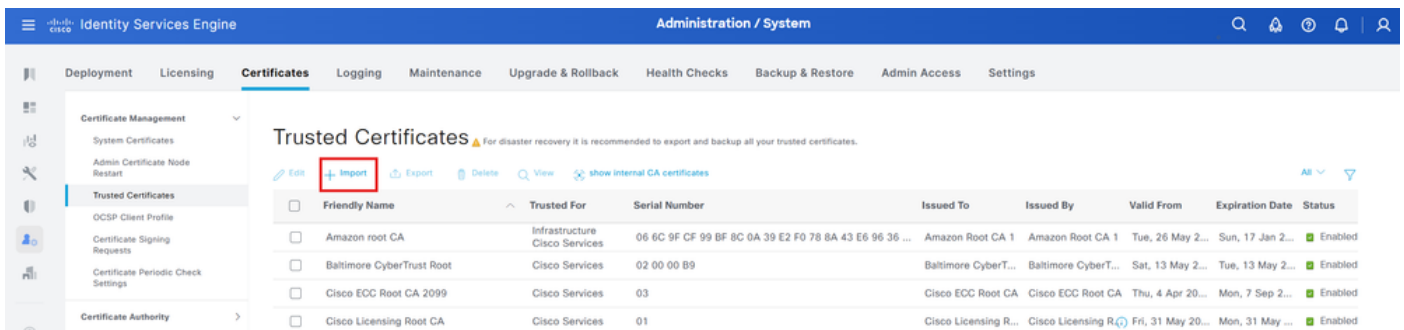
[Download CA certificate](#)

[Download CA certificate chain](#)

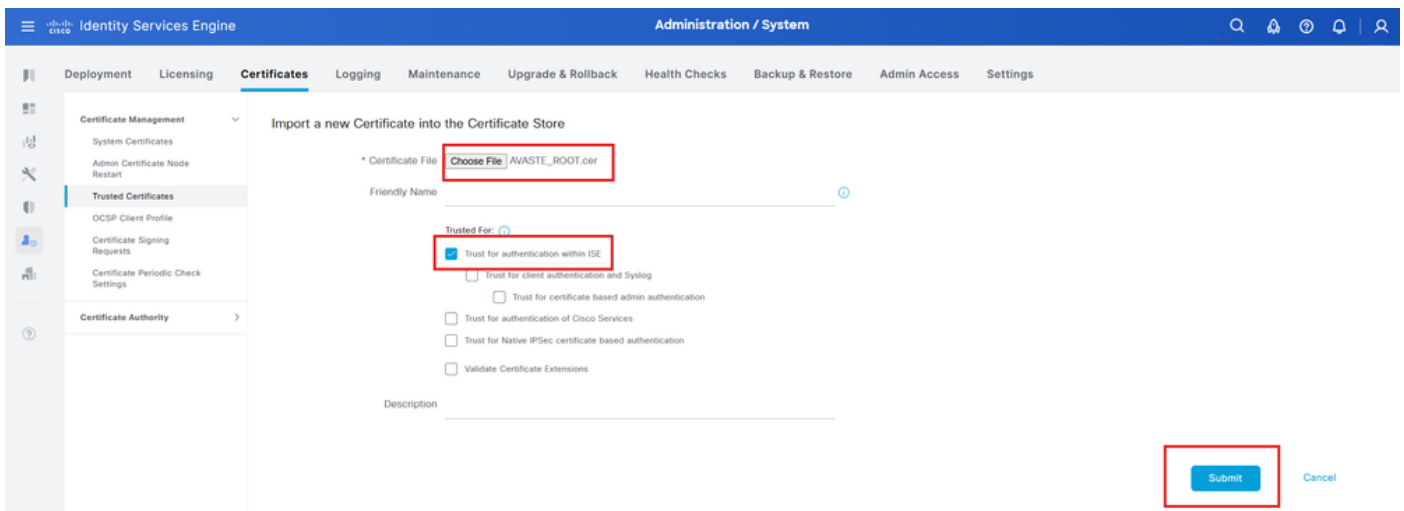
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Sla het certificaat op als CA_Root.cer.
4. Log in op Cisco Identity Services Engine (ISE) GUI.
5. Selecteer Beheer > Systeem > Certificaten > Certificaatbeheer > Betrouwbare certificaten.



6. Selecteer Importeren > Certificaatbestand en importeer het basiscertificaat.
7. Zorg ervoor dat het selectievakje Vertrouwen voor verificatie in ISE is geselecteerd.



8. Klik op Indienen.

DEEL IV - Binding van het ISE-certificaat aan het verzoek tot ondertekening van het certificaat (CSR)

1. Log in op Cisco Identity Services Engine (ISE) GUI.
2. Selecteer Beheer > Systeem > Certificaten > Certificaatbeheer > Aanvragen voor certificaatondertekening.
3. Selecteer de MVO die in de vorige sectie is gegenereerd en klik vervolgens op Bindcertificaat.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OSCP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete **Bind Certificate**

☐	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☒	avasteise271pxGrid	CN=avasteise271.avaste...	4096		Sat, 8 Feb 2025	avasteise271

4. Kies op het formulier Bind CA Signed Certificate het eerder gegenereerde ISE_pxGrid.cer certificaat.

5. Geef het certificaat een vriendschappelijke naam en klik op Indienen.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OSCP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File **Choose File** ISE_pxgrid.cer

Friendly Name **ISE-pxGRID**

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

Submit Cancel

7. Klik op Ja als het systeem wordt gevraagd het certificaat te vervangen.

8. Selecteer Beheer > Systeem > Certificaten > Systeemcertificaten.

9. In de lijst ziet u het gemaakte pxGrid-certificaat dat is ondertekend door de externe CA.

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OSCP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit + Generate Self Signed Certificate + Import Export Delete View

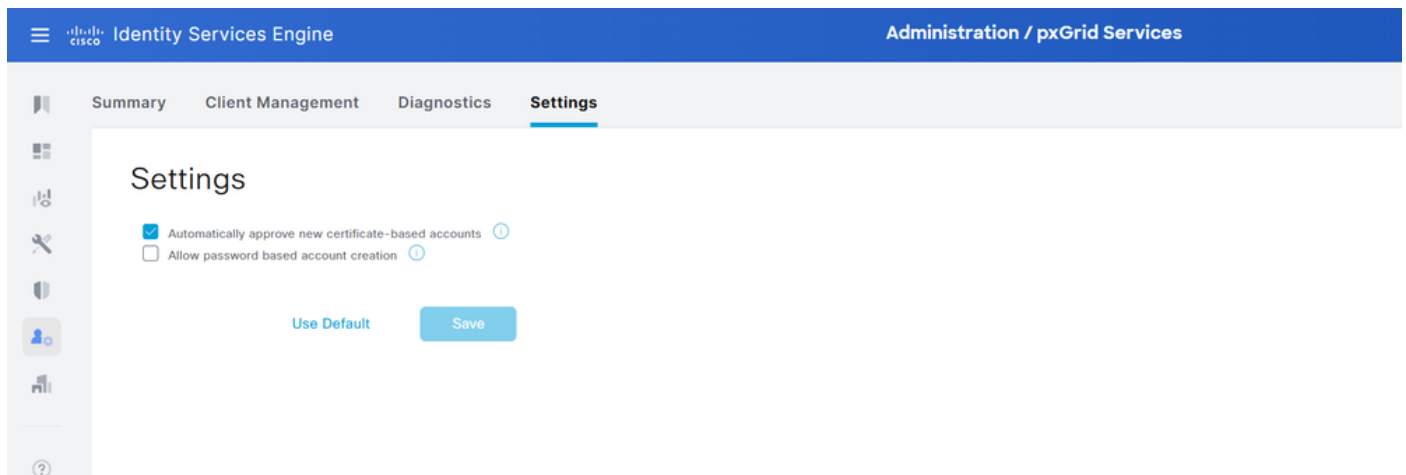
☐	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
☒	avasteise271							
☐	CN=avasteise271.avaste.local, OU=Certificate Services System, Certificate/Certificate Services Endpoint Sub CA - avasteise271800002	Not in use		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	Default self-signed server certificate	RADIUS DTLS		avasteise271.avaste.local	avasteise271.avaste.local	Fri, 16 Aug 2024	Tue, 2 Oct 2029	Active
☐	Default self-signed saml server certificate - CN=SAML_avasteise271.avaste.local	SAML		SAML_avasteise271.avaste.local	SAML_avasteise271.avaste.local	Fri, 16 Aug 2024	Wed, 15 Aug 2029	Active
☐	CN=avasteise271.avaste.local, OU=ISE Messaging Service Certificate Services Endpoint Sub CA - avasteise271800003	ISE Messaging Service		avasteise271.avaste.local	Certificate Services Endpoint Sub CA - avasteise271	Thu, 15 Aug 2024	Thu, 16 Aug 2029	Active
☐	ISE-pxGRID	pxGrid		avasteise271.avaste.local	Avaste-ISE	Sat, 8 Feb 2025	Mon, 8 Feb 2027	Active
☐	AVASTE-2024	Admin, Portal, EAP Authentication	Default Portal Certificate Group	avasteise271.avaste.local	Avaste-ISE	Sun, 25 Aug 2024	Tue, 25 Aug 2026	Active

Certificaten worden nu ingezet, ga verder met Integratie.

integreren

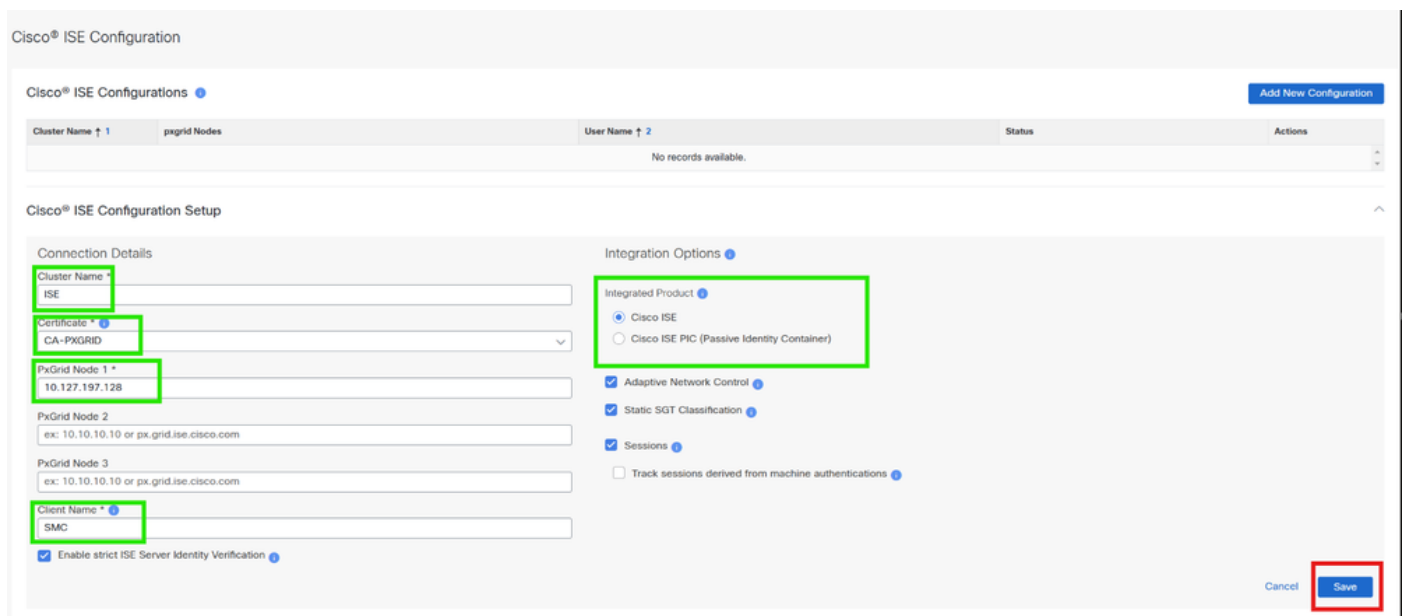
Alvorens over te gaan tot integratie, zorg ervoor dat:

Voor Cisco ISE onder Beheer > PxGrid Services > Instellingen en Controleer automatisch nieuwe op certificaat gebaseerde accounts voor clientverzoek om automatisch goed te keuren en op te slaan.



Op de Stealthwatch Management Console (SMC) opent u de Instellingspagina van de ISE-configuratie:

1. Selecteer Configureren > Integraties > Cisco ISE.
2. Klik in de rechterbovenhoek van de pagina op Nieuwe configuratie toevoegen.
3. Voer een clusternaam in, selecteer het certificaat- en integratieproduct, pxGrid-knooppunt, IP en klik op Opslaan.

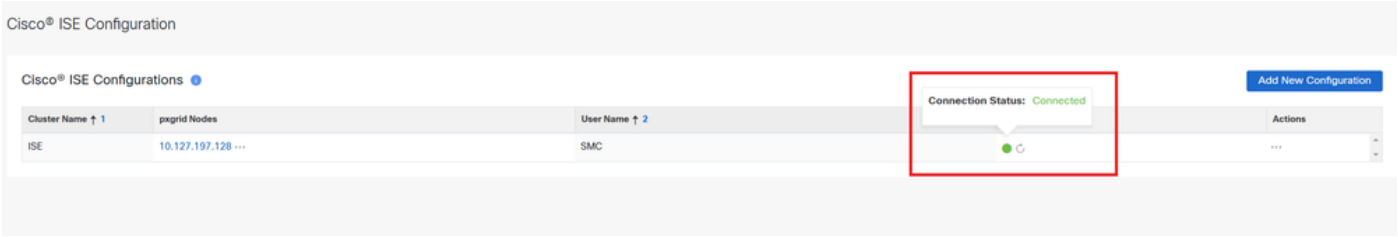


Verifiëren

Vernieuw de pagina ISE-configuratie op de Stealthwatch Management Console (SMC).

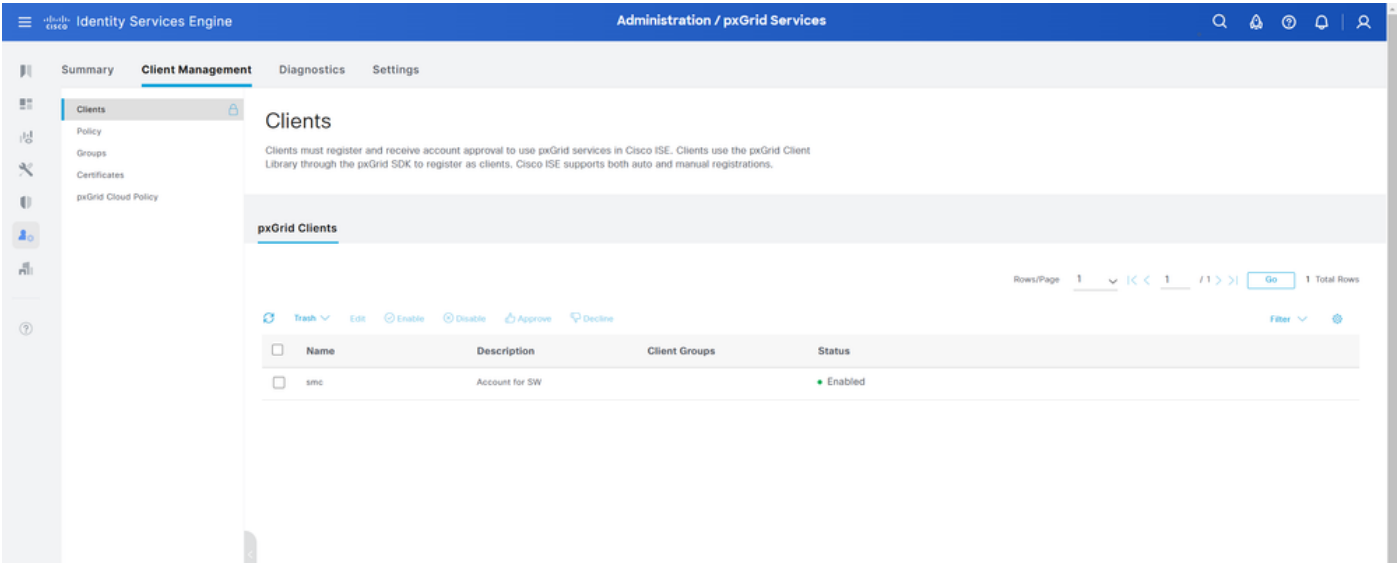
1. Ga terug naar de pagina ISE Configuration in de Web App en vernieuw de pagina.
2. Bevestig dat de statusindicator van het knooppunt naast het toepasselijke IP-adresveld Groen is, wat aangeeft dat een

verbinding met het ISE- of ISE-PIC-cluster tot stand is gebracht.



Ga op Cisco ISE naar Beheer >PxGrid Services > Clientbeheer > Clients.

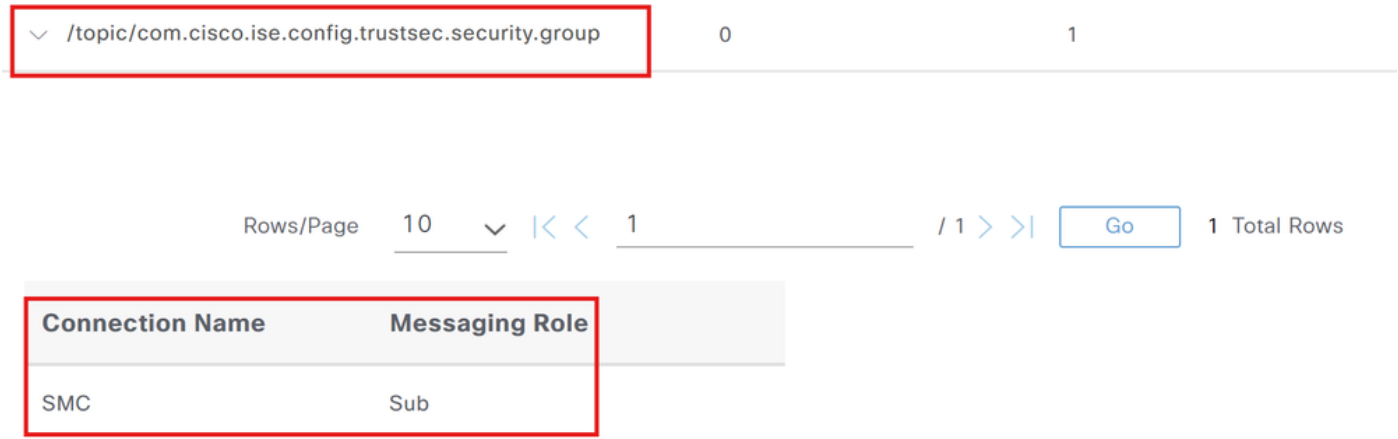
Dit genereert de SCM als een pxgrid-client met de status Ingeschakeld.



Om onderwerpabonnement op Cisco ISE te verifiëren, navigeer naar Beheer >pxGrid Services > Diagnostiek > Websocket > Onderwerpen

Dit levert een SCM op die is geabonneerd op deze onderwerpen.

Trustsec SGT-onderwerp



onderwerp ISE-sessiemap

▼ /topic/com.cisco.ise.session	1	1
--------------------------------	---	---

Rows/Page 10 1 / 1 > >| Go 2 Total Rows

Connection Name	Messaging Role
-ise-mnt-avasteise271	Pub
SMC	Sub

onderwerp ISE-SXP-banden

▼ /topic/com.cisco.ise.sxp.binding	0	1
------------------------------------	---	---

Rows/Page 10 1 / 1 > >| Go 1 Total Rows

Connection Name	Messaging Role
SMC	Sub

Cisco ISE-pakketserver.log in TRACE-niveau

```
2025-02-08 18:07:11,086 TRACE [pxgrid-http-pool15][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,087 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,102 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,110 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -::
2025-02-08 18:07:11,111 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.config.MyX509Filter -::
2025-02-08 18:07:11,112 DEBUG [pxgrid-http-pool22][[]] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -::::
2025-02-08 18:07:11,321 DEBUG [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu

]
2025-02-08 18:07:11,322 DEBUG [pxgrid-http-pool20][[]] cisco.cpm.pxgridwebapp.config.AuthzEvaluator -:
2025-02-08 18:07:11,322 INFO [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
```

```
] session=[id=8,client=SMC,server=wss://avasteise271.avaste.local:8910/pxgrid/ise/pubsub]
```

```

2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool19][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE [WsIseClientConnection-1010][[]] cpm.pxgrid.ws.client.WsEndpoint -:::
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,323 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu

]
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu

]
2025-02-08 18:07:11,324 TRACE [pxgrid-http-pool22][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistribu
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

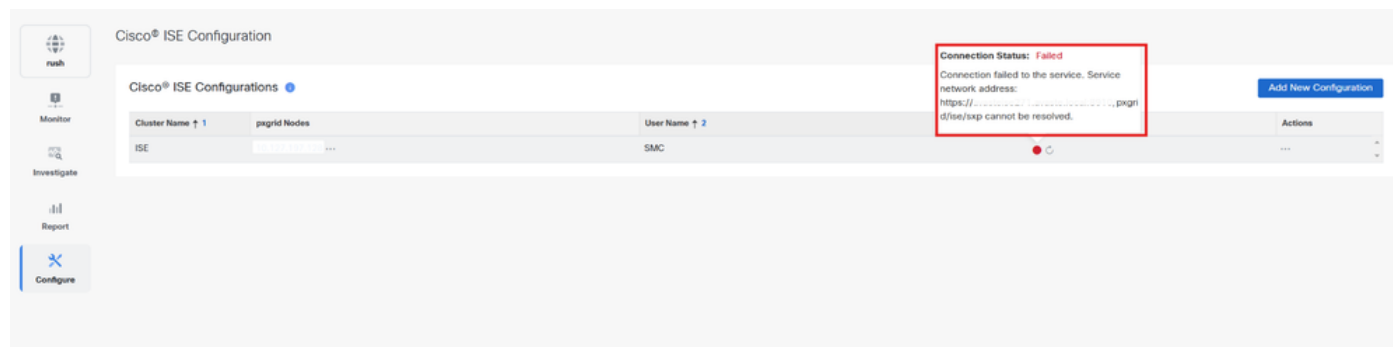
] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```

Probleemoplossing

Probleem met DNS-oplossing

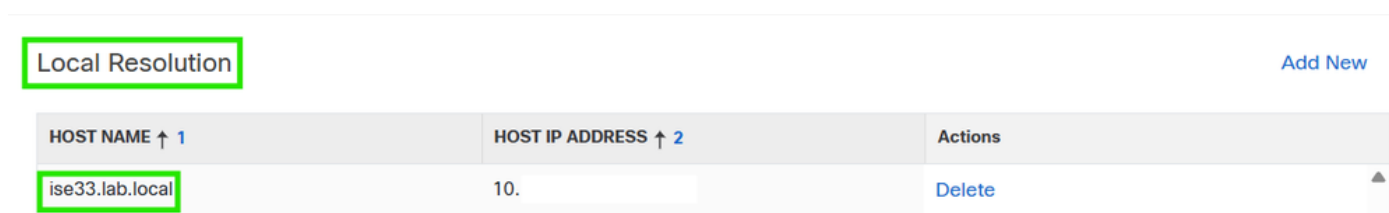
Dit geeft een foutbericht weer als "Verbindingsstatus; Verbinding met de service is mislukt. Netwerkadres van de dienst: <https://isehostnameeme.domain.com:891pxgridiisessxpxp> kan niet worden opgelost":



Oplossing

Dit moet idealiter op de DNS-server worden gerepareerd voor voorwaartse en omgekeerde zoekopdrachten voor deze ISE-FQDN. Maar er kan een tijdelijke oplossing worden toegevoegd voor de lokale oplossing:

1. Log in op de Stealthwatch Management Console (SMC).
2. Selecteer in het hoofdmenu de optie Configureren > Wereldwijd > Centraal beheer.
3. Klik op de pagina Inventaris op het pictogram (Ellipsis) voor het beheer.
4. Kies Applicatie configuratie bewerken.
5. Het tabblad Network Services en voegt een lokale resolutie toe voor dit ISE-FQDN.



Local Resolution Add New		
HOST NAME ↑ 1	HOST IP ADDRESS ↑ 2	Actions
ise33.lab.local	10.	Delete

Onbekende CA-fout of betrouwbaar certificaat ontbreekt

Dit geeft een foutmelding als "ISE presenteert een certificaat dat niet vertrouwd is door deze Manager":



Vergelijkbare logreferentie kan worden gevonden in het bestand SMCMsvcvise-client.log. Pad:
catlancopepe/var/logs/containsvcvise-client.log

```
snasmc1 docker/svc-ise-client[1453]: java.util.concurrent.ExecutionException: javax.net.ssl.SSLException
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:358)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:1960)
snasmc1 docker/svc-ise-client[1453]: at org.springframework.web.socket.client.jetty.JettyWebSocketClient.doHandshake(JettyWebSocketClient.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.FutureTask.run(FutureTask.java:280)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.lang.Thread.run(Thread.java:829)
snasmc1 docker/svc-ise-client[1453]: Caused by: javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFatalAlert(40): The certificate is not trusted by the peer
snasmc1 docker/svc-ise-client[1453]: at org.bouncycastle.jssse.provider.ProvSSLSessionImpl.unwrap(ProvSSLSessionImpl.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/javax.net.ssl.SSLSessionImpl.unwrap(SSLSessionImpl.java:637)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.unwrap(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.fill(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.process(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpReceiverOverHTTP.receive(HttpReceiverOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpChannelOverHTTP.receive(HttpChannelOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.client.http.HttpConnectionOverHTTP.onFillable(HttpConnectionOverHTTP.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractConnection$ReadCallback.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFillable(SslConnection$DecryptedEndPoint.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection.java:100)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnection$2.java:100)
```

```
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:10)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.io.SelectableChannelEndPoint$1.run(SelectableChannelEndPoint.java:43)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:673)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool.java:792)
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.
```

Oplossing

1. Log in op de Stealthwatch Management Console (SMC).
2. Selecteer in het hoofdmenu de optie Configureren > Wereldwijd > Centraal beheer.
3. Klik op de pagina Inventaris op het pictogram (ellips) voor de Manager.
4. Kies Applicatie configuratie bewerken.
5. Selecteer het tabblad General.
6. Navigeer naar het gedeelte Trust Store en zorg ervoor dat de emittent van het Prisma-certificaat van Cisco ISE deel uitmaakt van het Trust Store.

Bekende gebreken

ID bug	Beschrijving
18119 van Cisco-bug-id	ISE selecteert niet-ondersteunde applicatie voor CIPHER ITLS Server Hello Packet
01634 van Cisco-bug-id	Kan apparaten niet in quarantaine plaatsen met EPS-voorwaarde

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.