

Integrar o ISE 3.3 ao Stealthwatch 7.5.1 usando CA externa

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Seção A: Configuração do certificado Secure Network Analytics \(Stealthwatch\)](#)

[Parte I - Gerar um CSR para o certificado do Secure Network Analytics pxGrid Client](#)

[Parte II - Criação de um certificado de cliente pxGrid Secure Network Analytics usando uma CA externa](#)

[PARTE III - Adicionando o certificado pxGrid Client do Secure Network Analytics ao gerenciador](#)

[PARTE IV - Importar o certificado raiz de CA para o armazenamento confiável do gerenciador](#)

[Seção B: Configuração do certificado do Cisco Identity Services Engine 3.3](#)

[PARTE I - Geração de um certificado pxGrid do servidor ISE](#)

[PARTE II - Criação de um certificado pxGrid de servidor ISE usando uma CA externa](#)

[PARTE III - Importar o certificado raiz de CA para o armazenamento confiável do ISE](#)

[PARTE IV - Vincular o certificado ISE ao CSR \(Certificate Signing Request, Solicitação de assinatura de certificado\)](#)

[Integrar](#)

[Verificar](#)

[Troubleshooting](#)

[Problema de resolução de DNS](#)

[Solução](#)

[Erro desconhecido da autoridade de certificação ou certificado confiável ausente](#)

[Solução](#)

[Defeitos conhecidos](#)

Introdução

Este documento descreve procedimentos para integrar o ISE 3.3 com o Secure Network Analytics (Stealthwatch) usando conexões pxGrid.

Pré-requisitos

A Cisco recomenda conhecimento sobre estes tópicos:

- Identity Services Engine
- Platform Exchange Grid (pxGrid)
- Análise de rede segura(Stealthwatch)
- Certificados TLS/SSL.

- PKI no Windows Server 2016

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Patch 4 do Identity Services Engine (ISE) versão 3.3
- Análise de rede segura (Stealthwatch) 7.5.1
- O Windows Server 2016 como um servidor externo de Autoridade de Certificação (CA).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Seção A: Configuração do certificado Secure Network Analytics (Stealthwatch)

Parte I - Gerar um CSR para o certificado do Secure Network Analytics pxGrid Client

1. Faça login no Stealthwatch Management Console (SMC).
2. No menu principal, selecione Configure > Global > Central Management.



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

: O modelo de certificado pxGrid usado precisa da autenticação do cliente e da autenticação do servidor no campo "Uso avançado de chave".

6. Baixe um certificado gerado no formato Base-64 e Salve-o como 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](#)

PARTE III - Adicionando o certificado pxGrid Client do Secure Network Analytics ao gerenciador

1. Navegue até a seção Identidades Adicionais de Cliente SSL/TLS da Configuração do Gerenciador em Gerenciamento Central.
2. A seção Identidades Adicionais de Cliente SSL/TLS contém um formulário para importar o certificado de cliente criado.
3. Dê ao certificado um nome amigável e clique em Selecionar Arquivo para localizar o arquivo do certificado.
4. Selecione o arquivo raiz ou de CA do emissor .cer ou o arquivo da cadeia de certificados (.pem / .cer / .crt) na seção Arquivo do certificado da cadeia.
5. Clique em Adicionar Identidade do Cliente para adicionar o certificado ao sistema.

6. Clique em Aplicar Configurações para salvar as alterações.

PARTE IV - Importar o certificado raiz de CA para o armazenamento confiável do gerenciador

1. Navegue até a página inicial do MS Active Directory Certificate Service e selecione Baixar um certificado CA, uma cadeia de certificados ou uma 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](#)

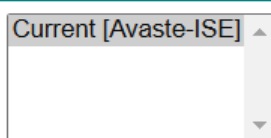
2. Selecione o formato Base-64 e clique em Download do certificado CA.

3. Salve o certificado como 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. Faça login no Stealthwatch Management Console (SMC).

5. No menu principal, selecione Configure > Global > Central Management.

6. Na página Inventário, clique no ícone (reticências) do Gerente.

7. Escolha Editar configuração do dispositivo.

8. Selecione a guia Geral.

9. Navegue até a seção Trust Store e importe o certificado CA_Root.cer exportado anteriormente.

10. Clique em Adicionar Novo.

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	66c9cf998f8c0a39e2f0788a43e69...	2048	Delete

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

11. Dê um nome amigável ao certificado e clique em Selecionar arquivo... para selecionar o certificado de autoridade de certificação ISE exportado anteriormente.

12. Clique em Adicionar Certificado para salvar as alterações.

Add Certification Authority Certificate

Friendly Name *

AVASTEROOTCA

Certificate File *

AVASTE_ROOT.cer

Select file...

Cancel Add Certificate

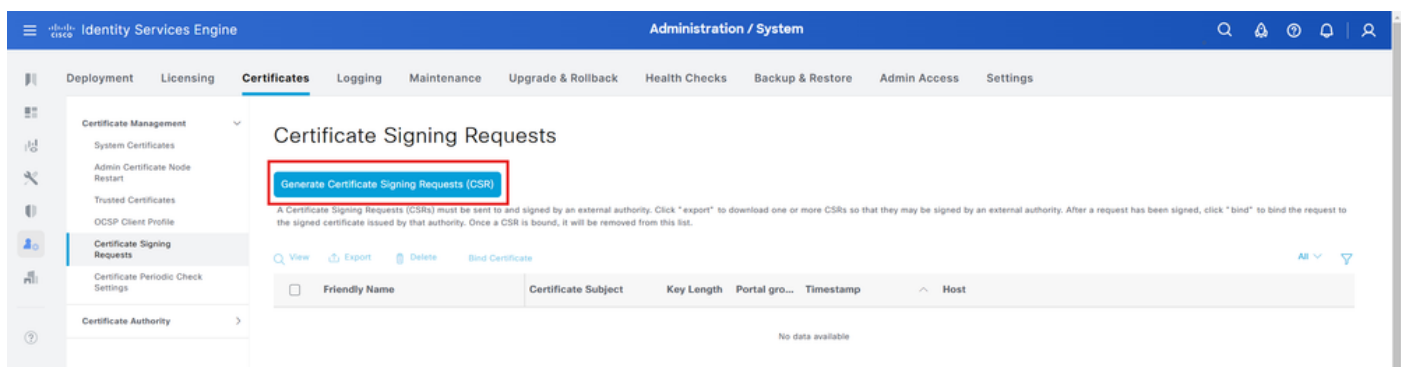
13. Clique em Aplicar Configurações para salvar as alterações.

Seção B: Configuração do certificado do Cisco Identity Services Engine 3.3

PARTE I - Geração de um certificado PxGrid do servidor ISE

Gere um CSR para um certificado pxGrid de servidor ISE:

1. Faça login na GUI do Cisco Identity Services Engine (ISE).
2. Navegue até Administração > Sistema > Certificados > Gerenciamento de Certificados > Solicitações de Assinatura de Certificado.
3. Selecione Gerar CSR (Certificate Signing Request).



4. Selecione pxGrid no campo Certificado(s) usado para.
5. Selecione o nó ISE para o qual o certificado é gerado.
6. Preencher outros detalhes dos certificados, conforme necessário.
7. Clique em Gerar.

Usage

Certificate(s) will be used for pxGrid

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. Clique em Exportar e Salvar o arquivo localmente.

✕

Successfully generated CSR(s) ✓

Certificate Signing request(s) generated:

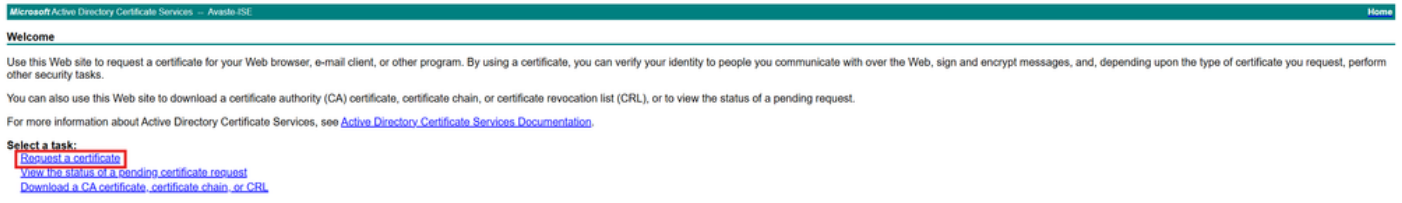
avasteise271#pxGrid

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

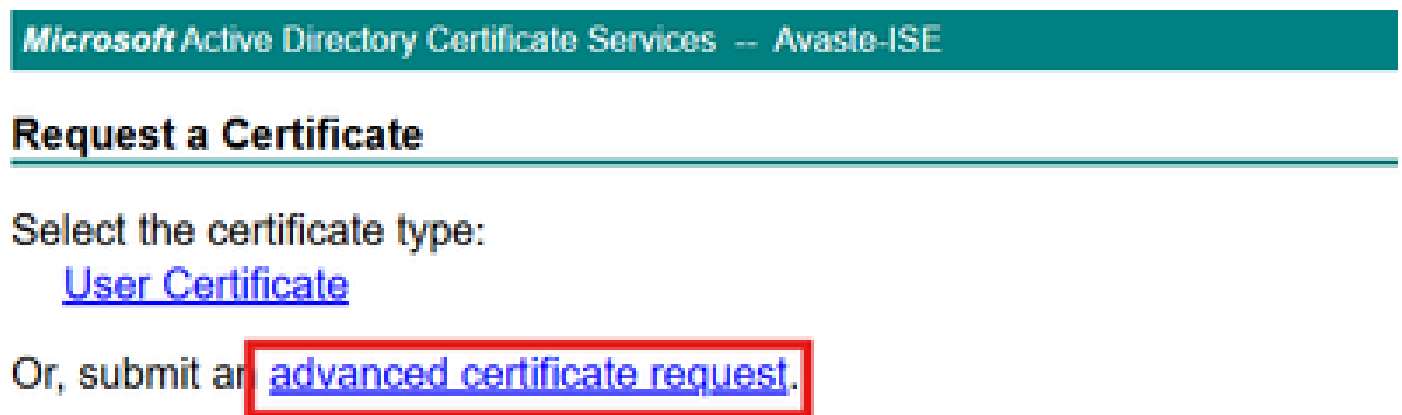
OK Export

PARTE II - Criação de um certificado pxGrid de servidor ISE usando uma CA externa

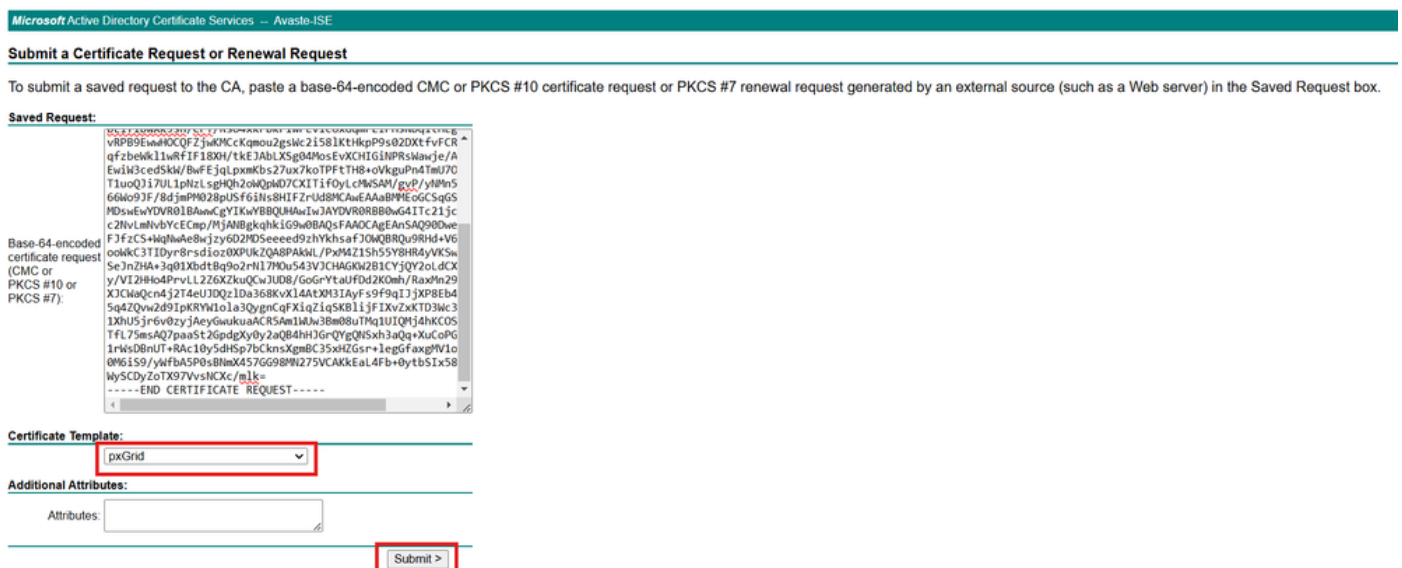
1. Navegue até o MS Active Directory Certificate Service, <https://server/certsrv/>, onde o servidor é IP ou DNS do seu MS Server.
2. Clique em Solicitar um certificado.

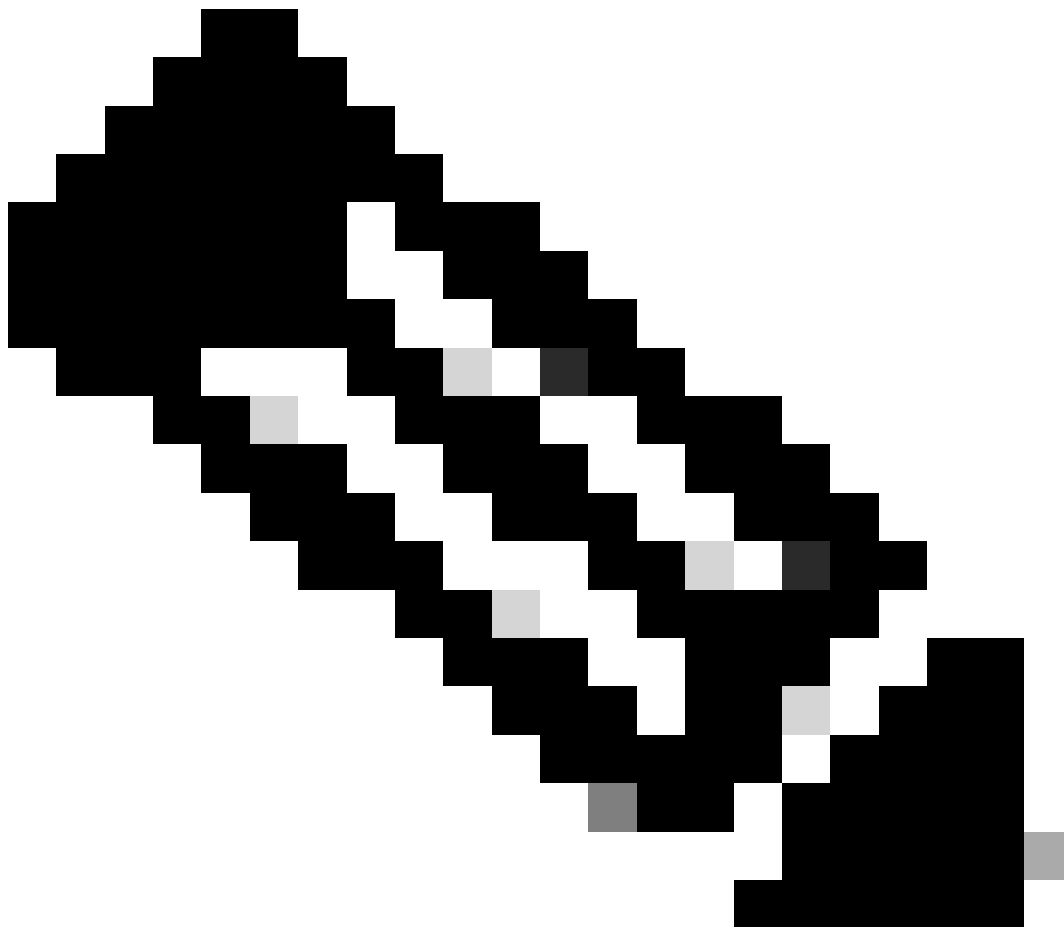


3. Escolha submeter uma solicitação avançada de certificado.



4. Copie o conteúdo do CSR gerado na seção anterior para o campo Solicitação salva.
5. Selecione pxGrid como o Modelo de certificado e clique em Enviar.





Note: O modelo de certificado pxGrid usado precisa da autenticação do cliente e da autenticação do servidor no campo "Uso avançado de chave".

6. Baixe o certificado gerado no formato Base-64 e Salve-o como ISE_pxGrid.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

PARTE III - Importar o certificado raiz de CA para o armazenamento confiável do ISE

1. Navegue até a home page do MS Active Directory Certificate Service e selecione Download de um certificado CA, cadeia de certificados ou 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. Selecione o formato Base-64 e clique em Download do certificado CA.

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](#)

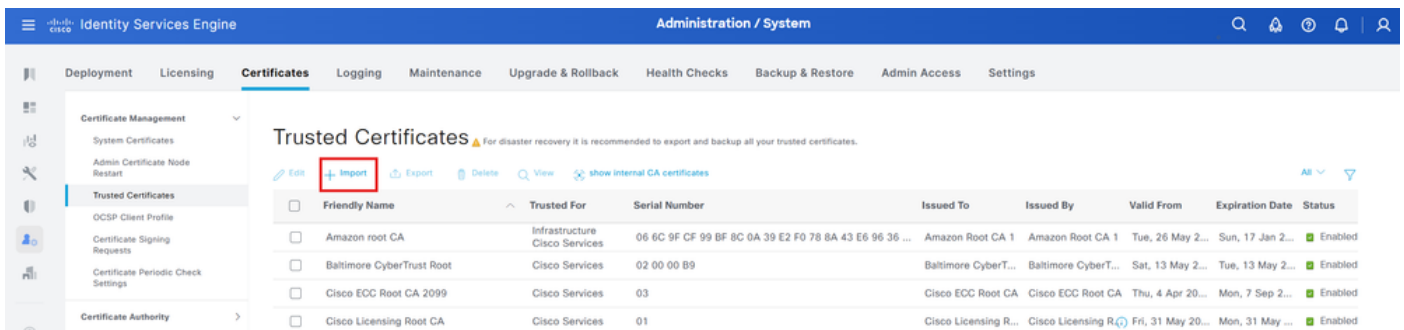
[Download CA certificate](#)

[Download CA certificate chain](#)

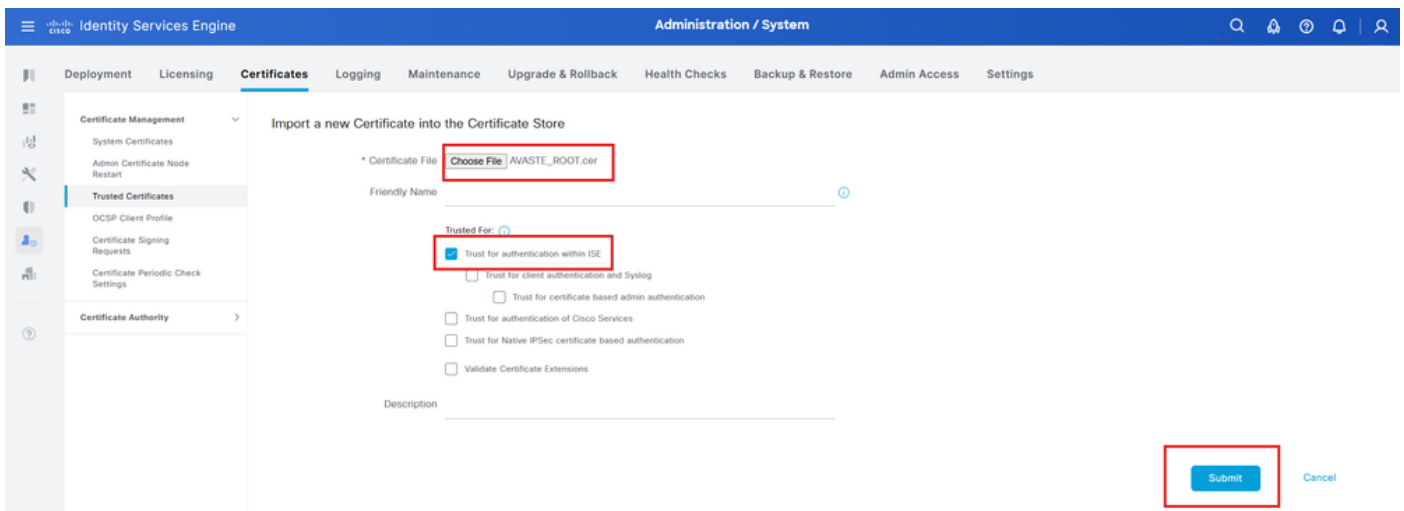
[Download latest base CRL](#)

[Download latest delta CRL](#)

3. Salve o certificado como CA_Root.cer.
4. Faça login na GUI do Cisco Identity Services Engine (ISE).
5. Selecione Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados de Confiabilidade.



6. Selecione Importar > Arquivo de certificado e Importar o certificado raiz.
7. Verifique se a caixa de seleção Confiar para autenticação no ISE está marcada.



8. Clique em Submeter.

PARTE IV - Vincular o certificado ISE ao CSR (Certificate Signing Request, Solicitação de assinatura de certificado)

1. Faça login na GUI do Cisco Identity Services Engine (ISE).
2. Selecione Administração > Sistema > Certificados > Gerenciamento de Certificado > Solicitações de Assinatura de Certificado.
3. Selecione o CSR gerado na seção anterior e clique em Vincular Certificado.

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
- OCSP 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. No formulário Vincular certificado assinado pela CA, escolha o certificado ISE_pxGrid.cer gerado anteriormente.

5. Dê um nome amigável ao certificado e clique em Submeter.

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
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File [Choose File](#) ISE_pxgrid.cer

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ pxGrid: Use certificate for the pxGrid Controller

[Submit](#) [Cancel](#)

7. Clique em Sim se o sistema solicitar a substituição do certificado.

8. Selecione Administração > Sistema > Certificados > Certificados do Sistema.

9. Você pode ver na lista o certificado pxGrid assinado pela CA externa.

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
- OCSP 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](#)

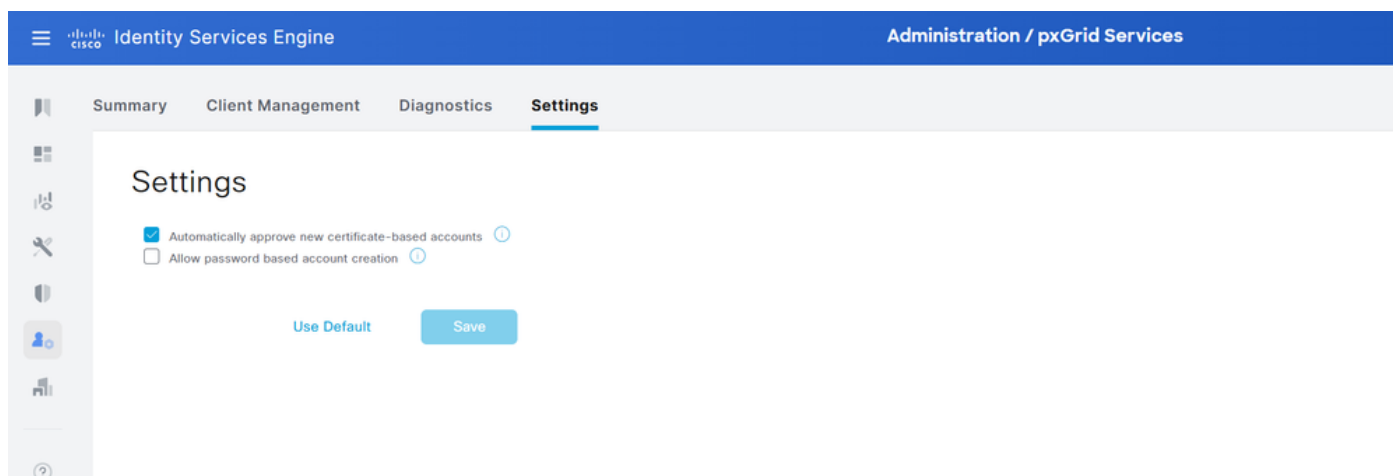
☐	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
☒	avasteise271							
☐	CN=avasteise271.avaste.local, OU=Certificate Services System, Certificate/Certificate Services Endpoint Sub CA - avasteise271800002	Not in use		avasteise271.avaste.local	Certificate 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

Os certificados foram implantados. Prossiga para a integração.

Integrar

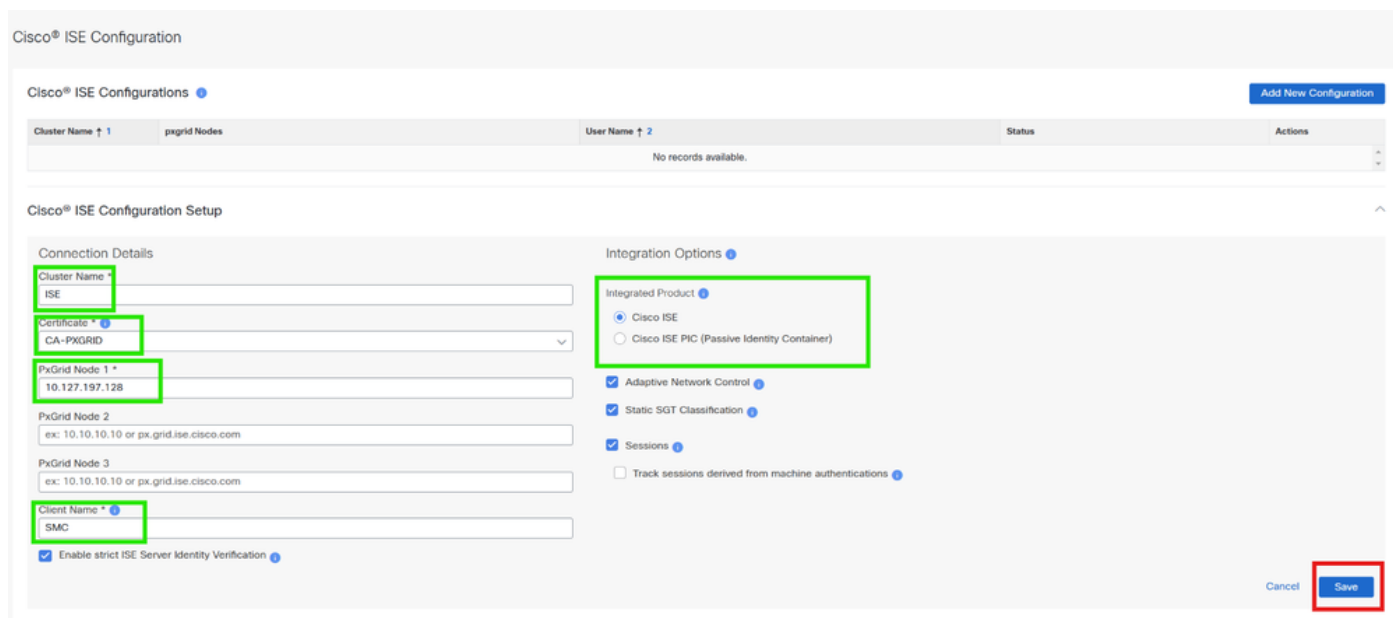
Antes de prosseguir com a integração, verifique se:

Para o Cisco ISE em Administration > pxGrid Services > Settings e Check Approve automaticamente novas contas baseadas em certificado para solicitação do cliente para aprovação automática e Save.



No Stealthwatch Management Console (SMC), para abrir a página de configuração do ISE:

1. Selecione Configure > Integrations > Cisco ISE.
2. No canto superior direito da página, clique em Adicionar nova configuração.
3. Insira o Nome do cluster, selecione o certificado & Produto de integração, nó pxGrid IP e clique em Salvar.

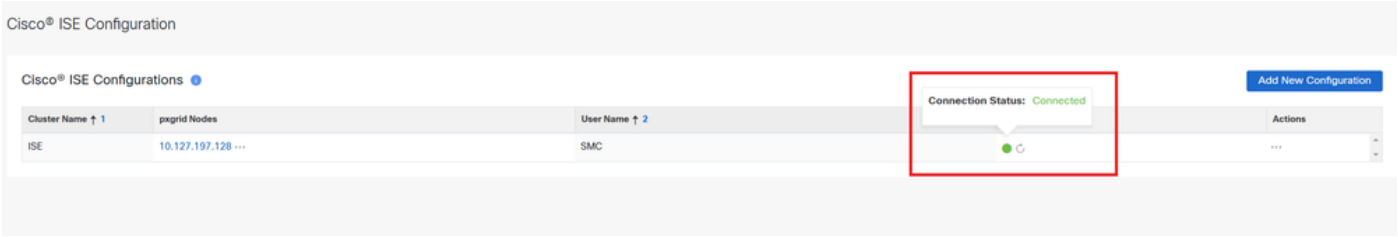


Verificar

Atualize a página de configuração do ISE no Stealthwatch Management Console (SMC).

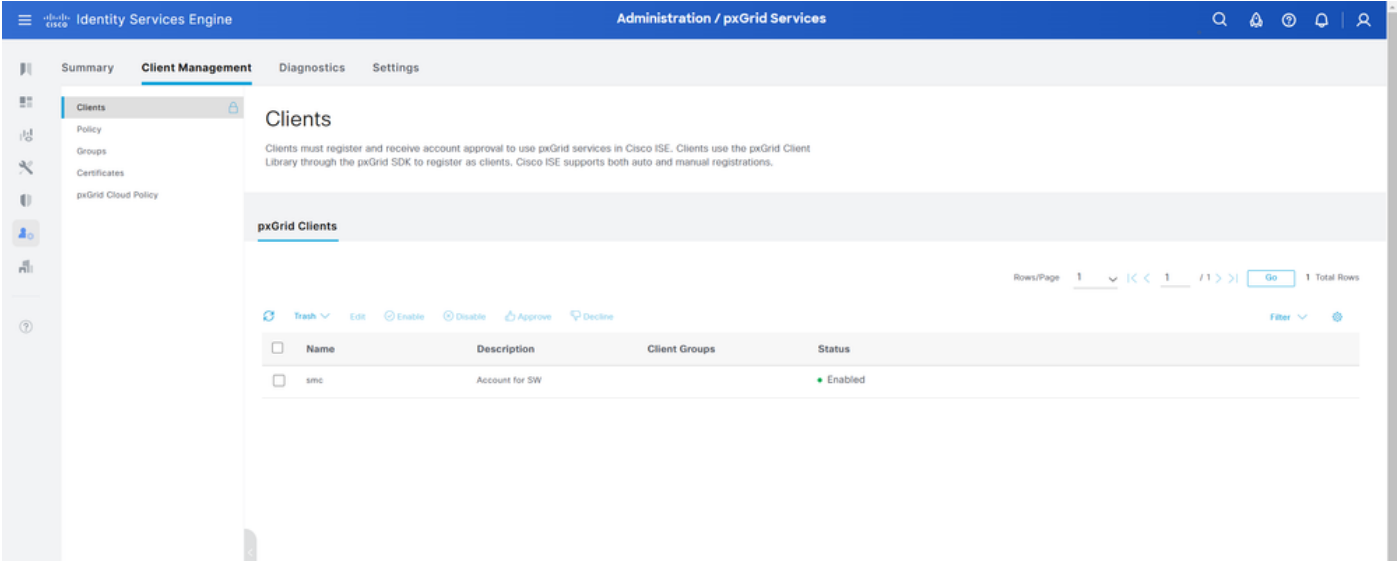
1. Retorne à página Configuração do ISE no Web App e atualize a página.
2. Confirme se o indicador de status do nó, localizado ao lado do campo Endereço IP aplicável, está em Verde,

indicando que foi estabelecida uma conexão com o cluster ISE ou ISE-PIC.



No Cisco ISE, navegue até Administração >pxGrid Services > Gerenciamento de cliente > Clientes.

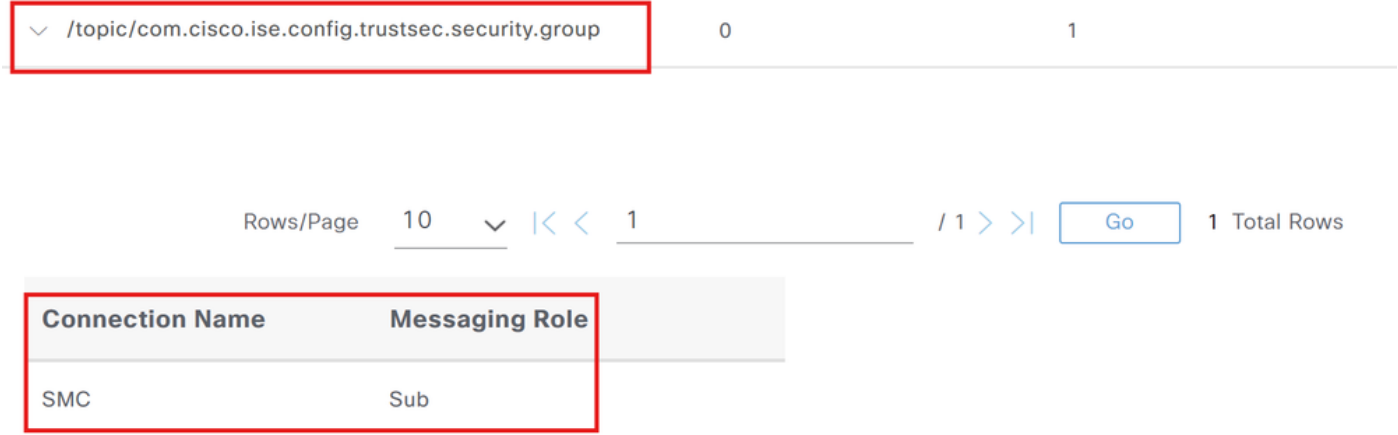
Isso gera o SMC como um cliente pxgrid com o status Enabled.



Para verificar a inscrição de tópico no Cisco ISE, navegue para Administração >serviços pxGrid > Diagnóstico > Websocket > Tópicos

Isso produz um SMC inscrito nesses tópicos.

Tópico SGT Trustsec



Tópico do diretório de sessões do ISE

▼ /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	

Tópico de Ligações ISE SXP

▼ /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 Pxgrid-server.log no nível TRACE.

```
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 -:::

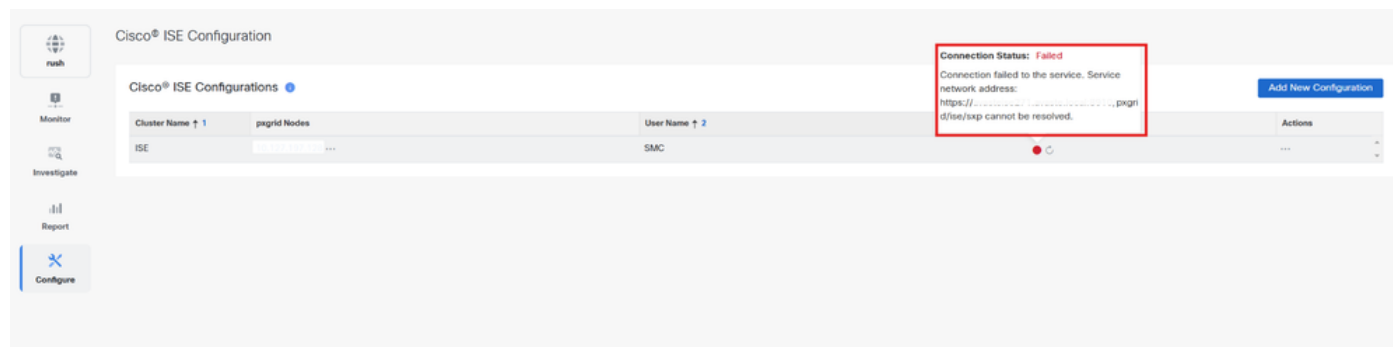
] from=[id=7,client=~ise-admin-avasteise271,server=wss://avasteise271.avaste.local:8910/pxgr
2025-02-08 18:07:11,324 TRACE [sub-sender-0][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::

```

Troubleshooting

Problema de resolução de DNS

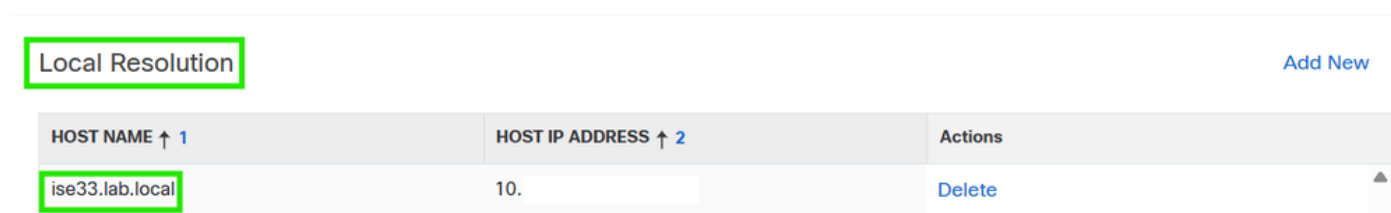
Isso produz uma mensagem de erro como "Connection Status; Falha na conexão com o serviço. Endereço de rede do serviço: <https://isehostnameeme.domain.com:891pxgridiisessxpxp> não pode ser resolvido":



Solução

O ideal é que isso seja corrigido no servidor DNS para pesquisas de encaminhamento e reversão desse FQDN do ISE. Mas uma solução temporária pode ser adicionada para resolução local:

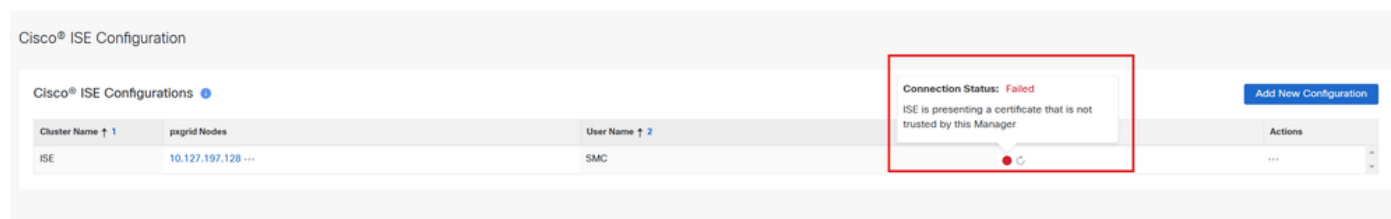
1. Faça login no Stealthwatch Management Console (SMC).
2. No menu principal, selecione Configure > Global > Central Management.
3. Na página Inventário, clique no ícone (Elipse) do Gerente.
4. Escolha Edit Appliance Configuration.
5. Guia Serviços de Rede e adicione uma entrada de resolução local para este FQDN do ISE.



HOST NAME ↑ 1	HOST IP ADDRESS ↑ 2	Actions
ise33.lab.local	10.	Delete

Erro desconhecido da autoridade de certificação ou certificado confiável ausente

Isso produz uma mensagem de erro, pois "o ISE está apresentando um certificado que não é confiável para este Gerenciador":



Cluster Name ↑ 1	pxgrid Nodes	User Name ↑ 2	Actions
ISE	10.127.197.128 ...	SMC	...

Uma referência de log semelhante pode ser vista no arquivo OSMCMsvcvise-client.log. Caminho: 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:395)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.util.concurrent.CompletableFuture.get(CompletableFuture.java:1990)
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:286)
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.ProvSSLContext.unwrap(ProvSSLContext.java:100)
snasmc1 docker/svc-ise-client[1453]: at java.base/java.net.ssl.SSLContext.unwrap(SSLContext.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.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:10)
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$1.java:10)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:10)
snasmc1 docker/svc-ise-client[1453]: at org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool$Runner.java:10)
snasmc1 docker/svc-ise-client[1453]: ... 1 more
snasmc1 docker/svc-ise-client[1453]: Suppressed: javax.net.ssl.SSLHandshakeException: org.bouncycastle.
```

Solução

1. Faça login no Stealthwatch Management Console (SMC).
2. No menu principal, selecione Configure > Global > Central Management.
3. Na página Inventário, clique no ícone (reticências) do Gerente.
4. Escolha Edit Appliance Configuration.
5. Selecione a guia Geral.
6. Navegue até a seção Trust Store e certifique de que o emissor do certificado Pxgridid do Cisco ISE seja parte do armazenamento Trust.

Defeitos conhecidos

ID do bug	Descrição
ID de bug da Cisco 18119	O ISE está selecionando o pacote Hello do servidor ITLS de cifra sem suporte
ID de bug da Cisco 01634	Não é possível colocar dispositivos em quarentena usando a condição EPS

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.