

Integrar o ISE 3.3 com o WSA usando CA externa

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

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

[Passo 1: Gerar um certificado pxGrid do ISEServer](#)

[Passo 2: Criar um certificado pxGrid do ISE Server usando uma CA externa](#)

[Passo 3: Importar o certificado raiz da autoridade de certificação para o armazenamento confiável do ISE](#)

[Passo 4: Vinculando o certificado ISE à CSR \(Certificate Signing Request, Solicitação de assinatura de certificado\).](#)

[Seção B: Adicionando certificado raiz de autoridade de certificação ao armazenamento confiável de certificados WSA](#)

[Integração](#)

[Seção A: Habilite o WSA para integração com ISE e gere CSR para o certificado de cliente WSA.](#)

[Seção B: Assinar um CSR de cliente WSA usando uma CA externa](#)

[Seção C: Vinculando o certificado do cliente WSA à CSR \(Certificate Signing Request, Solicitação de assinatura de certificado\) e integrando.](#)

[Verificar](#)

[Troubleshooting](#)

[Problema](#)

[Solução](#)

[Defeitos conhecidos](#)

Introdução

Este documento descreve os procedimentos para integrar o ISE 3.3 com o Cisco Secure Web Appliance (WSA) usando conexões pxGrid.

Pré-requisitos

Requisitos

A Cisco recomenda conhecimento sobre estes tópicos:

- Identity Services Engine
- Cisco Secure Web Appliance (WSA)
- Platform Exchange Grid (pxGrid)

- 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
- Cisco Secure Web Appliance versão 15.2.0-16
- O Windows Server 2016 como um servidor de Autoridade de Certificação Externa.

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.

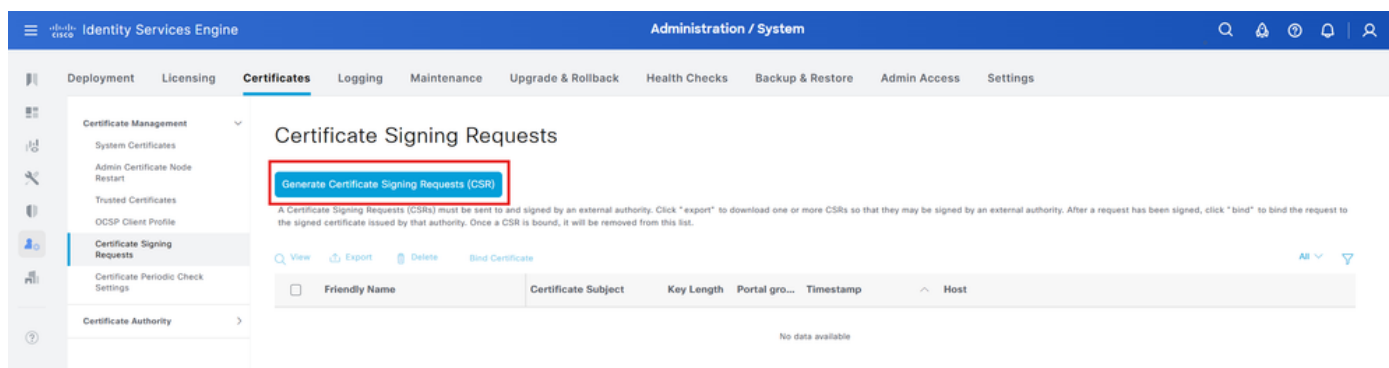
Configurar

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

Passo 1: Gerar um certificado pxGrid do ISEServer

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 Certificado > Solicitações de Assinatura de Certificado.
3. Selecione Gerar CSR (Certificate Signing Request, Solicitação de assinatura de certificado).



4. Selecione pxGridin campo Certificado(s) é usado.
5. Nó SelectISE para o qual o certificado é gerado.
6. Preencha outros detalhes de 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



ise33

ise33#pxGrid

Subject

Common Name (CN)

\$FQDN\$



Organizational Unit (OU)

AAA



Organization (O)

Cisco



City (L)

Bangalore

State (ST)

KA

Country (C)

IN

Subject Alternative Name (SAN)



DNS Name



ise33.lab.local



IP Address



10.127.197.128



* Key type

RSA



* Key Length

4096



* Digest to Sign With

SHA-384



Certificate Policies

: 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.

Microsoft Active Directory Certificate Services -- Avast-ISE

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Passo 3: Importar o certificado raiz da autoridade de certificação para o armazenamento confiável do ISE

1. Navegue até a home page do Serviço de Certificados do MS Active Directory e selecione Baixar um certificado de autoridade de certificação, cadeia de certificados ou CRL.

Microsoft Active Directory Certificate Services -- Avast-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. Formato Select Base-64 e, em seguida, clique em Download CA certificate.

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](#)

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.

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐ Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF 99 BF 8C 0A 39 E2 F0 78 8A 43 E6 96 36 ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2...	Sun, 17 Jan 2...	Enabled
☐ Baltimore CyberTrust Root	Cisco Services	02 00 00 B9	Baltimore CyberT...	Baltimore CyberT...	Sat, 13 May 2...	Tue, 13 May 2...	Enabled
☐ Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 20...	Mon, 7 Sep 2...	Enabled
☐ Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Fri, 31 May 20...	Mon, 31 May ...	Enabled

6. Selecione Import > Certificate e importe o certificado raiz.

7. Verifique se a caixa de seleção Confiar para autenticação no ISE está marcada.

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

Import a new Certificate into the Certificate Store

* Certificate File **Choose File** AWASTE_ROOT.cer

Friendly Name

Trusted For:

☒ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

☐ Trust for authentication of Cisco Services

☐ Trust for Native IPsec certificate based authentication

☐ Validate Certificate Extensions

Description

Submit Cancel

8. Clique em Enviar.

Passo 4: Vinculando o certificado ISE à 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 Certificados > Solicitações de Assinatura de Certificado.

3. Selecione o CSR gerado na seção anterior e, em seguida, clique em Vincular Certificado.

Identity Services Engine Administration / System Evaluation Mode 83 Days

Bookmarks Dashboard Context Visibility Operations Policy **Administration** Work Centers Interactive Features

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 Request (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.

Bind Certificate

☐	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☒	ise33pxGrid	CN=ise33.lab.local,OU=...	4096		Wed, 19 Mar 2025	ise33

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

5. Dê um nome amigável ao certificado e, em seguida, clique em Enviar.

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.cer

Friendly Name **ISE-pxGRID**

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below this, there are buttons for Edit, Generate Self Signed Certificate, Import, Export, Delete, and View. A table lists the system certificates:

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, EAP Authentication, Portal, RADIUS DTLS	Default Portal Certificate Group	ise33.lab.local	ise33.lab.local	Wed, 12 Mar 2025	Fri, 12 Mar 2027	Active
Default self-signed saml server certificate - CN=SAML_ise33.lab.local	SAML		SAML_ise33.lab.local	SAML_ise33.lab.local	Wed, 12 Mar 2025	Mon, 11 Mar 2030	Active
CN=ise33.lab.local, OU=ISE Messaging Service, Certificate Services Endpoint Sub CA - ise33r00005	ISE Messaging Service		ise33.lab.local	Certificate Services Endpoint Sub CA - ise33	Wed, 12 Mar 2025	Wed, 13 Mar 2030	Active
ISE-pxGRID	pxGrid		ise33.lab.local	Avaste-ISE	Wed, 19 Mar 2025	Fri, 19 Mar 2027	Active

Seção B: Adicionando certificado raiz de autoridade de certificação ao armazenamento confiável de certificados WSA

Adicionar Certificado Raiz de CA ao Repositório Confiável do WSA:

1. Faça login na GUI do Web Security Appliance (WSA).
2. Navegue até Rede > Gerenciamento de Certificados > Gerenciar Certificados Raiz Confiáveis.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

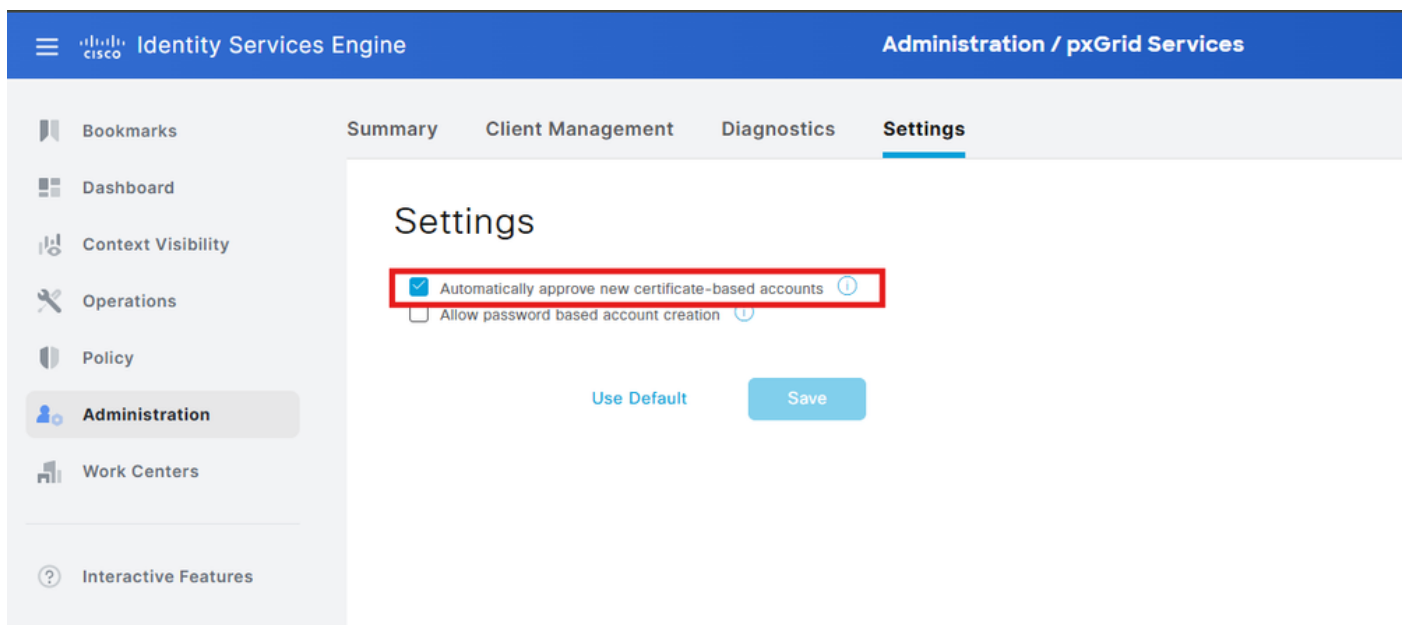
External DLP Servers

Web Traffic Tap

Certificate Management

Cloud Services Settings

Administration > pxGrid Services > Settings and Check Aprove automaticamente novas contas baseadas em certificado para solicitação do cliente para aprovação automática e Salvar.



Seção A: Habilite o WSA para integração com ISE e gere CSR para o certificado de cliente WSA.

1. Faça login na GUI do Web Security Appliance (WSA).

2. Navegue até Rede > Serviços de identificação > Mecanismo de serviço de identificação.

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy

External DLP Servers

Web Traffic Tap

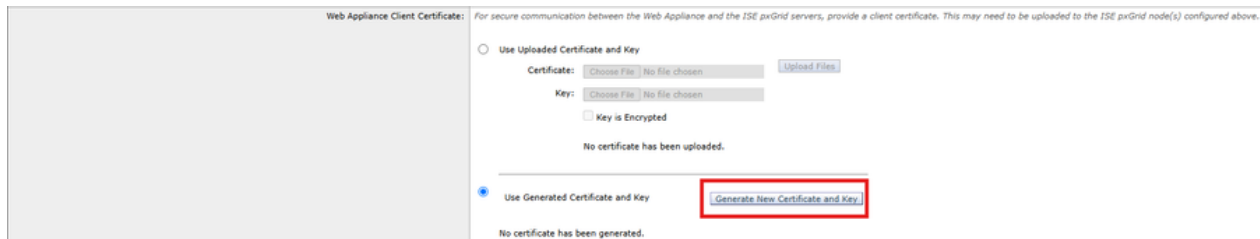
Certificate Management

Cloud Services Settings

Umbrella Settings

: Pode haver apenas dois nós pxGrid por implantação do ISE. Serve como uma configuração ativa-em espera do pxGrid; somente um nó ISE+pxGrid pode estar ativo por vez. Em uma configuração Ative-Standby do pxGrid, todas as informações são transmitidas pelo PPAN, onde o segundo nó ISE+pxGrid permanece inativo.

8. Role até a seção Certificado de cliente do equipamento da Web e clique em Gerar novo certificado e chave.



Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

☐ Use Uploaded Certificate and Key

Certificate: No file chosen

Key: No file chosen

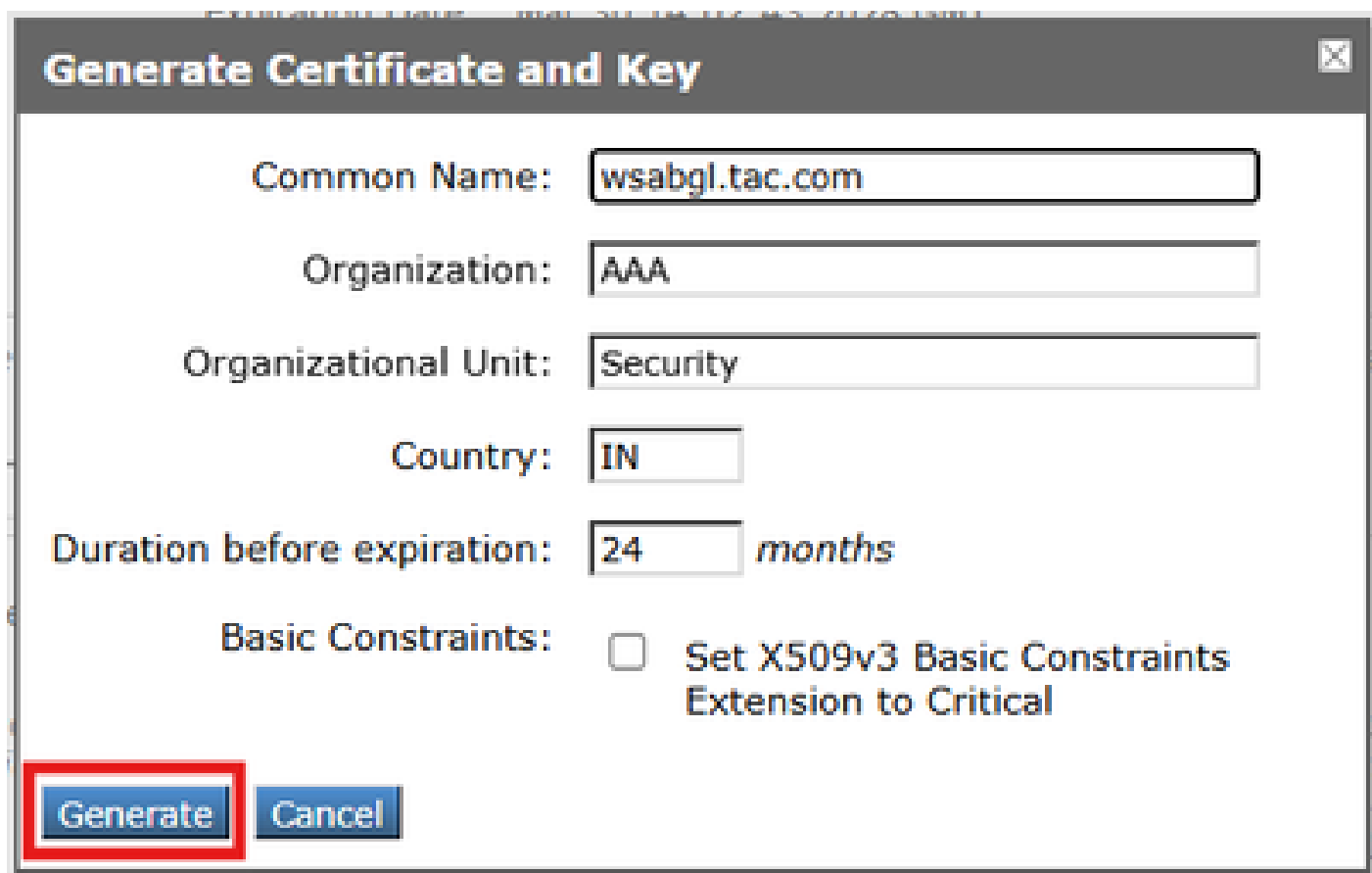
☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

No certificate has been generated.

9. Preencha os detalhes do certificado conforme necessário e clique em Gerar.



Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: ☐ Set X509v3 Basic Constraints Extension to Critical



Note: A duração do certificado deve ser um inteiro entre 24 e 60 meses e o país deve ser um código de país ISO de dois caracteres (somente letras maiúsculas).

10. Clique em Baixar solicitação de assinatura de certificado.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

☐ Use Uploaded Certificate and Key

Certificate: No file chosen

Key: No file chosen

☐ Key is Encrypted

No certificate has been uploaded.

☒ Use Generated Certificate and Key

Common name: wsibgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 19:56:43 2027 GMT

Basic Constraints: Not Critical

Download Certificate...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: No file chosen

11. Clique em Enviar.

12. Clique em Confirmar Alterações para Aplicar as alterações.

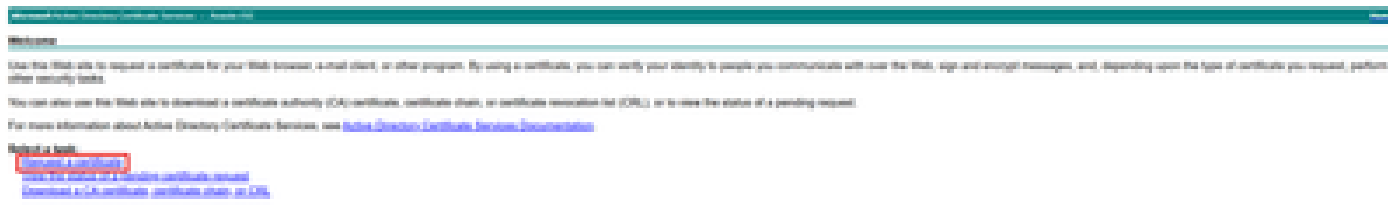


aviso: Se você não enviar e confirmar as alterações mencionadas, carregar diretamente o certificado assinado e executar a confirmação, poderá ter problemas durante a integração.

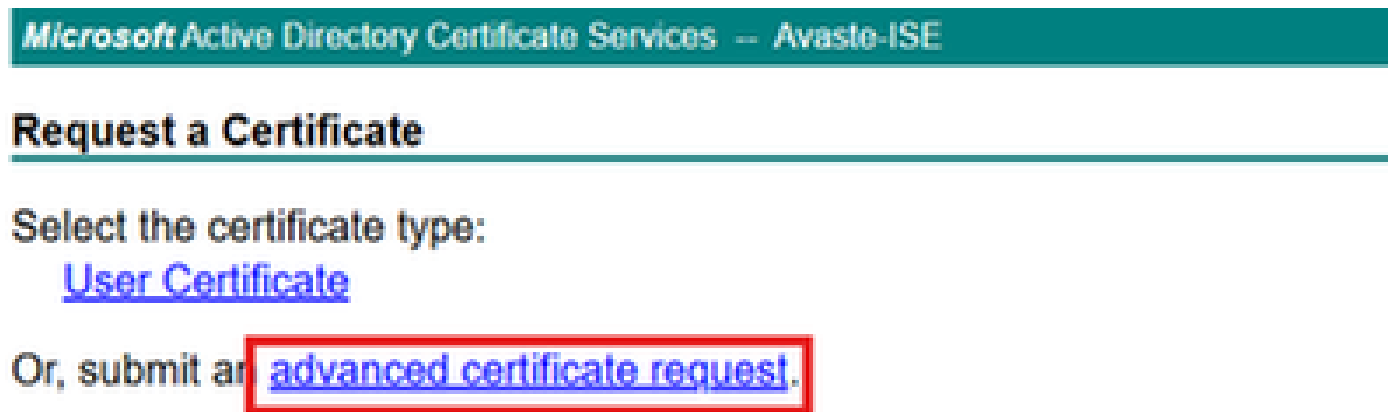
Seção B: Assinar um CSR de cliente WSA usando uma CA externa

1. Navegue para 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.

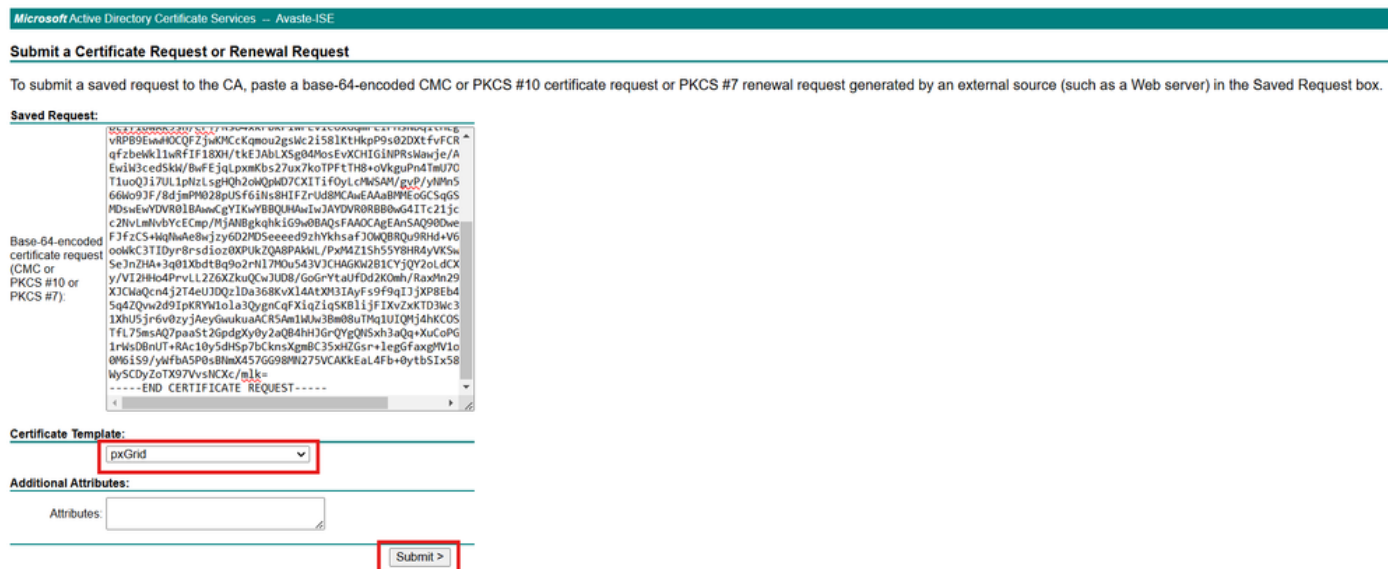


3. Escolha submeter uma solicitação avançada de certificado.



4. Copie o conteúdo do CSR gerado na seção anterior para o campo Solicitação salva.

5. Selecione pxGridas no Modelo de Certificado e, em seguida, clique em Enviar.





Note: 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 WSA-Client.cer.

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

Seção C: Vinculando o certificado do cliente WSA à CSR (Certificate Signing Request, Solicitação de assinatura de certificado) e integrando.

1. Navegue até a GUI do WSA (Web Security Appliance).
2. Navegue até Rede > Serviços de identificação > Mecanismo de serviço de identificação.
3. Clique em Edit Settings.
4. Navegue para a seção Certificado de cliente de equipamento da Web.
5. Na seção signed certificate, Upload do certificado assinado WSA-Client.cer



Use Generated Certificate and Key

[Generate New Certificate and Key](#)

Common name: wsabgl.tac.com

Organization: AAA

Organizational Unit: Security

Country: IN

Expiration Date: Mar 19 14:21:32 2027 GMT

Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: WSA-Client.cer.cer

6.Clique em Enviar.

7.Clique em Commit Changes para aplicar as alterações.

8.Clique em Editar configurações.

9.Role para Test Communication with ISE Nodes e clique em Start Test, o que pode resultar da seguinte forma:

Testar a comunicação com os nós do ISE

Testar a comunicação com os nós do ISE

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '10.127.197.128' address: 10.127.197.128
Validating WSA client certificate ...
Success: Certificate validation successful
Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful
Checking connection to ISE pxGrid Node(s) ...
Trying primary PxGrid server...
SXP not enabled.
ERS not enabled.
Preparing TLS connection...
Completed TLS handshake with PxGrid successfully.
Trying download user-session from (https://ise33.lab.local:8910)...
Failure: Failed to download user-sessions.
Trying download SGT from (https://ise33.lab.local:8910)...
Able to Download 17 SGTs.
Skipping all SXP related service requests as SXP is not configured.
Success: Connection to ISE pxGrid Node was successful.
Test completed successfully.
```

Verificar

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

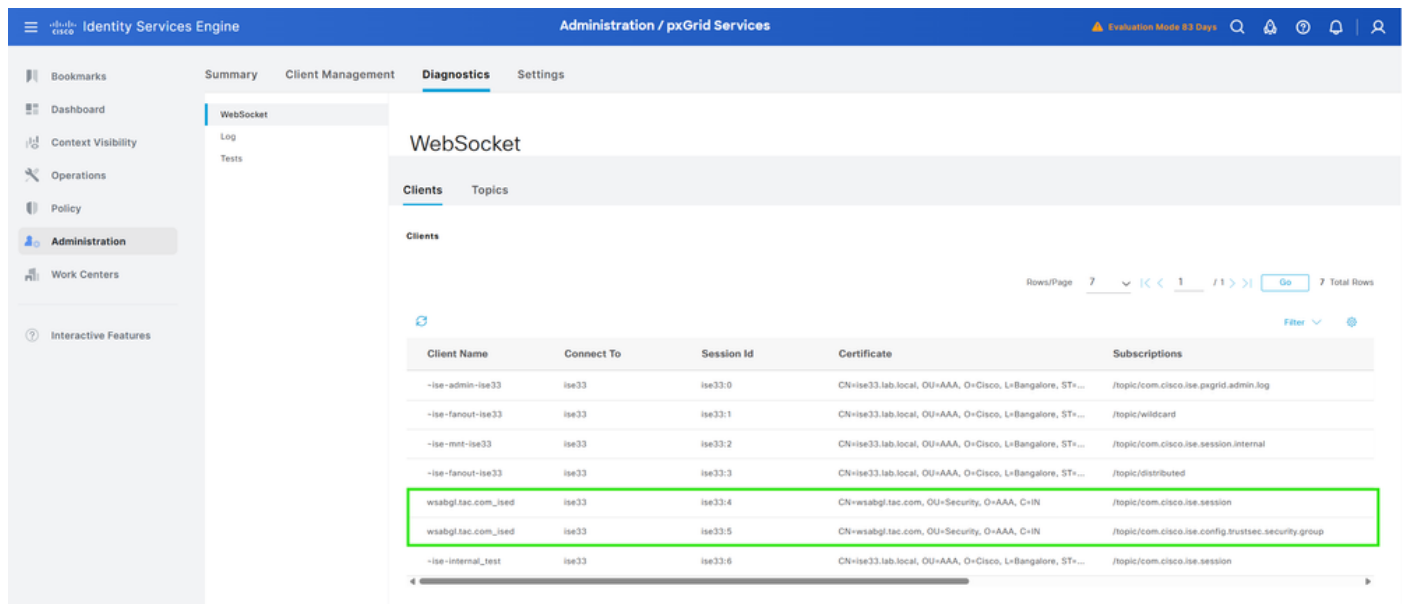
Isso gera o WSA como um cliente pxgrid com o statusEnabled.

The screenshot shows the Cisco ISE Administration console. The top navigation bar is blue with the text 'Identity Services Engine' and 'Administration / pxGrid Services'. Below the navigation bar, there's a sidebar on the left with various menu items. The main content area is titled 'Clients' and contains a table of pxGrid Clients. The table has columns for Name, Description, Client Groups, and Status. One client is listed: 'wsa@tac.com_iseif' with description 'ISED' and status 'Enabled'. The status 'Enabled' is highlighted with a green box.

Name	Description	Client Groups	Status
wsa@tac.com_iseif	ISED		Enabled

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

Websocket > Clientes:



Client Name	Connect To	Session Id	Certificate	Subscriptions
-ise-admin-ise33	ise33	ise33:0	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.pxgrid.admin.log
-ise-fanout-ise33	ise33	ise33:1	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/wildcard
-ise-mnt-ise33	ise33	ise33:2	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.session.internal
-ise-fanout-ise33	ise33	ise33:3	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/distributed
wsabgl.tac.com_ised	ise33	ise33:4	CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN	/topic/com.cisco.ise.session
wsabgl.tac.com_ised	ise33	ise33:5	CN=wsabgl.tac.com, OU=Security, O=AAA, C=IN	/topic/com.cisco.ise.config.trustsec.security.group
-ise-internal_test	ise33	ise33:6	CN=ise33.lab.local, OU=AAA, O=Cisco, L=Bangalore, ST=...	/topic/com.cisco.ise.session

Cisco ISE Pxgrid-server.log TRACE level.reference

<#root>

```
{ "timestamp":1742395398803, "level":"INFO", "type":"WS_SERVER_CONNECTED", "host":"ise33", "client":"
```

wsabgl.lab.local_ised

```
", "server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message":"WebSocket connected. session\u003d
TRACE [Thread-8][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Drop. exclude=[id=3,cl
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Authenticating null
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Certs up to date. user=~ise-pu
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- preAuthenticatedPrincipal = ~i
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- X.509 client authentication ce
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.config.MyX509Filter -:::- Authentication
```

success

```
: PreAuthenticatedAuthenticationToken [Principal=org.springframework.security.core.userdetails.User [Us
DEBUG [Thread-8][ ] cisco.cpm.pxgridwebapp.data.AuthzDaoImpl -:::- requestNodeName=wsabgl.lab.local
DEBUG [Thread-13][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Adding subscription=[
INFO [Thread-13][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Pubsub subscribe. subscrip
TRACE [WsIseClientConnection-804][ ] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. session=[id=34eae1
```

"wsabgl.lab.local_ised

```
", "server":"wss://ise33.lab.local:8910/pxgrid/ise/pubsub", "message":"Pubsub subscribe. subscription\u003d
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Received frame=[command=SE
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Authorized to send (cached
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute from=[id=0,
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute distributed
TRACE [Thread-3][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::- Distribute distributed
TRACE [sub-sender-1][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::- Send. subscription=[id=
TRACE [sub-sender-0][ ] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::- Send. subscription=[id=
DEBUG [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsSubscriber -:::- onStompMessage session=[id=34eae17d-5
DEBUG [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsSubscriber -:::- onStompMessage session=[id=4b4d7de4-b
TRACE [Grizzly(1)][ ] cpm.pxgrid.ws.client.WsEndpoint -:::- Send. session=[id=dd1d138d-a640-4f4f-bd
TRACE [Grizzly(1)][ ] cpm.pxgridwebapp.ws.distributed.FanoutDistributor -:::- DownstreamHandler sen
TRACE [Thread-10][ ] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::- Received frame=[command=S
```

```
TRACE [Thread-10][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Authorized to send (cached
```

Troubleshooting

Problema

Problema de CA desconhecido. No WSA, o teste de conexão do ISE falha com erro. Falha: A conexão com o servidor ISE PxGrid atingiu o tempo limite.

Test Communication with ISE Server

Start Test

Validating ISE Portal certificate ...

Success: Certificate validation successful

Checking connection to ISE PxGrid server...

Failure: Connection to ISE PxGrid server timed out

Test interrupted: Fatal error occurred, see details above.

Cisco ISE Pxgrid-server.log TRACE level.reference

<#root>

ERROR

```
[Thread-8][[]] cisco.cpm.pxgrid.cert.LoggingTrustManagerWrapper -:::-- checkClientTrusted exception.  
unable to find valid certification path to requested target principle=CN=wsabgl.lab.local, OU=Security,
```

```
TRACE [WsIseClientConnection-804][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=34eae1  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Received frame=[command=SE  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.StompPubsubEndpoint -:::-- Authorized to send (cached  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute from=[id=0,  
unable to find valid certification path to requested target
```

```
principle\u003dCN\u003dwsabgl.lab.local, OU\u003dSecurity, O\u003dAAA, C\u003dIN"}  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute distributed  
TRACE [Thread-9][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionDistributor -:::-- Distribute distributed  
TRACE [sub-sender-1][[]] cpm.pxgridwebapp.ws.pubsub.SubscriptionSender -:::-- Send. subscription=[id=  
DEBUG [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsSubscriber -:::-- onStompMessage session=[id=4b4d7de4-b  
TRACE [Grizzly(2)][[]] cpm.pxgrid.ws.client.WsEndpoint -:::-- Send. session=[id=dd1d138d-a640-4f4f-bd
```

O motivo da falha pode ser visto com capturas de pacotes,

Source	Destination	Protocol	Length	Info
10.76.105.168	10.127.197.128	TCP	74	42883 → 8910 [SYN] Seq=0 Win=65535 Len=0 MSS=1254 WS=64 SACK_PERM TSval=984988989 TSecr=0
10.127.197.128	10.76.105.168	TCP	74	8910 → 42883 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1459800712 TSecr=984988989 WS=128
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1 Ack=1 Win=66496 Len=0 TSval=984988999 TSecr=1459800712
10.76.105.168	10.127.197.128	TLSv1.2	583	Client Hello (SNI=10.127.197.128)
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=1459800715 TSecr=984988999
10.127.197.128	10.76.105.168	TLSv1.2	4818	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=1243 Win=65280 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=2485 Win=65280 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=3727 Win=64064 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=518 Ack=4753 Win=65472 Len=0 TSval=984989019 TSecr=1459800739
10.76.105.168	10.127.197.128	TLSv1.2	1526	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=4753 Ack=1978 Win=33024 Len=0 TSval=1459800761 TSecr=984989039
10.127.197.128	10.76.105.168	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [FIN, ACK] Seq=4760 Ack=1978 Win=33024 Len=0 TSval=1459800769 TSecr=984989039
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1978 Ack=4760 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.76.105.168	10.127.197.128	TCP	66	42883 → 8910 [FIN, ACK] Seq=1978 Ack=4761 Win=66496 Len=0 TSval=984989049 TSecr=1459800769
10.127.197.128	10.76.105.168	TCP	66	8910 → 42883 [ACK] Seq=4761 Ack=1979 Win=33024 Len=0 TSval=1459800770 TSecr=984989049

Solução

1. Verifique se o certificado assinado do equipamento para Web está associado com êxito ao WSA e se as alterações foram confirmadas.
2. Verifique se o emissor ou o certificado de CA raiz do certificado do cliente WSA faz parte do Repositório Confiável no Cisco ISE.

Defeitos conhecidos

ID de bug da Cisco	Descrição
ID de bug da Cisco 23986	A solicitação da API getUserGroups do Pxgrid retornou uma resposta vazia.
ID de bug da Cisco 77321	O WSA recebe SIDs em vez de grupos do AD do ISE.

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.