

Solucionar problemas de certificado de administrador do ISE expirado

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Certificado do administrador do ISE \(expirado\)](#)

[Validar Status do Certificado do Administrador](#)

[Plano de ação](#)

[Troubleshooting](#)

[Caso de uso 1: Nó secundário não registrado preso no estado distribuído \(ise-psn1\)](#)

[Validar o status](#)

[Solução](#)

[Caso de uso 2: GUI de nó secundário cancelada inacessível \(ise-psn2\)](#)

[Validar o status](#)

[Solução](#)

[Referências](#)

[Relevante](#)

Introdução

Este documento descreve como solucionar problemas e renovar um certificado de administrador do Cisco Identity Services Engine (ISE) expirado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha o conhecimento destes tópicos:

- Implantação do Cisco ISE.
- Gerenciamento de certificados no Cisco ISE.

Componentes Utilizados

As informações neste documento são baseadas nesta versão de software:

- Cisco Identity Services Engine (ISE) versão 3.3 Patch4.

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.

Informações de Apoio

Este documento se concentra na implantação distribuída; no entanto, você pode usar o mesmo plano de solução de problemas em um nó autônomo.

Na Implantação distribuída do ISE, o nó é o nó de administração primário (PPAN) ou secundário.

Este documento usa o certificado do administrador do ISE como um certificado autoassinado para demonstrar o impacto do certificado expirado, mas essa abordagem não é recomendada para um sistema de produção. É melhor usar o certificado assinado por autoridade para uso administrativo.

 Note: A Cisco recomenda que você mantenha o seu certificado de administrador em estado de integridade e planeje a renovação com antecedência. Encontre este guia para ajudá-lo a rastrear e renovar os certificados do sistema ISE ([Configurar renovações de certificado no ISE](#)).

Certificado do administrador do ISE (expirado)

Validar Status do Certificado do Administrador

Etapa 1. Verifique o status da implantação. Navegue até Administração > Sistema > Implantação.

Você pode verificar o status dos nós secundários, como mostrado, os três nós secundários são (Not in Sync).

1. Nó Admin Principal (PPAN):

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node Restart

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

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

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
Default self-signed server certificate - CN=SA ML_ise-ppan.kdlab2.local	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdlab2.local	ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml s...	SAML		SAML_ise-ppan.kdlab2.lo...	SAML_ise-ppan.kdlab2.lo...	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-ppan#000003	pxGrid		ise-ppan.kdlab2.local	Certificate Services Endp...	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=ISE Messaging Service	ISE Messaging Service		ise-ppan.kdlab2.local	Certificate Services Endp...	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
> ise-psn1							
> ise-psn2							
> ise-span							

Status do Certificado de Administrador do PPAN

2. Nós secundários.

Para os nós secundários, pode ser 1 de 2 opções e, em ambos os casos, você deve aplicar o mesmo plano de ação:

R. É possível expandir o certificado do sistema do nó e confirmar se o certificado admin está expirado:

Identity Services Engine

Administration / System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Admin Certificate Node Restart

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

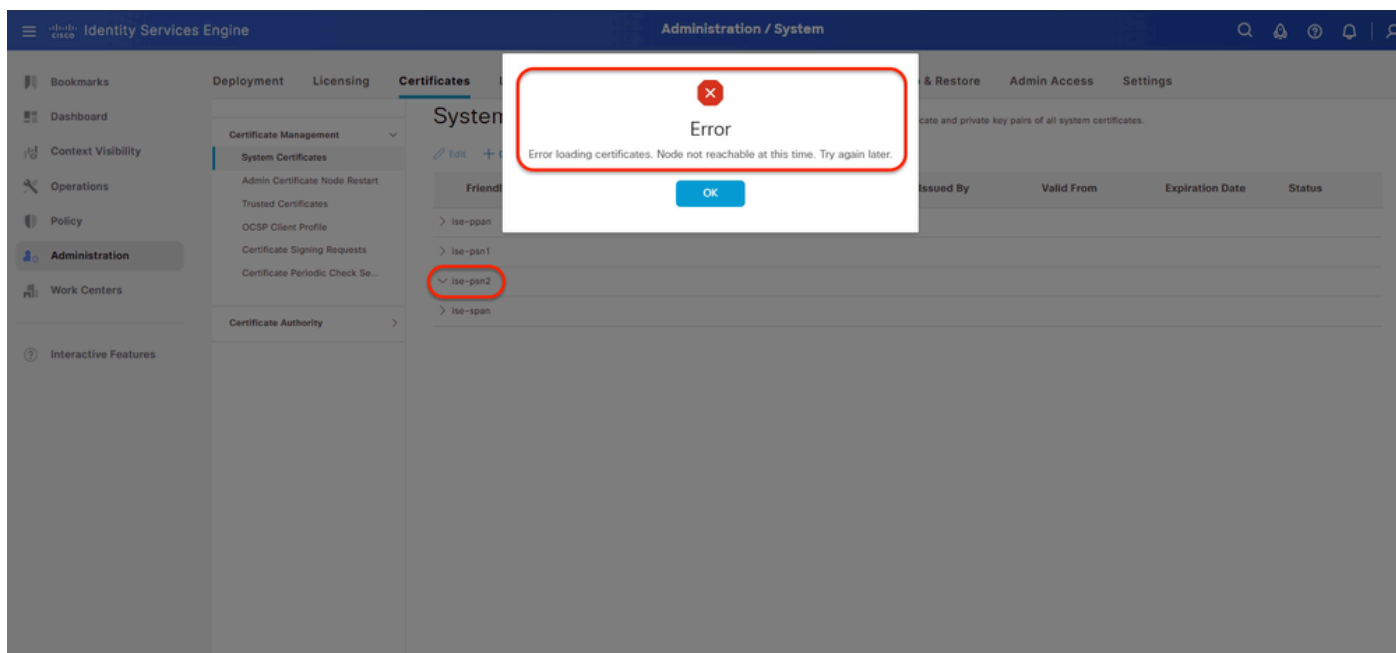
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ise-ppan							
ise-psn1							
ise-psn2							
ise-span							
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml s...	SAML		SAML_ise-ppan.kdlab2.lo...	SAML_ise-ppan.kdlab2.lo...	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-span#000005	pxGrid		ise-span.kdlab2.local	Certificate Services Endp...	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endp...	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Status do certificado de administrador do nó secundário

B. Lançar erro ("Erro ao carregar certificados. Nó não alcançável no momento. Tente novamente mais tarde.") conforme mostrado para (ise-psn2



Nó secundário não alcançável

Plano de ação

Após confirmar que o certificado admin expirou para todos os 4 nós, você deve aplicar estas etapas:

Etapa 1. Cancele o registro de todos os nós secundários da implantação distribuída (somente se o certificado do administrador tiver expirado).

Navegue até Administration > System > Deployment > Check [✓] dos nós secundários e clique em Deregister.

 Note: Cancelar o registro do nó significa que ele será movido para autônomo para que você possa renovar o certificado de administrador neste nó.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 3 Total 4

1

2

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-psn1	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-psn2	Policy Service, pxGrid		SESSION, PROFILER	⚠
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	⚠

Cancelar Registro de Nós Secundários

 Note: Lembre-se de cancelar o registro apenas dos nós secundários em que o certificado de administrador já expirou e de manter o restante. Neste documento, todos os nós secundários estão expirados.

Identity Services Engine Administration / System

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

Deployment Nodes

Selected 0 Total 1

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	✓

Todos os nós secundários estão com registro cancelado

Etapa 2. Renove o certificado admin do Nó Admin Primário (PPAN).

1. Navegue para Administração > Sistema > Certificados > Gerenciamento de certificado > Certificados do sistema > Clique em +Gerar certificado autoassinado:

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

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
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-ppan.kdlab2.local	ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdlab2.local	SAML		SAML_ise-ppan.kdlab2.local	SAML_ise-ppan.kdlab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ise-ppan#00003	pxGrid		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdlab2.local, OU=ISE Messaging Service Ice#Certificate Services Endpoint Sub CA - ise-ppan#00004	ISE Messaging Service		ise-ppan.kdlab2.local	Certificate Services Endpoint Sub CA - ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active

Gerar novo Certificado de Administrador Autoassinado

2. Selecione o Nó Admin Primário (PPAN) (ise-ppan) e preencha as informações do certificado:

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade 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 Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node **ise-ppan**

Subject

Common Name (CN)
\$FQDN\$

Organizational Unit (OU)
Tech

Organization (O)
KD

City (L)

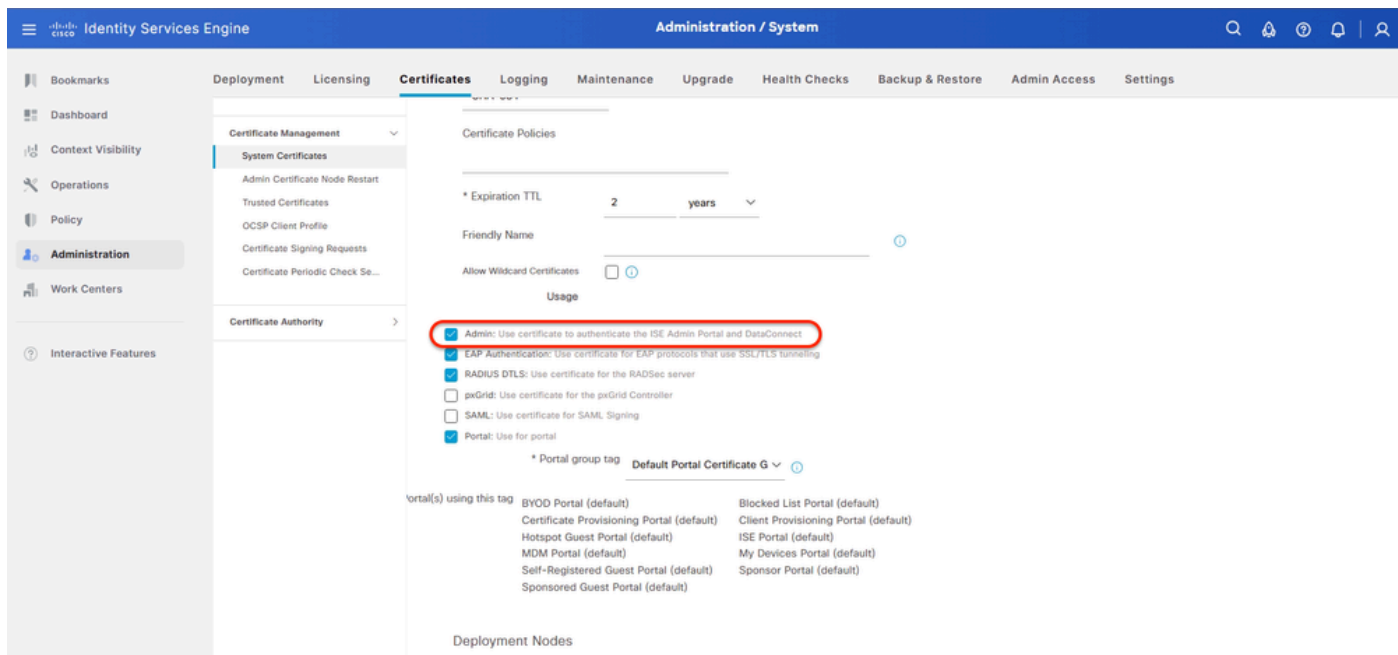
State (ST)

Country (C)

Subject Alternative Name (SAN)

Selecione o Nó Admin Principal (PPAN)

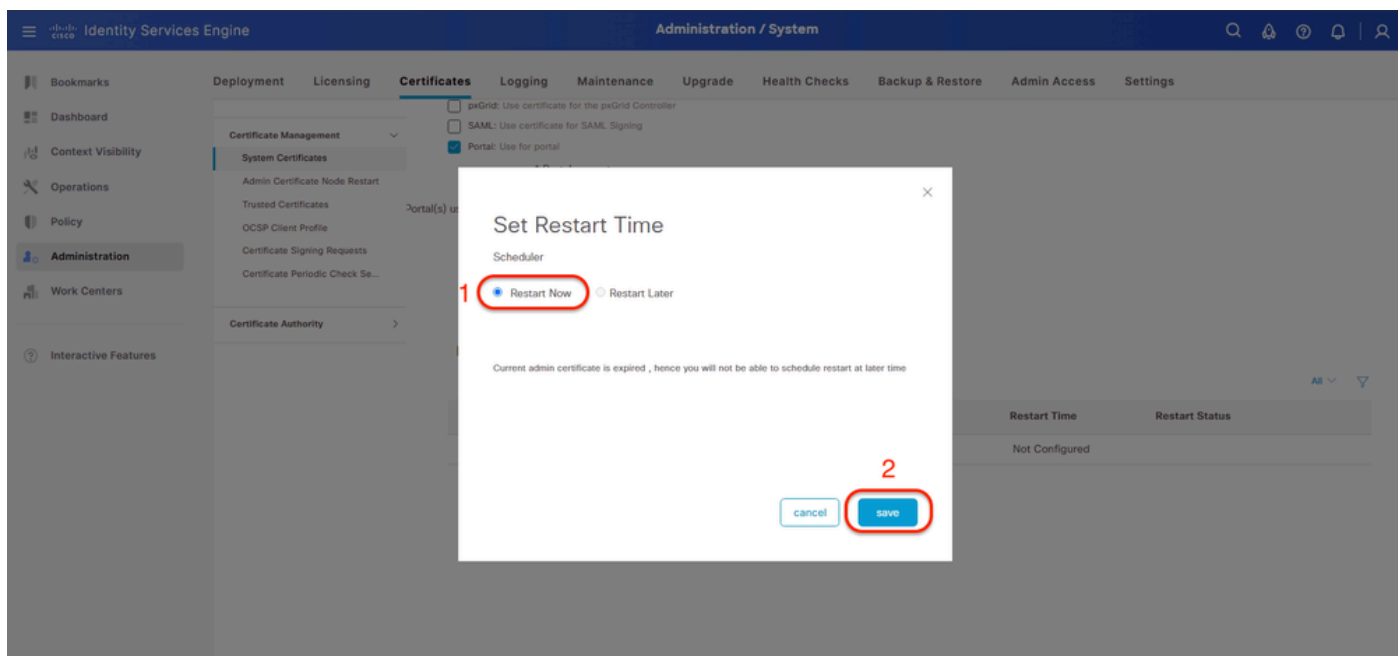
3. Marque [✓] o uso de Admin.



Uso do administrador

4. Defina a Hora de Reinicialização como Reiniciar Agora para o Nó Admin Primário (PPAN). Defina todos os nós na implantação como Reiniciar agora ou Reiniciar mais tarde.

Depois de renovar um certificado de administrador (um certificado configurado para uso administrativo) no Nó Admin Primário (PPAN), todos os nós em sua implantação devem ser reiniciados.



Definir a hora de reinicialização como Agora

5. Clique em Submeter.

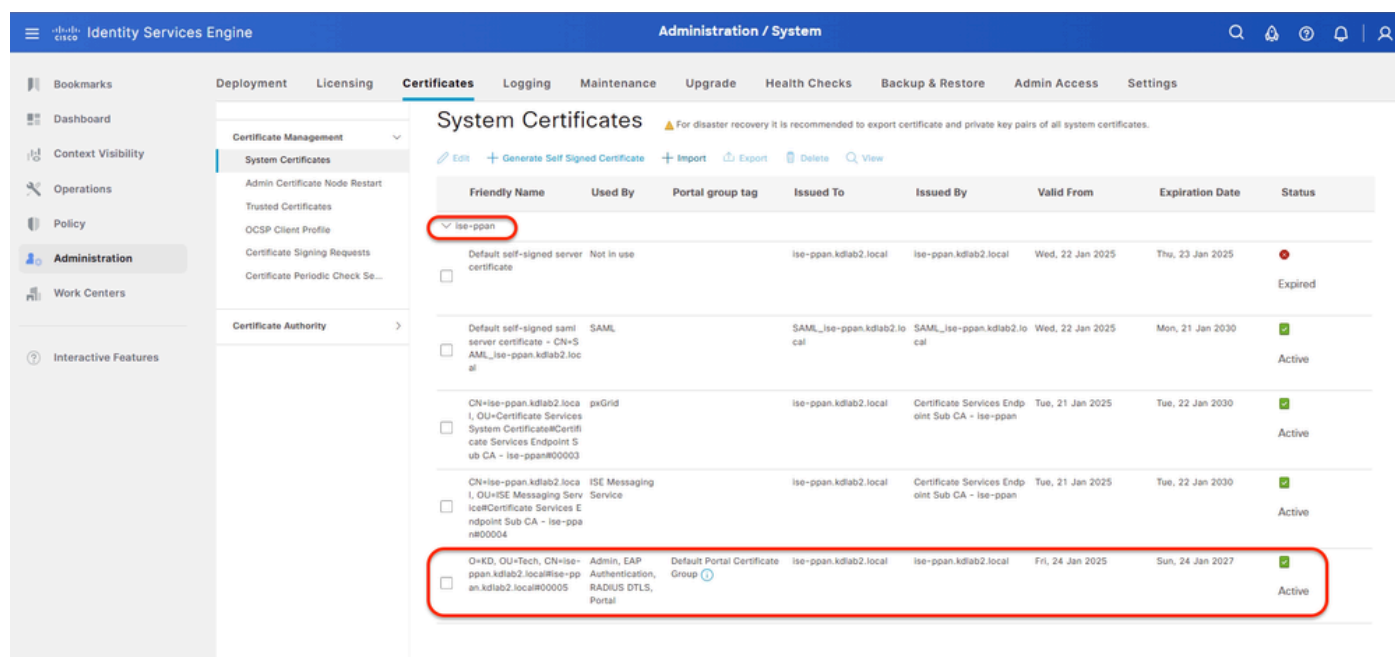
 Note: Depois de renovar um certificado de administrador (um certificado configurado para uso administrativo) no Nó Admin Primário (PPAN), todos os nós em sua implantação devem

 ser reiniciados. Você pode reiniciar cada nó imediatamente ou agendar as reinicializações mais tarde. Esse recurso permite garantir que nenhum processo em execução seja interrompido pelas reinicializações automáticas, proporcionando maior controle sobre o processo.

Você pode exibir e editar as reinicializações agendadas na janela Administration > System > Certificates > Admin Certificate Node Restart, disponível no Cisco ISE Release 3.3.

6. Verifique o novo certificado admin do Nó Admin Primário (PPAN).

Navegue até Administration > System > Certificates > Certificate Management > System Certificates > Expand (ise-ppan).



Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Not in use		ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
Default self-signed saml server certificate - CN=SAML_ise-ppan.kdiab2.local	SAML		SAML_ise-ppan.kdiab2.local	SAML_ise-ppan.kdiab2.local	Wed, 22 Jan 2025	Mon, 21 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=Certificate Services, System Certificate Services Endpoint Sub CA - Ise-ppan#00003	peGrid		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
CN=ise-ppan.kdiab2.local, OU=ISE Messaging Service, IseCertificate Services Endpoint Sub CA - Ise-ppan#00004	ISE Messaging Service		ise-ppan.kdiab2.local	Certificate Services Endpoint Sub CA - Ise-ppan	Tue, 21 Jan 2025	Tue, 22 Jan 2030	Active
O=ED, OU=Tech, CN=ise-ppan.kdiab2.local, OU=ise-ppan.kdiab2.local#00005	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-ppan.kdiab2.local	ise-ppan.kdiab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active

Novo certificado do administrador (ise-ppan)

Etapa 3. Renove o certificado de administrador dos nós secundários.

1. Confirme o nó secundário na implantação autônoma depois de cancelar o registro da implantação distribuída.

Navegue até o nó via GUI (<https://<FQDN/IP>>) e navegue até Administração > Sistema > Implantação.

The screenshot shows the 'Deployment Nodes' table in the Identity Services Engine Administration / System interface. The table has columns: Hostname, Personas, Role(s), Services, and Node Status. The 'ise-span' node is highlighted with a red circle, and its role 'STANDALONE' is also highlighted with a red circle.

Hostname	Personas	Role(s)	Services	Node Status
ise-span	Administration, Monitoring, Policy Service	STANDALONE	SESSION_PROFILER	✓

(ise-span) na implantação independente

2. Navegue até Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados do Sistema > Clique em +Gerar Certificado AutoAssinado.

The screenshot shows the 'System Certificates' section in the Identity Services Engine Administration / System interface. The '+ Generate Self Signed Certificate' button is highlighted with a red circle. Below the button is a table of system certificates.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	ise-span.kdiab2.local	ise-span.kdiab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
CN=ise-span.kdiab2.local, OU=Certificate Services System Certificate@Certificate Services Endpoint Sub CA - ise-span#00007	pxGrid		ise-span.kdiab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
CN=ise-span.kdiab2.local, OU=ISE Messaging Service Ice@Certificate Services Endpoint Sub CA - ise-span#00008	ISE Messaging Service		ise-span.kdiab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
Default self-signed saml server certificate - CN=SAML_ise-span.kdiab2.local	SAML		SAML_ise-span.kdiab2.local	SAML_ise-span.kdiab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Gerar novo Certificado de Administrador Autoassinado

3. Selecione (ise-span) e preencha as informações do certificado.

Identity Services Engine Administration / System

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 Se...

Certificate Authority

Generate Self Signed Certificate

* Select Node **ise-span**

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

Selecione o nó

4. Marque [✓] o uso de Admin.

Identity Services Engine Administration / System

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 Se...

Certificate Authority

* Digest to Sign With **SHA-384**

Certificate Policies

* Expiration TTL **2** years

Friendly Name

Allow Wildcard Certificates ☐

Usage

☒ Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

☒ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

☒ RADIUS DTLS: Use certificate for the RADSec server

☐ pxGrid: Use certificate for the pxGrid Controller

☐ SAML: Use certificate for SAML Signing

☒ Portal: Use for portal

* Portal group tag **Default Portal Certificate G**

Portal(s) using this tag

BYOD Portal (default)	Blocked List Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	ISE Portal (default)
MDM Portal (default)	My Devices Portal (default)
Self-Registered Guest Portal (default)	Sponsor Portal (default)
Sponsored Guest Portal (default)	

Uso do administrador

Note: A alteração do certificado da função do administrador no nó ISE reinicia os serviços.

5. Clique em Submeter.

6. Verifique o novo certificado de administrador em (ise-span).

Navegue até Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados do Sistema > Expandir (ise-span).

System Certificates

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

Actions: 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
ise-span	Default self-signed server certificate	Not in use	ise-span.kdlab2.local	ise-span.kdlab2.local	Wed, 22 Jan 2025	Thu, 23 Jan 2025	Expired
O=ED, OU=Tech, CN=ise-span.kdlab2.local@ise-span.kdlab2.local	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ise-span.kdlab2.local	ise-span.kdlab2.local	Fri, 24 Jan 2025	Sun, 24 Jan 2027	Active
CN=ise-span.kdlab2.local, OU=Certificate Services Endpoint Sub CA - ise-span00007	pxGrid		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
CN=ise-span.kdlab2.local, OU=ISE Messaging Service	ISE Messaging Service		ise-span.kdlab2.local	Certificate Services Endpoint Sub CA - ise-span	Wed, 22 Jan 2025	Wed, 23 Jan 2030	Active
Default self-signed saml server certificate - CN=SAML_ise-span.kdlab2.local	SAML		SAML_ise-span.kdlab2.local	SAML_ise-span.kdlab2.local	Thu, 23 Jan 2025	Tue, 22 Jan 2030	Active

Novo certificado de administrador (ise-span)

Etapa 4. Registrar os nós secundários para a implantação distribuída.

Configure suas personalidades e funções de implantação como antes (Admin, MNT, PSN, etc.).

1. Na GUI do Nó Admin Primário (PPAN). Navegue até Administração > Sistema > Disponibilização > Clique em Registrar.

Deployment Nodes

Selected 0 Total 1

Actions: Edit, Register, Sync, Deregister

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), PRI(M)	NONE	Active

GUI do nó administrativo primário (PPAN)

2. Informe o FQDN e as credenciais do nó secundário (Nome de Usuário/Senha).

Insira o FQDN (nome de domínio totalmente qualificado) resolvível por DNS do nó autônomo que você vai registrar. O FQDN do (PPAN) e o nó que está sendo registrado devem poder ser resolvidos um do outro.

Identity Services Engine Administration / System

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

Deployment Nodes List > Specify Hostname

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*
ise-span.kdlab2.local

User Name*
admin

Password*

Next Cancel

Inserir acesso ao nó secundário

3. Ative a pessoa e os serviços corretos.

Identity Services Engine Administration / System

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

Deployment Nodes List > Configure Node

Register ISE Node - Step 2: Configure Node

General Settings

Hostname ise-span

FQDN ise-span.kdlab2.local

IP Address

Node Type Identity Services Engine (ISE)

Role SECONDARY

Administration

Monitoring

Role PRIMARY

Other Monitoring Node ise-ppan

Dedicated MnT

Registrar nó secundário (ise-span)

Etapa 5. Verificar o status da implantação.

Navegue até Administração > Sistema > Implantação.

Identity Services Engine Administration / System

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Deployment Nodes

Selected 0 Total 2

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓

(ise-span) Adicionado à implantação

Troubleshooting

Caso de uso 1: Nó secundário não registrado preso no estado distribuído (ise-psn1)

Validar o status

Etapa 1. Confirmar o status da implantação distribuída.

Na GUI do Nó Admin Primário (PPAN). Navegue até Administração > Sistema > Implantação. Você pode confirmar que esse nó (ise-psn1) já está com o registro cancelado.

Identity Services Engine Administration / System

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

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Deployment Nodes

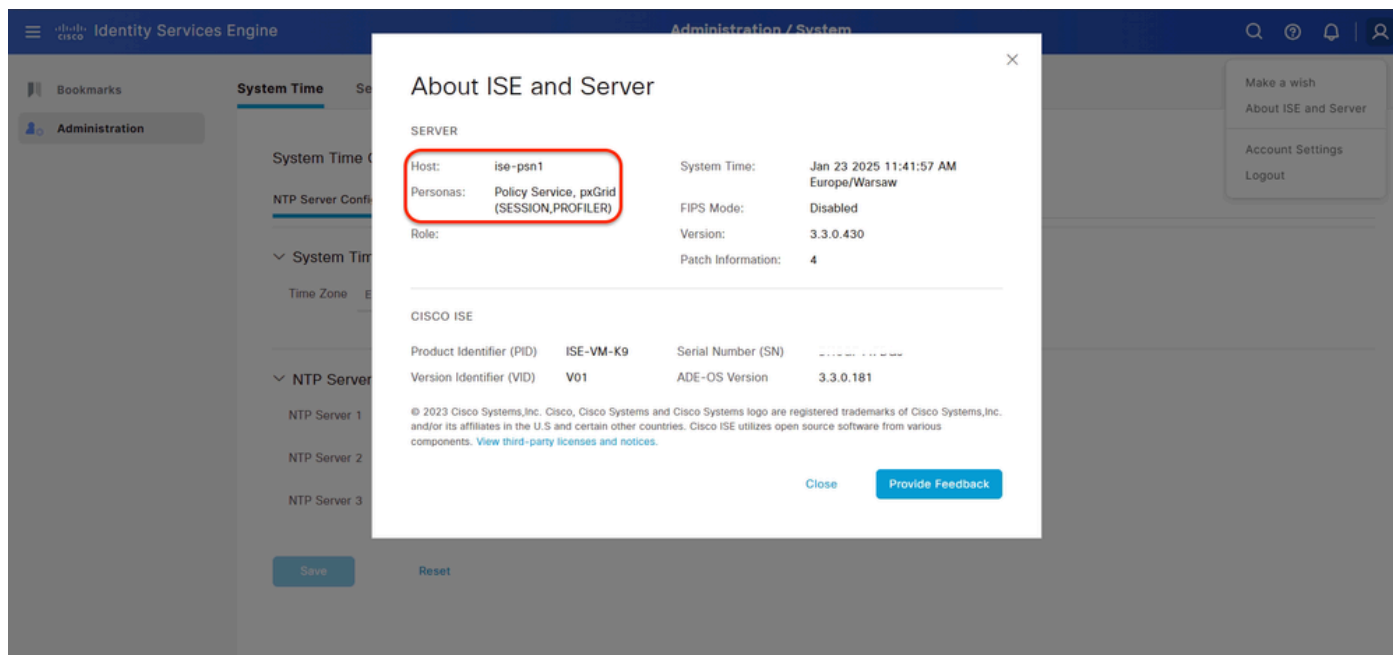
Selected 0 Total 2

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓

(PPAN) Nós de Implantação

Etapa 2. Confirmar o status do nó (ise-psn1).

Navegue no nó secundário via GUI (<https://ise-psn1.kdlab.local>) e navegue Login > Sobre o ISE e o Servidor.

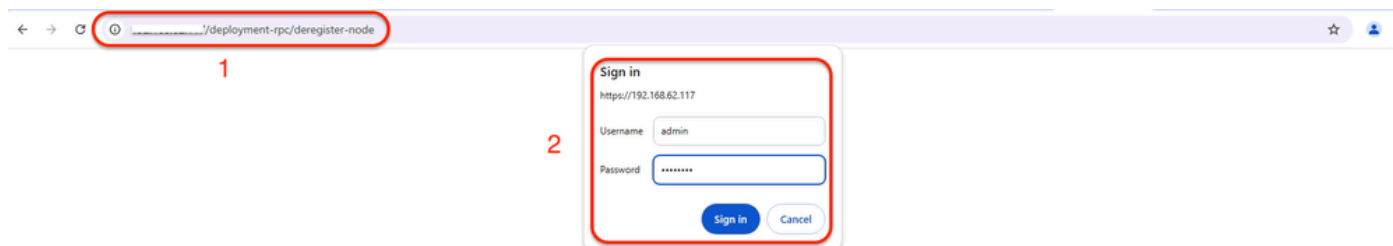


Nó secundário (ise-psn1) travado no status da implantação distribuída

Solução

Etapa 1. Cancele o registro do nó (ise-psn1) manualmente.

Aplique o nó (ise-psn1) à implantação autônoma via GUI (<https://<ise-psn1 IP>/deployment-rpc/deregister-node>).



Cancelar o registro do nó manualmente - GUI

Etapa 2. Verifique o (ise-psn1) agora na implantação autônoma.

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), Work Centers, and Interactive Features. The main content area is titled 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. The table contains one row for 'ise-psn1' with the following values: Administration, Monitoring, Policy Service; STANDALONE; SESSION, PROFILER; and a green checkmark indicating the node status. The 'ise-psn1' hostname and the 'STANDALONE' role are circled in red.

Hostname	Personas	Role(s)	Services	Node Status
ise-psn1	Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER	✓

(ise-psn1) em implantação autônoma

Etapa 3. Depois que você puder confirmar o nó no status autônomo, prossiga com as mesmas etapas na seção Plano de Ação:

1. Remova o certificado admin do nó (ise-psn1).
2. Registre o nó (ise-psn1) para a implantação distribuída.
3. Verifique o status da implantação.

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), Work Centers, and Interactive Features. The main content area is titled 'Deployment Nodes' and shows a table with the following columns: Hostname, Personas, Role(s), Services, and Node Status. The table contains three rows: 'ise-ppan' (Administration, Monitoring; PRI(A), SEC(M); NONE; ✓), 'ise-psn1' (Policy Service, pxGrid; SESSION, PROFILER; ✓), and 'ise-span' (Administration, Monitoring; SEC(A), PRI(M); NONE; ✓). The 'ise-psn1' row is highlighted with a red circle, and its Role(s) 'Policy Service, pxGrid' is also highlighted with a red circle.

Hostname	Personas	Role(s)	Services	Node Status
ise-ppan	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
ise-psn1	Policy Service, pxGrid	SESSION, PROFILER		✓
ise-span	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓

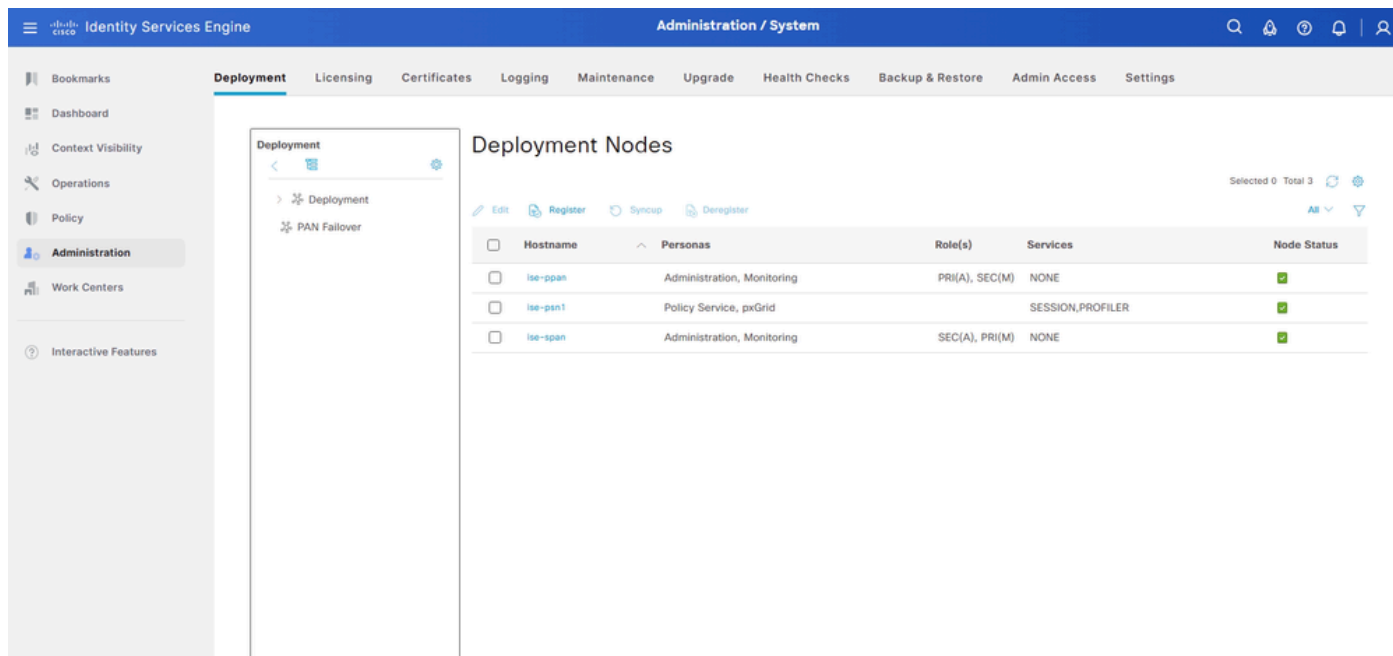
(ise-psn1) Adicionado à implantação

Caso de uso 2: GUI de nó secundário cancelada inacessível (ise-psn2)

Validar o status

Etapa 1. Confirmar o status da implantação distribuída.

Na GUI do Nó Admin Primário (PPAN). Navegue até Administração > Sistema > Implantação. Você pode confirmar que esse nó (ise-psn2) já está com o registro cancelado.

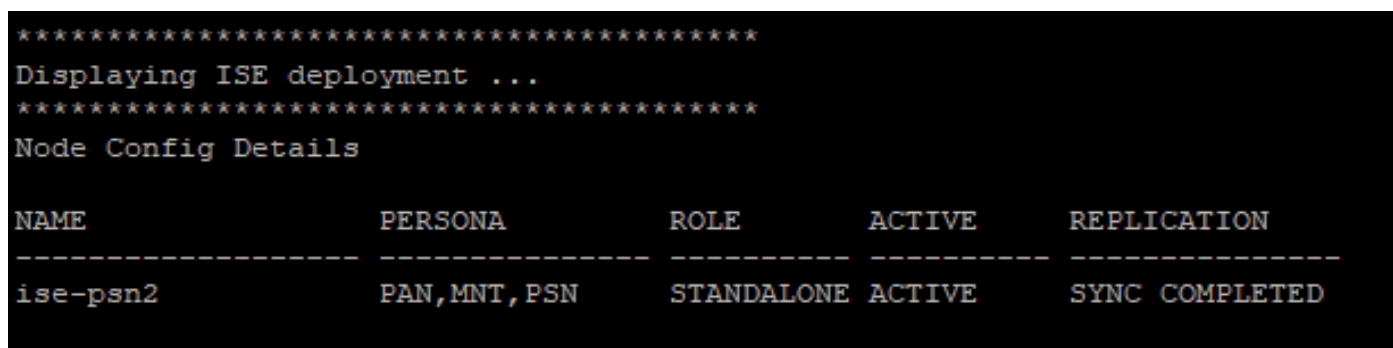


(PPAN) Nós de Implantação

Etapa 2. Confirmar (ise-psn2).

Como o certificado do administrador expirou em alguns casos, você pode ter estes sintomas:

- GUI (ise-psn2) inalcançável.
- (ise-psn2) CLI (show application status ise) Aplicativo ISE travado em (inicializando ou não executando).
- (ise-psn2) CLI (show tech) o nó já está na implantação autônoma.



(ise-psn2) em implantação autônoma

Solução

Etapa 1. Renove o certificado admin do nó (ise-psn2).

1. Faça login em (ise-psn2) via CLI.
2. Insira application configure ise.
3. Insira 31 ([31] Gerar certificado administrativo autoassinado).
4. Deseja continuar? s/[n]: y
5. Deseja substituir o certificado existente após a geração? s/[n]: y

```
ise-psn2/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
[36]Check and Repair Filesystem
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
[38]Localised ISE Install
[39]Reset System 360 Monitoring Page
[40]Enable/Disable Explicit EC Check
[41]Gather Diagnostic data for Certificates
[42]Enable/Disable Parse SAN DirName Extension
[0]Exit

31
After this operation, the ISE node will restart
Do you want to continue? y/[n]: y
Certificate Subject
  *Common Name (CN) : ise-psn2.kdlab2.local
  Enter Organization Unit (OU) : Tech
  Enter Organization (O) : KD
Do you want to replace existing certificate after generation? y/[n]: y
Old Memory Size : 32639004
```


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.