

Entender os serviços de autoridade de certificação interna do ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Serviço de autoridade de certificação \(CA\)](#)

[Funcionalidade de CA do ISE](#)

[Certificados de CA do ISE provisionados em nós de serviço de administração e política](#)

[Inscrição no Serviço de Transporte Seguro \(EST\)](#)

[Casos de uso EST](#)

[Por que EST?](#)

[EST no ISE](#)

[Tipos de solicitações no ISE EST](#)

[Solicitação de certificados CA \(com base no RFC 7030\)](#)

[Solicitação de inscrição simples \(com base no RFC 7030\)](#)

[Status do serviço EST e CA](#)

[Status mostrado na GUI](#)

[Status mostrado na CLI](#)

[Alarmes no painel](#)

[Impacto se os serviços CA e EST não estiverem em execução](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o serviço CA e o serviço Enrollment over Secure Transport (EST) presentes no Cisco Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE
- Certificados e infraestrutura de chave pública (PKI)
- Protocolo SCEP (Simple Certificate Enrollment Protocol)
- Protocolo de Status de Certificados Online (OCSP)

Componentes Utilizados

As informações neste documento são baseadas no Identity Services Engine 3.0.

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.

Serviço de autoridade de certificação (CA)

Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação (CA) externa. A Autoridade de Certificação Interna (CA) do Cisco ISE emite e gerencia certificados digitais para endpoints a partir de um console centralizado para permitir que os funcionários usem seus dispositivos pessoais na rede da empresa. Um certificado digital assinado pela CA é considerado um padrão do setor e mais seguro. O PAN (nó primário de administração de política) é a CA raiz. Os nós de serviço de política (PSNs) são CAs subordinadas ao PAN principal.

Funcionalidade de CA do ISE

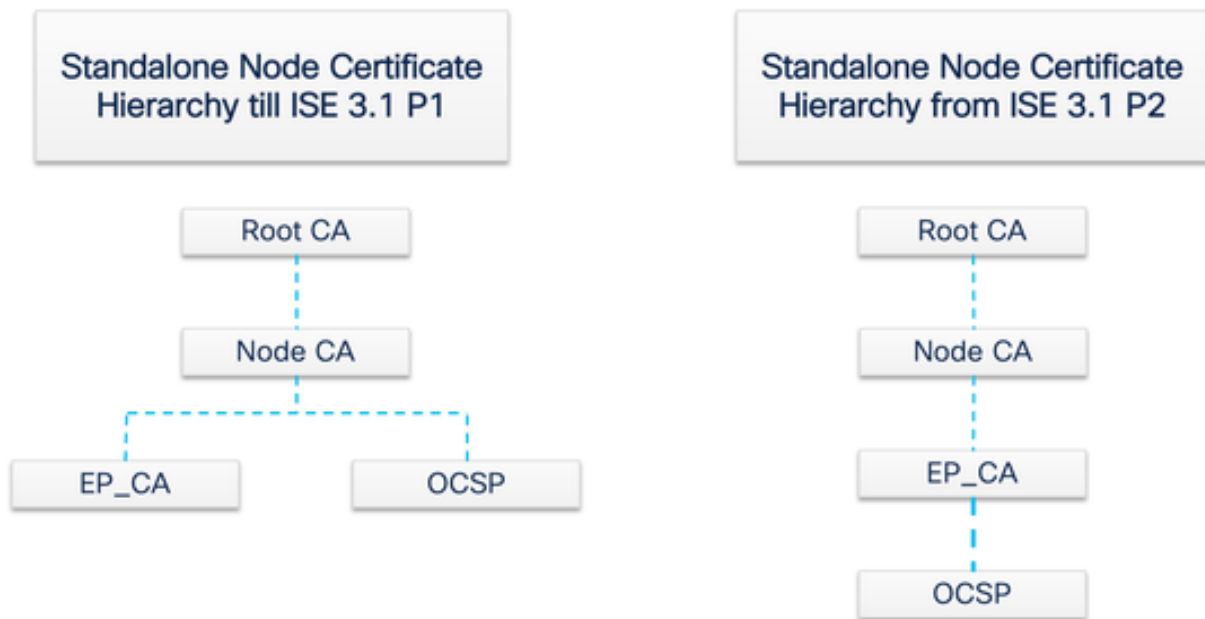
A CA do ISE oferece esta funcionalidade:

- Emissão de certificado: Valida e assina CSRs (Certificate Signing Requests, Solicitações de Assinatura de Certificado) para terminais que se conectam à rede.
- Gerenciamento de chaves: Gera e armazena com segurança chaves e certificados nos nós PAN e PSN.
- Armazenamento do certificado: Armazena certificados emitidos para usuários e dispositivos.
- Suporte ao Protocolo de Status de Certificados Online (OCSP - Online Certificate Status Protocol): Fornece um respondente OCSP para verificar a validade dos certificados.

Certificados de CA do ISE provisionados em nós de serviço de administração e política

Após a instalação, um nó do Cisco ISE é provisionado com um certificado de CA raiz e um certificado de CA de nó para gerenciar certificados para endpoints.

Quando uma implantação é configurada, o nó designado como o PAN (Primary Administration Node, nó primário de administração) se torna a CA raiz. O PAN tem um certificado CA raiz e um certificado CA de nó que é assinado pela CA raiz.



Quando um nó de administração secundário (SAN) é registrado no PAN, um certificado CA de nó é gerado e assinado pela CA raiz no nó de administração primário.

Qualquer Nó de serviço de política (PSN) registrado com o PAN recebe uma CA de endpoint e um certificado OCSP assinado pela CA de nó do PAN. Os Policy Service Nodes (PSNs) são CAs subordinadas ao PAN. Quando a CA do ISE é usada, a CA do endpoint no PSN emite os certificados para os endpoints que acessam a rede.



Note: A partir do ISE 3.1 Patch 2 e do ISE 3.2 FCS, a Hierarquia de Certificados OCSP foi alterada.

De acordo com o RFC 6960:

"O emissor do certificado DEVE executar uma das seguintes ações:

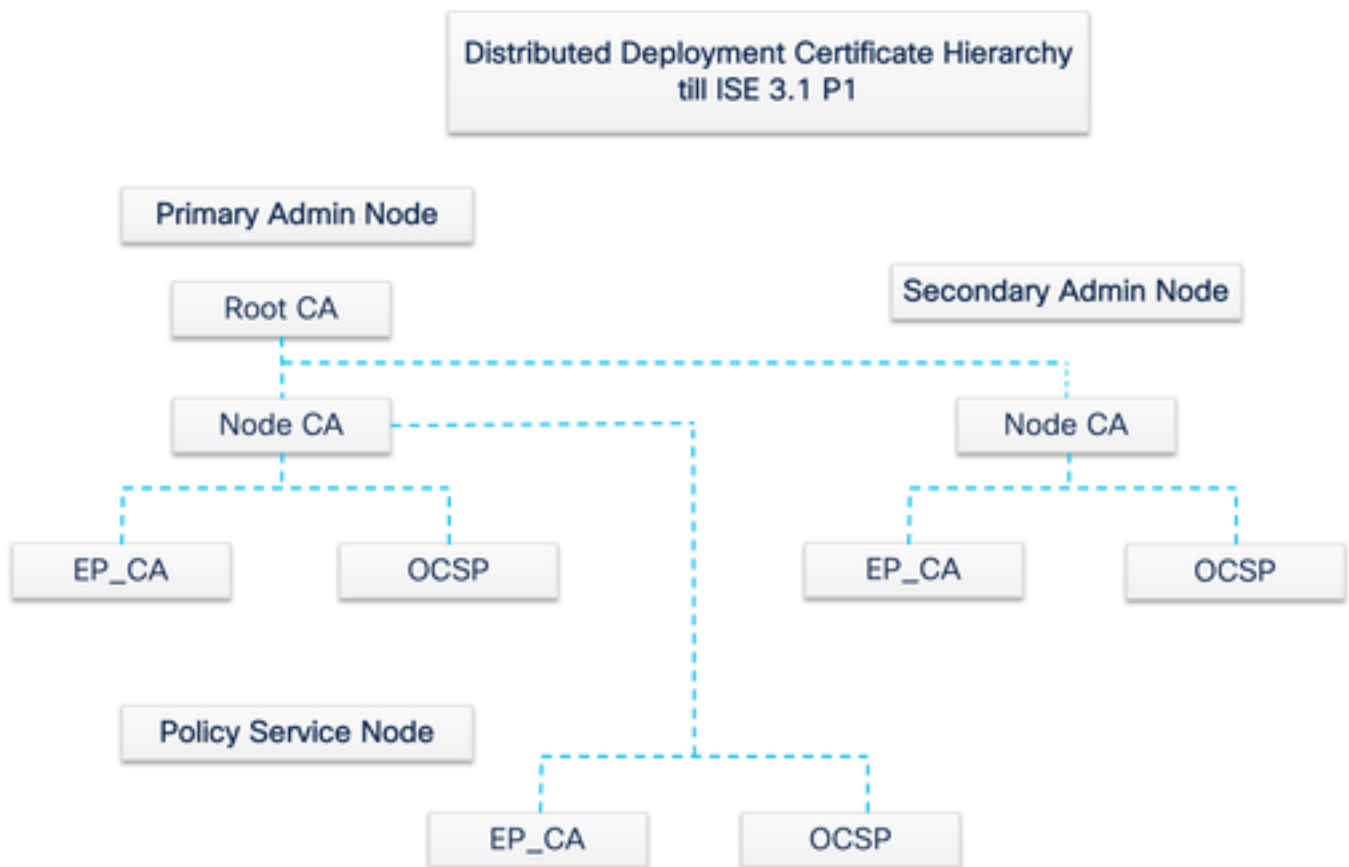
- assinar as próprias respostas OCSP, ou
- designar expressamente essa autoridade a outra entidade"

"O certificado de signatário de resposta OCSP DEVE ser emitido diretamente pela CA identificada na solicitação. "

"Sistema (depende) de respostas OCSP DEVE reconhecer um certificado de delegação como emitido pela CA que emitiu o certificado em questão somente se o certificado de delegação e o

certificado (está) verificado para revogação tiverem sido assinados pela mesma chave."

Para estar em conformidade com o Padrão RFC mencionado anteriormente, a hierarquia de certificados para o Certificado de Respondente OCSP é alterada no ISE. O Certificado do Respondente OCSP agora é emitido pela Sub CA do Ponto de Extremidade do mesmo nó, em vez da CA do Nó no PAN.



Inscrição no Serviço de Transporte Seguro (EST)

O conceito de infraestrutura de chave pública (PKI) existe há muito tempo. A PKI autentica a identidade dos utilizadores e dispositivos através de pares de chaves públicas assinados sob a forma de certificados digitais. A inscrição no Transporte Seguro (EST) é um protocolo para fornecer esses certificados. O serviço EST define como executar o registro de certificado para clientes que usam o Gerenciamento de Certificado sobre a Sintaxe de Mensagem Criptográfica (CMC) sobre um transporte seguro. De acordo com a IETF - "EST descreve um protocolo de gerenciamento de certificados simples, mas funcional, que tem como alvo clientes de infraestrutura de chave pública (PKI - Public Key Infrastructure) que precisam adquirir certificados de cliente e certificados de autoridade de certificação (CA - Certification Authority) associados. Ele também suporta pares de chaves públicas/privadas gerados pelo cliente, bem como pares de chaves gerados pela CA."

Casos de uso EST

O protocolo EST pode ser usado:

- Inscrever dispositivos de rede por meio da Secure Unique Device Identity
- Para soluções BYOD

Por que EST?

Os protocolos EST e SCEP abordam o provisionamento de certificados. EST é um sucessor do Protocolo de Registro de Certificado Simples (SCEP). Por causa de sua simplicidade, o SCEP tem sido o protocolo de fato no provisionamento de certificados por muitos anos. No entanto, o uso de EST sobre SCEP é recomendado pelas seguintes razões:

- Uso de TLS para transporte seguro de certificados e mensagens - No EST, a solicitação de assinatura de certificado (CSR) pode ser vinculada a um solicitante que já é confiável e autenticado com TLS. Os clientes não podem obter um certificado para ninguém além deles mesmos. No SCEP, o CSR é autenticado por um segredo compartilhado entre o cliente e a CA. Isso gera preocupações de segurança, pois alguém com acesso ao segredo compartilhado pode gerar certificados para outras entidades que não elas.
- Suporte para registro de certificados assinados por ECC - EST fornece agilidade criptográfica. Ele suporta criptografia de curva elíptica (ECC). O SCEP não suporta ECC e depende da criptografia RSA. O ECC oferece mais segurança e melhor desempenho do que outros algoritmos criptográficos, como o RSA, mesmo que use um tamanho de chave muito menor.
- O EST foi criado para suportar a reinscrição automática de certificados.

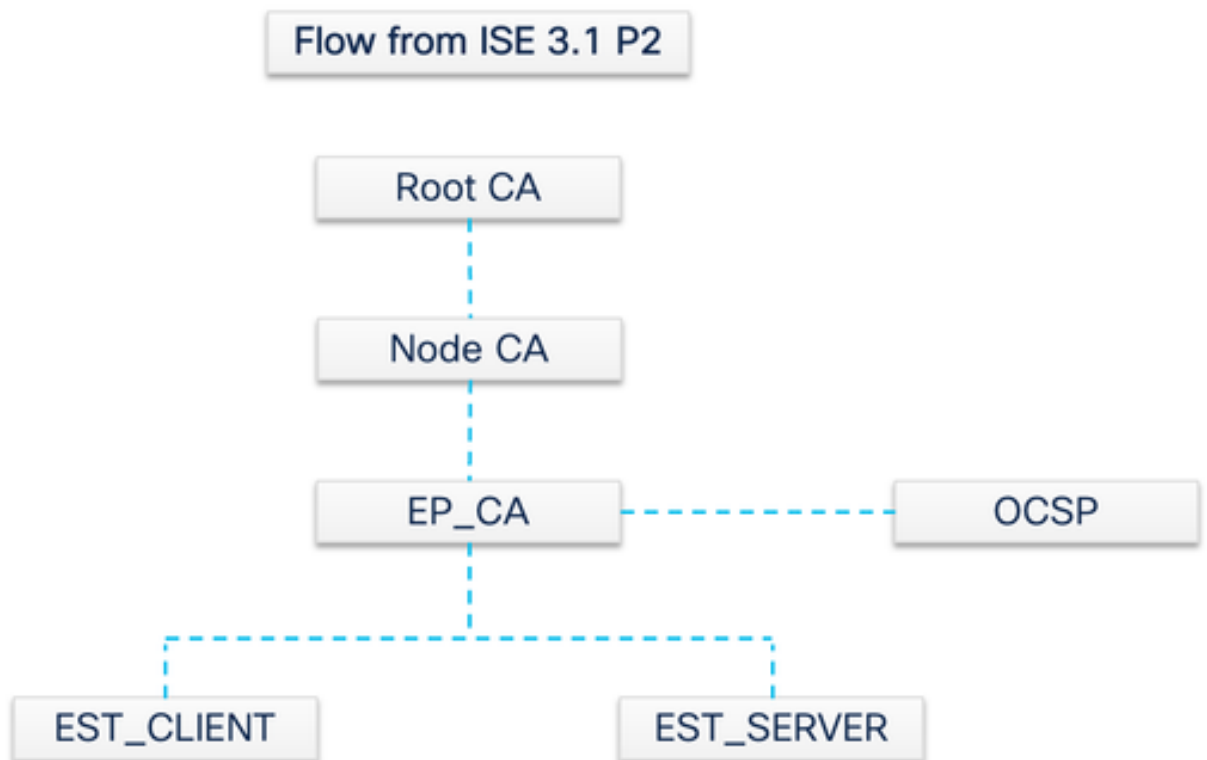
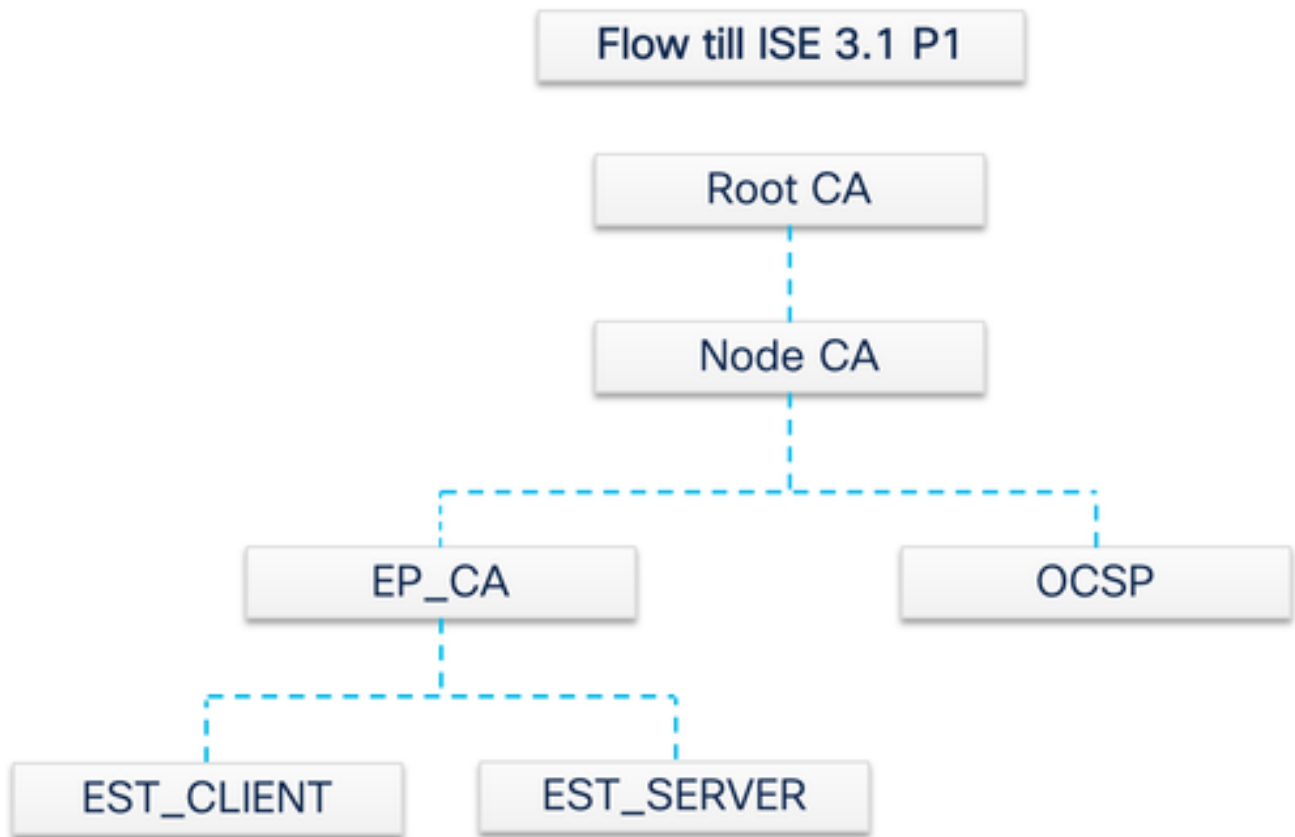
A segurança comprovada por TLS e o aprimoramento contínuo ajudam a garantir que as transações EST sejam seguras em termos de proteção criptográfica. A integração total do SCEP com a RSA para proteger os dados apresenta preocupações de segurança à medida que a tecnologia avança.

EST no ISE

Para implementar esse protocolo, são necessários um módulo de cliente e um módulo de servidor:

- Cliente EST - incorporado no tomcat ISE regular.
- Servidor EST - implantado em um servidor web de código aberto chamado NGINX. Isso é executado como um processo separado e ouve na porta 8084.

A autenticação de cliente e servidor baseada em certificado é suportada por EST. A CA do ponto final emite o certificado para o cliente EST e o servidor EST. Os certificados de Cliente e Servidor EST e suas respectivas chaves são armazenados no NSS DB da CA do ISE.



Tipos de solicitações no ISE EST

Sempre que o servidor EST é ativado, ele obtém a cópia mais recente de todos os certificados CA do servidor CA e a armazena. Em seguida, o cliente EST pode fazer uma solicitação de certificado CA para obter toda a cadeia desse servidor EST. Antes de fazer uma solicitação de inscrição simples, o cliente EST deve emitir a solicitação de certificado CA primeiro.

Solicitação de certificados CA (com base no RFC 7030)

1. O cliente EST solicita uma cópia dos certificados CA atuais.
2. Mensagem HTTPS GET com um valor de caminho de operação de `/cacerts`.
3. Essa operação é executada antes de qualquer outra solicitação de EST.
4. É feita uma solicitação a cada 5 minutos para obter uma cópia dos certificados CA mais atualizados.
5. O servidor EST não deve exigir autenticação de cliente.

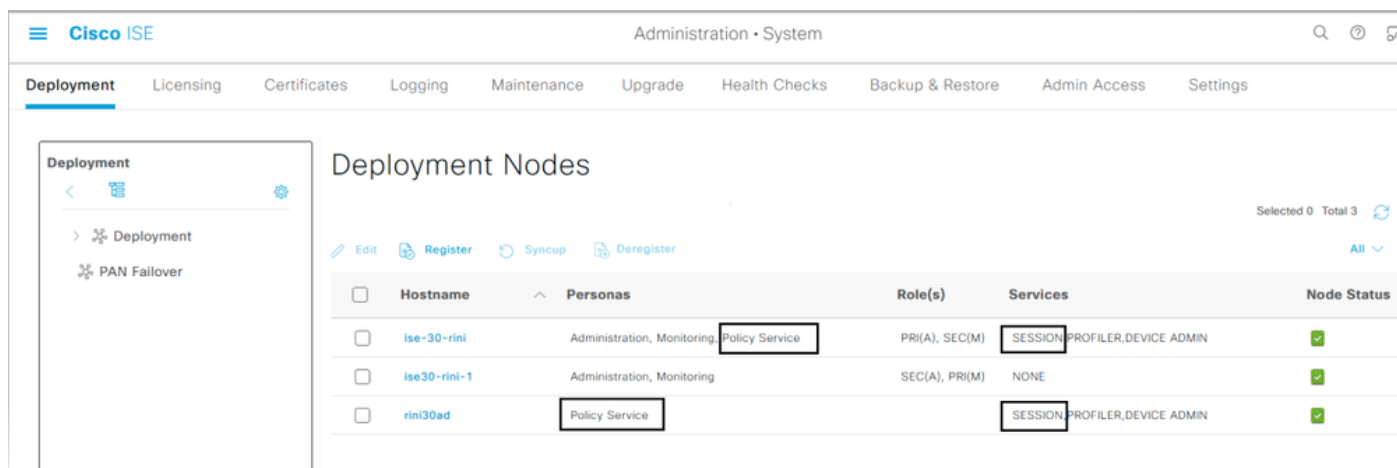
A segunda solicitação é uma solicitação de inscrição simples e precisa de autenticação entre o cliente EST e o servidor EST. Isso acontece toda vez que um endpoint se conecta ao ISE e faz uma solicitação de certificado.

Solicitação de inscrição simples (com base no RFC 7030)

1. O cliente EST solicita um certificado do servidor EST.
2. Mensagem HTTPS POST com o valor de caminho de operação de `/simpleenroll`.
3. O cliente EST incorpora a solicitação PKCS#10 nessa chamada que é enviada ao ISE.
4. O servidor EST deve autenticar o cliente.

Status do serviço EST e CA

Os serviços CA e EST só podem ser executados em um nó Serviço de política que tenha serviços de sessão habilitados. Para habilitar os serviços de sessão em um nó, navegue para **Administration > System > Deployment**. Selecione o nome de host do servidor no qual os serviços de sessão precisam ser ativados e clique em **Edit**. Marque a caixa de seleção em **Persona** de serviços de política **Enable Session Services**.



☐	Hostname	Personas	Role(s)	Services	Node Status
☐	ise-30-rini	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	SESSION PROFILER, DEVICE ADMIN	✓
☐	ise30-rini-1	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓
☐	rini30ad	Policy Service		SESSION PROFILER, DEVICE ADMIN	✓

Status mostrado na GUI

O status do serviço EST está vinculado ao status do serviço da CA do ISE no ISE. Se o serviço CA estiver ativo, o serviço EST está ativo e, se o serviço CA estiver inativo, o serviço EST também está inativo.

Cisco ISE Administration • System

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

Certificate Management >

Certificate Authority ▾

Overview

Issued Certificates

Certificate Authority Certificat...

Internal CA Settings

Certificate Templates

External CA Settings

Internal CA Settings

⚠ For disaster recovery it is recommended to Export Internal CA Store using Command Line Interface (CLI).

[Disable Certificate Authority](#)

Host Name	Personas	Role(s)	CA, EST & OCSP Responder Status	OCSP Responder URL	SCEP URL
ise-30-rini	Administration, Monitoring, Policy Service	PRIMARY	✓	http://ise-30-rini.gce.iselab.local:2560/ocsp/	http://ise-30-rini.gce.iselab.l
ise30-rini-1	Administration, Monitoring	SECONDARY	⊗	http://ise30-rini-1.gce.iselab.local:2560/ocsp/	http://ise30-rini-1.gce.iselab
rini30ad	Policy Service	SECONDARY	✓	http://rini30ad.gce.lab.local:2560/ocsp/	http://rini30ad.gce.lab.local:5

Status mostrado na CLI

```
ise-30-rini/admin# sh app status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	61993
Database Server	running	159 PROCESSES
Application Server	running	72240
Profiler Database	running	68224
ISE Indexing Engine	running	74972
AD Connector	running	78912
M&T Session Database	running	68007
M&T Log Processor	running	70533
Certificate Authority Service	running	63090
EST Service	running	64492
SXP Engine Service	disabled	
Docker Daemon	running	64427
TC-NAC Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	

Alarmes no painel

O alarme será exibido no painel do ISE se os serviços EST e CA estiverem inoperantes.

ALARMS ⓘ				⏏ ⌂ ✕
✕	DNS Resolution Failure	1720	8 days ago	^
⚠	CA Server is down	12	17 days ago	
⚠	AD: Machine TGT ref...	5	1 month ago	
✕	NTP Sync Failure	277	1 month ago	
⚠	EST Service is down	1	2 months ago	
ⓘ	Supplciant stopped r	1	2 months ago	▼
Last refreshed:2021-04-26 03:52:00				

Impacto se os serviços CA e EST não estiverem em execução

- A falha de chamada do cliente/cacertsEST pode ocorrer quando o servidor EST está inativo. A falha/cacertsde chamada também pode ocorrer se a cadeia de CA do certificado da cadeia de CA EST estiver incompleta.
- Falha nas solicitações de registro de certificado de ponto final baseado em ECC.
- O fluxo de BYOD será interrompido se qualquer uma das duas falhas anteriores ocorrer.
- Os alarmes de erro de link de fila podem ser gerados.

Troubleshooting

Se o fluxo de BYOD com o protocolo EST não funcionar corretamente, verifique estas condições:

- A cadeia de certificados da Subautoridade de Certificação do Ponto de Extremidade dos Serviços de Certificado foi concluída. Para verificar se a cadeia de certificados está completa:

1. Navegue até Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates.

2. Marque a caixa de seleção ao lado do certificado e clique em View para verificar um certificado específico.

- Certifique-se de que os serviços CA e EST estejam ativos e em execução. Se os serviços não estiverem em execução, navegue até Administration > System > Certificates > Certificate Authority > Internal CA Settings para habilitar o serviço CA.
- Se uma atualização tiver sido executada, substitua a cadeia de certificados da CA raiz do ISE após a atualização. Para fazer isso:
 1. Escolha .Administration > System > Certificates > Certificate Management > Certificate Signing Requests
 2. Clique em .Generate Certificate Signing Requests (CSR)
 3. Selecione ISE Root CA na lista suspensa Certificate(s) will be used for.
 4. Clique em .Replace ISE Root CA Certificate Chain
- A depuração útil que pode ser habilitada para verificar os logs inclui est, provisioning, ca-service e ca-service-cert. Consulte os arquivos ise-psc.log, catalina.out, caservice.log , e error.log.

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

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.