Configurar renovações de certificado no ISE

Contents

Introduction

Este documento descreve as melhores práticas e os procedimentos proativos para renovar certificados no Cisco Identity Services Engine (ISE). Ele também analisa como configurar alarmes e notificações para que os administradores sejam avisados de eventos iminentes, como a expiração de certificados.

> **Note**: Este documento não se destina a ser um guia de diagnóstico para certificados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados X509
- Configuração de um Cisco ISE com certificados

Componentes Utilizados

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

- Cisco ISE versão 3.0.0.458
- Dispositivo ou VMware

Informações de Apoio

Como administrador do ISE, eventualmente você se depara com o fato de que os certificados ISE expiram. Se o servidor ISE tiver um certificado expirado, problemas sérios poderão surgir, a menos que você substitua o certificado expirado por um novo certificado válido.

> **Note**: Se o certificado usado para o EAP (Extensible Authentication Protocol) expirar, todas as autenticações poderão falhar porque os clientes não confiam mais no certificado ISE. Se o certificado de administrador do ISE expirar, o risco será ainda maior: um administrador não poderá mais fazer login no ISE e a implantação distribuída poderá deixar de funcionar e ser replicada.

O administrador do ISE deve instalar um certificado novo e válido no ISE antes que o certificado antigo expire. Essa abordagem proativa evita ou minimiza o período de inatividade e evita o impacto nos usuários finais. Quando o período de tempo do certificado recém-instalado começar, você poderá habilitar o EAP/Admin ou qualquer outra função no novo certificado.

Você pode configurar o ISE para que ele gere alarmes e notifique o administrador para instalar novos certificados, antes que os certificados antigos expirem.

> **Note**: Este documento usa o certificado do administrador do ISE como um certificado autoassinado para demonstrar o impacto da renovação do certificado, mas essa abordagem não é recomendada para um sistema de produção. É melhor usar um certificado CA para as funções EAP e Admin.

Configurar

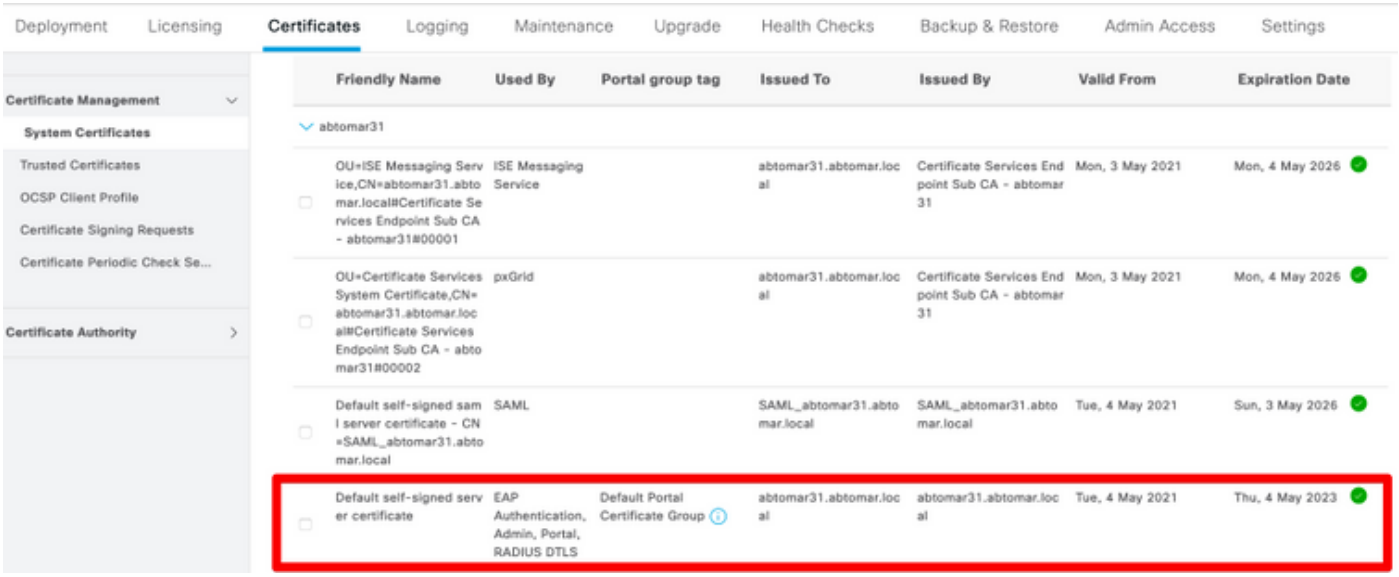
Exibir certificados autoassinados ISE

Quando o ISE é instalado, gera um certificado autoassinado. O certificado autoassinado é usado para acesso administrativo e para comunicação na implantação distribuída (HTTPS), bem como para autenticação de usuário (EAP). Em um sistema ativo, use um certificado CA, em vez de um certificado autoassinado.

> **Tip**: Consulte o gerenciamento de certificados na seção Cisco ISE do guia de instalação de hardware do Cisco Identity Services Engine, versão 3.0 , para obter informações adicionais.

Um certificado ISE deve ser no formato de Privacy Enhanced Mail (PEM) ou Distinguished Encoding Rules (DER).

Para ver o certificado autoassinado inicial, navegue até **Administração > Sistema > Certificados > Certificados do sistema** na GUI do ISE, conforme mostrado nesta imagem.



Se você instalar um certificado de servidor no ISE usando uma solicitação de assinatura de certificado (CSR) e alterar o certificado para o protocolo Admin ou EAP, o certificado de servidor autoassinado ainda estará presente, mas no status Não em uso.

> **Caution**: Para alterações no protocolo de admin, é necessária uma reinicialização dos serviços ISE, o que cria alguns minutos de período de inatividade. As alterações no protocolo EAP não acionam uma reinicialização dos serviços ISE e não causam o período de inatividade.

Determinar quando alterar o certificado

Suponha que o certificado instalado expirará em breve. É melhor deixar o certificado expirar antes de renovar ou alterar antes de expirar? Você deve alterar o certificado antes da expiração para que tenha tempo para planejar a troca de certificados e gerenciar qualquer tempo de inatividade causado pela troca.

Quando você deve alterar o certificado? Obtenha um novo certificado com uma data de início anterior à data de validade do certificado antigo. O período entre essas duas datas é a janela de alteração.

> **Caution**: Se você ativar o Admin, o serviço será reiniciado no servidor ISE e haverá alguns minutos de inatividade.

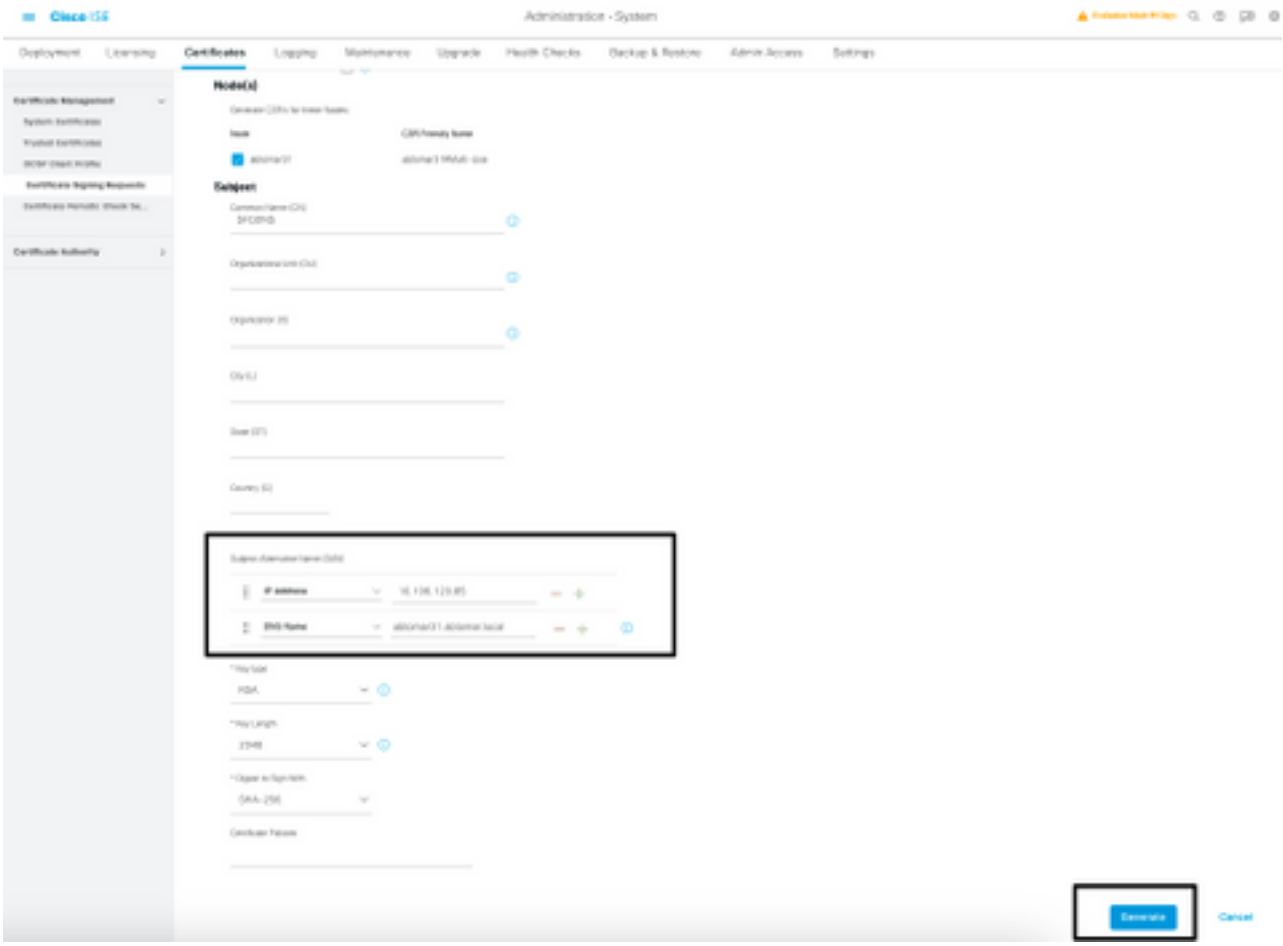
Esta imagem mostra as informações de um certificado que expirará em breve:

Gerar solicitação de assinatura de certificado

Este procedimento descreve como renovar o certificado por meio de um CSR:

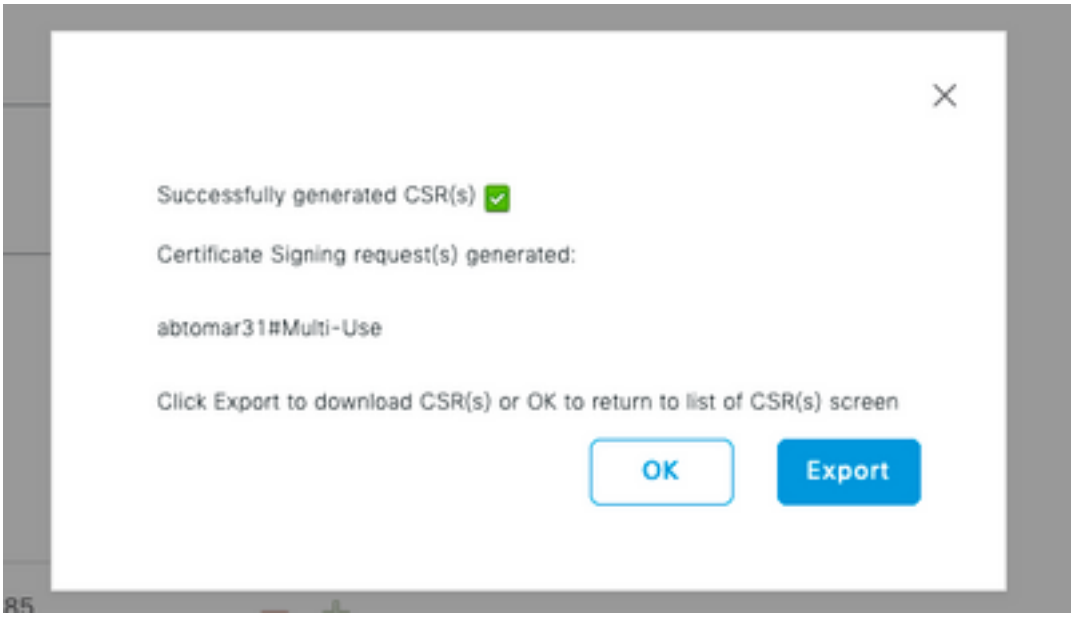
1. No console do ISE, navegue até **Administração > Sistema > Certificados > Solicitações de assinatura de certificado** e clique em **Gerar solicitação de assinatura de certificado:**

2. A informação mínima que você deve inserir no campo de texto **Assunto do certificado** é CN = *ISEfqdn*, onde *ISEfqdn* é o nome de domínio totalmente qualificado (FQDN) do ISE. Adicione campos adicionais, como O (empresa), OU (unidade organizacional) ou C (país) no assunto do certificado usando vírgulas:

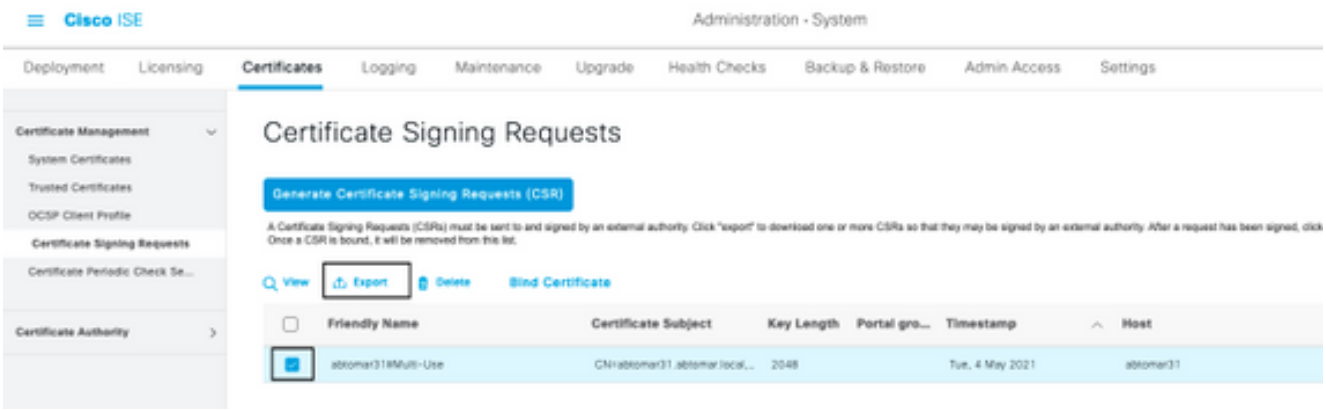


3. Uma das linhas de campo de texto **Nome alternativo do assunto (SAN)** deve repetir o FQDN do ISE. Você pode adicionar um segundo campo SAN, se desejar usar nomes alternativos ou um certificado coringa.

4. Ao clicar em **Gerar**, uma janela pop-up indicará se os campos CSR foram preenchidos corretamente:



5. Para exportar o CSR, clique em **Solicitações de assinatura de certificado** no painel esquerdo, selecione o CSR e clique em **Exportar**:

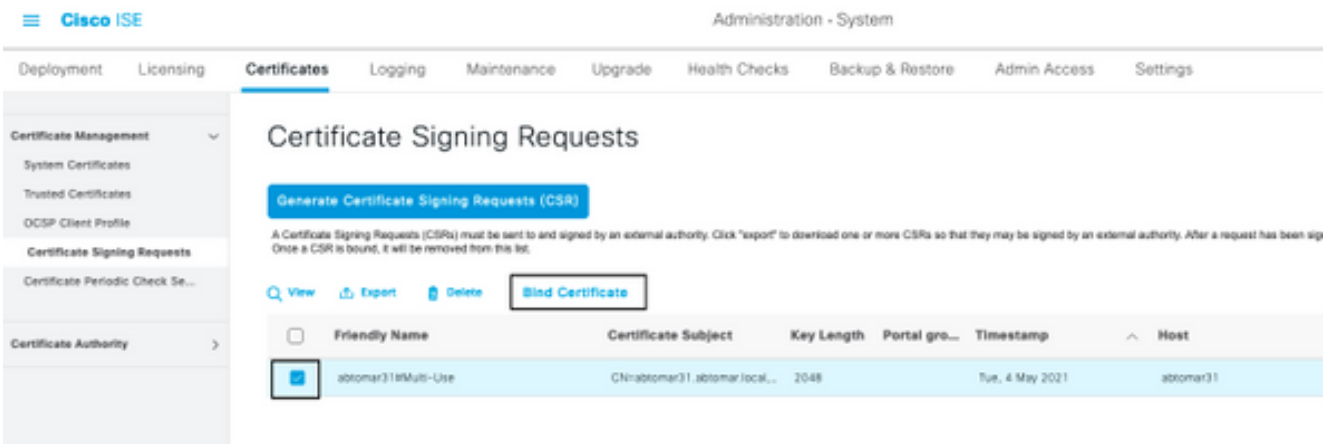


6. O CSR é armazenado no computador. Envie-o à CA para assinatura.

Instalar certificado

Depois de receber o certificado final da CA, você deve adicionar o certificado ao ISE:

1. No console do ISE, navegue até **Administração > Sistema > Certificados > Solicitações de assinatura de certificado**, marque a caixa de seleção em CRS e clique em **Vincular certificado**:

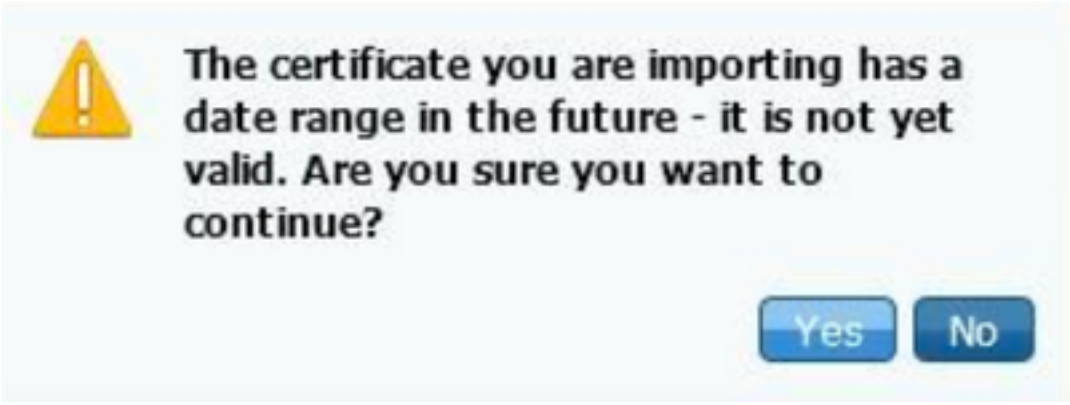


2. Insira uma descrição simples e clara do certificado no campo de texto **Nome amigável** e pressione Enviar.

Note: Não ative o protocolo EAP ou Admin nesse momento.

3. Em Certificado do sistema, você tem um novo certificado que não está em uso, conforme mostrado aqui:

4. Como o novo certificado é instalado antes que o antigo expire, você verá um erro que relata um intervalo de datas no futuro:



5. Clique em **Sim** para continuar. Agora, o certificado está instalado, mas não está em uso, conforme destacado em verde.

Note: Se você usar certificados autoassinados em uma implantação distribuída, o certificado autoassinado primário deverá ser instalado no armazenamento de certificados confiáveis do servidor ISE secundário. Da mesma forma, o certificado autoassinado secundário deverá ser instalado no armazenamento de certificados confiáveis do servidor ISE primário. Isso permite que os servidores ISE se autentiquem mutuamente. Sem isso, a implantação pode ser interrompida. Se você renovar certificados de uma CA de terceiros, verifique se a cadeia de certificados de origem foi alterada e atualize o armazenamento de

certificados confiáveis no ISE adequadamente. Em ambos os cenários, certifique-se de que os nós do ISE, os sistemas de controle de endpoint e os solicitantes sejam capazes de validar a cadeia de certificados raiz.

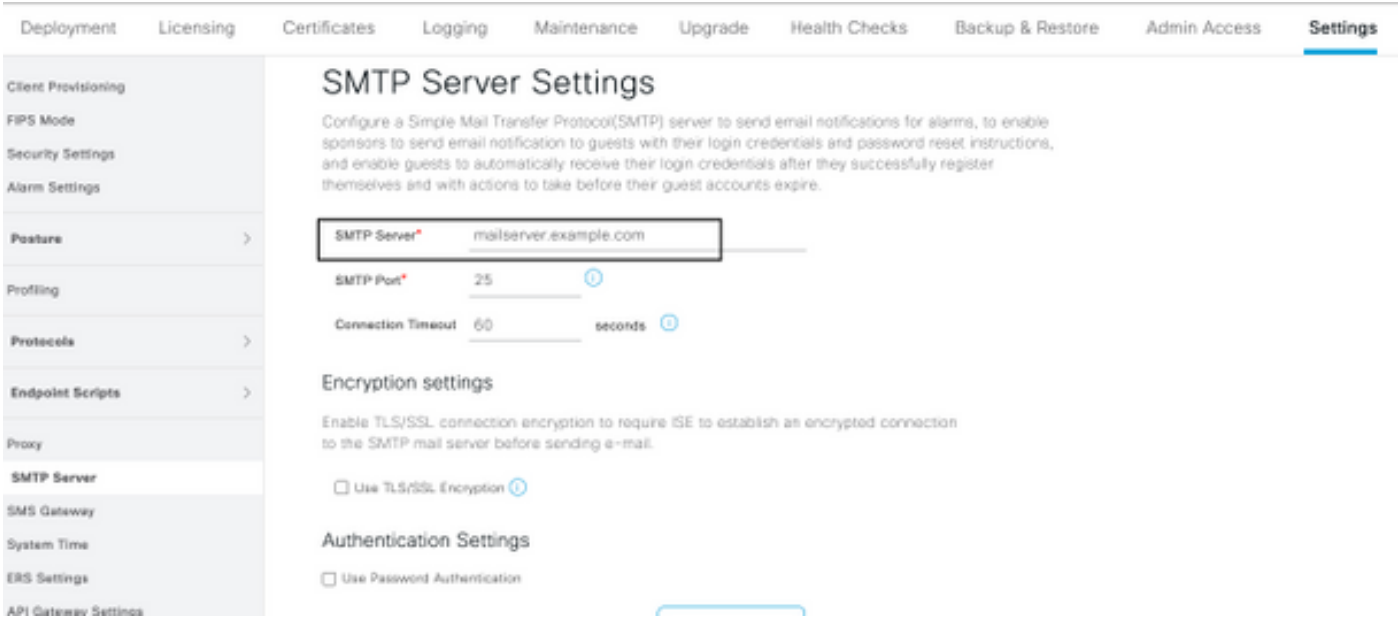
Configurar sistema de alerta

O Cisco ISE notifica você quando a data de validade de um certificado local é em 90 dias. Essa notificação antecipada ajuda a evitar certificados expirados, planejar a alteração de certificado e evitar ou minimizar o período de inatividade.

A notificação é exibida de várias maneiras:

- Os ícones coloridos de status de expiração são exibidos na página Certificados locais.
- As mensagens de expiração são exibidas no relatório de diagnóstico do sistema do Cisco ISE.
- Os alarmes de expiração são gerados em 90 e em 60 dias, e depois diariamente nos últimos 30 dias antes da expiração.

Configure o ISE para notificação por e-mail dos alarmes de expiração. No console do ISE, navegue até **Administração > Sistema > Configurações > Servidor SMTP**, identifique o servidor SMTP e defina as outras configurações do servidor para que as notificações por e-mail sejam enviadas para os alarmes:

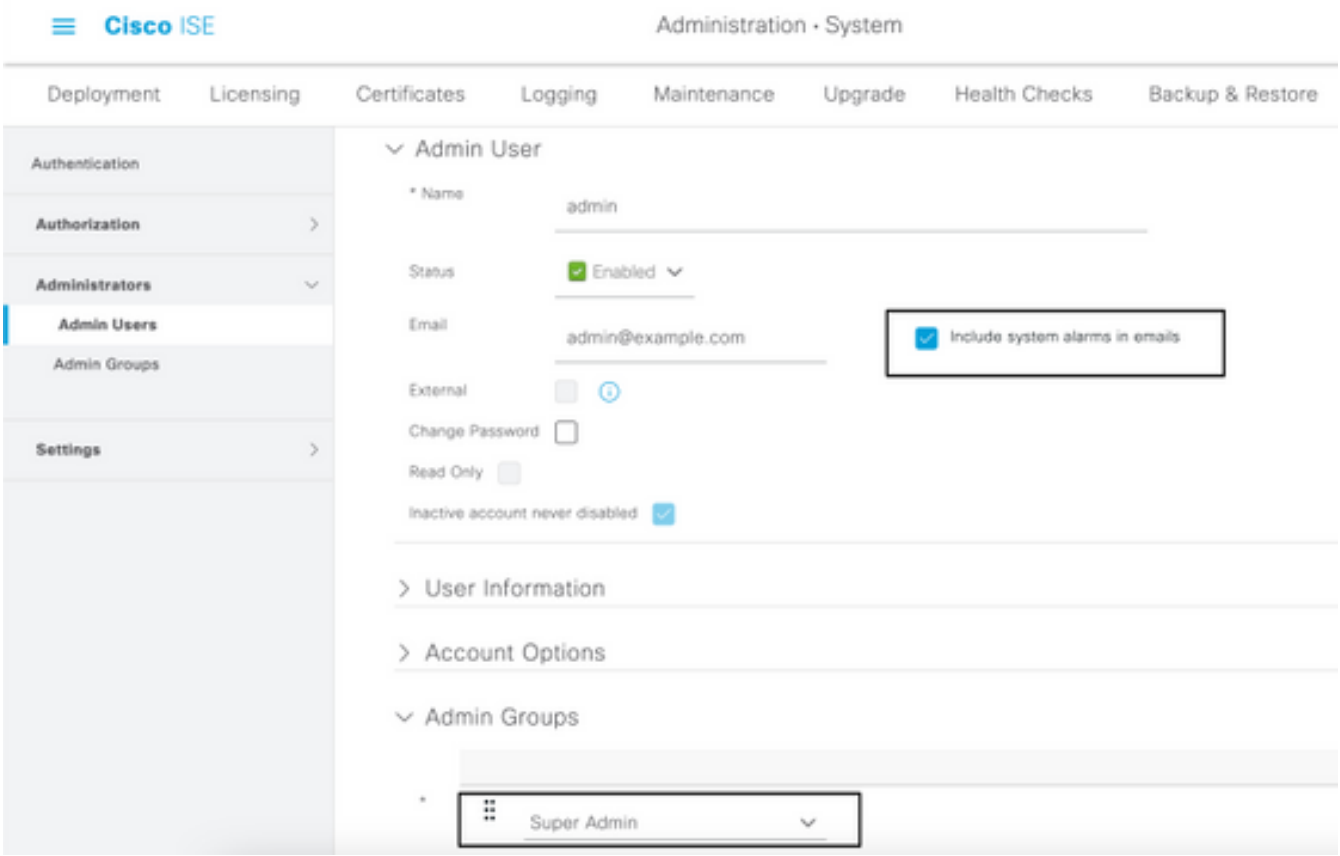


Há duas maneiras de configurar notificações:

- Use o acesso de admin para notificar os administradores:

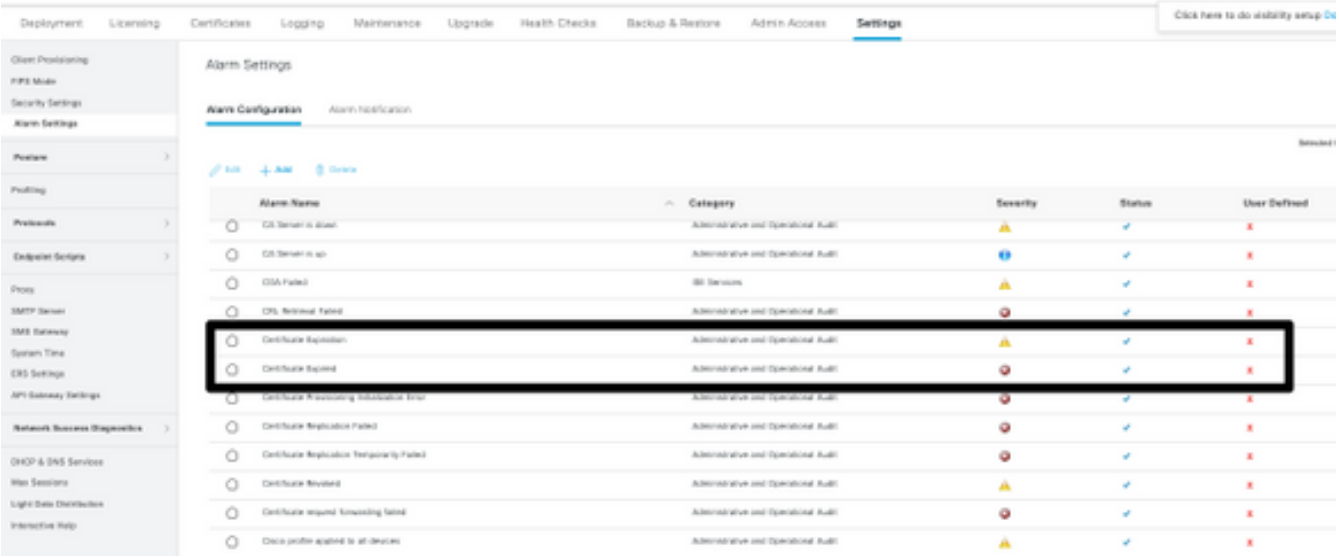
  Navegue até **Administração > Sistema >** Acesso de Admin > Administradores > Usuários de admin.

Marque a caixa de seleção **Incluir alarmes do sistema em e-mails** para os usuários de admin que precisam receber notificações de alarme. O endereço de e-mail do remetente das notificações de alarme é codificado como ise@*hostname*.



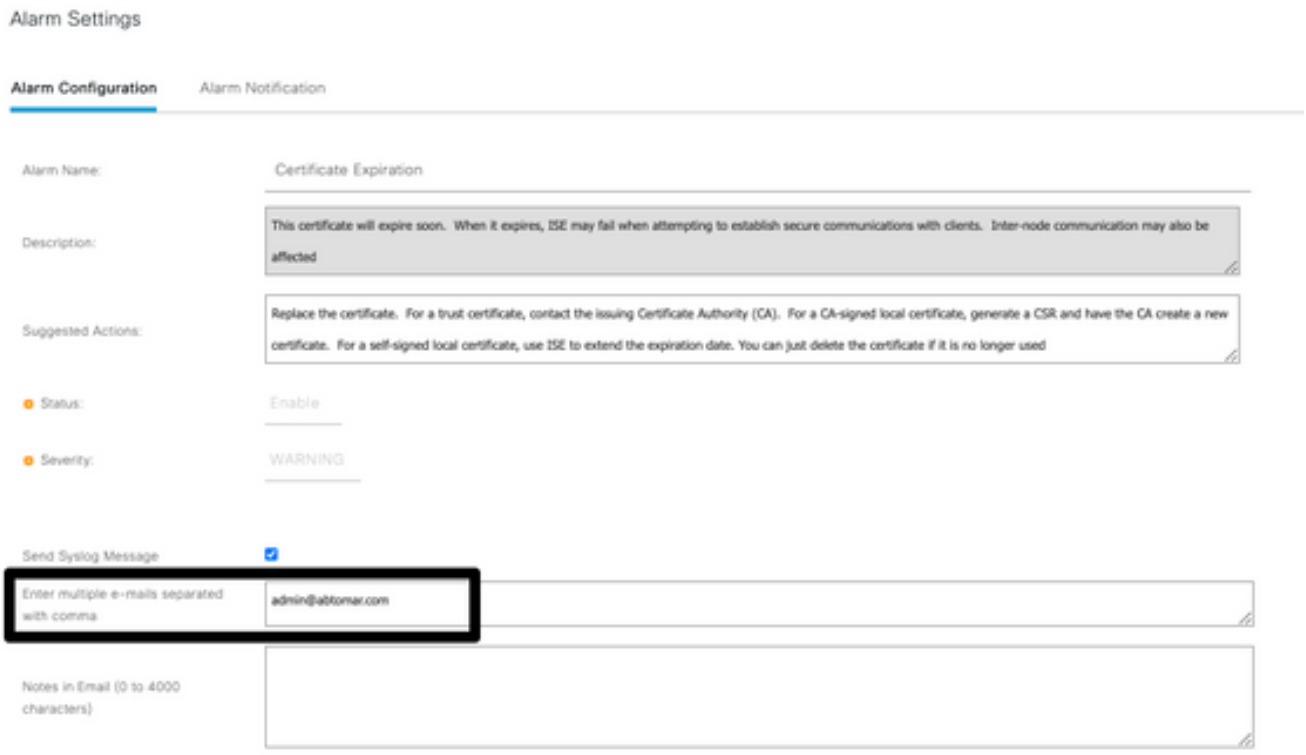
- Defina as configurações de alarme do ISE para notificar usuários:

  Navegue até **Administração > Sistema > Configurações > Configurações de alarme > Configuração de alarme**, conforme mostrado nesta imagem.



Note: Desative o status de uma categoria, se desejar evitar alarmes dessa categoria.Selecione Expiração do certificado e clique em **Notificação de alarme**, insira os endereços de e-mail dos usuários a serem notificados e salve a alteração de configuração.

As alterações podem levar até 15 minutos antes de serem ativadas.

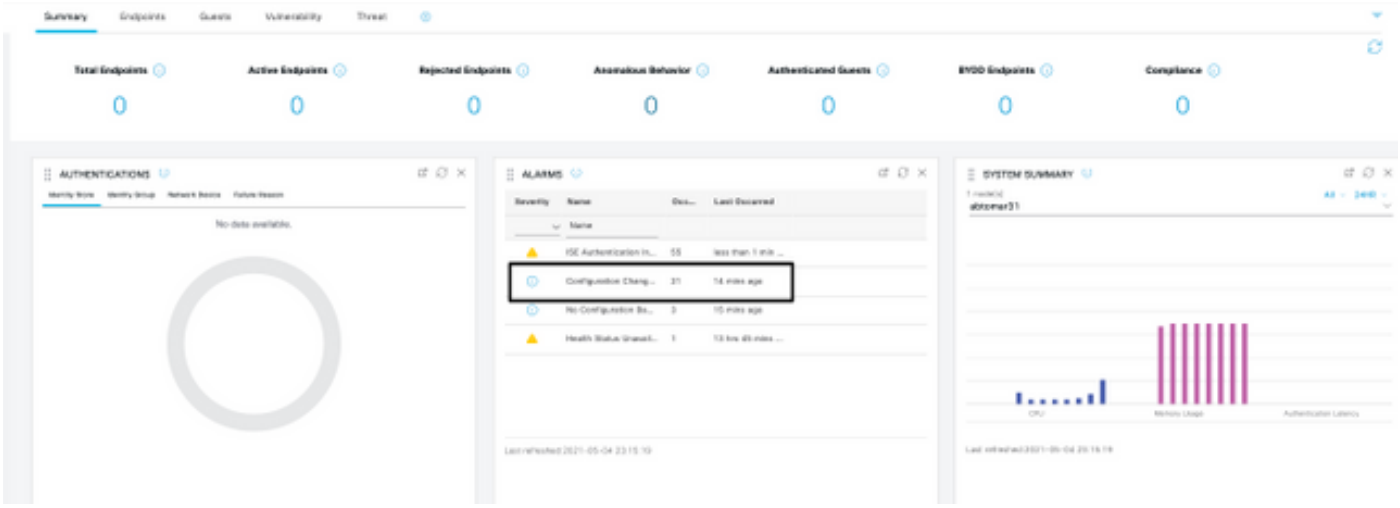


Verificar

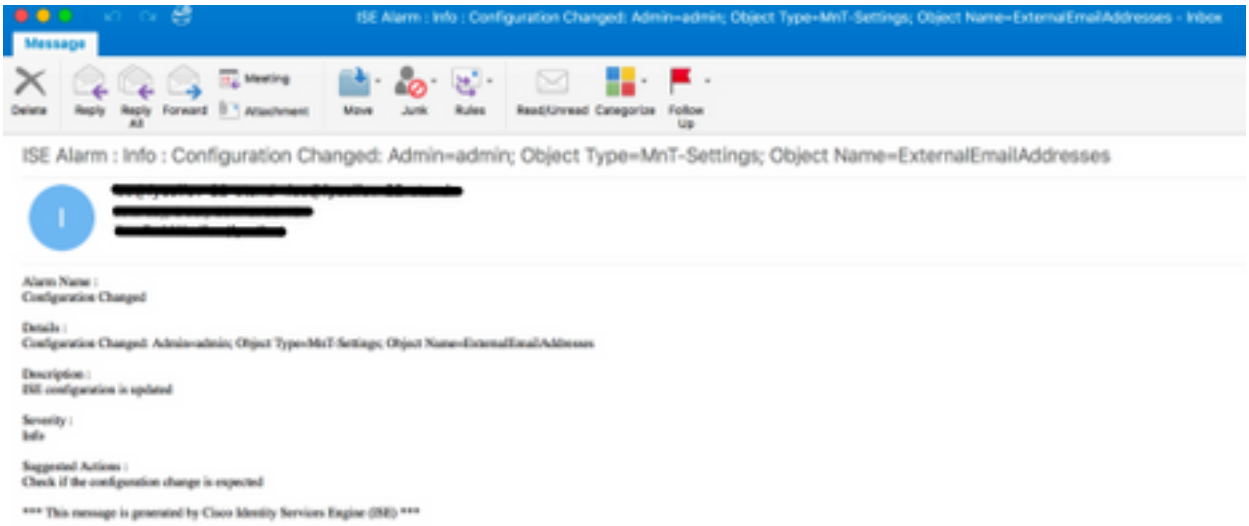
Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificar sistema de alerta

Verifique se o sistema de alerta funciona corretamente. Neste exemplo, uma alteração de configuração gera um alerta com um nível de gravidade de informações. (Um alarme de informações é a gravidade mais baixa, enquanto as expirações de certificado geram um nível de gravidade mais alto de aviso.)



Este é um exemplo do alarme de e-mail enviado pelo ISE:

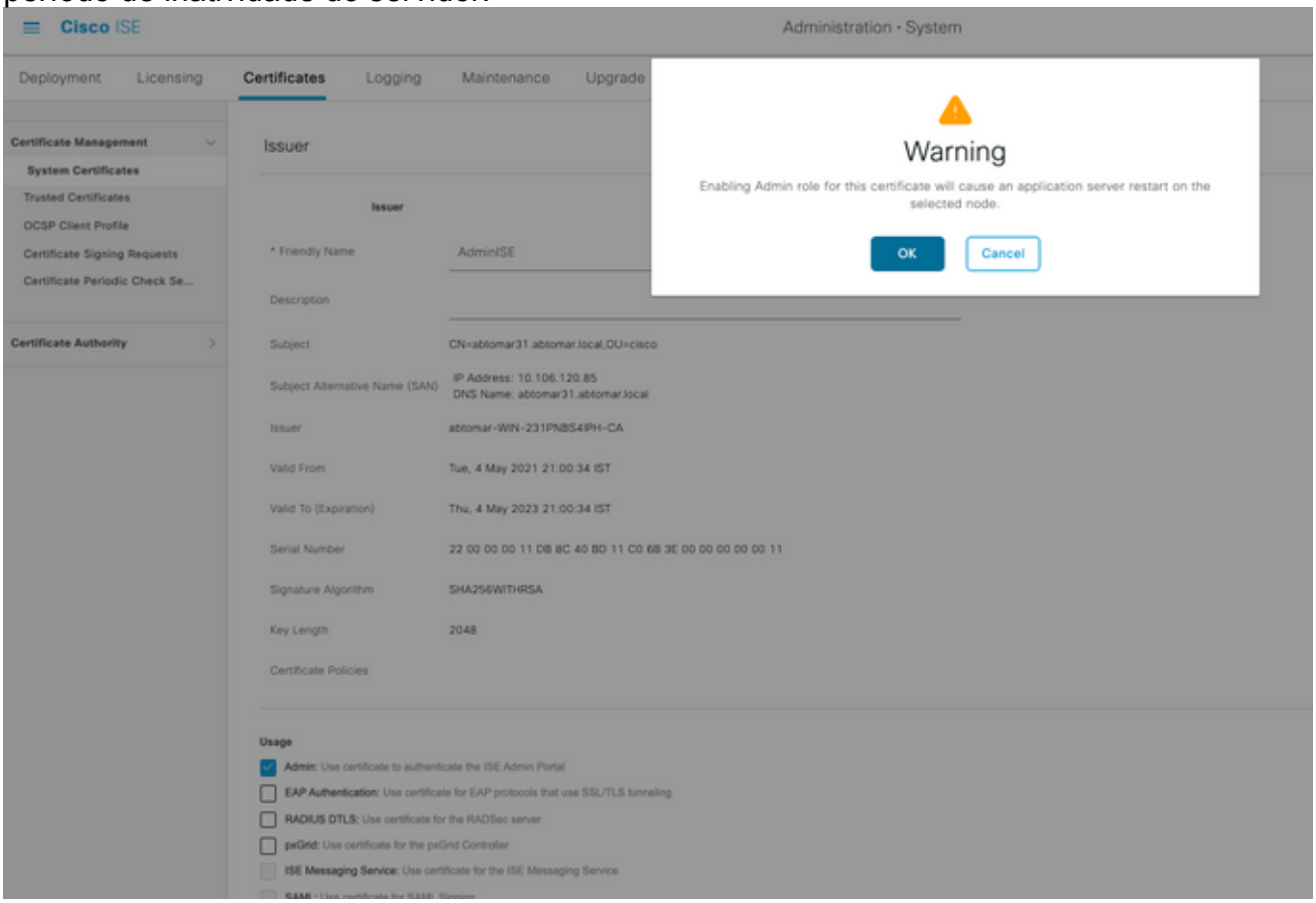


Verificar alteração de certificado

Este procedimento descreve como verificar se o certificado está instalado corretamente e como alterar as funções EAP e/ou Admin:

1. No console do ISE, navegue até **Administração > Certificados > Certificados do sistema** e selecione o novo certificado para exibir os detalhes.

   Caution: Se você ativar o uso de admin, o serviço ISE será reiniciado, o que causará o período de inatividade do servidor.



2. Para verificar o status do certificado no servidor ISE, insira este comando na CLI:

```
CLI:> show application status ise
```

3. Quando todos os serviços estiverem ativos, tente fazer login como administrador.

4. Para um cenário de implantação distribuída, navegue para **Administração > Sistema > Implantação.** Verifique se o nó tem um ícone verde. Coloque o cursor sobre o ícone para verificar se a legenda mostra "Conectado".

5. Verifique se a autenticação do usuário final foi realizada com sucesso. Para fazer isso, navegue **paraOperations > RADIUS > Livelogs.** Você pode encontrar uma tentativa de autenticação específica e verificar se essas tentativas foram autenticadas com êxito.

Verificar certificado

Se você quiser verificar o certificado externamente, pode usar as ferramentas integradas do Microsoft Windows ou o kit de ferramentas OpenSSL.

OpenSSL é uma implementação de código aberto do protocolo Secure Sockets Layer (SSL). Se os certificados usarem sua própria CA privada, você deve colocar o certificado da CA de origem em um computador local e usar a opção OpenSSL *-CApath*. Se você tiver uma CA intermediária, deverá colocá-la também no mesmo diretório.

Para obter informações gerais sobre o certificado e verificá-lo, use:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Também pode ser útil converter os certificados com o kit de ferramentas OpenSSL:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Troubleshoot

No momento, não há informações de diagnóstico específicas disponíveis para esta configuração.

Conclusão

Como você pode instalar um novo certificado no ISE, antes que ele esteja ativo, a Cisco recomenda que você instale o novo certificado, antes que o certificado antigo expire. Esse período de sobreposição entre a data de validade do certificado antigo e a data de início do novo certificado fornece tempo para renovar certificados e planejar a instalação com pouco ou nenhum período de inatividade. Quando o novo certificado entrar no intervalo de datas válido, ative o EAP e/ou Admin. Lembre-se, se você ativar o uso de admin, haverá uma reinicialização do serviço.

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.