Renovação do certificado no manual de configuração do Cisco Identity Services Engine

Índice

Introdução

Este documento descreve melhores prática e procedimentos dinâmicos renovar Certificados no Cisco Identity Services Engine (ISE). Igualmente revê como estabelecer alarmes e notificações assim que os administradores são advertidos de próximos eventos tais como a expiração do certificado.

> Nota: Este documento não é pretendido ser um guia de Troubleshooting para Certificados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados X509

- Configuração de Cisco ISE com Certificados

Componentes Utilizados

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

- Liberação 1.2.0.899 de Cisco ISE
- Dispositivo ou VMware

Informações de Apoio

Como um administrador ISE, você encontrará eventualmente o fato de que os Certificados ISE expiram. Se seu server ISE tem um certificado expirado, os problemas graves puderam elevarar a menos que você substituísse o certificado expirado com um novo, certificado válido.

> Nota: Se o certificado que está usado para o Extensible Authentication Protocol (EAP) expira, todas as autenticações puderam falhar porque os clientes não confiam o certificado ISE anymore. Se o certificado do protocolo de HTTPS expira, o risco é mesmo maior: um administrador não pôde poder entrar anymore ao ISE, e o desenvolvimento distribuído pôde cessar de funcionar e replicate.

Neste exemplo, o ISE tem um certificado instalado de um server do Certificate Authority (CA) que expire em um mês. O administrador ISE deve instalar um novo, certificado válido no ISE antes que o certificado velho expire. Este abordagem proativa impede ou minimiza o tempo ocioso da máquina e evita um impacto em seus utilizadores finais. Uma vez o período de tempo do certificado recentemente instalado começa, você pode permitir o EAP e/ou o protocolo de HTTPS no certificado novo.

Você pode configurar o ISE de modo que gerencia alarmes e notifique o administrador para instalar Certificados novos antes que os Certificados velhos expirem.

> Nota: Este documento usa o HTTPS com um certificado auto-assinado a fim demonstrar o impacto da renovação do certificado, mas esta aproximação não é recomendada para um sistema vivo. É melhor usar um certificado de CA para o EAP e protocolos de HTTPS.

Configurar

Veja certificados auto-assinados ISE

Quando o ISE é instalado, gerencie um certificado auto-assinado. O certificado auto-assinado é usado para o acesso da administração e para uma comunicação dentro do desenvolvimento distribuído (HTTPS) assim como para a autenticação de usuário (EAP). Em um sistema vivo, use um certificado de CA em vez de um certificado auto-assinado.

> Dica: Refira o gerenciamento certificado na seção de Cisco ISE do guia de instalação de

hardware do Cisco Identity Services Engine, libere 1.2 para a informação adicional.

O formato para um certificado ISE deve ser o Privacy Enhanced Mail (PEM) ou as distintas regras da codificação (DER).

A fim ver o certificado auto-assinado inicial, navegue à **administração** > aos **Certificados de System> > Certificados locais no** console ISE:

Se você instala um certificado de servidor no ISE através de uma solicitação de assinatura de certificado (CSR) e muda o certificado para o protocolo HTTPS ou EAP, o certificado de servidor auto-assinado está ainda atual mas está usado já não.

> Cuidado: Para mudanças do protocolo de HTTPS, um reinício dos serviços ISE é exigido, que crie alguns minutos do tempo ocioso da máquina. As mudanças do protocolo EAP não provocam um reinício dos serviços ISE e não causam o tempo ocioso da máquina.

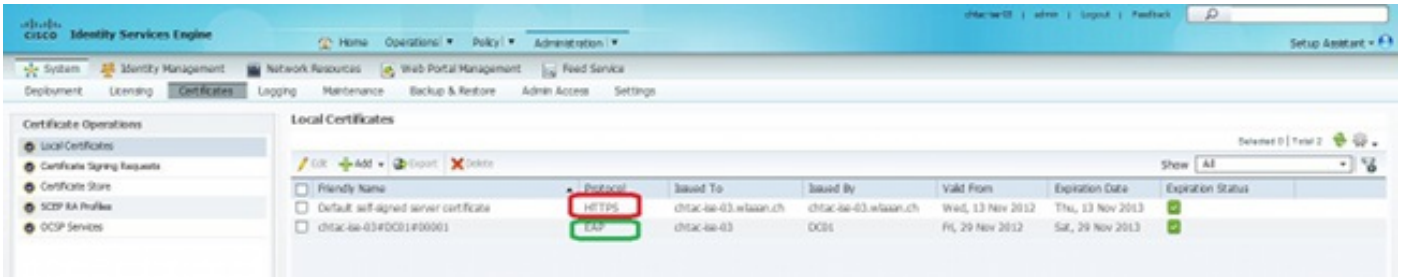
Determine quando mudar o certificado

Supõe que o certificado instalado expira logo. É melhor deixar o certificado expirar antes que você o renove ou mudar o certificado antes da expiração? Você deve mudar o certificado antes da expiração de modo que você tenha o tempo para planejar a troca do certificado e para controlar todo o tempo ocioso da máquina causado pela troca.

Quando deve você mudar o certificado? Obtenha um certificado novo com uma data de início que preceda a data de expiração do certificado velho. O período de tempo entre aquelas duas datas é o indicador da mudança.

> Cuidado: Se você permite o HTTPS, causa um reinício do serviço no server ISE, e você experimenta alguns minutos do tempo ocioso da máquina.

Esta imagem descreve a informação para um certificado que seja emitido por CA e expira o 29 de novembro 2013:



Gerencia a solicitação de assinatura de certificado

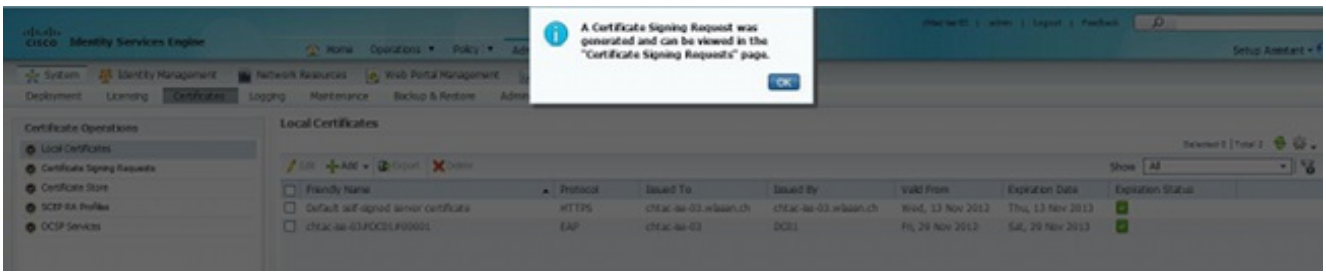
Este procedimento descreve como renovar o certificado com um CSR:

1. No console ISE, navegue **para adicionar > gerenciem a solicitação de assinatura de certificado**.

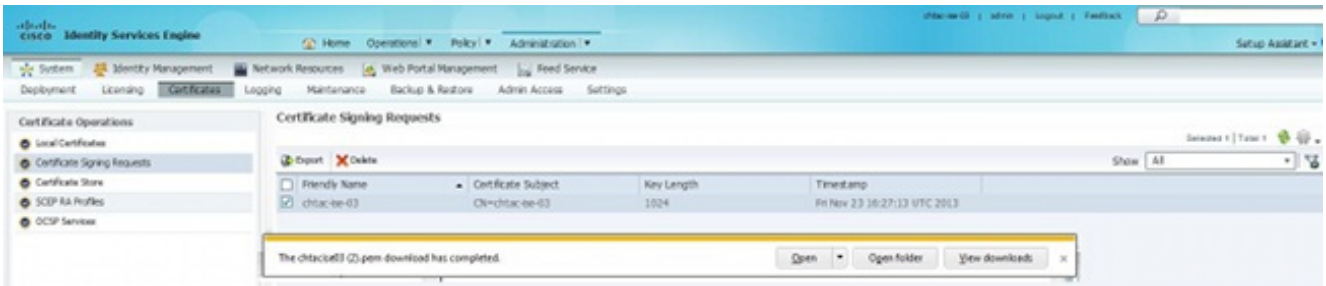
2. A informação mínima que você deve incorporar ao campo de texto do **assunto do certificado** é CN=ISEfqdn, onde *ISEfqdn* é o nome de domínio totalmente qualificado (FQDN) do ISE. Adicionar campos adicionais tais como O (organização), OU (unidade organizacional), ou C (país) no assunto do certificado com o uso das vírgulas:

3. Uma das linhas de campo de texto **alternativas sujeitas do nome (SAN)** deve repetir o FQDN ISE. Você pode adicionar um segundo campo SAN se você quer usar nomes alternativos ou um certificado do convite.

4. Uma janela pop-up indica se os campos CSR estão terminados corretamente:



5. A fim exportar o CSR, **solicitações de assinatura de certificado do** clique no painel esquerdo, selecionar seu CSR, e **exportação do** clique:

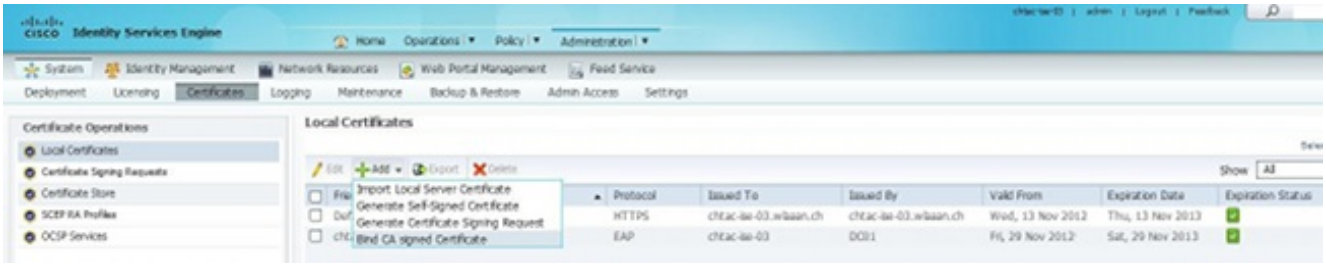


6. O CSR salvar em seu computador. Submeta-o a seu CA para a assinatura.

Instale o certificado

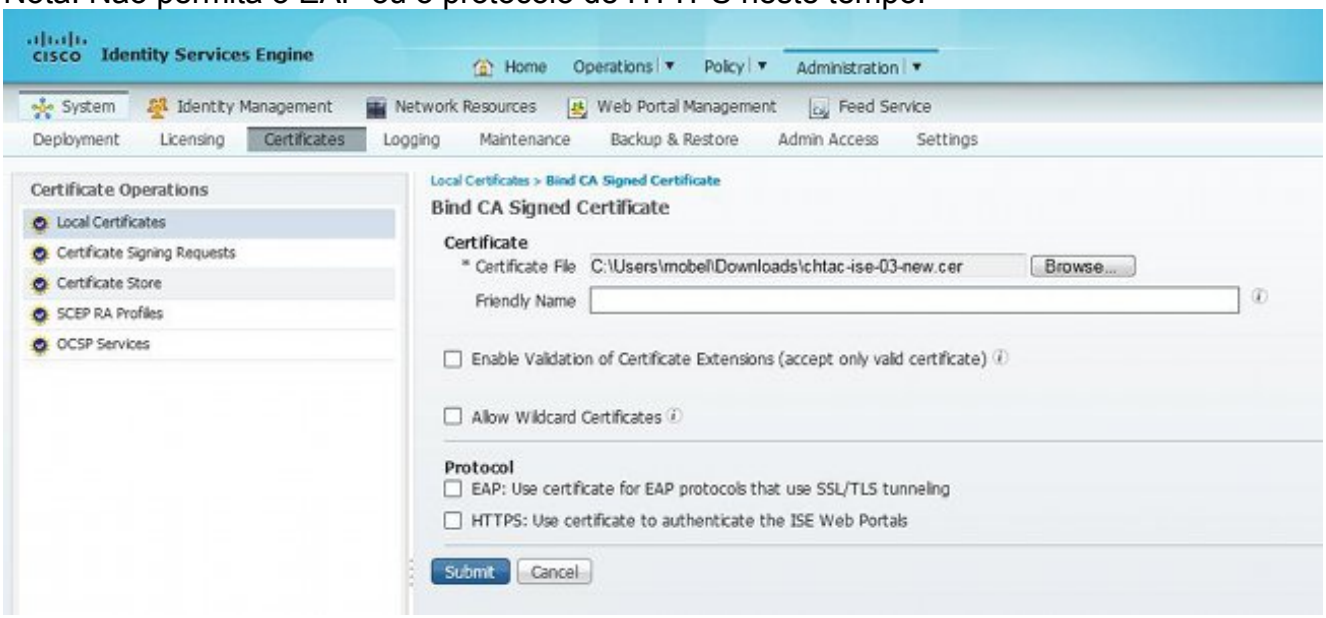
Uma vez que você recebe o certificado final de seu CA, você deve adicionar o certificado ao ISE:

1. No console ISE, clique **Certificados locais no** painel esquerdo, a seguir clique-os **adicionam** e **ligam o certificado assinado de CA**:

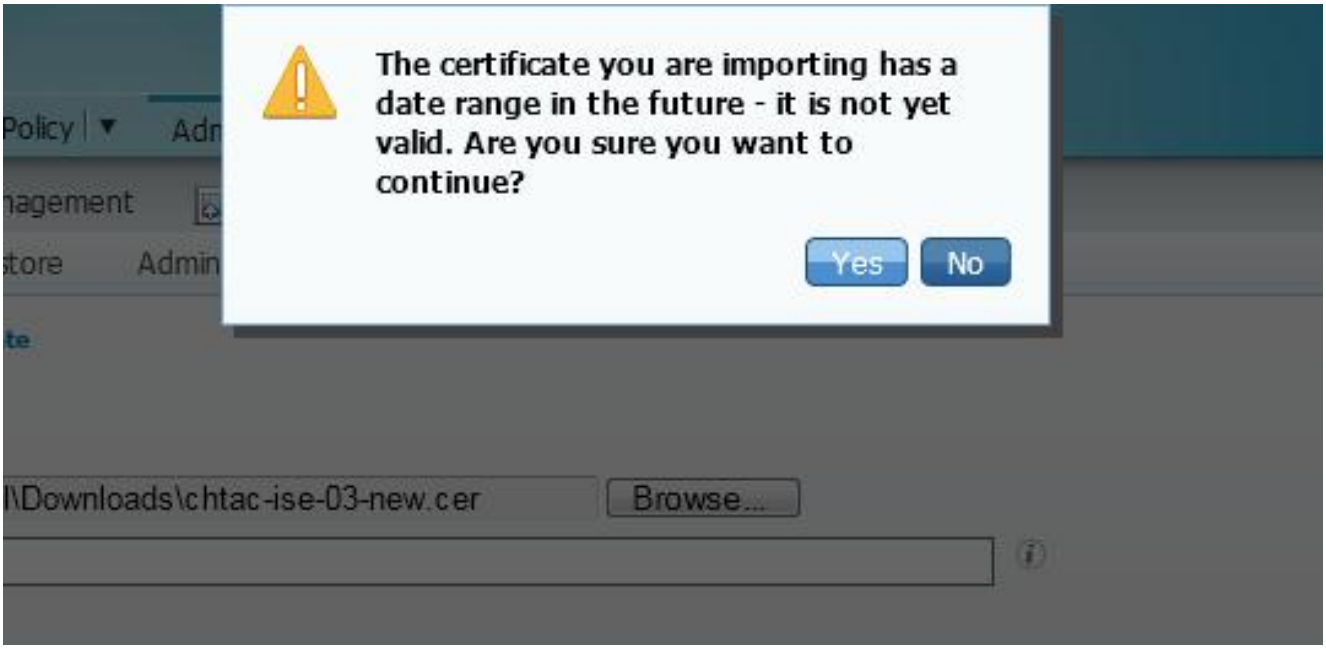


2. Incorpore uma descrição simples, clara do certificado ao campo de texto **amigável do nome**:

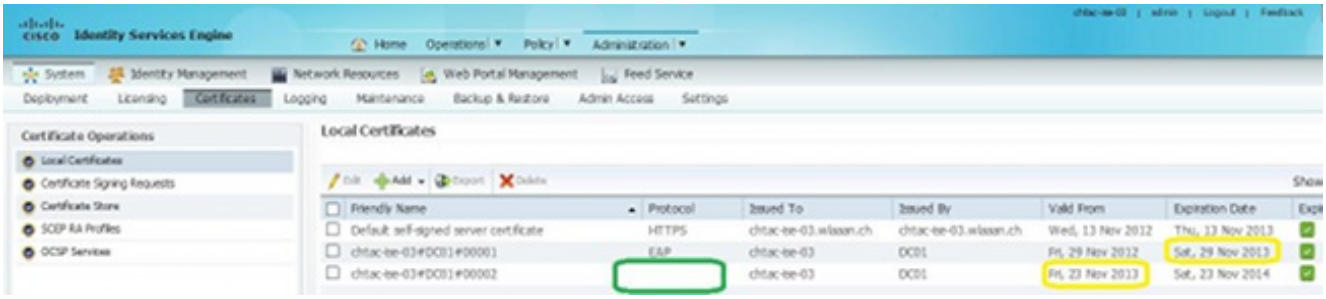
   Nota: Não permita o EAP ou o protocolo de HTTPS neste tempo.



3. Porque você está instalando o certificado novo antes que velho expire, você vê um erro que relate uma escala da data no futuro (23 de novembro de 2013 neste exemplo).



4. Clique **sim** a fim continuar. O certificado é instalado agora mas não no uso, como destacado no verde. A sobreposição entre a data de expiração e a data válida é destacada no amarelo:



Nota: Se você usa certificados auto-assinados em um desenvolvimento distribuído, o certificado auto-assinado preliminar deve ser instalado na loja do certificado confiável do server secundário ISE. Igualmente, o certificado auto-assinado secundário deve ser instalado na loja do certificado confiável do server preliminar ISE. Isto permite que os server ISE autentiquem-se mutuamente. Sem isto, o desenvolvimento pôde quebrar. Se você renova Certificados de CA da terceira, verifique se a corrente de certificado de raiz mudou e atualize a loja do certificado confiável no ISE em conformidade. Em ambas as encenações, assegure-se de que os Nós ISE, os sistemas operacionais do valor-limite, e os suplicantes possam validar a corrente de certificado de raiz.

Configurar o sistema de alerta

Cisco ISE notifica-o quando a data de expiração de um certificado local se realiza no prazo de 90 dias. Tal notificação avançada ajuda-o a evitar certificados expirados, planejar a mudança do certificado, e a impedir ou minimizar o tempo ocioso da máquina.

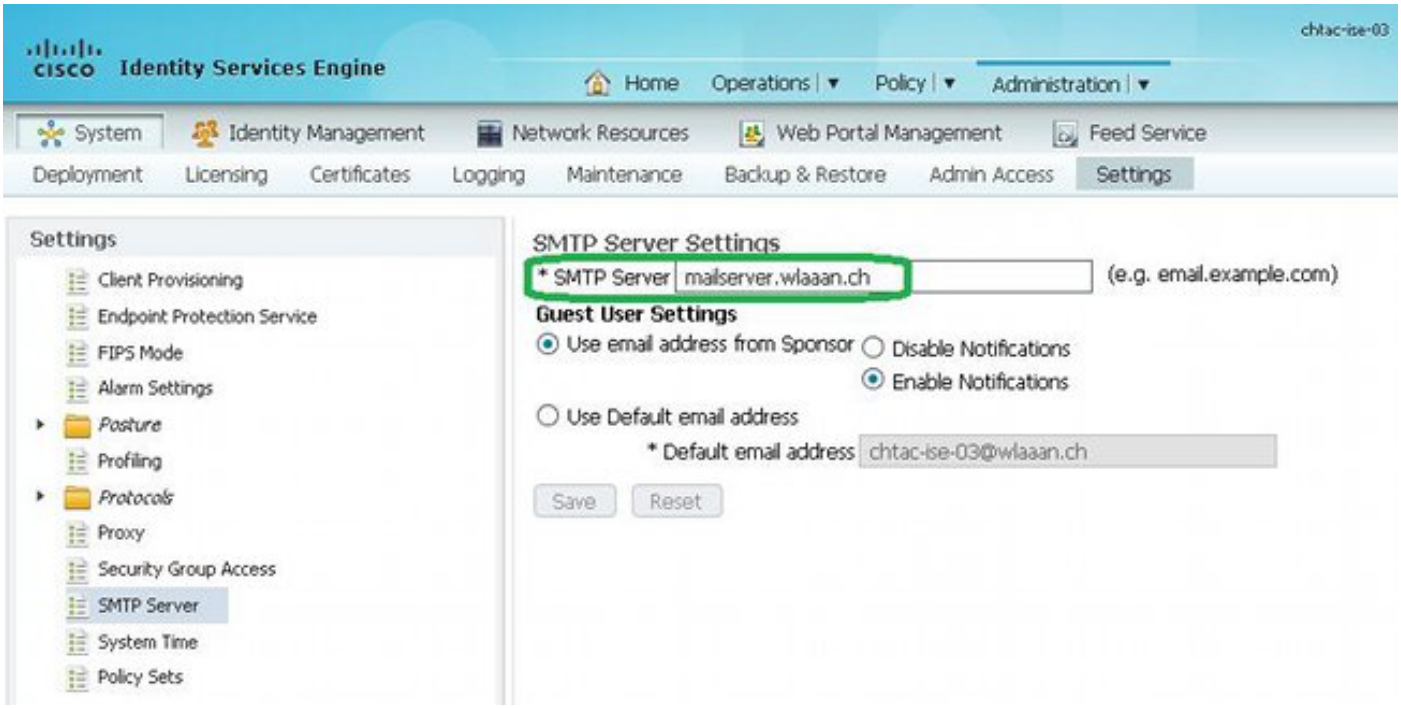
A notificação aparece em diversas maneiras:

- Os ícones do estado da expiração da cor aparecem na página local dos Certificados.

- Os mensagens de expiração aparecem no relatório do Diagnóstico do Sistema de Cisco ISE.

- Os alarmes da expiração são gerados em 90 dias e em 60 dias, então diariamente nos 30 dias finais antes da expiração.

Configurar o ISE para a notificação de Email de alarmes da expiração. No console ISE, navegue à **administração > ao sistema > aos ajustes > ao servidor SMTP**, identifique o server do Simple Mail Transfer Protocol (SMTP), e defina as outras configurações de servidor de modo que as notificações de Email sejam enviadas para os alarmes:

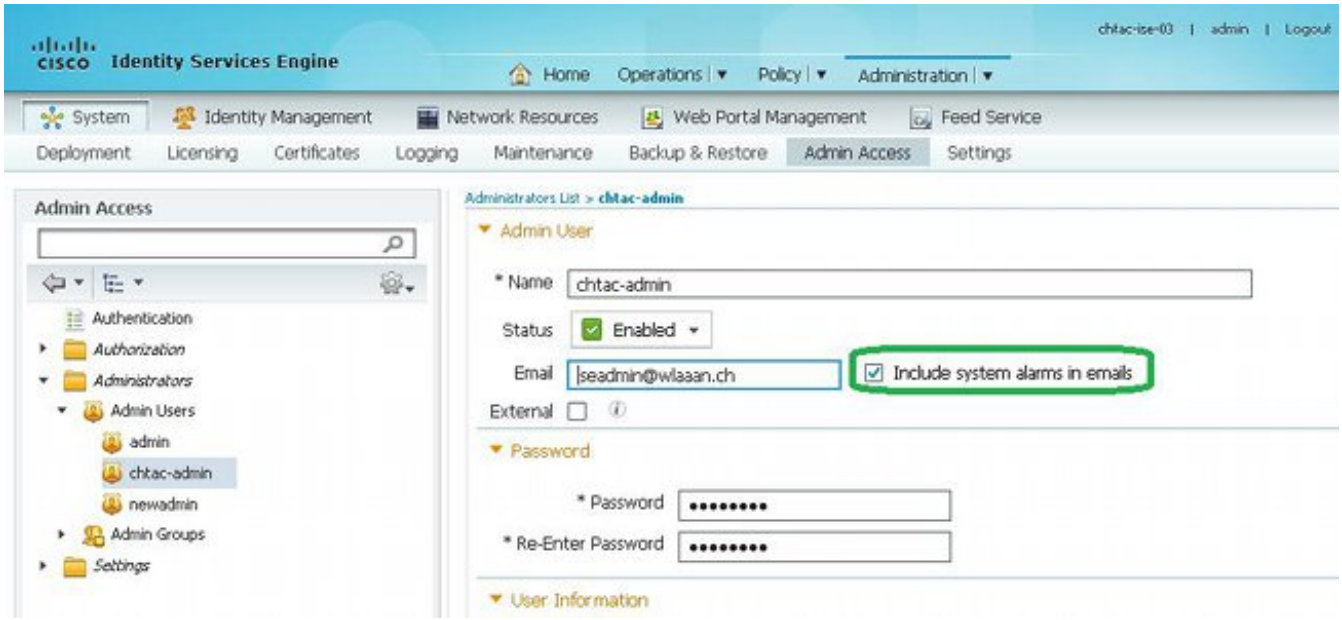


Há duas maneiras que você pode estabelecer notificações:

- Use o acesso Admin a fim notificar administradores:

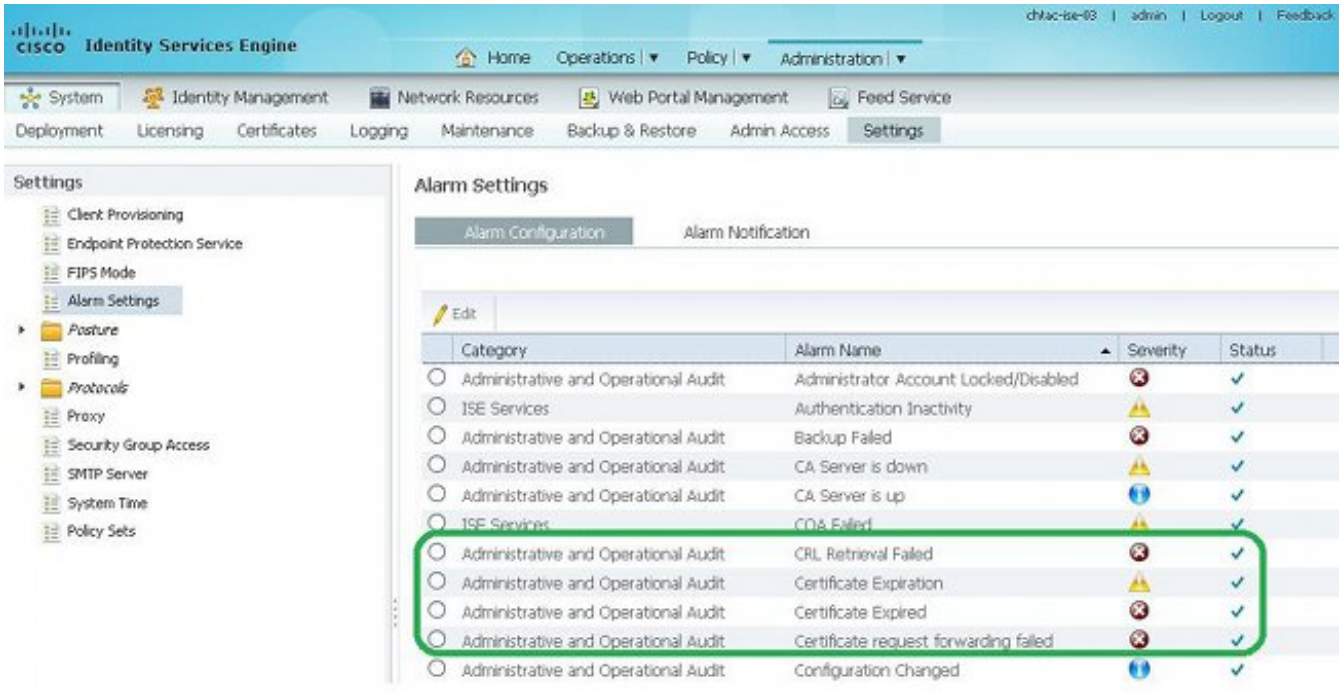
  Navegue à **administração > ao sistema > ao acesso > aos administradores > aos usuários admin Admin**.

  Verifique os **alarmes de sistema incluir na** caixa de seleção dos **email** para ver se há os usuários admin que precisam de receber notificações de alarme. O endereço email para o remetente das notificações de alarme é codificado como o ise@hostname.

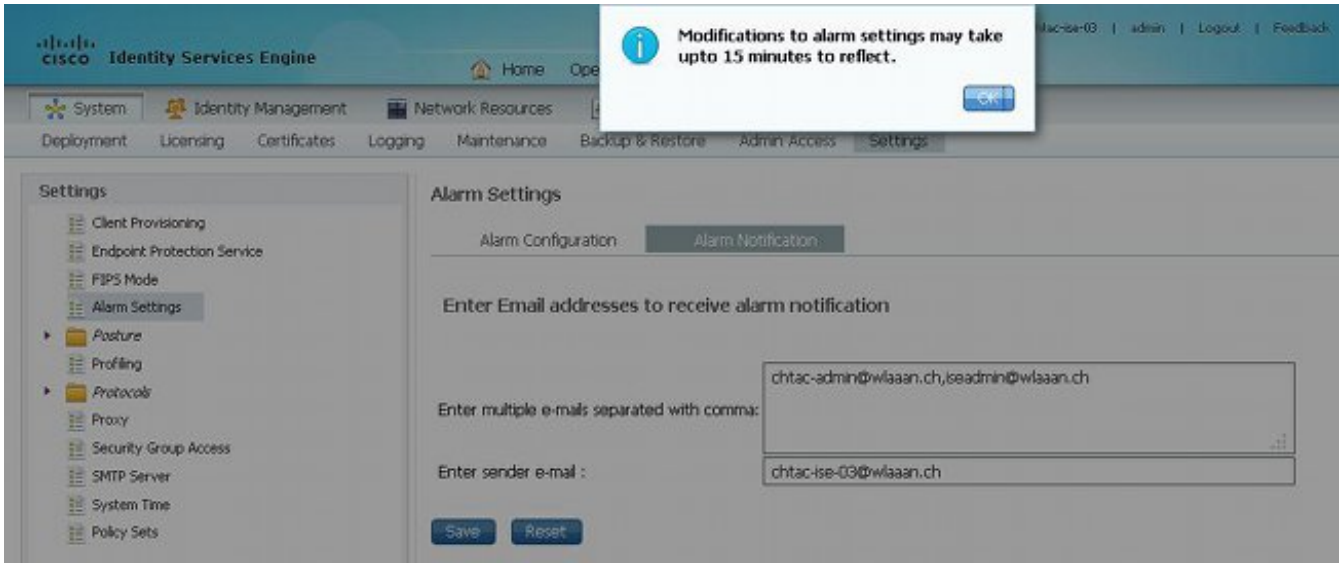


- Configurar os ajustes de alarme ISE a fim notificar usuários:

  Navegue à **administração > ao sistema > aos ajustes > aos ajustes de alarme > à configuração do alarme**:



  Nota: Desabilite o estado para uma categoria se você deseja impedir alarmes dessa categoria.Clique a **notificação de alarme,** incorpore os endereços email dos usuários a ser notificados, e salvar a alteração de configuração. As mudanças puderam tomar até 15 minutos antes que estejam ativas.

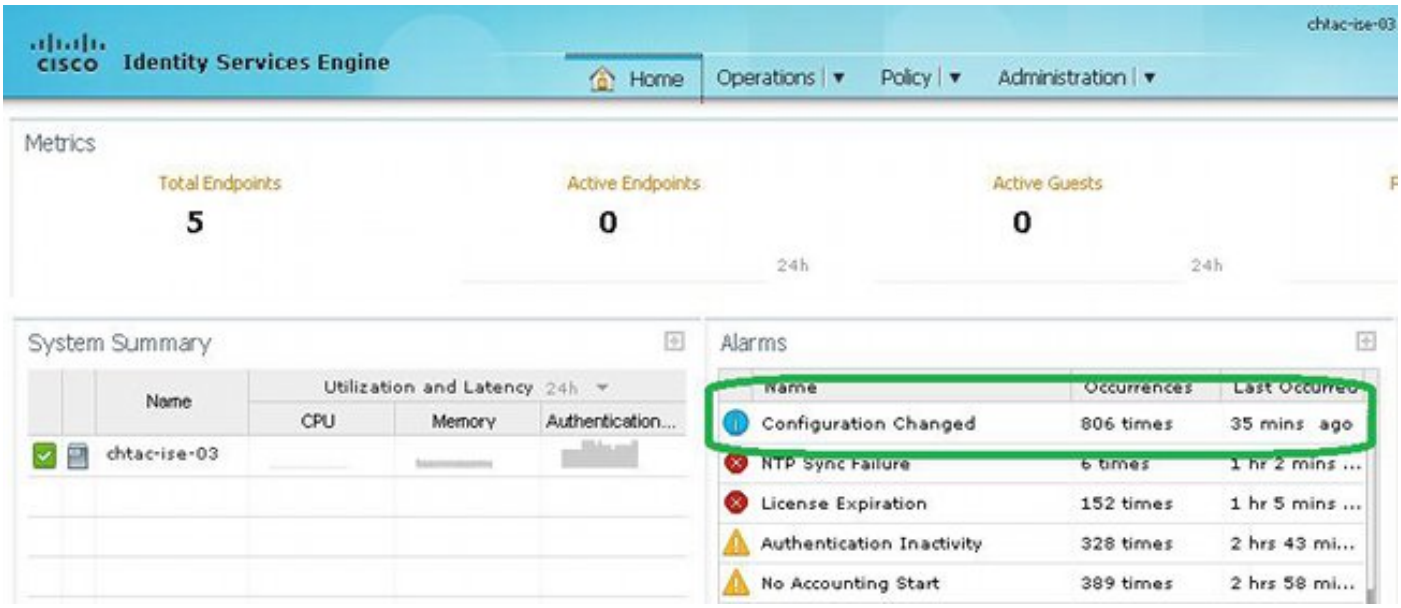


Verificar

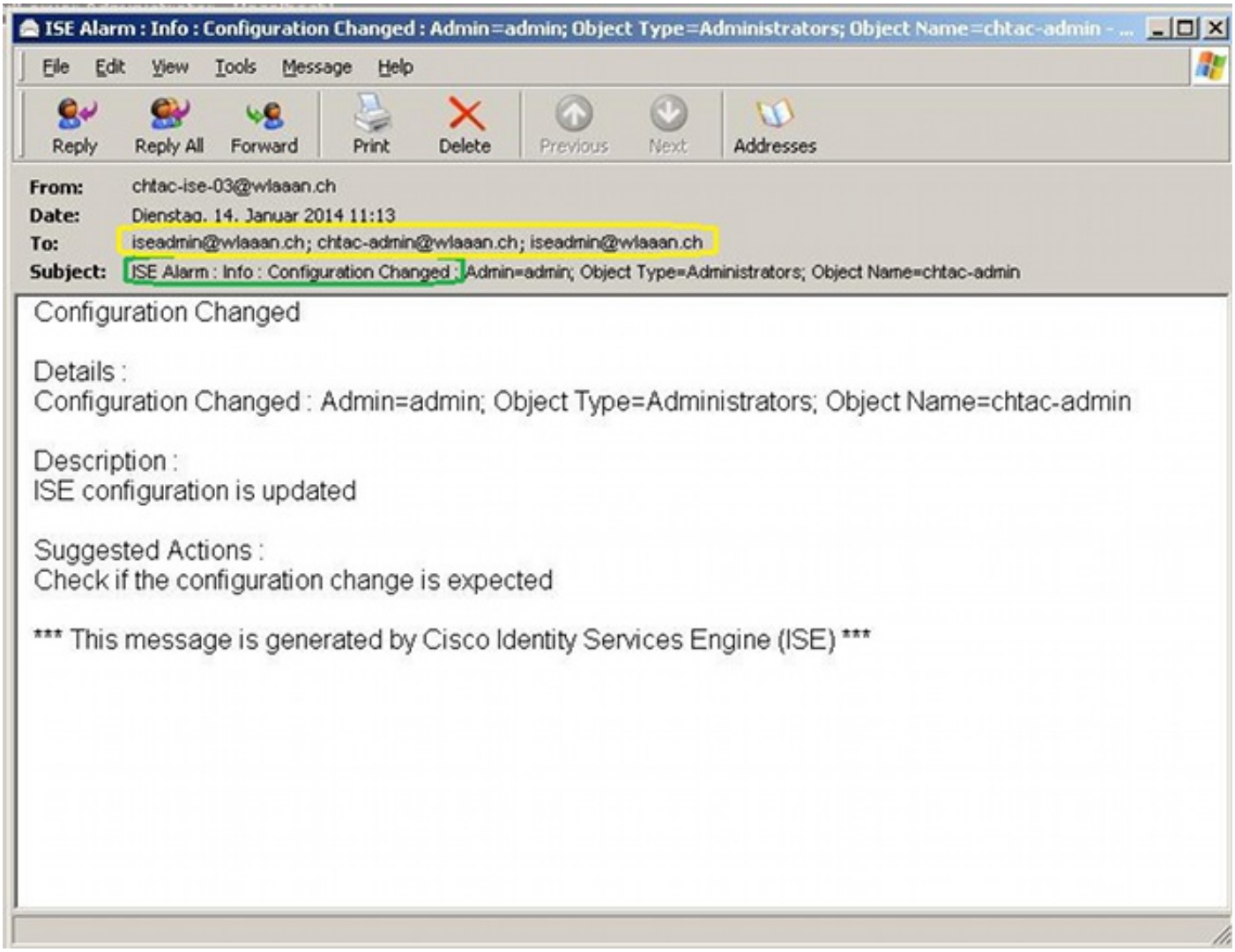
Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique o sistema de alerta

Verifique que o sistema de alerta trabalha corretamente. Neste exemplo, uma alteração de configuração gerencie um alerta com um nível de seriedade da informação. (Um alarme da informação é a mais baixa severidade, quando as expirações do certificado gerarem uma severidade mais elevada em nível do aviso.)



Este é um exemplo do alarme do email que é enviado pelo ISE:



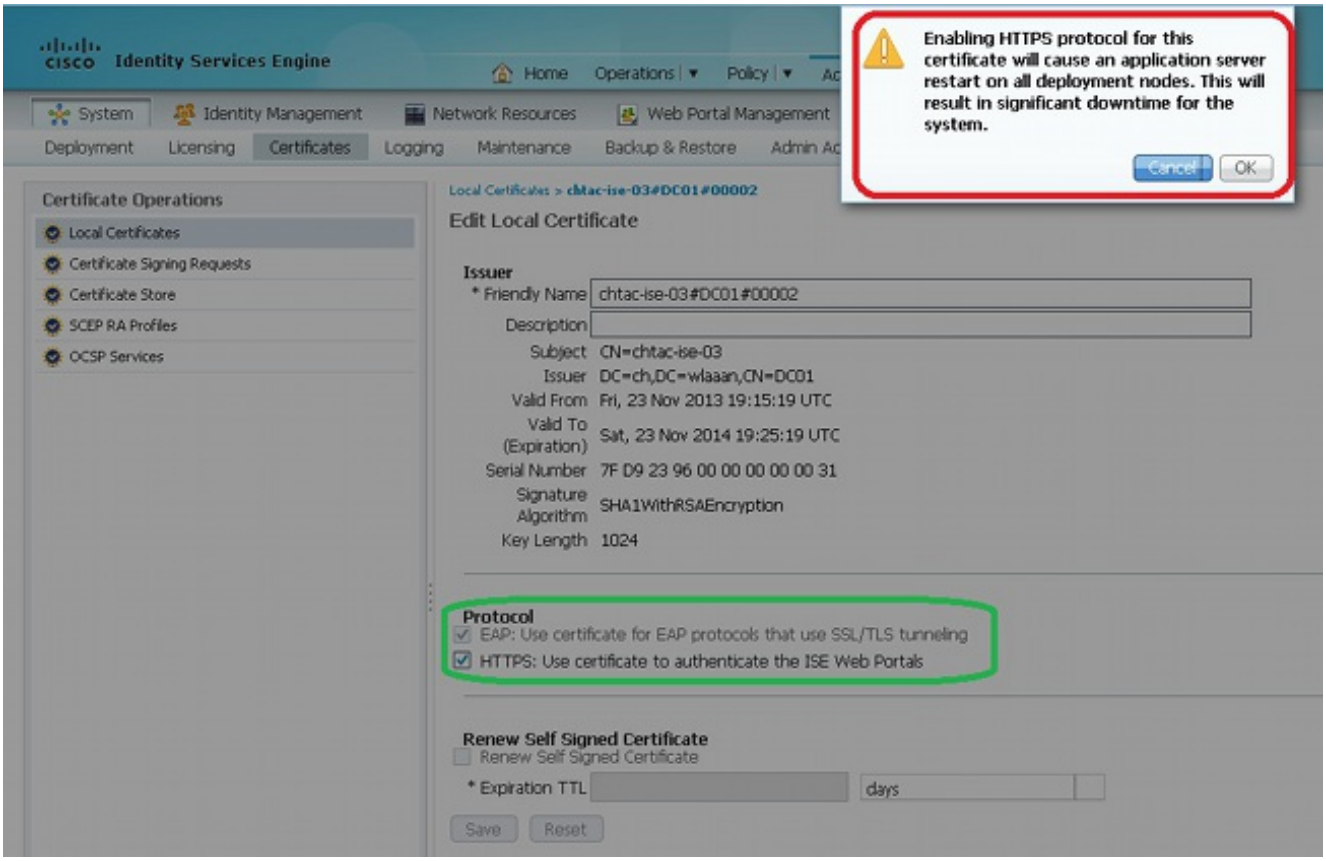
Nota: Neste exemplo, o ISE envia o mensagem de alarme do email duas vezes a iseadmin@wlaaan.ch, como destacado no amarelo. Este endereço email estabeleceu-se para receber notificações por ambos os métodos explicados dentro configura o sistema de alerta.

Verifique a mudança do certificado

Este procedimento descreve como verificar que o certificado está instalado corretamente e como mudar os protocolos para o EAP e/ou o HTTPS:

1. No console ISE, navegue à **administração > aos Certificados > Certificados locais**, e selecione o certificado novo a fim ver os detalhes.

   Cuidado: Se você permite o protocolo de HTTPS, o serviço ISE reinicia, que causa o tempo ocioso de servidor.



Neste exemplo, supõe que o HTTPS reinicia o serviço ISE.

2. A fim verificar o estado do certificado no server ISE, incorpore este comando no CLI:

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

3. Uma vez que todos os serviços são ativos, tente entrar como um administrador.

4. Para um cenário de distribuição distribuído, navegue à **administração > ao sistema > ao desenvolvimento > ao status do nó no** console ISE, e verifique o status do nó.

5. Certifique-se da autenticação do utilizador final esteja bem sucedida. No console ISE, navegue às **operações > às autenticações**, e reveja o certificado para a autenticação protegida da Segurança da camada do protocolo extensible authentication (PEAP) /EAP-Transport (TLS).

Verifique o certificado

Se você quer verificar externamente o certificado, você pode usar as ferramentas encaixadas de Microsoft Windows ou o conjunto de ferramentas do OpenSSL.

O OpenSSL é uma aplicação da aberta do protocolo do secure sockets layer (SSL). Se os Certificados usam seu próprio CA privado, você deve colocar seu certificado CA raiz em uma máquina local e usar a opção do OpenSSL - *CApath*. Se você tem CA intermediário, você deve colocá-lo no mesmo diretório também.

A fim obter a informação geral sobre o certificado e verificá-la, uso:

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

Pôde igualmente ser útil converter os Certificados com o conjunto de ferramentas do OpenSSL:

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Conclusão

Porque você pode instalar um certificado novo no ISE antes que esteja ativo, Cisco recomenda que você instala o certificado novo antes que o certificado velho expire. Este período da sobreposição entre a data de expiração do certificado velha e a data de início nova do certificado dá-lhe a hora de renovar Certificados e planejar sua instalação com pouco ou nenhum o tempo ocioso da máquina. Uma vez que o certificado novo incorpora sua escala válida da data, permita o EAP e/ou o protocolo de HTTPS. Recorde, se você permite o HTTPS, haverá um reinício do serviço.