Renovación del certificado en la guía de configuración del Cisco Identity Services Engine

Contenido

Introducción

Este documento describe las mejores prácticas y los procedimientos dinámicos de renovar los Certificados en el Cisco Identity Services Engine (ISE). También revisa cómo configurar las alarmas y las notificaciones así que advierten los administradores de los eventos próximos tales como vencimiento del certificado.

> **Note**: Este documento no se piensa para ser guía de Troubleshooting para los Certificados.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados X509

- Configuración de Cisco ISE con los Certificados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.2.0.899 de Cisco ISE
- Dispositivo o VMware

Antecedentes

Como administrador ISE, usted encontrará eventual el hecho de que expiran los Certificados ISE. Si su servidor ISE tiene un certificado vencido, los problemas graves pudieron presentarse a menos que usted substituya el certificado vencido por un nuevo, certificado válido.

> **Note**: Si expira el certificado que se utiliza para el Protocolo de Autenticación Extensible (EAP), todas las autenticaciones pudieron fallar porque los clientes no confían en el certificado ISE más. Si expira el certificado del protocolo HTTP, el riesgo es incluso mayor: un administrador no pudo poder iniciar sesión al ISE más, y el despliegue distribuido pudo dejar de funcionar y de replicar.

En este ejemplo, el ISE tiene un certificado instalado de un servidor del Certificate Authority (CA) que expire en un mes. El administrador ISE debe instalar un nuevo, certificado válido en el ISE antes de que expire el certificado viejo. Este enfoque proactivo previene o minimiza el tiempo muerto y evita un impacto en sus usuarios finales. El período de tiempo del certificado nuevamente instalado comienza una vez, usted puede habilitar el EAP y/o el protocolo HTTP en el nuevo certificado.

Usted puede configurar el ISE de modo que genere las alarmas y notifique al administrador para instalar los nuevos Certificados antes de que expiren los Certificados viejos.

> **Note**: Este documento utiliza el HTTPS con un certificado autofirmado para demostrar el impacto de la renovación del certificado, pero este acercamiento no se recomienda para un sistema vivo. Es mejor utilizar un certificado de CA para el EAP y los protocolos HTTP.

Configurar

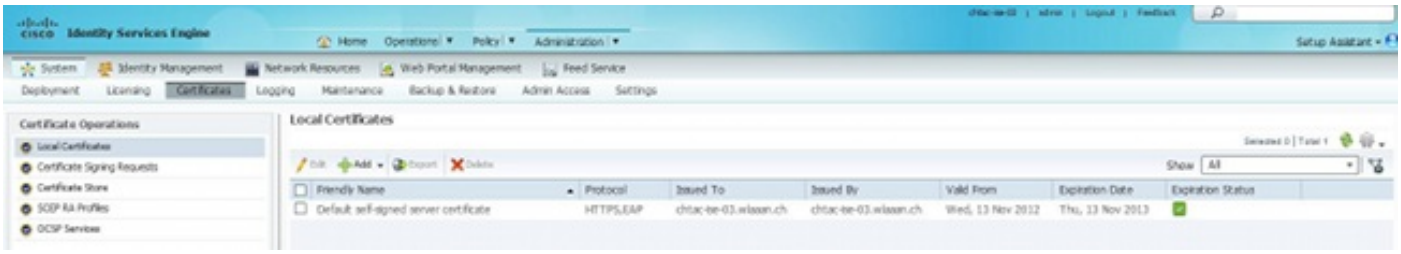
Certificados autofirmados de la visión ISE

Cuando el ISE está instalado, genera un certificado autofirmado. El certificado autofirmado se utiliza para el acceso de la administración y para la comunicación dentro del despliegue distribuido (HTTPS) así como para la autenticación de usuario (EAP). En un sistema vivo, utilice un certificado de CA en vez de un certificado autofirmado.

> **Tip**: Refiera a la [administración de certificados en la](#) sección de [Cisco ISE del guía de instalación del hardware del Cisco Identity Services Engine, libere 1.2](#) para la información adicional.

El formato para un certificado ISE debe ser Privacy Enhanced Mail (PEM) o las reglas distinguidas de la codificación (DER).

Para ver el certificado autofirmado inicial, navegue a la **administración** > a **System> certifica** > los **Certificados locales** en la consola ISE:



Si usted instala un certificado de servidor en el ISE vía un pedido de firma de certificado (CSR) y cambia el certificado para el protocolo HTTPS o EAP, el certificado de servidor uno mismo-firmado está todavía presente pero es no se utilizan más.

> **Caution**: Para los cambios del protocolo HTTP, un reinicio de los servicios ISE se requiere, que crea algunos minutos del tiempo muerto. Los cambios del protocolo EAP no accionan un reinicio de los servicios ISE y no causan el tiempo muerto.

Determine cuando cambiar el certificado

Asuma que expira el certificado instalado pronto. ¿Es mejor dejar el certificado expirar antes de que usted lo renueve o cambiar el certificado antes de la expiración? Usted debe cambiar el certificado antes de la expiración de modo que usted tenga tiempo para planear el intercambio del certificado y para manejar cualquier tiempo muerto causado por el intercambio.

¿Cuándo debe usted cambiar el certificado? Obtenga un nuevo certificado con una Fecha de inicio que preceda la fecha de vencimiento del certificado viejo. El período de tiempo entre esas dos fechas es la ventana del cambio.

> **Caution**: Si usted habilita el HTTPS, causa un reinicio del servicio en el servidor ISE, y usted experimenta algunos minutos del tiempo muerto.

Esta imagen representa la información para un certificado que sea publicado por CA y expira el 29 de noviembre 2013:

Genere el pedido de firma de certificado

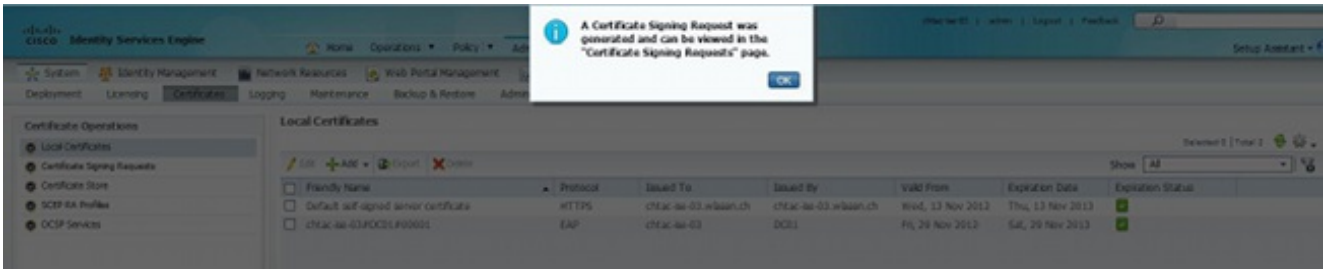
Este procedimiento describe cómo renovar el certificado con un CSR:

1. En la consola ISE, navegue **para agregar > generan el pedido de firma de certificado**.

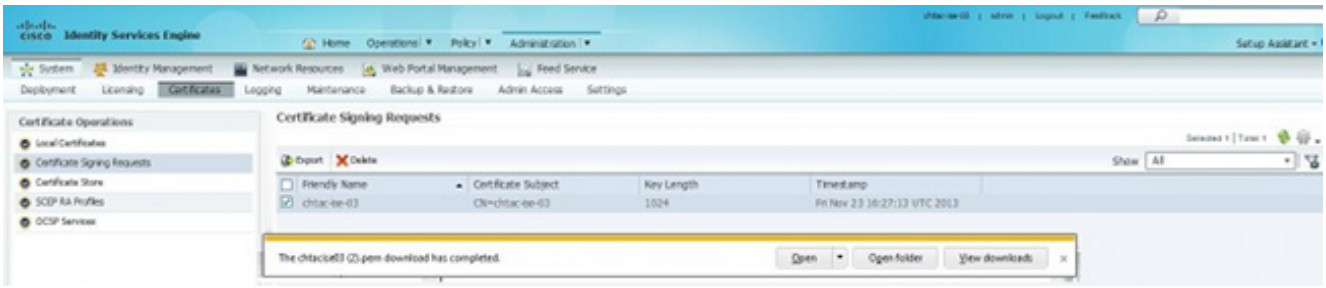
2. La información mínima que usted debe ingresar en el campo de texto del **tema del certificado** es CN=ISEfqdn, donde está el Nombre de dominio totalmente calificado (FQDN) *ISEfqdn* (FQDN) del ISE. Agregue los campos adicionales tales como O (organización), OU (unidad organizativa), o C (país) en el tema del certificado con el uso de las comas:

3. Una de las líneas de campo de texto **alternativas sujetas del nombre (SAN)** debe relanzar el ISE FQDN. Usted puede agregar un segundo campo SAN si usted quiere utilizar los nombres alternativos o un certificado del comodín.

4. Una ventana emergente indica si los campos CSR están completados correctamente:



5. Para exportar el CSR, los **pedidos de firma de certificado del** tecleo en el panel izquierdo, seleccionar su CSR, y la **exportación del** tecleo:

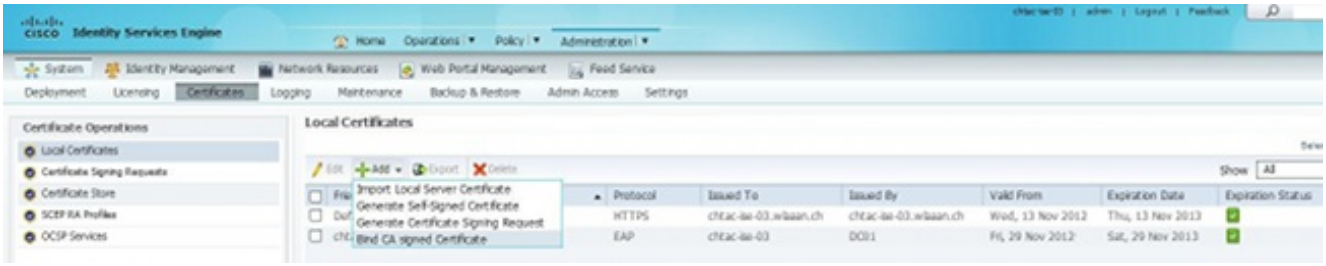


6. El CSR se guarda en su ordenador. Sométalo a su CA para la firma.

Instale el certificado

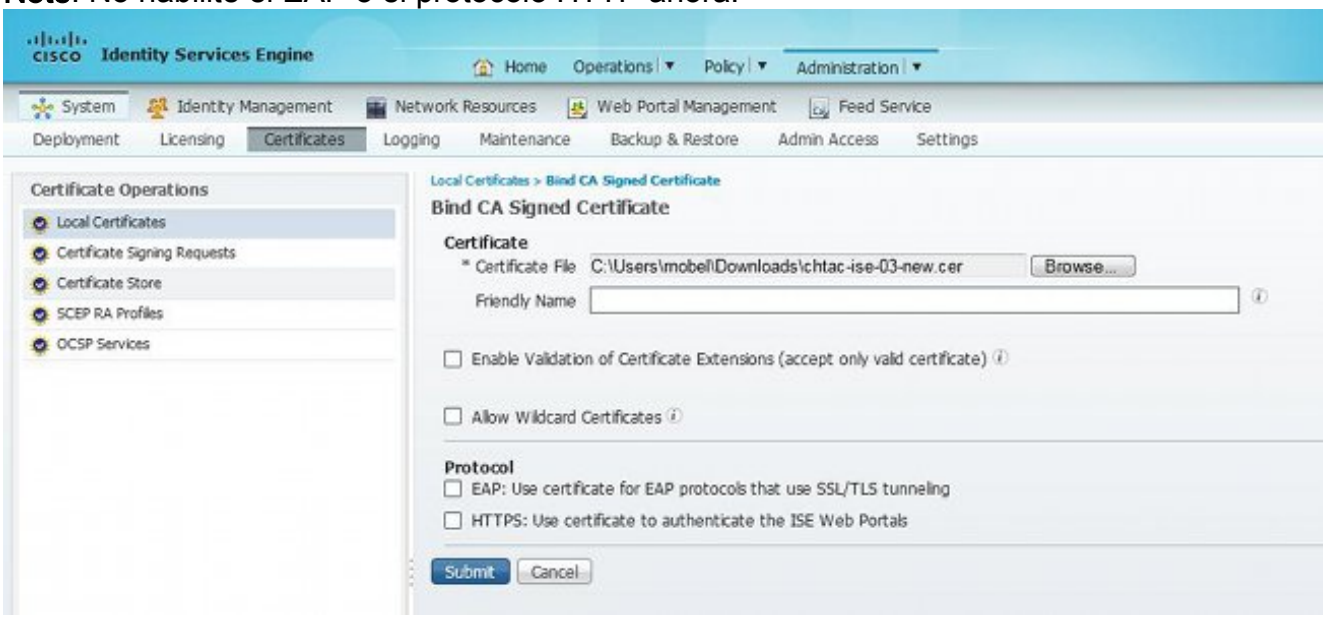
Una vez que usted recibe el certificado final de su CA, usted debe agregar el certificado al ISE:

1. En la consola ISE, haga clic los **Certificados locales** en el panel izquierdo, después haga clic **agregan** y **atan el certificado firmado de CA**:

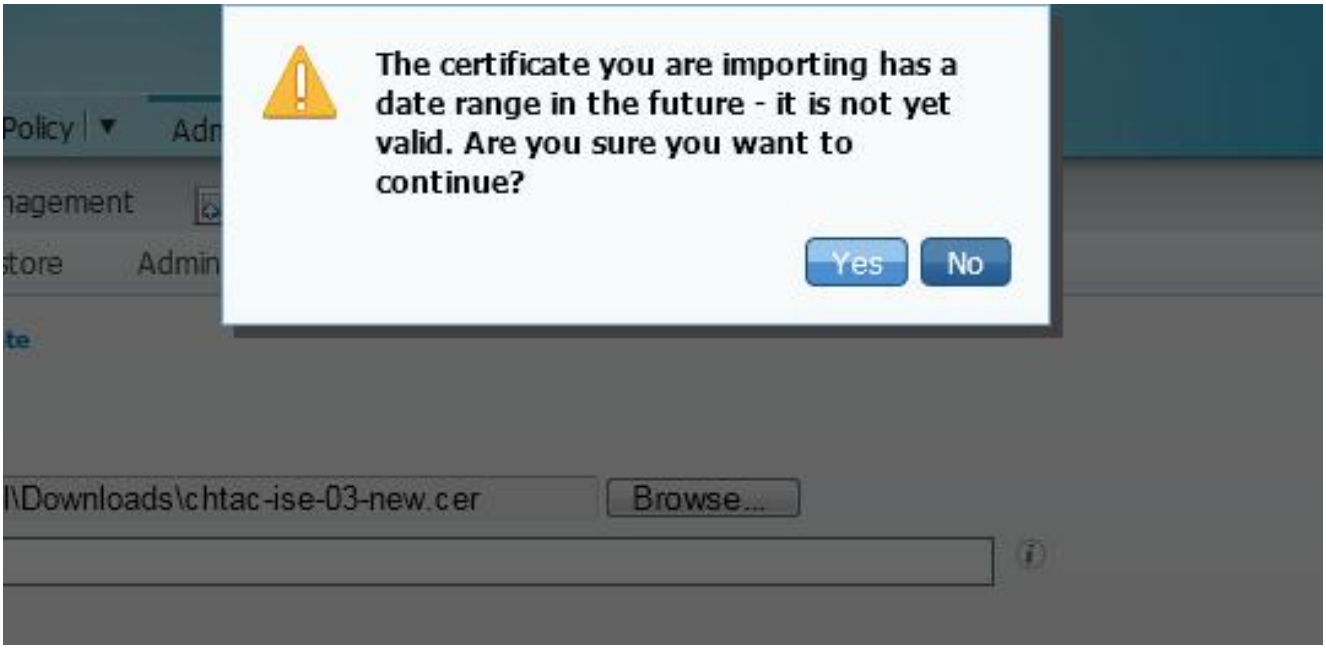


2. Ingrese una descripción simple, clara del certificado en el campo de texto **cómodo del nombre**:

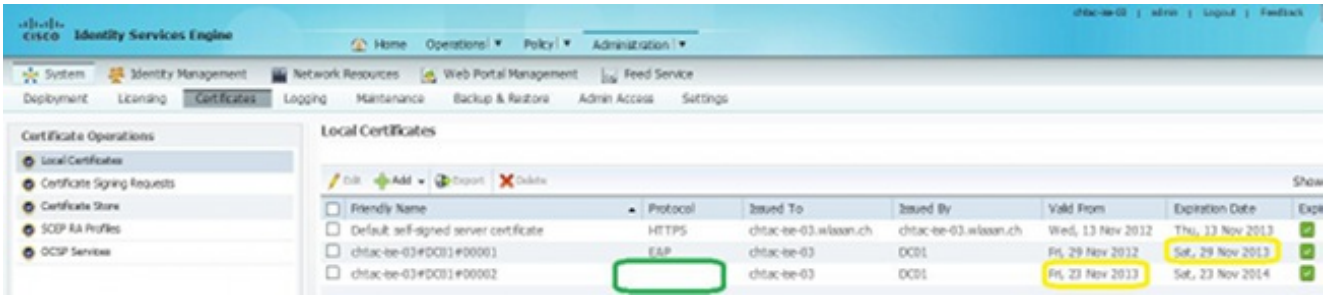
   Note: No habilite el EAP o el protocolo HTTP ahora.



3. Porque usted está instalando el nuevo certificado antes de que expire el viejo, usted ve un error que señale un rango de la fecha en el futuro (23 de noviembre de 2013 en este ejemplo).



4. Tecleo **sí** para continuar. El certificado ahora está instalado pero parado, según lo resaltado en el verde. La coincidencia entre la fecha de vencimiento y la fecha válida se resalta en el amarillo:



Note: Si usted utiliza los certificados autofirmados en un despliegue distribuido, el certificado autofirmado primario se debe instalar en el almacén del certificado confiable del servidor secundario ISE. Asimismo, el certificado autofirmado secundario se debe instalar en el almacén del certificado confiable del servidor primario ISE. Esto permite que los servidores ISE se autentiquen mutuamente. Sin esto, el despliegue pudo romperse. Si usted renueva los Certificados de CA de tercera persona, verifique si el encadenamiento de certificado raíz haya cambiado y ponga al día el almacén del certificado confiable en el ISE por consiguiente. En ambos escenarios, asegúrese de que los Nodos ISE, los sistemas operativos del punto final, y los suplicantes puedan validar el encadenamiento de certificado raíz.

Configure el sistema de alerta

Cisco ISE le notifica cuando la fecha de vencimiento de un certificado local es en el plazo de 90 días. Tal notificación anticipada le ayuda a evitar los certificados vencidos, a planear el cambio del certificado, y a prevenir o a minimizar el tiempo muerto.

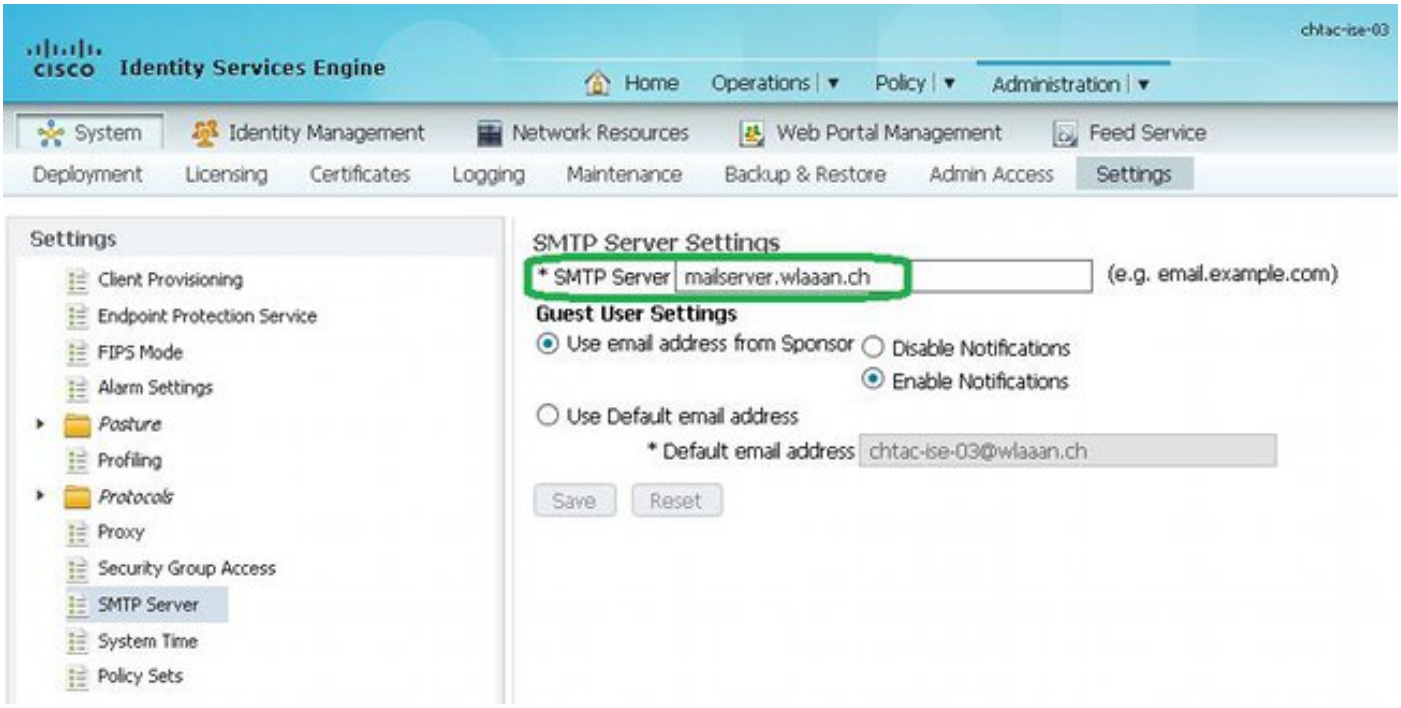
La notificación aparece de varias maneras:

- Los iconos del estatus de la expiración del color aparecen en la página local de los Certificados.

- Los mensajes de vencimiento aparecen en el informe del Diagnóstico de sistema de Cisco ISE.

- Las alarmas de la expiración se generan en 90 días y 60 días, entonces diariamente en los 30 días finales antes de la expiración.

Configure el ISE para la notificación por correo electrónico de las alarmas de la expiración. En la consola ISE, navegue a la **administración > al sistema > a las configuraciones > al servidor SMTP**, identifique el servidor del Simple Mail Transfer Protocol (SMTP), y defina los otros servidores establezca para enviar las notificaciones por correo electrónico para las alarmas:

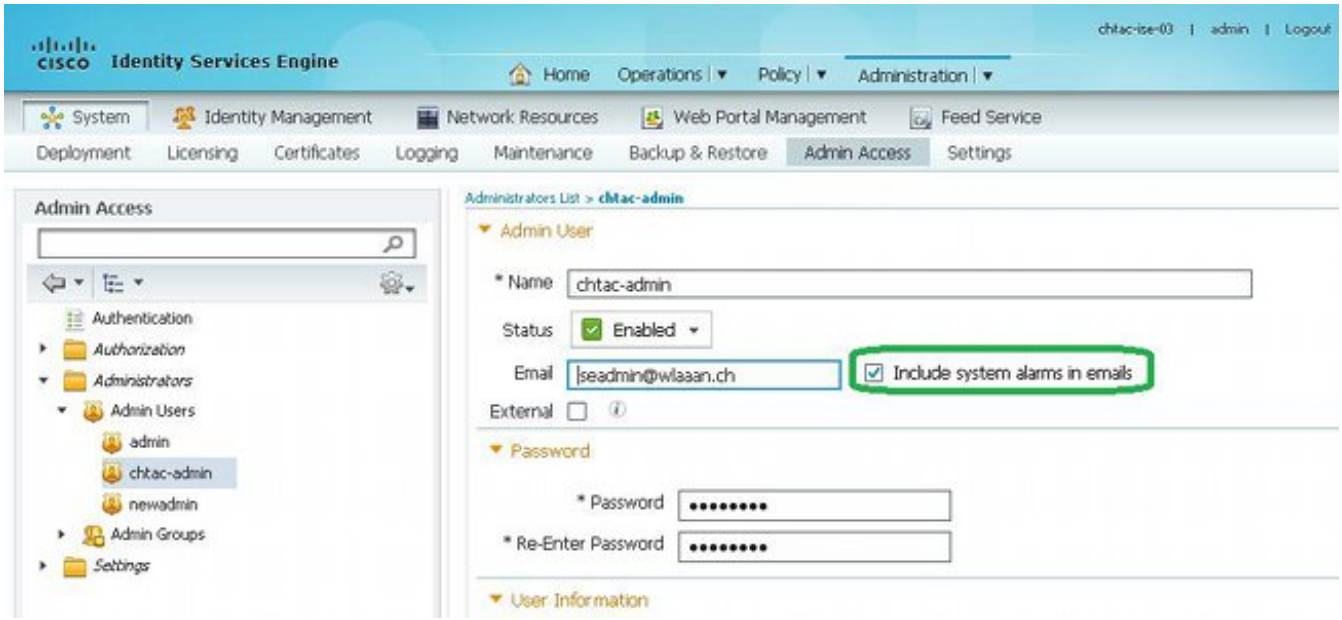


Hay dos maneras que usted puede configurar las notificaciones:

- Acceso Admin del uso para notificar a los administradores:

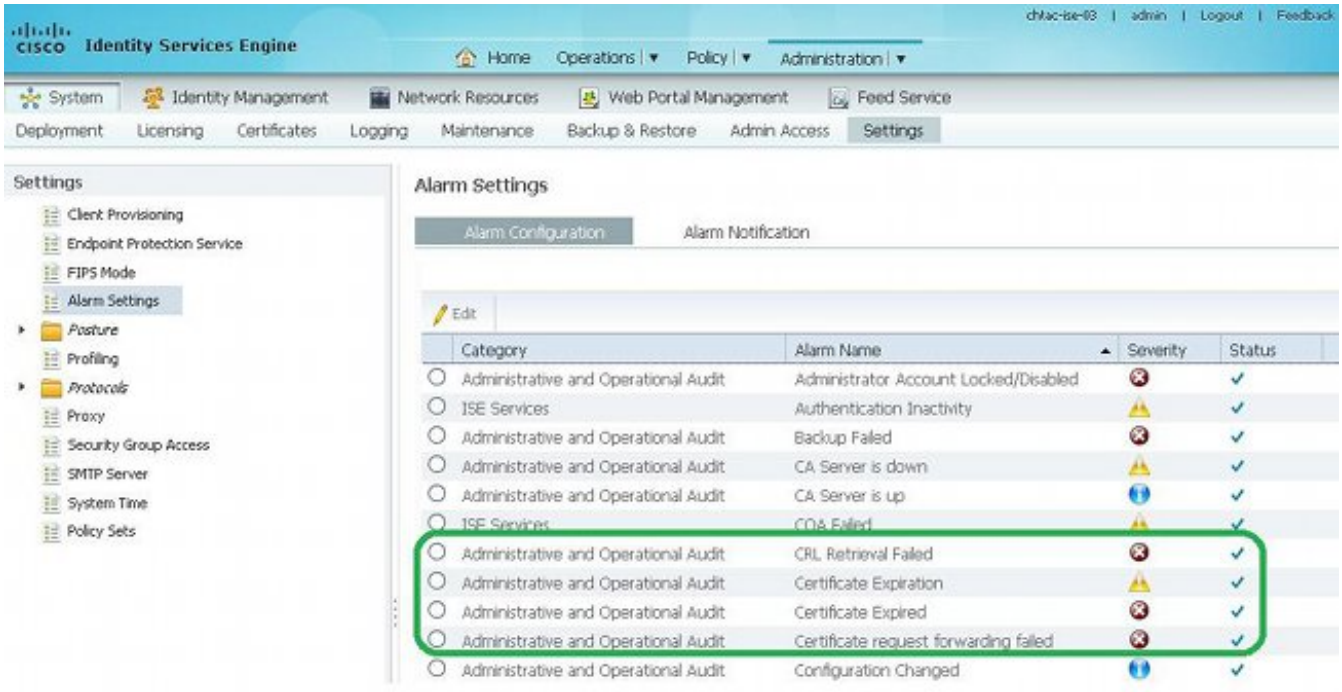
  Navegue a la **administración > al sistema > al acceso > a los administradores > a los Usuarios administradores Admin**.

  Marque las **Alarmas del sistema del incluido en el** checkbox de los **correos electrónicos** para los Usuarios administradores que necesitan recibir las notificaciones de alarma. La dirección de correo electrónico para el remitente de las notificaciones de alarma está puesta en hard-code como ise@hostname.

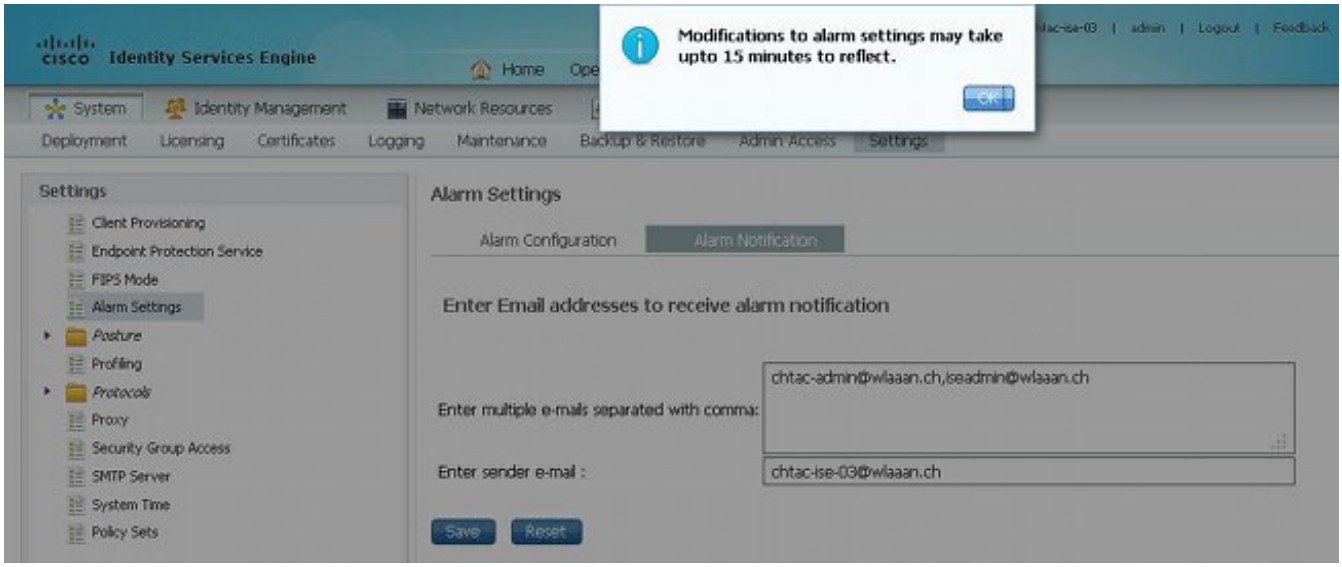


- Configure las configuraciones de alarma ISE para notificar a los usuarios:

  Navegue a la **administración > al sistema > a las configuraciones > a las configuraciones de alarma > a la configuración de la alarma**:



Note: Inhabilite el estatus para una categoría si usted desea prevenir las alarmas de esa categoría.Haga clic la **notificación de alarma,** ingrese las direcciones email de los usuarios que se notificarán, y salve el cambio de configuración. Los cambios pudieron tomar hasta 15 minutos antes de que son activos.

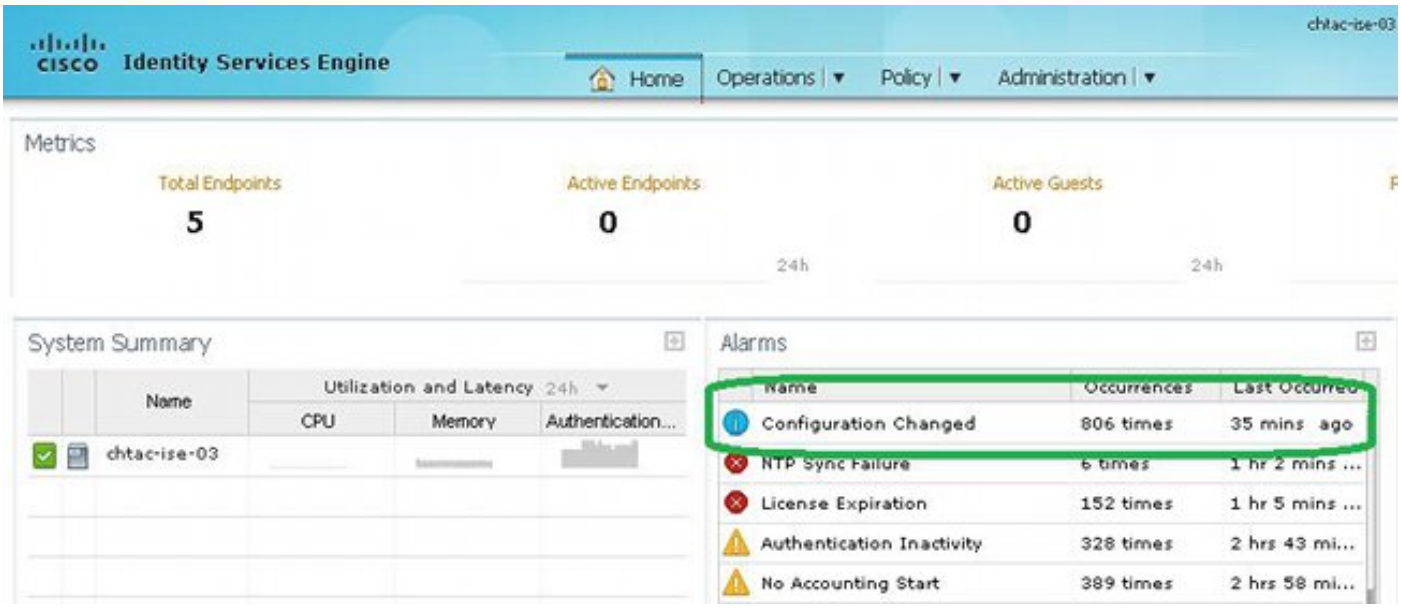


Verificación

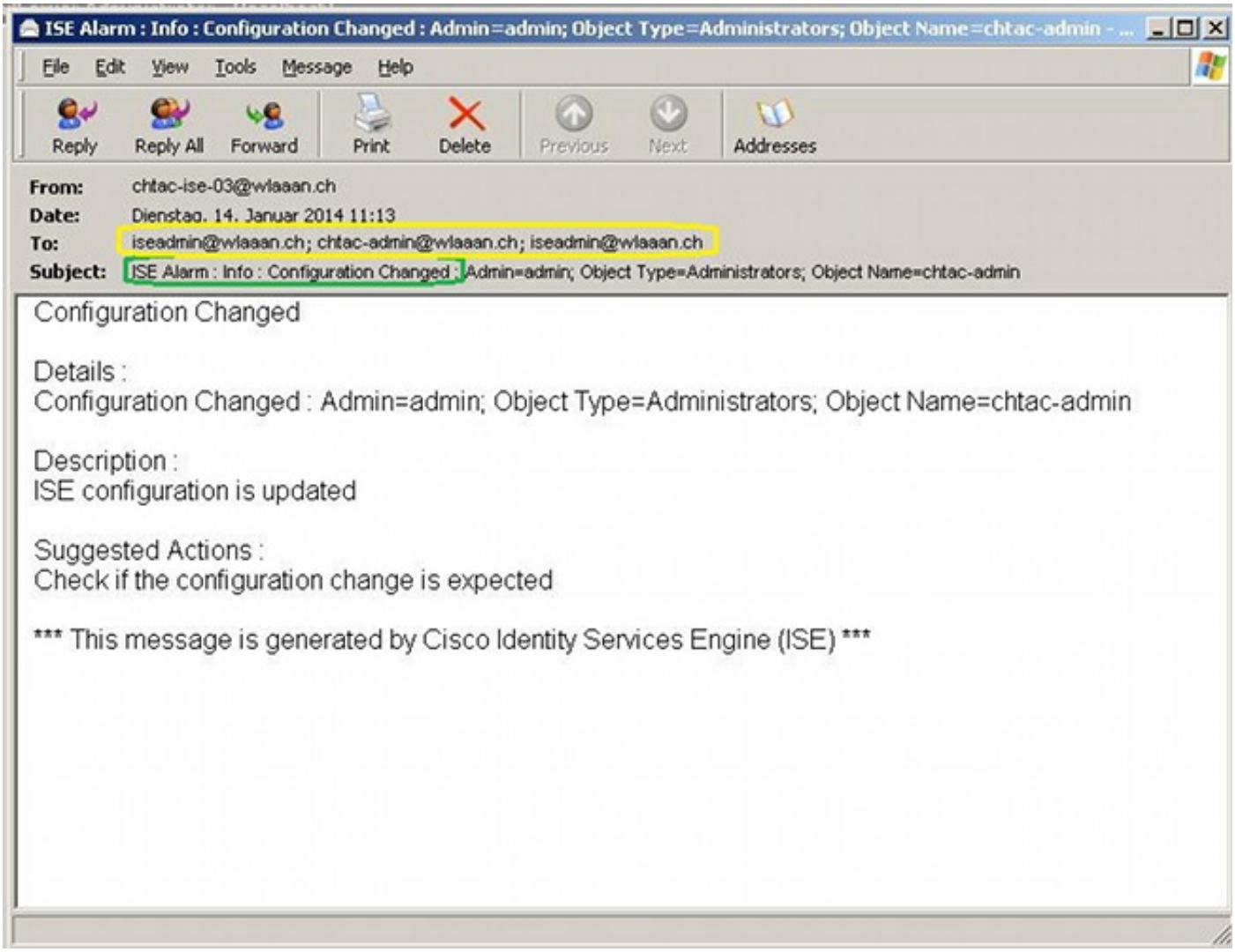
Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique el sistema de alerta

Verifique que el sistema de alerta trabaje correctamente. En este ejemplo, un cambio de configuración genera una alerta con un nivel de gravedad de información. (Una alarma de la información es la gravedad más baja, mientras que los vencimientos del certificado generan una mayor gravedad llana de la advertencia.)



Éste es un ejemplo de la alarma del correo electrónico que es enviada por el ISE:



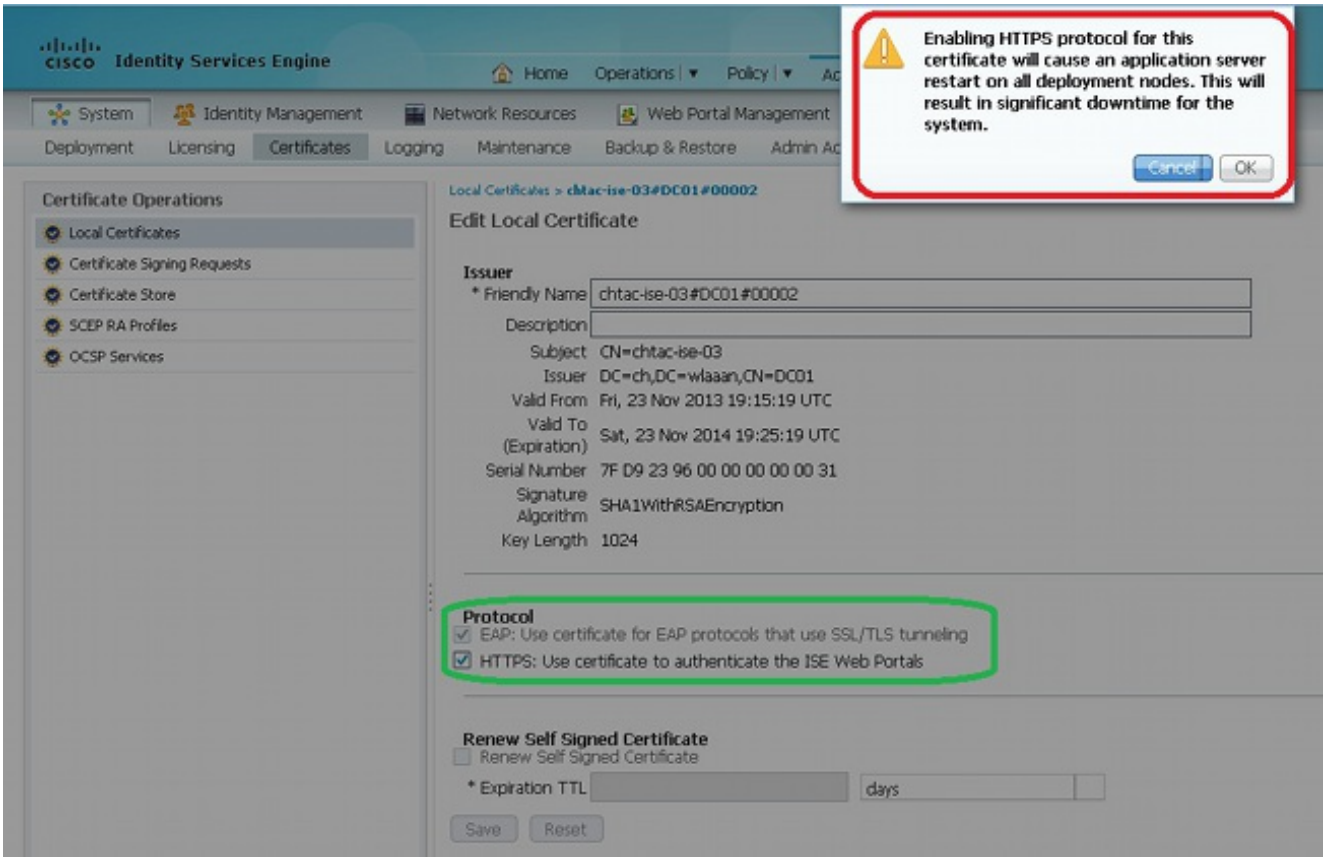
Note: En este ejemplo, el ISE envía el mensaje de alarma del correo electrónico dos veces a iseadmin@wlaaan.ch, según lo resaltado en el amarillo. Esta dirección de correo electrónico fue configurada para recibir las notificaciones por ambos métodos explicados en el sistema de alerta de la configuración.

Verifique el cambio del certificado

Este procedimiento describe cómo verificar que el certificado está instalado correctamente y cómo cambiar los protocolos para el EAP y/o el HTTPS:

1. En la consola ISE, navegue a la **administración > a los Certificados > los Certificados locales**, y seleccione el nuevo certificado para ver los detalles.

   Caution: Si usted habilita el protocolo HTTP, el servicio ISE recomienza, que causa el tiempo de inactividad del servidor.



En este ejemplo, asuma que el HTTPS recomienza el servicio ISE.

2. Para verificar el estatus del certificado en el servidor ISE, ingrese este comando en el CLI:

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

3. Una vez que todos los servicios son activos, intente iniciar sesión como administrador.

4. Para un escenario de instrumentación distribuido, navegue a la **administración > al sistema > al despliegue > al estado de nodo** en la consola ISE, y verifique el estado de nodo.

5. Marque que la autenticación del usuario final es acertada. En la consola ISE, navegue a las **operaciones > a las autenticaciones**, y revise el certificado para la autenticación protegida de la Seguridad de la capa del protocolo extensible authentication (PEAP) /EAP-Transport (TLS).

Verifique el certificado

Si usted quiere marcar el certificado externamente, usted puede utilizar las herramientas integradas de Microsoft Windows o el juego de herramientas del OpenSSL.

El OpenSSL es una aplicación de fuente abierta del protocolo de Secure Sockets Layer (SSL). Si los Certificados utilizan su propio CA privado, usted debe colocar su certificado raíz CA en una máquina local y utilizar la opción del OpenSSL - *CApath*. Si usted tiene CA intermedio, usted debe colocarlo en el mismo directorio también.

Para obtener la información general sobre el certificado y verificarla, uso:

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

Puede ser que también sea útil convertir los Certificados con el juego de herramientas del OpenSSL:

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

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Conclusión

Porque usted puede instalar un nuevo certificado en el ISE antes de que sea activo, Cisco recomienda que usted instala el nuevo certificado antes de que expire el certificado viejo. Este período de la coincidencia entre la vieja fecha del vencimiento del certificado y la nueva Fecha de inicio del certificado le da la hora de renovar los Certificados y de planear su instalación con poco o nada de tiempo muerto. Una vez que el nuevo certificado ingresa su rango válido de la fecha, habilite el EAP y/o el protocolo HTTP. Recuerde, si usted habilita el HTTPS, hay un reinicio del servicio.