Configuración de renovaciones de certificados en ISE

Contenido

Introducción

En este documento se describen las mejores prácticas y los procedimientos proactivos para renovar certificados en Cisco Identity Services Engine (ISE). También revisa cómo configurar alarmas y notificaciones para advertir a los administradores sobre eventos inminentes como la expiración de certificados.

> **Nota:** Este documento no pretende ser una guía de diagnóstico para certificados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Certificados X509
- Configuración de Cisco ISE con certificados

Componentes Utilizados

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

- Cisco ISE versión 3.0.0.458
- Dispositivo o VMware

Antecedentes

Como administrador de ISE, eventualmente descubrirá que los certificados ISE caducan. Si su servidor ISE tiene un certificado caducado, pueden surgir problemas graves a menos que reemplace el certificado caducado por uno nuevo y válido.

> **Nota:** Si el certificado utilizado para el protocolo de autenticación extensible (EAP) caduca, todas las autenticaciones pueden fallar porque los clientes ya no confían en el certificado de ISE. Si vence el certificado de administración de ISE, el riesgo es aún mayor: un administrador ya no podrá iniciar sesión en ISE y la implementación distribuida puede dejar de funcionar y replicarse.

El administrador de ISE debe instalar un certificado nuevo y válido en ISE antes de que caduque el certificado anterior. Este enfoque proactivo evita o minimiza el tiempo de inactividad y previene el impacto en los usuarios finales. Una vez que comienza el período de tiempo del certificado recién instalado, puede habilitar EAP/Admin o cualquier otro rol en el nuevo certificado.

Puede configurar ISE para que genere alarmas y notifique al administrador que instale nuevos certificados antes de que caduquen los antiguos.

> **Nota:** Este documento utiliza el certificado ISE Admin como certificado autofirmado para demostrar el impacto de la renovación de certificados, pero este enfoque no se recomienda para un sistema de producción. Es mejor utilizar un certificado de CA para los roles EAP y Admin.

Configurar

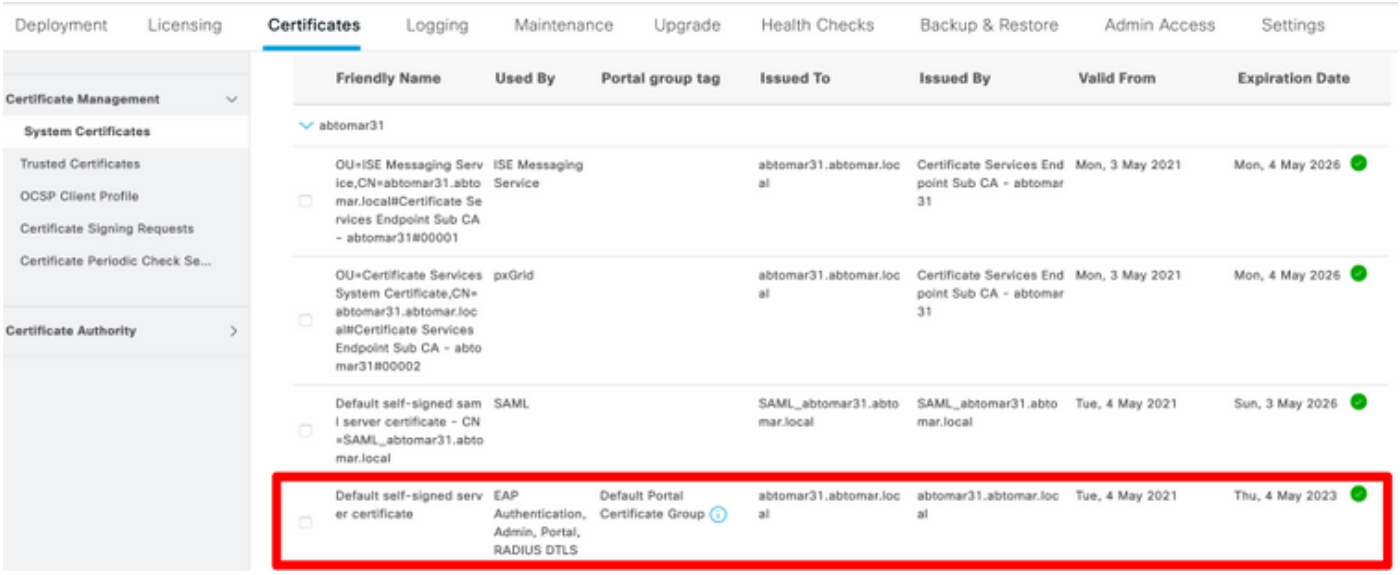
Ver certificados autofirmados de ISE

Cuando se instala ISE, genera un certificado autofirmado. El certificado autofirmado se utiliza para el acceso administrativo y para la comunicación dentro de la implementación distribuida (HTTPS), así como para la autenticación de usuarios (EAP). En un sistema en vivo, utilice un certificado de CA en lugar de un certificado firmado automáticamente.

> **Consejo:** Consulte la sección Administración de certificados en Cisco ISE de la Guía de instalación de hardware de Cisco Identity Services Engine versión 3.0 para obtener más información.

El formato para un certificado de ISE debe ser correo de privacidad mejorada (PEM) o reglas de codificación diferenciadas (DER).

Para ver el certificado autofirmado inicial, vaya a **Administración > Sistema > Certificados > Certificados del sistema** en la GUI de ISE, como se muestra en esta imagen.



Si instala un certificado de servidor en ISE a través de una solicitud de firma de certificado (CSR) y cambia el certificado para el protocolo de administración o EAP, el certificado de servidor autofirmado sigue presente pero está en el estado No en uso.

> **Precaución:** Para los cambios en el protocolo de administración, se requiere reiniciar los servicios de ISE, lo que genera unos minutos de tiempo de inactividad. Los cambios en el EAP no activan el reinicio de los servicios de ISE y no causan tiempo de inactividad.

Determinar cuándo cambiar el certificado

Suponga que el certificado instalado caduca pronto. ¿Es mejor dejar que el certificado caduque antes de renovarlo o cambiarlo antes de que caduque? Debe cambiar el certificado antes de la expiración para tener tiempo de planificar el intercambio de certificados y gestionar el tiempo de inactividad causado por el intercambio.

¿Cuándo debe cambiar el certificado? Obtenga un nuevo certificado con una fecha de inicio previa a la fecha de vencimiento del certificado anterior. El período de tiempo entre esas dos fechas es la ventana de cambio.

> **Precaución:** Si habilita Admin, se reinicia el servicio en el servidor ISE y experimenta algunos minutos de tiempo de inactividad.

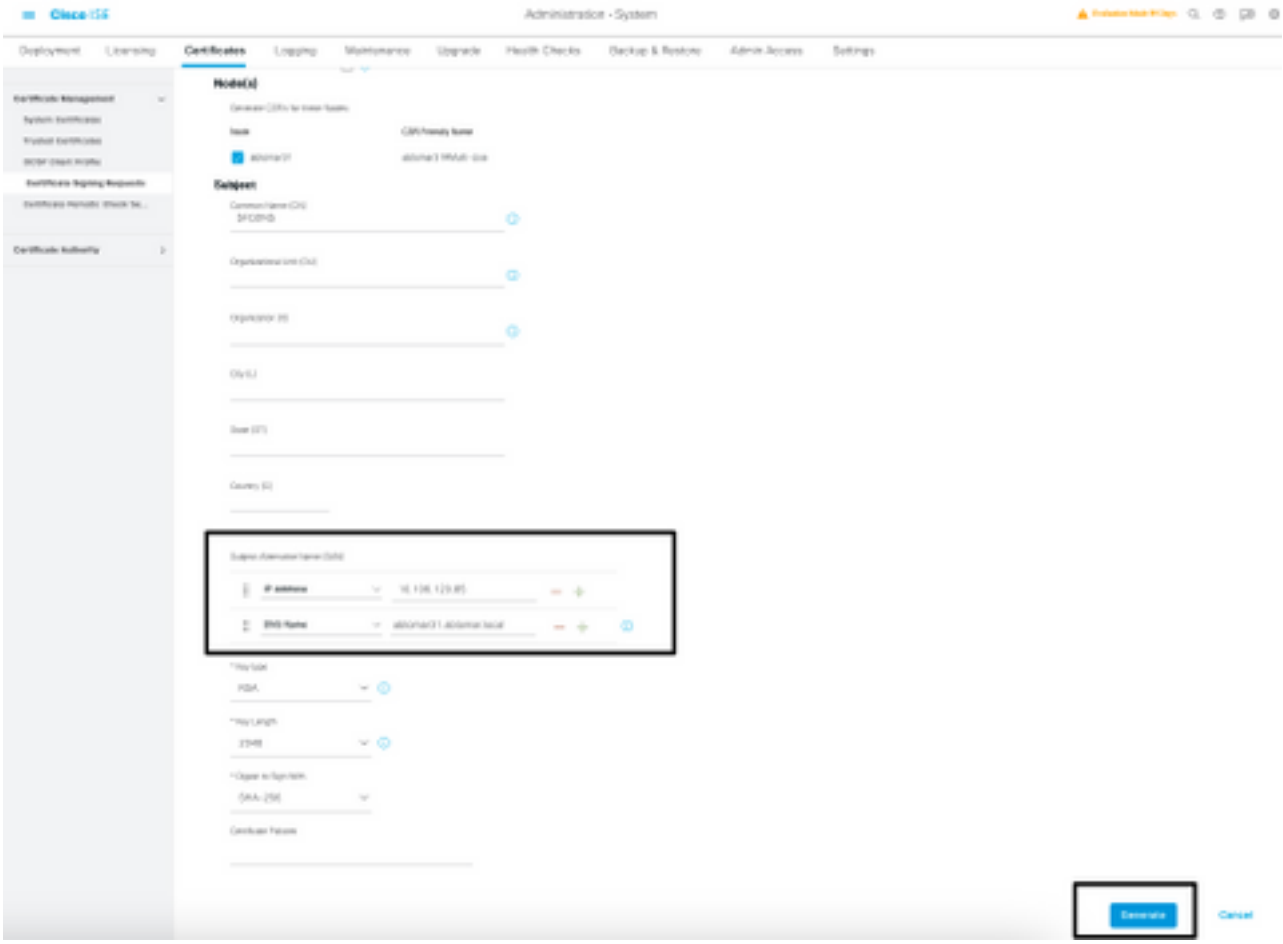
Esta imagen muestra la información de un certificado que caduca pronto:

Generar solicitud de firma de certificado

Este procedimiento describe cómo renovar el certificado a través de una CSR:

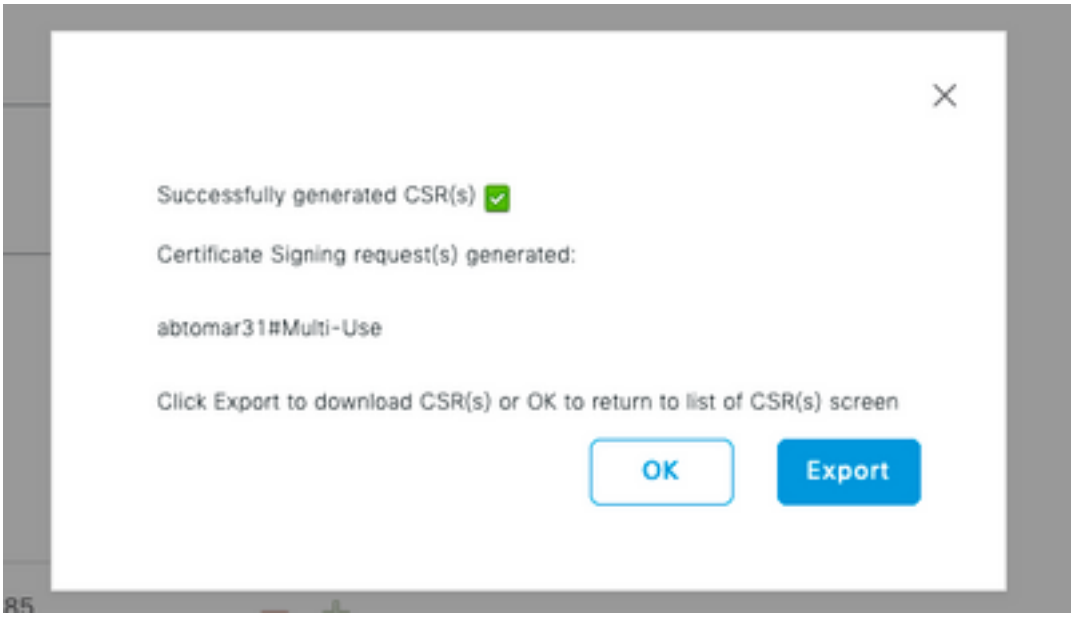
1. En la consola de ISE, vaya a **Administración > Sistema > Certificados > Solicitudes de firma de certificados** y haga clic en **Generar solicitud de firma de certificado:**

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

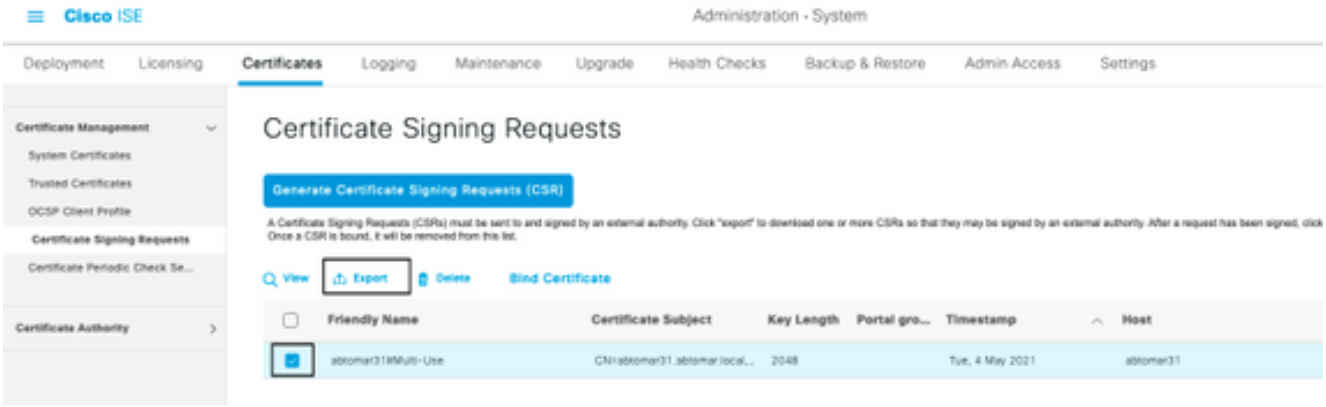


3. Una de las líneas de campo de texto de **Nombre alternativo de sujeto (SAN)** debe repetir el FQDN de ISE. Puede agregar un segundo campo SAN si desea utilizar nombres alternativos o un certificado comodín.

4. Haga clic en **Generar**; una ventana emergente indica si los campos de CSR se completaron correctamente o no.



5. Para exportar la CSR, haga clic en **Solicitudes de firma de certificado** en el panel izquierdo, seleccione su CSR y haga clic en **Exportar**:

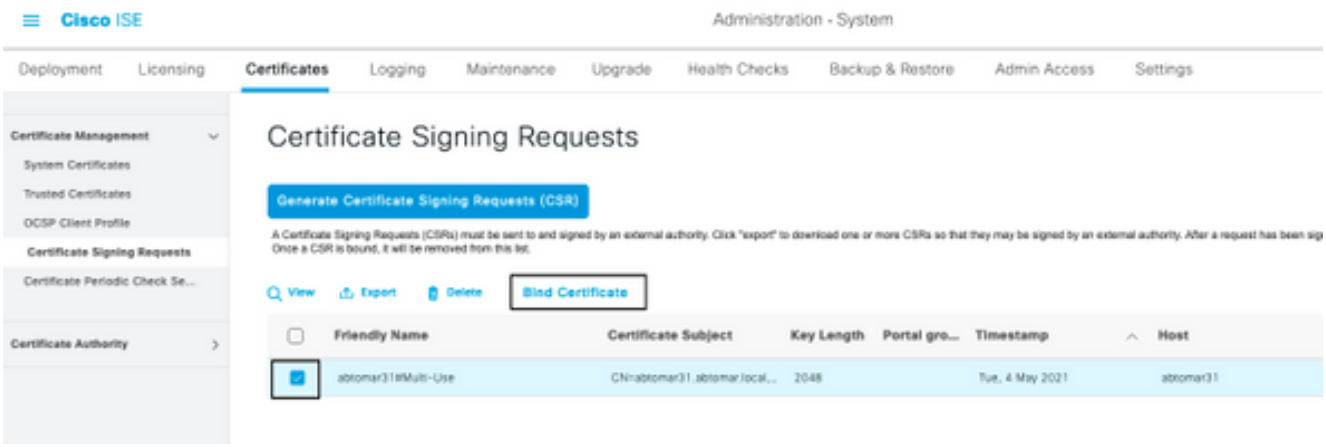


6. El CSR se almacena en el equipo. Envíela a su CA para su firma.

Instalar certificado

Una vez que reciba el certificado final de su CA, debe agregar el certificado a ISE:

1. En la consola de ISE, navegue a **Administración > Sistema > Certificados > Solicitudes de firma de certificado**, marque la casilla de verificación en CRS y haga clic en **Vincular certificado**:

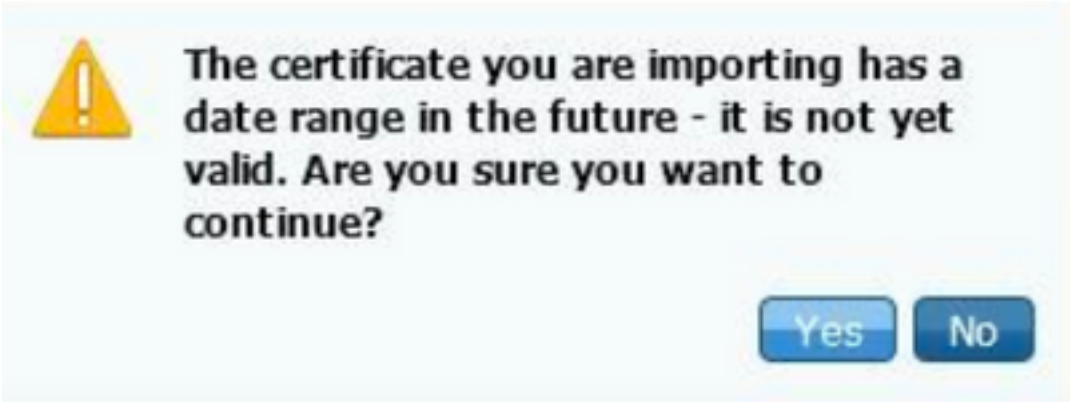


2. Ingrese una descripción simple y clara del certificado en el campo de texto **Nombre descriptivo** y presione Enviar.

Nota: No habilite el protocolo de administración o EAP en este momento.

3. En Certificado del sistema tiene un nuevo certificado que no está en uso, como se muestra aquí:

4. Debido a que el nuevo certificado se instala antes de que caduque el anterior, verá un error que informa un intervalo de fechas en el futuro:



5. Haga clic en **Sí** para continuar. El certificado ahora está instalado, pero no en uso, como se resalta en verde.

Nota: Si utiliza certificados autofirmados en una implementación distribuida, el certificado autofirmado principal debe instalarse en el almacén de certificados de confianza del servidor ISE secundario. Del mismo modo, el certificado autofirmado secundario debe instalarse en el almacén de certificados de confianza del servidor ISE principal. Esto permite que los servidores ISE se autentiquen mutuamente. Sin esto, el despliegue puede romperse. Si renueva certificados de una CA de terceros, verifique si la cadena de certificados raíz ha cambiado y actualice el almacén de certificados de confianza en ISE según corresponda. En

ambos casos, asegúrese de que los nodos ISE, los sistemas de control de terminales y los solicitantes puedan validar la cadena de certificados raíz.

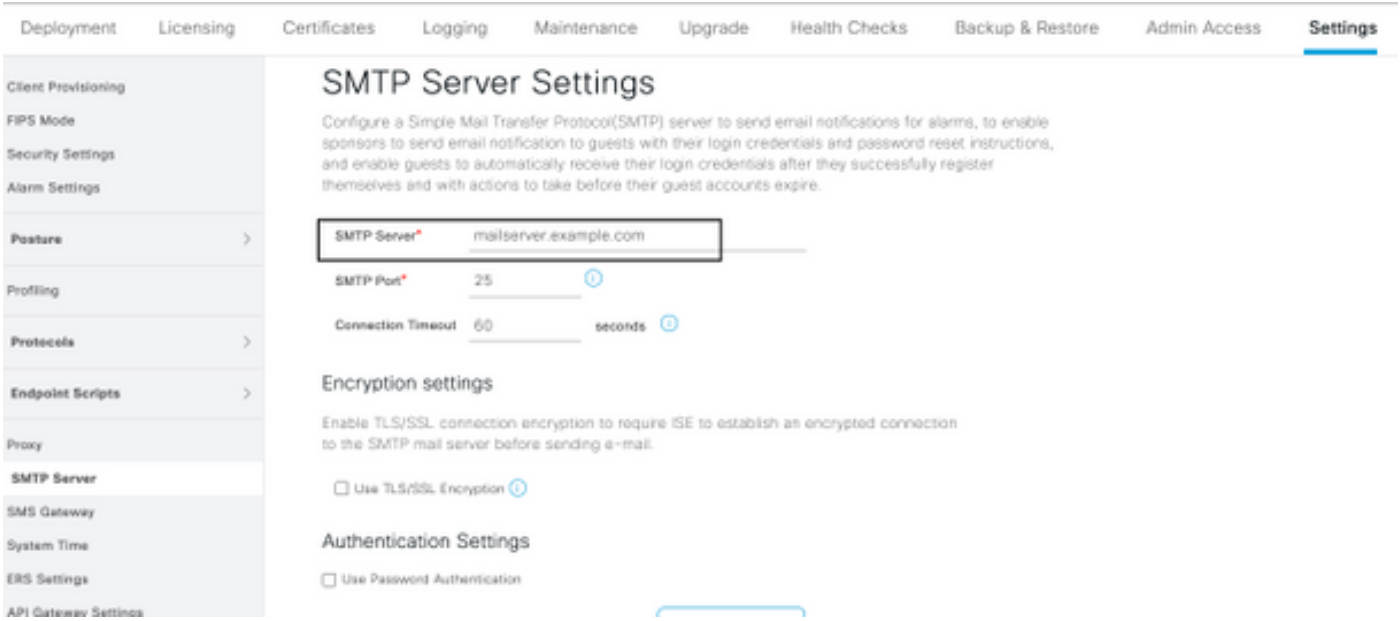
Configurar sistema de alertas

Cisco ISE le notifica cuando la fecha de vencimiento de un certificado local está dentro de los 90 días. Dicha notificación anticipada lo ayuda a evitar certificados vencidos, planificar el cambio de certificado y evitar o minimizar el tiempo de inactividad.

La notificación aparece de varias maneras:

- Los iconos de estado de vencimiento de color aparecen en la página Certificados locales.
- Los mensajes de vencimiento aparecen en el informe de diagnóstico del sistema Cisco ISE.
- Las alarmas de vencimiento se generan a los 90 y 60 días y, luego, diariamente en los últimos 30 días antes del vencimiento.

Configure ISE para la notificación por correo electrónico de las alarmas de vencimiento. En la consola de ISE, navegue hasta **Administración > Sistema > Configuración > Servidor SMTP**, identifique el servidor de protocolo simple de transferencia de correo (SMTP) y defina las otras configuraciones del servidor para que se envíen notificaciones por correo electrónico para las alarmas.



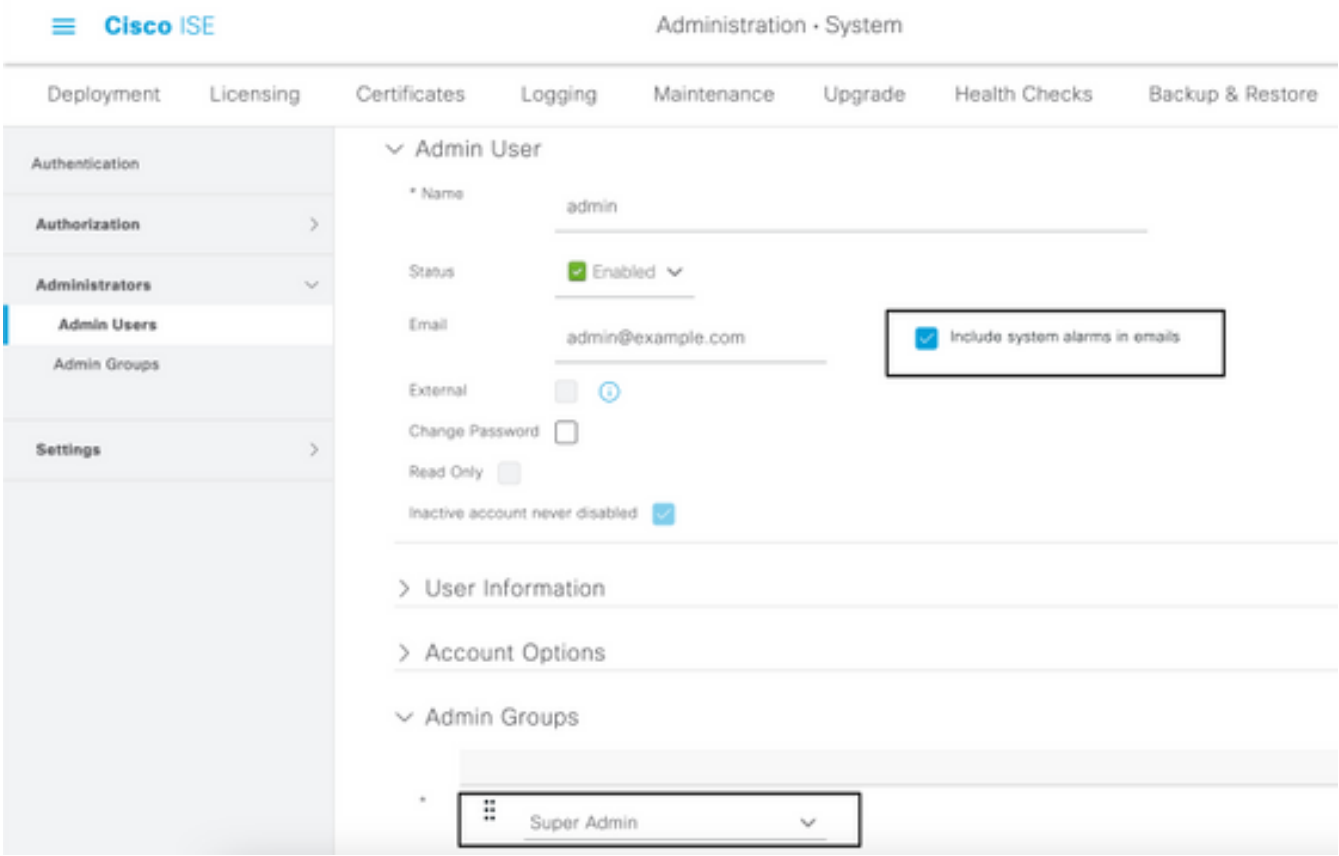
Existen dos maneras de configurar las notificaciones:

- Utilice el acceso de administrador para notificar a los administradores:

  Vaya a **Administración > Sistema >** Acceso de administrador **>** Administradores **>** Usuarios administradores.

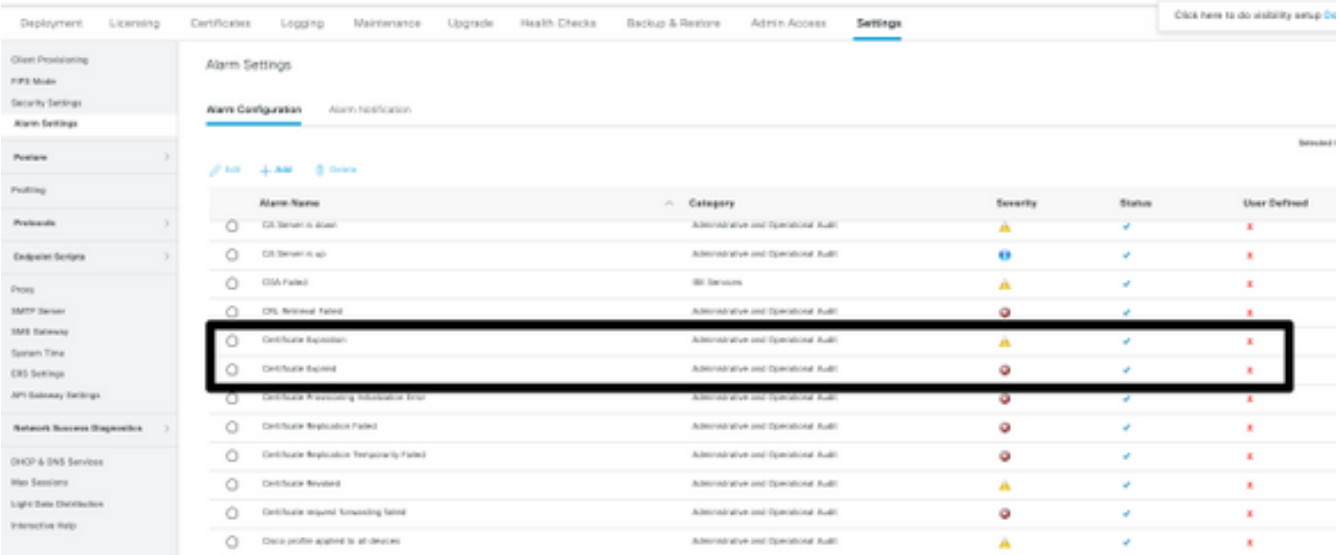
  Marque la casilla de verificación **Incluir alarmas del sistema en correos electrónicos** para los

usuarios administradores que necesiten recibir notificaciones de alarmas. La dirección de correo electrónico del remitente de las notificaciones de alarma está codificada como *ise@hostname*.



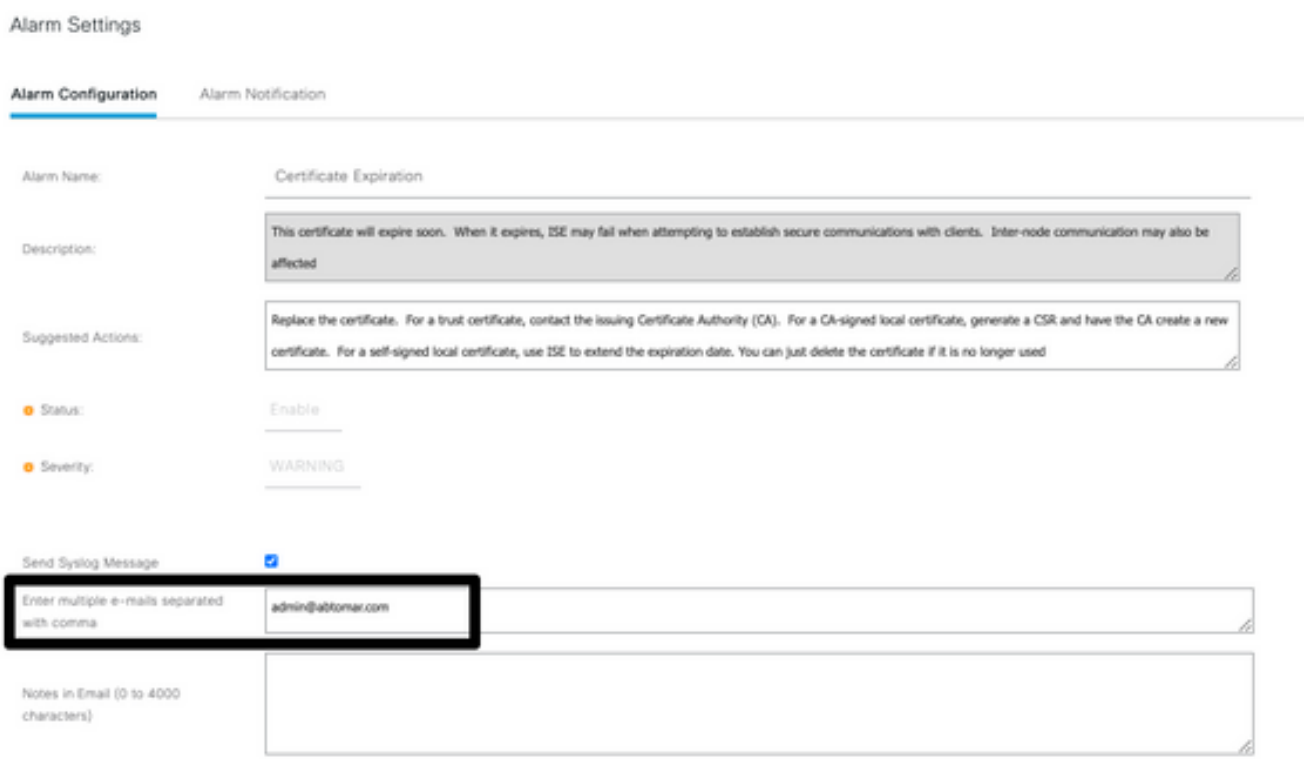
- Configure los parámetros de la alarma de ISE para notificar a los usuarios:

  Navegue hasta **Administración > Sistema > Configuración > Ajuste de alarma > Configuración de alarma**, como se muestra en esta imagen.



Nota: Deshabilite el estado de una categoría si desea evitar las alarmas de esa categoría.Seleccione Certificado de vencimiento y, a continuación, haga clic en **Notificación de alarma**, introduzca las direcciones de correo electrónico de los usuarios que se notificarán

y guarde el cambio de configuración. Los cambios pueden tardar hasta 15 minutos en activarse.

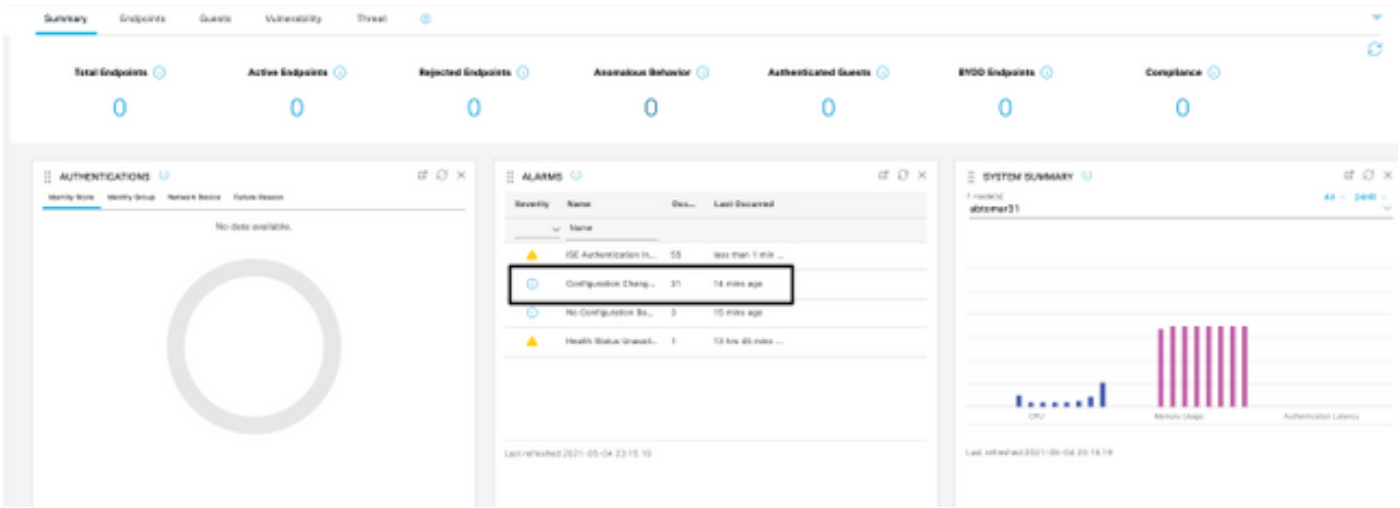


Verificación

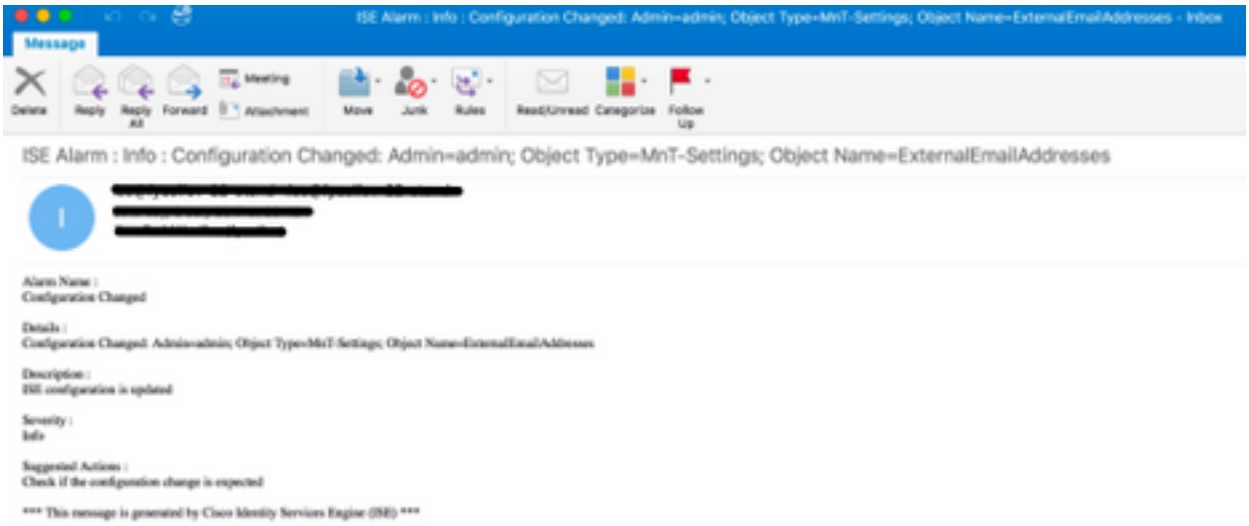
Utilize esta sección para confirmar que su configuración funcione correctamente.

Verificar el sistema de alertas

Verifique que el sistema de alertas funcione correctamente. En este ejemplo, un cambio de configuración genera una alerta con un nivel de gravedad de información. (Una alarma de información es la gravedad más baja, mientras que los vencimientos de certificados generan un nivel de gravedad de advertencia más alto).



Este es un ejemplo de la alarma de correo electrónico que envía ISE:

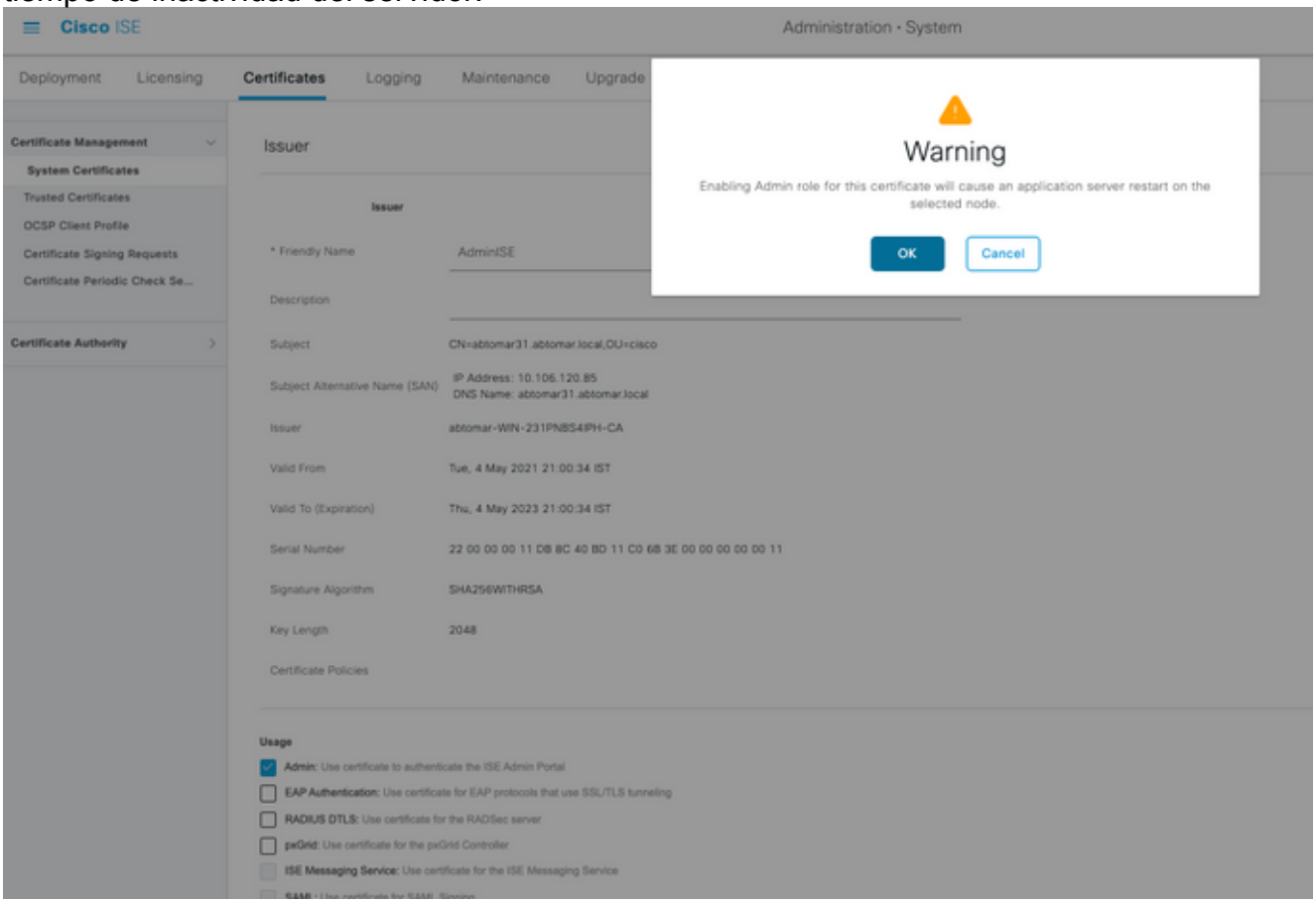


Verificar el cambio de certificado

Este procedimiento describe cómo verificar que el certificado está instalado correctamente y cómo cambiar los roles de EAP y/o Admin:

1. En la consola de ISE, navegue hasta **Administración > Certificados > Certificados del sistema** y seleccione el nuevo certificado para ver los detalles.

   Precaución: Si habilita el uso del administrador, se reinicia el servicio ISE, lo que provoca tiempo de inactividad del servidor.



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

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

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

4. Para un escenario de implementación distribuida, navegue hasta **Administration > System > Deployment.** Compruebe que el nodo tiene un icono verde. Coloque el cursor sobre el icono para comprobar que la leyenda muestra "Conectado".

5. Verifique que la autenticación del usuario final se realice correctamente. Para ello, vaya **a Operaciones > RADIUS > Livelogs.** Puede encontrar un intento de autenticación específico y comprobar que dichos intentos se autenticaron correctamente.

Verifica el certificado

Si desea verificar el certificado externamente, puede utilizar las herramientas integradas de Microsoft Windows o el kit de herramientas de OpenSSL.

OpenSSL es una implementación de código abierto del protocolo de capa de sockets seguros (SSL). Si los certificados utilizan su propia CA privada, debe colocar su certificado de CA raíz en una máquina local y utilizar la opción *-CApath* de OpenSSL. Si tiene una CA intermedia, también debe colocarla en el mismo directorio.

Para obtener información general sobre el certificado y verificarlo, utilice:

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

También puede ser útil convertir los certificados con OpenSSL toolkit:

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

Troubleshoot

Actualmente no hay información de diagnóstico específica disponible para esta configuración.

Conclusión

Como puede instalar un nuevo certificado en ISE antes de que esté activo, Cisco recomienda que instale el nuevo certificado antes de que caduque el antiguo. Este período de superposición entre la fecha de vencimiento del certificado anterior y la fecha de inicio del nuevo certificado le da tiempo para renovar los certificados y planificar su instalación con poco o ningún tiempo de inactividad. Una vez que el nuevo certificado ingrese a su rango de fechas válido, habilite el EAP o el administrador. Recuerde que si habilita el uso del administrador, se reinicia el servicio.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).