Configuración de la autenticación basada en certificado o Smartcard para la administración de ISE

Contenido

Introducción

Este documento describe cómo configurar la autenticación basada en certificados de cliente para el acceso de administración de Identity Services Engine (ISE). En este ejemplo, el administrador de ISE se autentica con el certificado de usuario para obtener acceso de administrador a la GUI de gestión de Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Configuración de ISE para la autenticación de contraseñas y certificados.
- Microsoft Active Directory (AD)

Componentes Utilizados

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

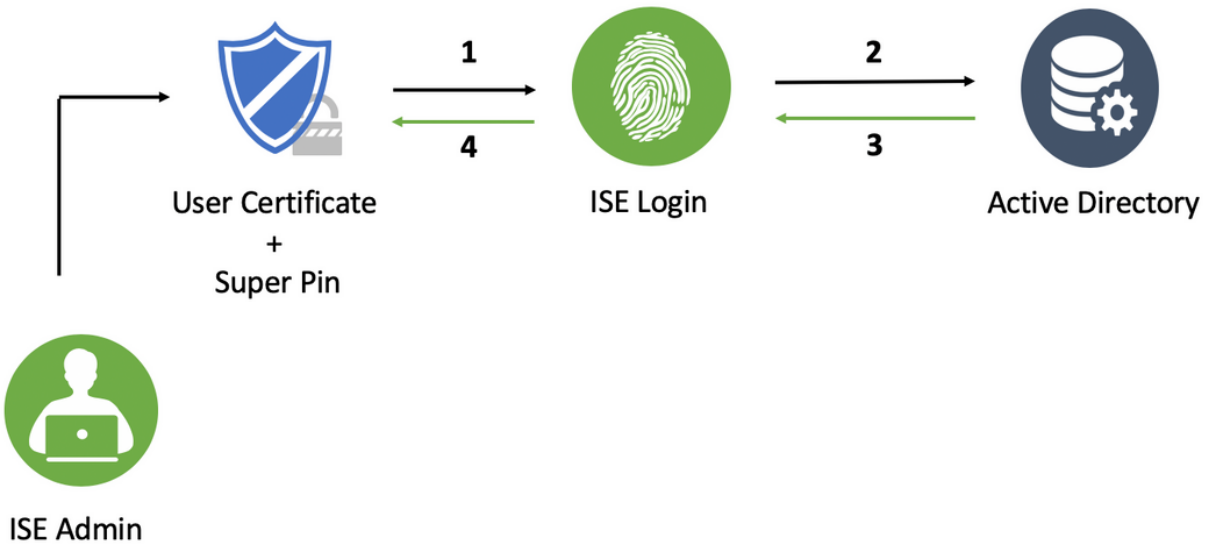
- Cisco Identity Services Engine (ISE) versión 2.6
- Windows Active Directory (AD) Server 2008 Versión 2
- Certificado

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si la red está activa, asegúrese de comprender el impacto potencial de cualquier configuración.

Configurar

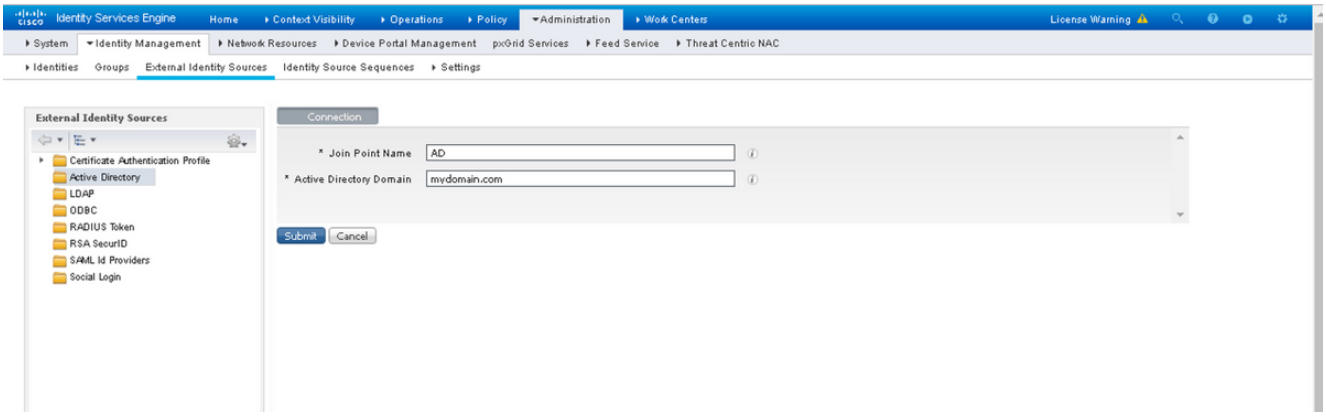
Utilice esta sección para configurar el certificado de cliente o la tarjeta inteligente como identidad externa para el acceso administrativo a la GUI de administración de Cisco ISE.

Diagrama de la red

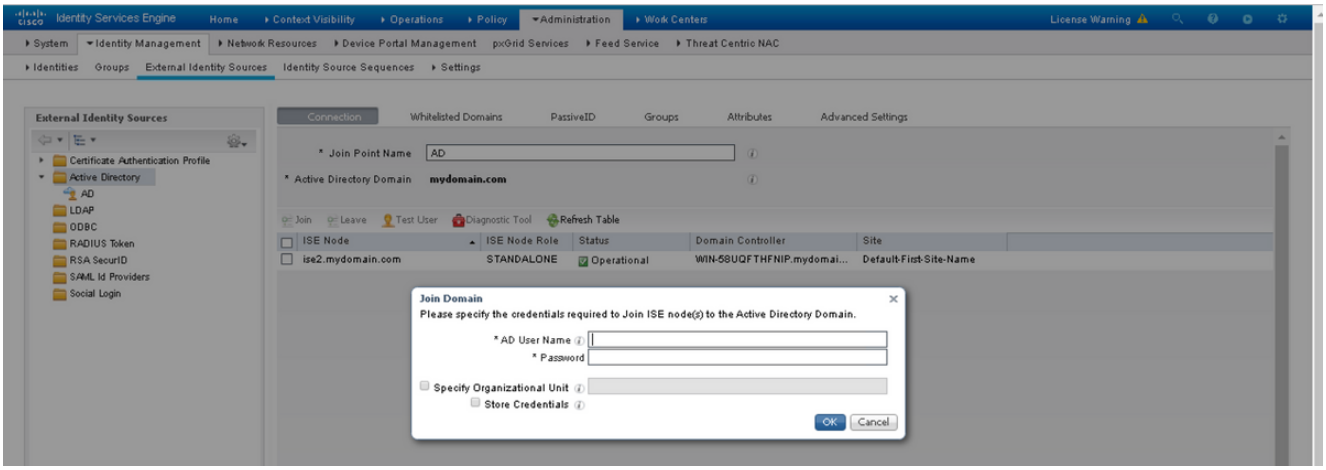


Unirse a ISE en Active Directory

1. Elija **Administration > Identity Management > External Identity Sources > Active Directory.**
2. Cree una instancia de Active Directory con el **nombre del punto de unión** y el **dominio AD** en Cisco ISE.
3. Haga clic en Submit (Enviar).



4. Únase a todos los nodos con el **nombre de usuario** y la **contraseña** adecuados en el mensaje.



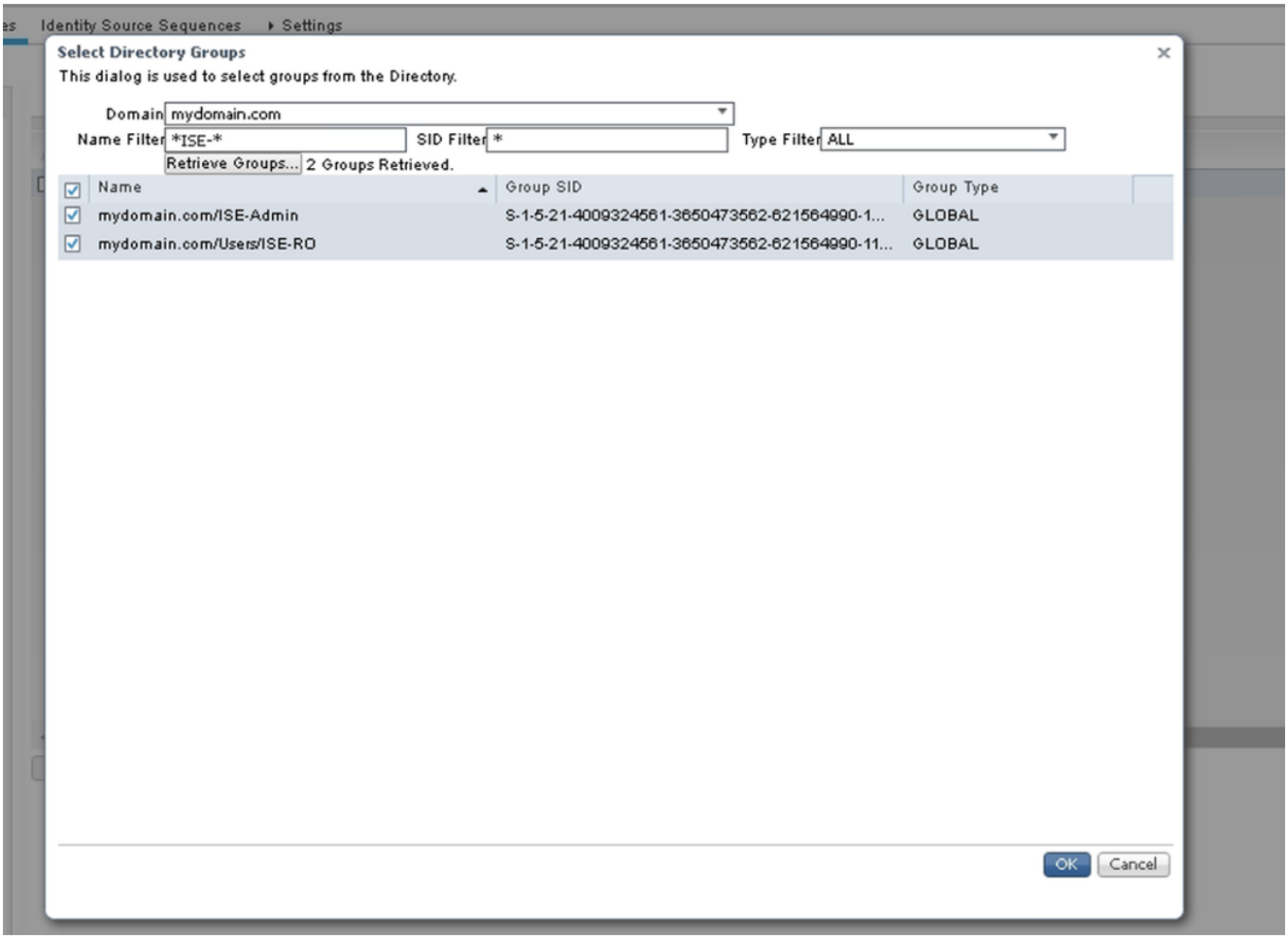
5. Click **Save**.

Seleccionar grupos de directorios

1. Cree un grupo de administradores externo y asígnelo al grupo de directorios activos.

2. Elija **Administration >Identity Management > External Identity Sources > Active Directory > Groups > Select Groups from Directory.**

3. Recupere al menos un grupo AD al que pertenece el administrador.

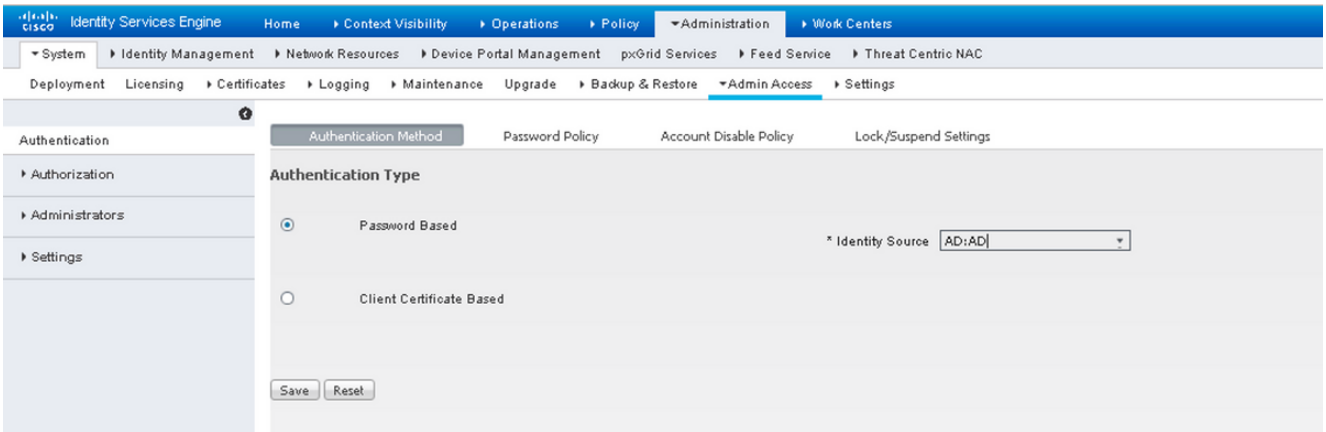


4. Click **Save**.

Habilitar autenticación basada en contraseña de Active Directory para acceso administrativo

1. Habilite la instancia del directorio activo como método de autenticación basado en contraseña que se ha unido a ISE anteriormente.

2. Elija **Administration > System > Admin access > Authentication**, como se muestra en la imagen.



3. Click **Save**.

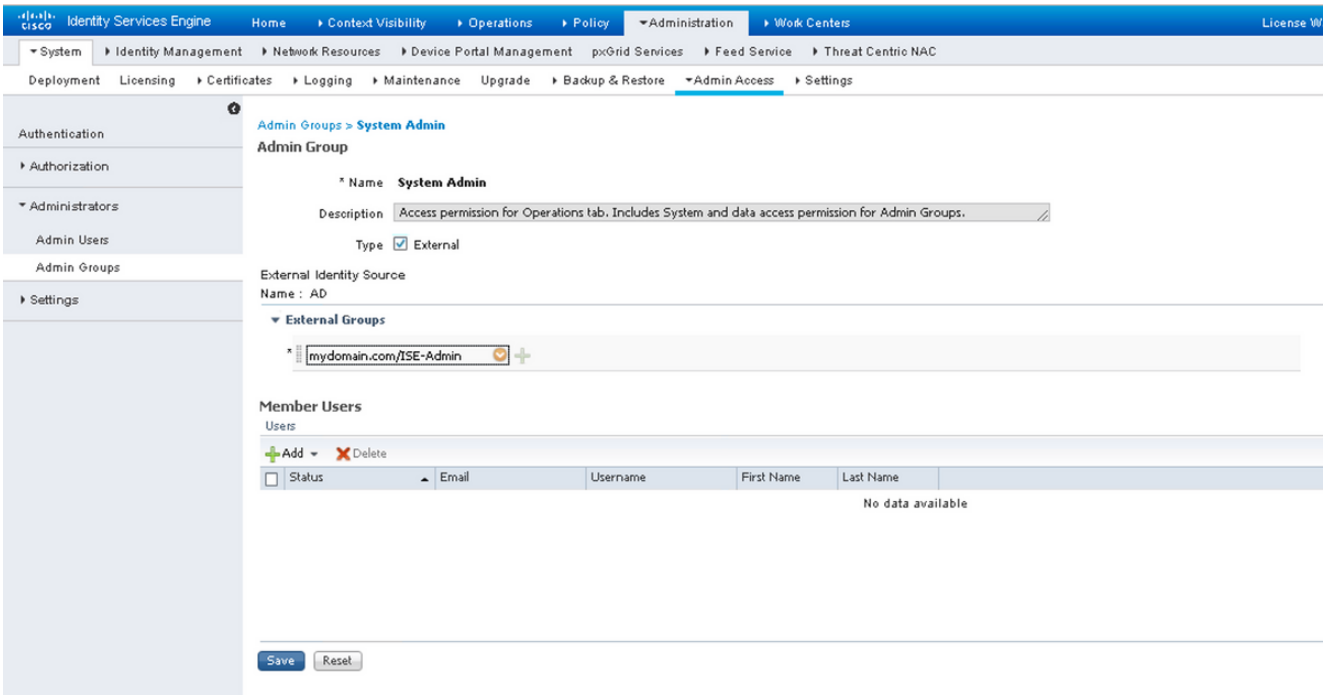
Nota: La configuración de autenticación basada en contraseña es necesaria para habilitar la autenticación basada en certificados. Esta configuración debe revertirse después de una configuración exitosa de la autenticación basada en certificados.

Asignar grupos de identidad externos a grupos de administradores

En este ejemplo, el grupo de AD externo se mapea al grupo Admin predeterminado.

1. Elija **Administration > System > Admin Access > Administradores >Admin Groups > Super admin.**

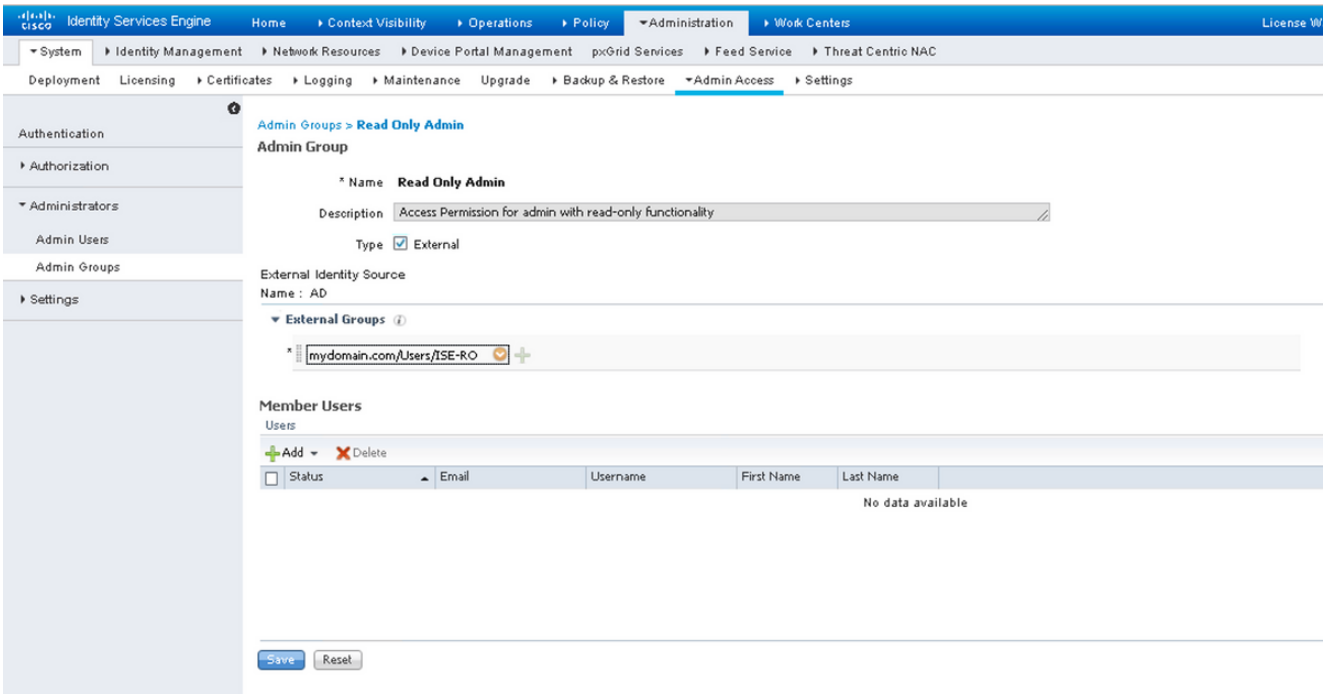
2. Verifique el Tipo como **Externo** y seleccione el grupo AD en **Grupos Externos**.



3. Click **Save**.

4. Elija **Administration > System > Admin Access > Administradores > Admin Groups > Read Only Admin**.

5. Verifique el Tipo como **Externo** y seleccione el grupo AD en **Grupos Externos**, como se muestra en la imagen.



6. Click **Save**.

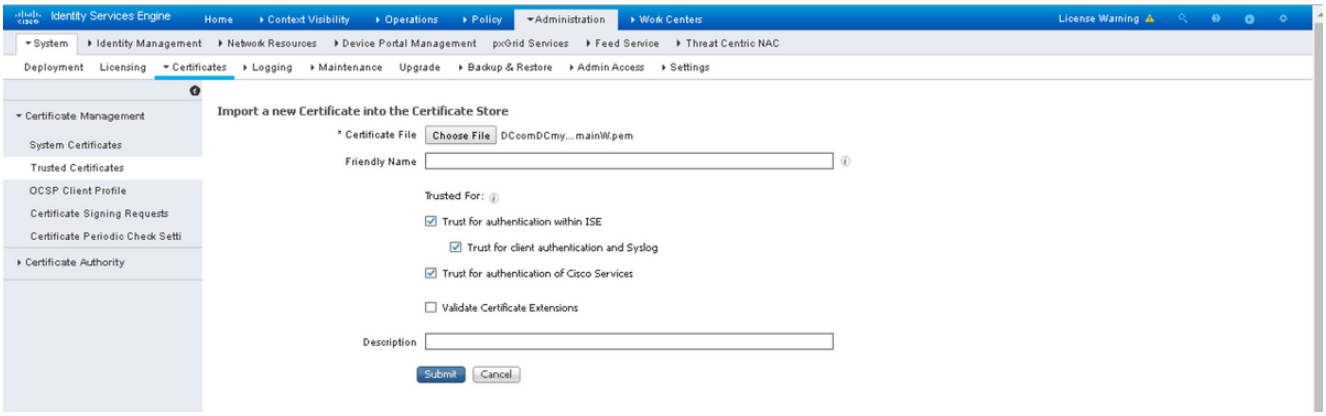
Importar certificado de confianza

1. Importe el certificado de la autoridad certificadora (CA) que firma el certificado de cliente.

2. Elegir **Administrator > System > Certificates > Trusted Certificate > Import .**

3. Haga clic en Examinar y elija el certificado de CA.

4. Marque la **casilla de verificación Confiar en la autenticación del cliente y Syslog**, como se muestra en la imagen.



5. Haga clic en Submit (Enviar).

Configurar perfil de autenticación de certificado

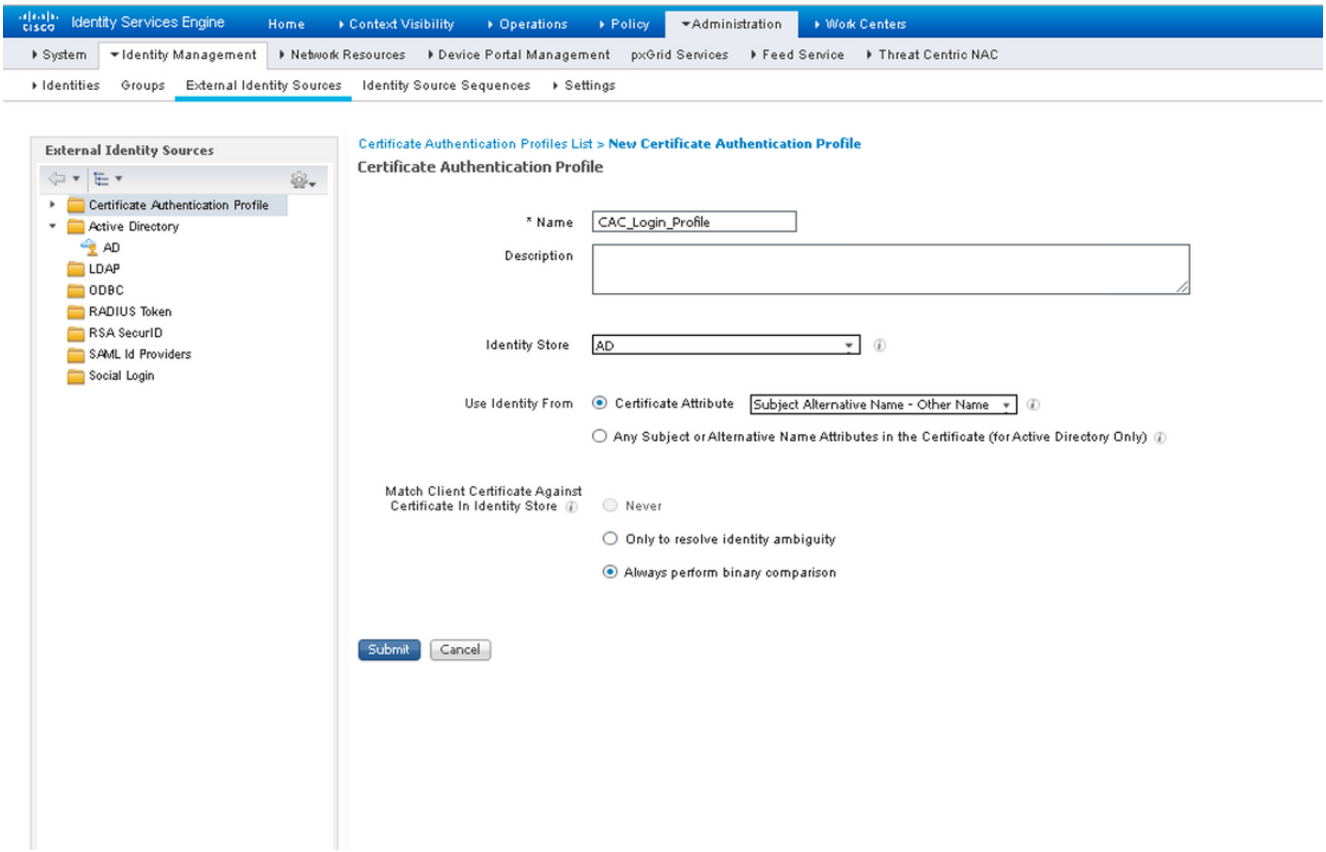
1. Para crear el perfil de autenticación de certificados para la autenticación basada en certificados de cliente, elija **Administration >Identity Management > External Identity Sources**

> Certificate Authentication Profile > Add.

2. Agregar nombre de perfil.

3. Seleccione el atributo adecuado que contiene el nombre de usuario del administrador en el atributo certificate.

4. Si el registro AD para el usuario contiene el certificado del usuario y desea comparar el certificado que se recibe del explorador con el certificado en AD, marque la casilla de verificación **Realizar siempre la comparación binaria** y seleccione el nombre de instancia de Active Directory especificado anteriormente.

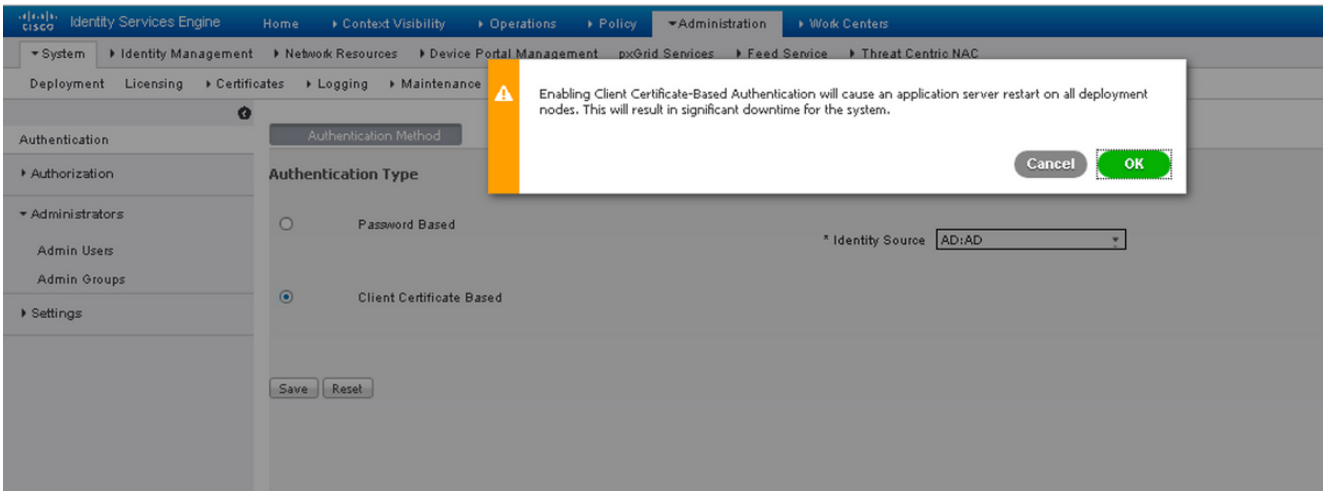


5. Haga clic en Submit (Enviar).

Nota: También se puede consumir el mismo perfil de autenticación de certificado para la autenticación basada en identidad del terminal.

Habilitar autenticación basada en certificado de cliente

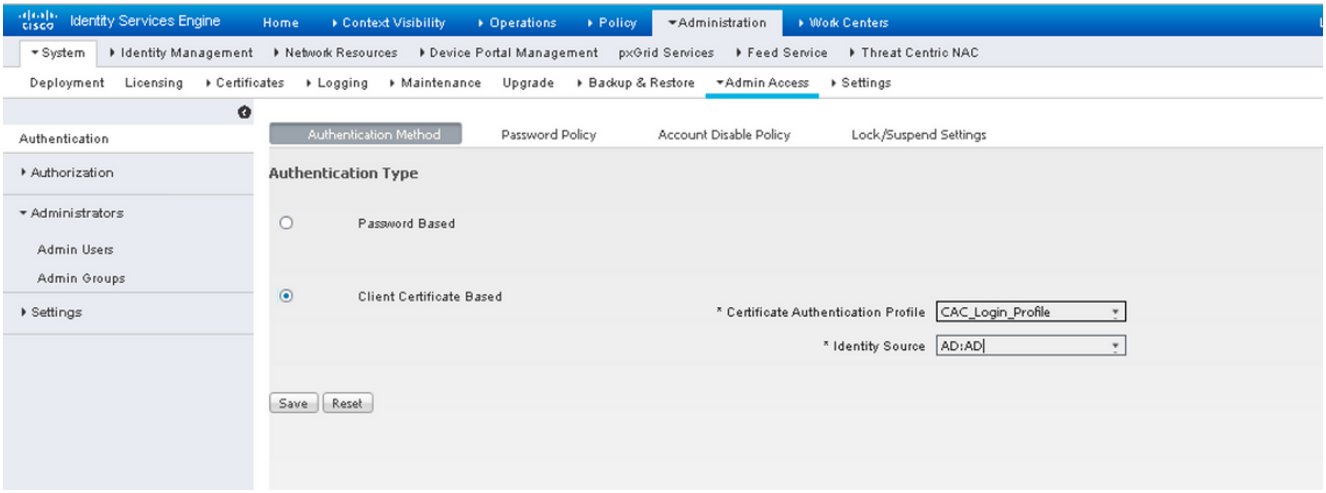
1. Elegir **Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based.**



2. Click OK.

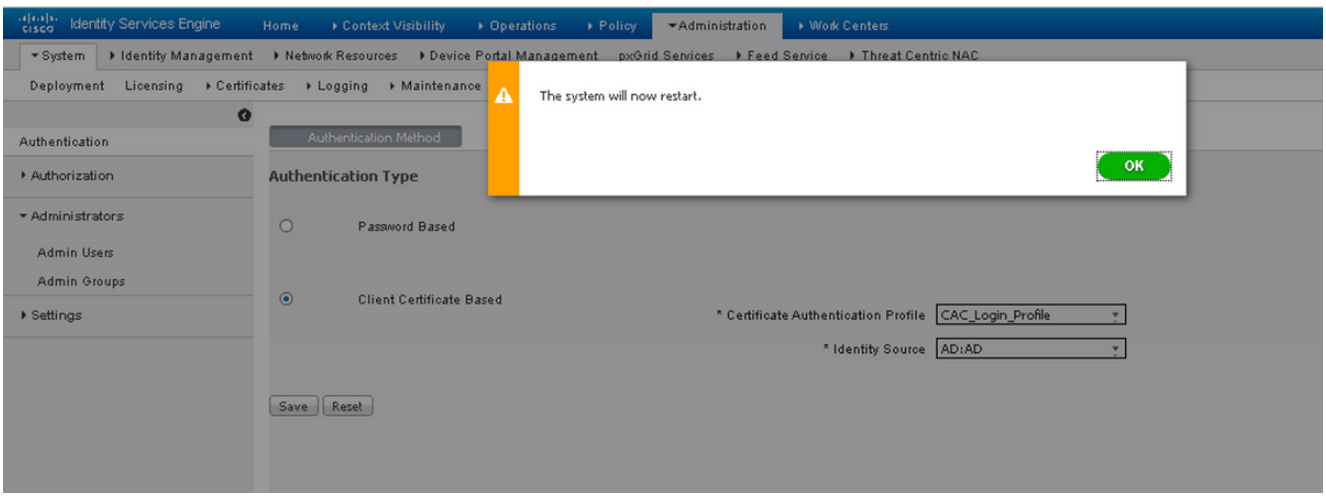
3. Elija el **perfil de autenticación de certificados** que se configuró anteriormente.

4. Seleccione el nombre de la instancia de Active Directory.



5. Click **Save**.

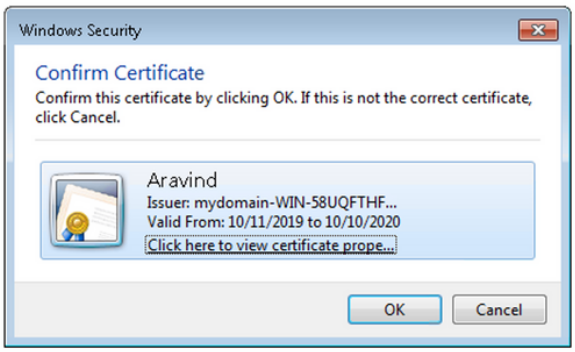
6. Se reinician los servicios de ISE en todos los nodos de la implementación.

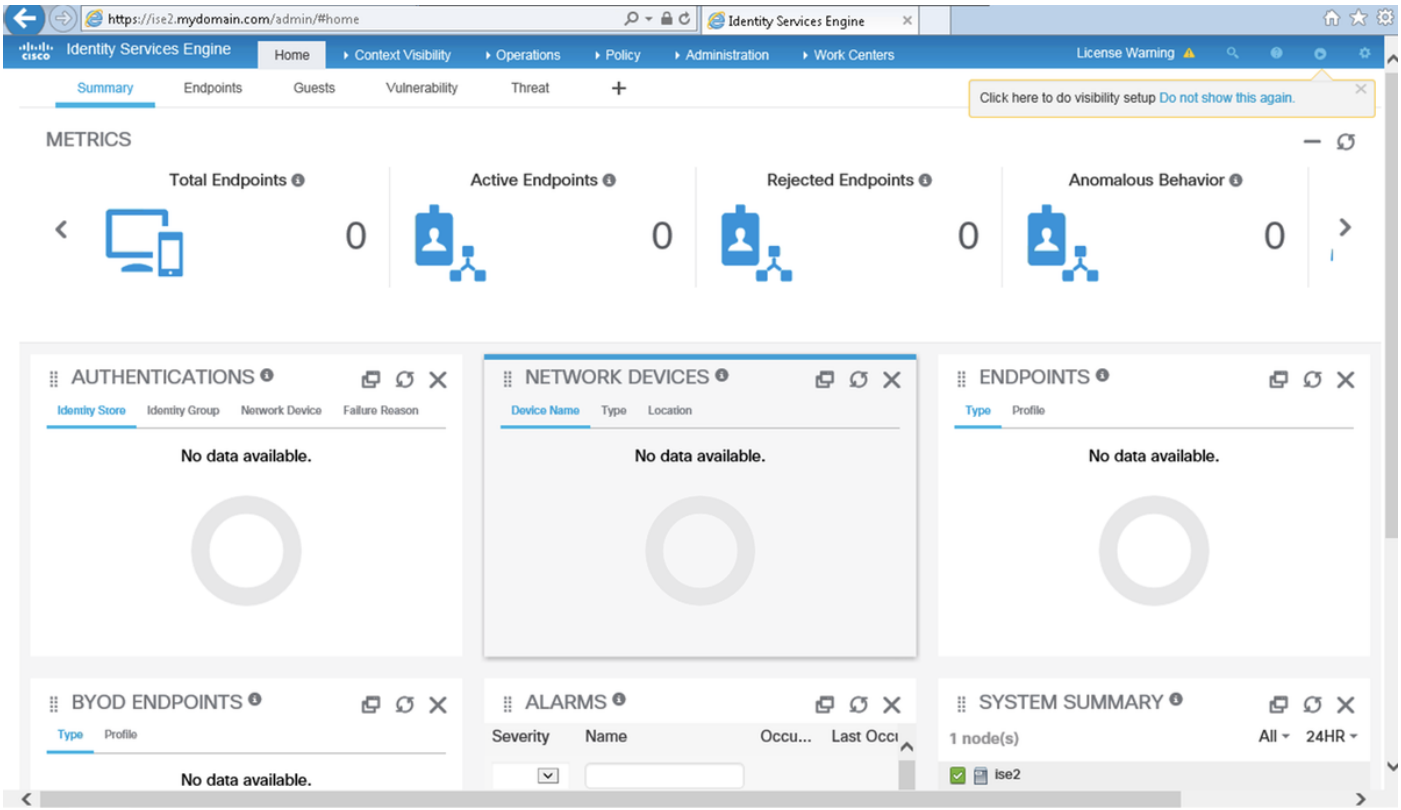


Verificación

Verifique el acceso a la GUI de ISE después de que el estado del servicio **del servidor de aplicaciones** cambie a **ejecución.**

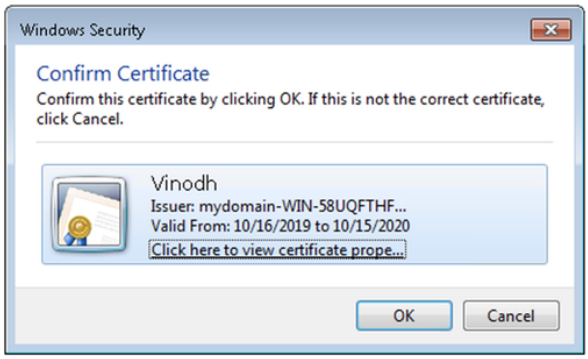
Usuario superadministrador: Verifique que se le pida al usuario que elija un certificado para iniciar sesión en la GUI de ISE y se le otorguen privilegios de superadministrador si el certificado es de una parte del usuario del grupo de Identidad externa de Super Admin.

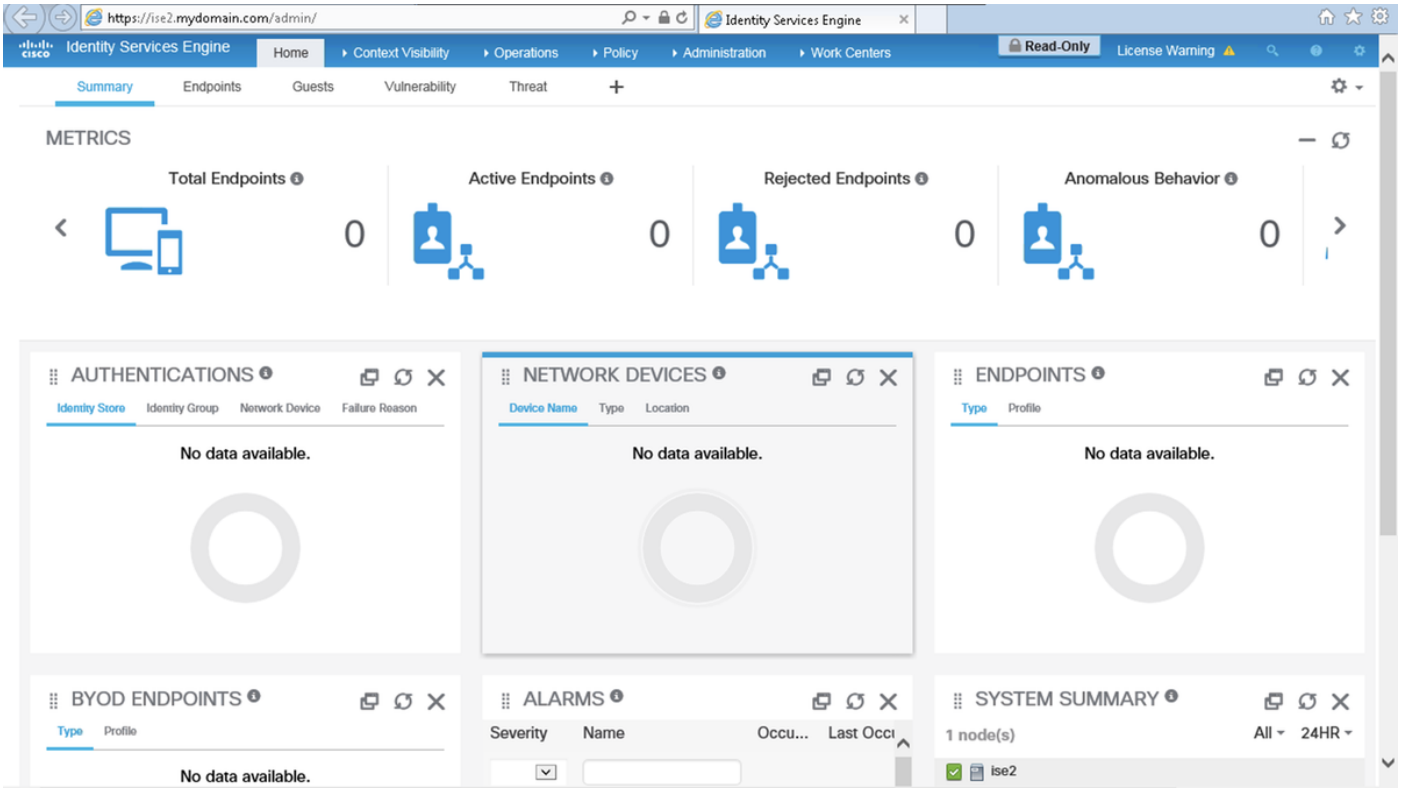




Usuario administrador de sólo lectura: Verifique que se le pida al usuario que elija un certificado

para iniciar sesión en la GUI de ISE y se le otorguen privilegios de administrador de sólo lectura si el certificado es de una parte del usuario del grupo de identidad externa de administrador de sólo lectura.





Nota: Si la tarjeta de acceso común (CAC) está en uso, Smartcard presenta el certificado de usuario a ISE después de que el usuario introduzca su superpin válido.

Troubleshoot

1. Utilice el comando **application start ise safe** para iniciar Cisco ISE en un modo seguro que permita inhabilitar temporalmente el control de acceso al portal de administración y Corrija la configuración y reinicie los servicios de ISE con el comando **application stop ise** seguido de **application start ise.**
2. La opción safe proporciona un medio de recuperación si un administrador bloquea de forma inadvertida el acceso al portal de administración de Cisco ISE para todos los usuarios. Este evento puede ocurrir si el administrador configuró una lista de **acceso IP** incorrecta en la **página Administration > Admin Access > Settings > Access**. La opción **safe** también **omite la autenticación basada en certificados** y vuelve a la autenticación predeterminada de nombre de usuario y contraseña para iniciar sesión en el portal de administración de Cisco ISE.