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

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Unirse a ISE en Active Directory Seleccionar grupos de directorios Habilitar autenticación basada en contraseña de Active Directory para acceso administrativo Asignar grupos de identidad externos a grupos de administradores Importar certificado de confianza Configurar perfil de autenticación de certificado Habilitar autenticación basada en certificado de cliente Verificación Troubleshoot

## 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.

cisco Identity Services Engine Home (	→ Context Visibility → Ope	rations + Policy - Admin	nistration 🔹 Work	Centers		License Warning 🔺	Q,	0 C	ø	
System      Identity Management      Network	Resources Device Portal	Management pxGrid Services	Feed Service	Threat Centric NAC						1
+ Identities Groups External Identity Sources	Identity Source Sequence	; ▶ Settings								1
										l
External Identity Sources	Connection	Whitelisted Domains Pas	siveID Group	s Attributes Advanc	ced Settings					l
↓ E •	* Join Point Name	AD		æ					-	l
AD     Athentication Profile	* Active Directory Domain	mydomain.com		Ŧ						
LDAP	👷 Join 👷 Leave 🧕 Tes	t User  💼 Diagnostic Tool 🔗 R	efresh Table							l
Contraction Contraction Contraction	ISE Node	▲ ISE Node Role	Status	Domain Controller	Site					1
RSA SecuriD	ise2.mydomain.com	STANDALONE	🛛 Operational	WIN-58UQFTHFNIP.mydomai	Default-First-Site-Name					l
SAML Id Providers										1
🥁 Social Lagin		Join Domain Please specify the credentials * AD User Name * Passe Specify Organizational Unit Store Credentials	required to Join ISE n	ode(d) to the Active Directory Domain	Cancel					
					_					

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.

es	dentity Source Sequences + Settings			
	Select Directory Groups		×	
	This dialog is used to select groups from the Di	rectory.		
	Domain mydomain.com	*		
112	Name Filter *ISE-*	SID Filter * Type Filter ALL	*	
	Retrieve Groups 2 Groups Ret	rieved.		
	✓ Name	<ul> <li>Group SID</li> </ul>	Group Type	
	mydomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1	GLOBAL	
	mydomain.com/Users/ISE-RO	S-1-5-21-4009324561-3650473562-621564990-11	GLOBAL	
ſ				
			OK Cancel	

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.

dials. Identity Services Engine	Home  Context Visibility  Operations  Policy  Administration  Work Centers
▼ System → Identity Management	Network Resources     Povice Portal Management     pxGrid Services     Peed Service     Threat Centric NAC
Deployment Licensing + Certific	cates → Logging → Maintenance Upgrade → Backup & Restore ▼Admin Access → Settings
() Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
+ Administrators	Password Based
Settings	* Identity Source AD:AD  *
	O Client Certificate Based
	Save Reset

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.

dentity Services Engine	Home + Context Vi	sibility + Operations	→ Policy ▼Adminis	tration 🔷 Work Ce	nters		License W
▼ System → Identity Management	Network Resources	Device Portal Managem	ent p×Grid Services	▶ Feed Service →	Threat Centric NAC		
Deployment Licensing + Certifi	cates + Logging + M	faintenance Upgrade	▶ Backup & Restore 🔹	Admin Access + Set	ttings		
Authentication  + Authorization	Admin Groups > Syste Admin Group * Name	m Admin System Admin					
▼ Administrators	Description	Access permission for Oper	ations tab. Includes System	n and data access pern	hission for Admin Gr	oups.	
Admin Users	Туре	🗹 External					
Admin Groups	External Identity Sour	ce					
<ul> <li>Settings</li> </ul>	Name: AD						
	* mydomain.com Member Users Users	n/ISE-Admin 💟 🕂					
	🕂 Add 👻 🗶 Delete						
	Status	🔺 Email	Username	First Name	Last Name		
	Save Reset				No data ava	ilable	

- 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.

dentity Services Engine	Home → Context Visibility → Operatio	ns ▶ Policy ▼Administration	▶ Work Centers		License W
▼System → Identity Managemen	Network Resources     Device Portal Man	agement pxGrid Services + Feed	Service I Threat Centric NAC	:	
Deployment Licensing + Certif	ates + Logging + Maintenance Upgra	le → Backup & Restore →Admin A	ccess + Settings		
Authentication  Authorization  Authorization  Administrators	Admin Groups > Read Only Admin Admin Group * Name Read Only Admin Description Access Permission for	admin with read-only functionality		*	
Admin Users	Type 🗹 External				
Admin Groups	External Identity Source				
, seungs	✓ External Groups ⑦     * I mydomain.com/Users/ISE-RO ○     * I mydomain.com/Users/ISE-RO ○     * I mydomain.com/Users/ISE-RO ○     * Member Users Users     ↓Add ~ XDelete	ŀ			
	Status Email	Username	First Name Last Name		
	Save Reset		No data ava	ilable	

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.

diality Identity Services Engine	Home	License Warning 🔺	्	θ	•	•
▼ System → Identity Management	Network Resources     Device Portal Management     pxGrid Service     Feed Service     Threat Centric NAC					
Deployment Licensing - Certifi	ates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings					
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Signing Certificate	Import a new Certificate into the Certificate Store  * Certificate File DCcomDCmymainW.pem  Friendly Name  Trusted For:   Trusted For:  Trust for authentication within ISE.					
Certificate Authority	Trust for client authentication and Syslog Trust for authentication of Cisco Services Utalidate Certificate Extensions					
	Description Cancel					

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.

cisco Identity Services Engine	Home + Context Visibility + Oper	rations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources     Device Portal I	Management pxGrid Services + Feed Service + Threat Centric NAC
Deployment Licensing + Certific	cates + Logging + Maintenance	Enabling Client Certificate-Based Authentication will cause an application server restart on all deployment
0		nodes. This will result in significant downtime for the system.
Authentication	Authentication Method	Consol Consol
Authorization	Authentication Type	Cancer
▼ Administrators	Password Based	
Admin Users		* Identity Source AD:AD *
Admin Groups		
Settings	<ul> <li>Client Certificate Based</li> </ul>	
	Save	

- 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.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy <a href="#">Administration</a> + Work Centers
▼ System → Identity Management	Network Resources     Device Portal Management     pxGrid Service     Feed Service     Threat Centric NAC
Deployment Licensing + Certifi	cates → Logging → Maintenance Upgrade → Backup & Restore <del>×</del> Admin Access → Settings
Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
▼ Administrators Admin Users	O Password Based
Admin Groups	Client Certificate Based
• settings	* Identity Source AD:AD
	Save Reset

- 5. Click Save.
- 6. Se reinician los servicios de ISE en todos los nodos de la implementación.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy <a href="https://www.www.centers">Administration</a> + Work Centers
▼ System → Identity Management	t > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC
Deployment Licensing + Certifi	icates + Logging + Maintenance The system will now restart.
0	
Authentication	Authentication Method
Authorization	Authentication Type
★ Administrators	O Password Based
Admin Users	
Admin Groups	
Settings	Citent Certificate Based     * Certificate Authentication Profile     CAC_Login_Profile     *
	* Identity Source AD:AD *
	Save Reset

## 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.

(&	)(=)	Mttps://ise2.mydomain.com/	x - ۵	O Waiting for ise2.mydomain ×	





**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

- 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.