Configurazione dell'autenticazione basata su certificato o smart card per l'amministrazione di ISE

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Partecipa ad ISE e Active Directory Seleziona gruppi di directory Abilita autenticazione basata su password di Active Directory per l'accesso amministrativo Mapping dei gruppi di identità esterni ai gruppi amministrativi Importa certificato protetto Configura profilo di autenticazione certificato Abilita autenticazione basata su certificati client Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare l'autenticazione basata su certificati client per l'accesso alla gestione di Identity Services Engine (ISE). Nell'esempio, l'amministratore ISE esegue l'autenticazione in base al certificato utente per ottenere l'accesso come amministratore alla GUI di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ISE per l'autenticazione di password e certificati.
- Microsoft Active Directory (AD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine (ISE) versione 2.6
- Windows Active Directory (AD) Server 2008 release 2
- Certificato

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dalla configurazione.

Configurazione

Utilizzare questa sezione per configurare il certificato client o la smart card come identità esterna per l'accesso amministrativo alla GUI di gestione di Cisco ISE.

Esempio di rete



Partecipa ad ISE e Active Directory

- 1. Scegliere Amministrazione > Gestione identità > Origini identità esterne > Active Directory.
- 2. Creare un'istanza di Active Directory con il **nome del punto di join** e il **dominio AD** in Cisco ISE.
- 3. Fare clic su Invia.



4. Unire tutti i nodi con il nome utente e la password appropriati nel prompt.

cisco Identity Services Engine Home	Context Visibility + Oper	rations + Policy -Admir	nistration 🔹 Work C	enters		License Warning 🔺	् (0	ø
System Identity Management Network	Resources Device Portal	Management pxGrid Services	Feed Service	Threat Centric NAC					
+ Identities Groups External Identity Sources	Identity Source Sequences	; ▶ Settings							
External Identity Sources	Connection	Whitelisted Domains Pass	siveID Groups	Attributes Advance	ced Settings				
	* Join Point Name	AD		Ð					-
Active Directory AD	* Active Directory Domain	mydomain.com		Ð					
DDBC	o Join o Leave 🤦 Tes	t User 🔹 Diagnostic Tool 🚳 Re	efresh Table						
RADIUS Token	ISE Node	 ISE Node Role 	Status	Domain Controller	Site				
E RSA SecurID	ise2.mydomain.com	STANDALONE	🖸 Operational	WIN-58UQFTHFNIP.mydomai	Default-First-Site-Name				
SAML Id Providers									
Social Login		Join Domain			×				
		Please specify the credentials	required to Join ISE no	de(s) to the Active Directory Domain	·				
		* AD User Name	e @ [
		* Passw	bron						
		Specify Organizational Unit	a.						
		Store Credentials	@						
				ОК	Cancel				

5. Fare clic su Salva.

Seleziona gruppi di directory

- 1. Creare un gruppo di amministratori esterno e mapparlo al gruppo di Active Directory.
- 2. Scegliere Amministrazione >Gestione identità > Origini identità esterne > Active Directory > Gruppi > Seleziona gruppi dalla directory.
- 3. Recuperare almeno un gruppo AD a cui appartiene l'amministratore.

es	Ic	lentity Source Sequences + Settings		
	ſ	Select Directory Groups		×
		This dialog is used to select groups from the Dir	ectory.	
		Domain mydomain.com	¥	
			SID Filter *	
	4	Retrieve Groups 2 Groups Retri	eved.	
	C	Name Name	▲ Group SID Group Type	
		mydomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1 GLOBAL	
		wydomain.com/Users/ISE-RO	S-1-5-21-4009324561-3650473562-621564990-11 GLOBAL	
			OK	ancel

4. Fare clic su Salva.

Abilita autenticazione basata su password di Active Directory per l'accesso amministrativo

- 1. Abilitare l'istanza di Active Directory come metodo di autenticazione basato su password che è stato aggiunto ad ISE in precedenza.
- 2. Scegliere Amministrazione > Sistema > Accesso amministratore > Autenticazione, come mostrato nell'immagine.

dials. Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Service Feed 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

3. Fare clic su Salva.

Nota: La configurazione dell'autenticazione basata su password è necessaria per abilitare l'autenticazione basata su certificati. È necessario ripristinare questa configurazione dopo aver configurato correttamente l'autenticazione basata su certificati.

Mapping dei gruppi di identità esterni ai gruppi amministrativi

In questo esempio, il gruppo AD esterno è mappato al gruppo Admin predefinito.

- 1. Scegliere Amministrazione > Sistema > Accesso amministratore >Amministratori >Gruppi amministrativi > Amministratore privilegiato.
- 2. Selezionare l'opzione Type as **External** (Tipo come esterno) e selezionare il gruppo AD in **External groups** (Gruppi esterni).

Gisco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License W
▼System → Identity Managemen	nt + Network Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC	
Deployment Licensing + Certif	ificates → Logging → Maintenance Upgrade → Backup & Restore _=Admin Access → Settings	
Authentication	Admin Groups > System Admin Admin Group	
* Administrators	* Name System Admin Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.	
Admin Users	Type 🗹 External	
Admin Groups	External Identity Source	
	✓ External Groups * Imydomain.com/ISE-Admin	
	Status Last Name First Name	
	No data available	

- 3. Fare clic su Salva.
- 4. Scegliere Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministratori > Amministratore di sola lettura.
- 5. Selezionare l'opzione Type as **External** (Tipo come esterno) e selezionare il gruppo AD in **External groups** (Gruppi esterni), come illustrato nell'immagine.

diath. cisco Identity Services Engine Home → Context \	fisibility → Operations → Policy <a>Administration → Work Centers License W
System Identity Management Network Resources	Device Portal Management px: Grid Services Feed Service Threat Centric NAC
Deployment Licensing + Certificates + Logging +	Maintenance Upgrade → Backup & Restore ▼Admin Access → Settings
Authentication Admin Groups > Rea Admin Group	d Only Admin
Authorization Name	Read Only Admin
* Administrators Description	Access Permission for admin with read-only functionality
Admin Users Tvo	V External
Admin Groups External Identity So	rce
Settings Name : AD	
▼ External Group	5 (D)
* mydomain.c	vm/Users/ISE-RO 🖸 🕂
Member Users Users	
🕂 Add 👻 🗙 Delet	ê
Status	Email Username First Name Last Name
	No data available
Save	

6. Fare clic su Salva.

Importa certificato protetto

- 1. Importare il certificato dell'Autorità di certificazione (CA) che firma il certificato client.
- 2. Scegli Amministratore > Sistema > Certificati > Certificato protetto > Importa.
- 3. Fare clic su Sfoglia e scegliere il certificato CA.
- 4. Selezionare la casella di controllo Considera attendibile l'autenticazione del client e Syslog, come mostrato nell'immagine.

diality Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🔺	¢,	0	0	0
▼ System → Identity Management	Network Resources Device Portal Management px9rid Service Feed Service Threat Centric NAC					
Deployment Licensing - Certifi	cates → Logging → Maintenance Upgrade → Backup & Restore → Admin Access → Settings					
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Octor Deced	Import a new Certificate into the Certificate Store * Certificate File Choose File DCcomDCmymainWpem Friendly Name Trusted For: ()					
Certificate Signing Requests Certificate Periodio Check Setti Certificate Authority	Trust for authentication within ISE Trust for client authentication and Syslog Trust for client authentication of Cisco Services Utheta Catificate Seductions					
	Description Cancel Cancel					

5. Fare clic su Invia.

Configura profilo di autenticazione certificato

1. Per creare il profilo di autenticazione certificato per l'autenticazione basata su certificati client, scegliere Amministrazione >Gestione delle identità > Origini identità esterne > Profilo

di autenticazione certificato > Aggiungi.

- 2. Aggiungere il nome del profilo.
- 3. Selezionare l'attributo appropriato che contiene il nome utente dell'amministratore nell'attributo del certificato.
- 4. Se il record AD per l'utente contiene il certificato dell'utente e si desidera confrontare il certificato ricevuto dal browser con quello in Active Directory, selezionare la casella di controllo **Esegui sempre confronto binario** e selezionare il nome dell'istanza di Active Directory specificato in precedenza.

()ca(b) cisco Identity Services Engine Home → C	ontext Visibility + Operations + P	Policy ←Administration → W	Vork Centers
System Identity Management Network Re	esources + Device Portal Management	pxGrid Services + Feed Servic	ce 🕨 Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences + Settings		
System * Identity Management Network Re Identities Groups External Identity Sources External Identity Sources External Identity Sources Certificate Authentication Profile Certificate Authentication Profile Active Directory Sources Social Login	Sources Device Portal Management Identity Source Sequences Settings Certificate Authentication Profiles List > N Certificate Authentication Profile Name CA Description Identity Store Use Identity Store Settificate Against Certificate In Identity Store	pxond Services + Feed Services	ee Inreat Centric NAC ofile v v v v v v v v v v v v v
	Cancel) Only to resolve identity ambiguity Always perform binary comparison	y n

5. Fare clic su Invia.

Nota: Lo stesso profilo di autenticazione certificato può essere utilizzato anche per l'autenticazione basata sull'identità dell'endpoint.

Abilita autenticazione basata su certificati client

1. Scegli Amministrazione > Sistema > Accesso amministratore > Autenticazione > Basato su certificato client metodo di autenticazione.

cisco Identity Services Engine	Home + Context Visibility + Oper	ations
▼ System → Identity Management	Network Resources Device Portal I	vlanagement 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	
Authorization	Authentication Type	Cancel
▼ Administrators	O Derround Derrod	
Admin Users	O Password Based	* Identity Source AD:AD *
Admin Groups		
Settings	Client Certificate Based	
	Save Reset	

- 2. Fare clic su OK.
- 3. Scegliere il profilo di autenticazione certificato configurato in precedenza.
- 4. Selezionare il nome dell'istanza di Active Directory.

dentity Services Engine	Home → Context Visibility → Operations → Policy ▼Administration → Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certifi	cates + Logging + Maintenance Upgrade + Backup & Restore - 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	Certificate Authentication Profile (CAC_Login_Profile * // Identity Source AD:AD) //
	Save Reset

- 5. Fare clic su Salva.
- 6. I servizi ISE vengono riavviati su tutti i nodi dell'implementazione.

disco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration	▶ Work Centers
▼ System → Identity Management	t > Network Resources > Device Portal Management pxGrid Services > Fee	I Service Threat Centric NAC
Deployment Licensing + Certifi	icates + Logging + Maintenance The system will now restart.	
0		
Authentication	Authentication Method	
Authorization	Authentication Type	ок
▼ Administrators	O Password Based	
Admin Users		
Admin Groups		
Settings	Client Certificate Based * Certifica	te Authentioation Profile CAC_Login_Profile *
		* Identity Source AD:AD *
	Save Reset	

Verifica

Verificare l'accesso all'interfaccia grafica di ISE dopo che lo stato del servizio **Application Server** è cambiato in **In esecuzione.**

Utente con privilegi di amministratore privilegiato: verificare che all'utente venga richiesto di scegliere un certificato per accedere alla GUI ISE e che disponga dei privilegi di amministratore privilegiato se il certificato appartiene a un utente del gruppo di identità esterna con privilegi di amministratore privilegiato.



Admin User di sola lettura: verificare che all'utente venga richiesto di scegliere un certificato per accedere alla GUI di ISE e che disponga dei privilegi Admin di sola lettura se il certificato appartiene a un utente che fa parte del gruppo Admin External Identity di sola lettura.

Windows Security
Confirm Certificate Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.
Vinodh Issuer: mydomain-WIN-S8UQFTHF Valid From: 10/16/2019 to 10/15/2020 Click here to view certificate prope
OK Cancel



Nota: Se è in uso una scheda CAC (Common Access Card), la smart card presenta il certificato utente ad ISE dopo che l'utente ha immesso il proprio super pin valido.

Risoluzione dei problemi

- 1. Utilizzare il comando **application start ise safe** per avviare Cisco ISE in una modalità provvisoria che consente di disabilitare temporaneamente il controllo dell'accesso al portale di amministrazione e correggere la configurazione e riavviare i servizi di ISE con il comando **application stop ise** seguito dal comando **application start ise**.
- 2. L'opzione safe consente il ripristino se un amministratore blocca inavvertitamente l'accesso al portale Cisco ISE Admin per tutti gli utenti. Questo evento può verificarsi se l'amministratore ha configurato un elenco di accesso IP errato nella pagina Amministrazione > Accesso amministratore > Impostazioni > Accesso. L'opzione safe ignora inoltre l'autenticazione basata su certificati e ripristina l'autenticazione predefinita di nome utente e password per accedere al portale Cisco ISE Admin.