Configurar autenticação baseada em certificado ou cartão inteligente para administração do ISE

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Diagrama de Rede Ingressar no ISE no Ative Diretory Selecionar grupos de diretórios Ativar autenticação baseada em senha do Ative Diretory para acesso administrativo Mapear grupos de identidade externos para grupos de administradores Importar certificado confiável Configurar perfil de autenticação de certificado Ativar autenticação baseada em certificado do cliente Verificar Troubleshoot

Introduction

Este documento descreve como configurar a autenticação baseada em certificado do cliente para o acesso de gerenciamento do Identity Services Engine (ISE). Neste exemplo, o administrador do ISE se autentica em relação ao certificado do usuário para obter acesso de administrador à GUI de gerenciamento do Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda ter conhecimento destes tópicos:

- Configuração do ISE para autenticação de senha e certificado.
- Microsoft Ative Diretory (AD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine (ISE) versão 2.6
- Windows Ative Diretory (AD) Server 2008 versão 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. Se a rede estiver ativa, certifique-se de entender o impacto potencial de qualquer configuração.

Configurar

Use esta seção para configurar o certificado do cliente ou o Smart Card como uma identidade externa para acesso administrativo à GUI de gerenciamento do Cisco ISE.

Diagrama de Rede



Ingressar no ISE no Ative Diretory

- 1. Escolha Administração > Identity Management > External Identity Sources > Ative Diretory.
- 2. Crie uma instância do Ative Diretory com o **nome do ponto de junção** e o **domínio do AD** no Cisco ISE.
- 3. Clique em Submit.



4. Junte-se a todos os nós com o Nome de usuário e Senha apropriados no prompt.

GISCO Identity Services Engine Home →	Context Visibility + Oper	ations + Policy -Admir	nistration 🔹 Work Ce	inters		License Warning 🔺	٩,	0 O	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		<i>D</i>					Ê
Active Directory AD Dag	* Active Directory Domain mydomain.com								
CODF ODBC	👷 Join 👷 Leave 🤦 Tes	: User 🛛 🔓 Diagnostic Tool 🛛 😵 Re	efresh Table						
RADIUS Token	ISE Node	 ISE Node Role 	Status	Domain Controller	Site				
RSA SecuriD	ise2.mydomain.com	ise2.mydomain.com STANDALONE 🔯 Operational WIN-58UQFTHFNIP.mydomai Default-First-Site-Name							
Social Login		Join Domain Please specify the oredentials * AD User Name * Passw Specify Organizational Unit Store Credentials	equired to Join ISE nor a () () () () () () () () () ()	de(;) to the Active Directory Domain	X Cancel				l

5. Click Save.

Selecionar grupos de diretórios

- 1. Crie um grupo de administradores externo e mapeie-o para o grupo de diretórios ativo.
- 2. Escolha Administração >Identity Management > External Identity Sources > Ative Diretory > Groups > Select Groups from Diretory.
- 3. Recupere pelo menos um grupo AD ao qual o administrador pertence.

Select Directory Groups X This dialog is used to select groups from the Directory. Name involvmain.com * Name Filted #TESE-# SID Filted # Type Filted ALL * Name involves froups 2 Groups Retrieved. Group Type Group Type * Name involves involves Group SID Group Type * * Name involves involves Admin \$-16-21-4000324661-3850473562-621664990-1 GLOBAL * mydomain.com/Users/ISE-RD \$-16-21-4000324661-3850473562-621664990-11 GLOBAL *	es	Identity Source Sequences 🔹 🕨 Settings		
This dialog is used to select groups from the Directory. Domain_mydomain.com " Name Filte *ISE-* Retireve Groups 2 Group SID Oroup SID Group Type mydomain.com/USE-Admin \$-1-5-21-4000324661-3650473562-6216644900-1 Group SID \$-1-5-21-4000324661-3650473562-6216644900-1 Mame \$-0 mydomain.com/USE-SISE-RO \$-1-5-21-4000324661-3650473562-6216644900-1		Select Directory Groups		×
Domain mydomain.com * Name Fittet *ISE:* Rettrave Groups 2 Groups Retrieved. Group SID Mame oroup SID mydomain.com/ISE:Admin S-16-21-4009324561-3860473562-621564990-1 mydomain.com/ISE:Admin S-16-21-4009324661-3860473662-621564990-1 mydomain.com/ISE:Admin S-16-21-4009324661-3860473662-621564990-1 mydomain.com/ISE:RD S-16-21-4009324661-3860473662-621564990-1 mydomain.com/ISE:RD S-16-21-4009324661-3860473662-621564990-1 Mame S-16-21-4009324661-3860473662-621564990-1 Mame S-16-21-4009324661-3860473662-621564990-1 Mame Group SID S-16-21-4009324661-3860473662-621564990-1 Mame Group SID S-16-21-4009324661-3860473662-621564990-1 Group SID Group SID	-	This dialog is used to select groups from the Dire	ectory.	
Name Filte Type Filte Type Filte * Retrieve Groups 2 Group Retrieved. Group SID Group Type Mame * Group SID Group Type mydomain.com/ISE.Admin \$-1-5-21-4009324561-3650473562-621564990-1 GLOBAL mydomain.com/Users/ISE.RD \$-1-5-21-4009324561-3650473562-621564990-1 GLOBAL		Domain mydomain.com	*	
Retrieve Groups 2 Groups Retrieved. Group SID Group Type Image: mydomain.com/ISE-Admin S-1-5-21-40009324561-3850473562-821564990-1 GLOBAL Imydomain.com/Usex/ISE-RD S-1-5-21-40009324561-3850473562-821564990-11 GLOBAL		Name Filter *ISE-*	SID Filter * Type Filter ALL *	1
Name Group SID Group Type mydomain.com//SE-Admin \$-1-5-21-4009324661-3850473562-621564990-1 GLOBAL mydomain.com/Users/ISE-RD \$-1-5-21-4009324661-3850473562-621564990-11 GLOBAL		Retrieve Groups 2 Groups Retrie	eved.	,
✓ mydomain.com/ISE-Admin \$-1-5-21-4009324561-3650473562-621564990-1 GLOBAL ✓ mydomain.com/Users/ISE-RD \$-1-5-21-4009324661-3650473562-621564990-11 GLOBAL		✓ Name	Group SID Group Type	
✓ mydomain.com/Users/ISE-RO \$-1-5-21-4009324581-3850473582-821584990-11 \$LOBAL		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	
OK Cancel	0			DK Cancel

4. Click Save.

Ativar autenticação baseada em senha do Ative Diretory para acesso administrativo

- 1. Ative a instância do ative diretory como método de autenticação baseado em senha que ingressou no ISE anteriormente.
- 2. Escolha Administration > System > Admin access > Authentication, como mostrado na imagem.

disco 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 + Certifica	ates + 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 * Identity Source AD:AD *
 Settings 	
	O Client Certificate Based
	Save Reset

3. Click Save.

Note: A configuração de autenticação baseada em senha é necessária para ativar a

autenticação baseada em certificado. Essa configuração deve ser revertida após uma configuração bem-sucedida da autenticação baseada em certificado.

Mapear grupos de identidade externos para grupos de administradores

Neste exemplo, o grupo de AD externo é mapeado para o grupo de Admin padrão.

- 1. Escolha Administração >Sistema >Acesso de Administrador > Administradores >Grupos Admin > Super administrador.
- 2. Marque Tipo como Externo e selecione o grupo AD em Grupos externos.

disco Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers	License W					
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC						
Deployment Licensing + Certifi	cates → Logging → Maintenance Upgrade → Backup & Restore - A dmin Access → Settings						
Authentication + Authorization	Admin Groups > System Admin Admin Group * Name System Admin						
▼ Administrators	Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.						
Admin Users	Type 🗹 External						
Admin Groups	External Identity Source						
 Settings 	Name : AD						
	* I mydomain.com/ISE-Admin C +- Member Users						
	+Add - XDelete						
	Status Email Username First Name Last Name						
	No data available						
	Save Reset						

- 3. Click Save.
- 4. Escolha Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin.
- 5. Marque Tipo como **Externo** e selecione o grupo AD em **Grupos externos**, como mostrado na imagem.

Gisco Identity Services Engine	Home	ibility + Operations	; → Policy ▼Administ	ration 🔹 Work Cer	nters		License W
▼ System → Identity Managemen	t 🔹 Network Resources	Device Portal Mana	gement p×Grid Services	Feed Service	Threat Centric NAC		
Deployment Licensing + Certif	icates ⊧Logging ⊧N	laintenance Upgrade	▶ Backup & Restore ▼A	dmin Access + Set	tings		
Authentication	Admin Groups > Read - Admin Group	Only Admin					
Addionzation	* Name	Read Only Admin					
▼ Administrators	Description	Access Permission for a	dmin with read-only functional	ity		11	
Admin Users	Туре	External					
Admin Groups	External Identity Sour	ce					
 Settings 	Name: AD						
	▼ External Groups	Ð					
	* mydomain.com	n/Users/ISE-RO 🛛 😒 🕂					
	Member Users						
	Status	Email	Username	First Name	Last Name		
					No data available		
	Save						

6. Click Save.

Importar certificado confiável

- 1. Importar o certificado da autoridade de certificação (AC) que assina o certificado do cliente.
- 2. Escolher Administrador > Sistema > Certificados > Certificado Confiável > Importar.
- 3. Clique em Procurar e escolha o certificado CA.
- 4. Marque a **caixa de seleção Confiar na autenticação do cliente e Syslog**, como mostrado na imagem.

diate Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers	License Warning 🚣 🔍 🤨 💿 🗢
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Deployment Licensing - Certifi	ates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings	
9		
▼ Certificate Management	Import a new Certificate into the Certificate Store	
System Cartificates	* Certificate File Choose File DCcomDCmy mainW.pem	
Trusted Certificates	Friendly Name 👔	
OCSP Client Profile	Trusted For:	
Certificate Signing Requests	Trust for authentication within ISE	
Certificate Periodic Check Setti		
Certificate Authority	Index nor client authentication and Systog	
	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
	Description	
	Submit Cancel	

5. Clique em Submit.

Configurar perfil de autenticação de certificado

1. Para criar o perfil de autenticação de certificado para autenticação baseada em certificado do cliente, escolha Administração >Identity Management > External Identity Source >

Certificate Authentication Profile > Add.

- 2. Adicionar nome de perfil.
- 3. Selecione o atributo apropriado que contém o nome de usuário do administrador no atributo de certificado.
- 4. Se o registro do AD do usuário contiver o certificado do usuário e quiser comparar o certificado recebido do navegador com o certificado no AD, marque a caixa de seleção Sempre executar comparação binária e selecione o nome da instância do Ative Diretory que foi especificado anteriormente.

5. Clique em Submit.

Note: O mesmo perfil de autenticação de certificado também pode ser consumido para autenticação baseada em identidade de ponto final.

Ativar autenticação baseada em certificado do cliente

1. Escolher Administração > Sistema > Acesso Admin > Autenticação > Método de Autenticação Baseado no Certificado do Cliente.

disco 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	
Authorization	Authentication Type	Cancel
▼ Administrators	O Password Based	
Admin Users		* Identity Source (AD:AD *
Admin Groups	Client Cartificate Racad	
Settings	G Chent Centincate Dased	
	Save	

- 2. Click OK.
- 3. Escolha o perfil de autenticação do certificado configurado anteriormente.
- 4. Selecione o nome da instância do Ative Diretory.

cisco 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	sates → Logging → Maintenance Upgrade → Backup & Restore →Admin Access → Settings
Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
▼ Administrators	O Password Based
Admin Users	
Admin Groups	Client Certificate Based
 Settings 	* Certificate Authentication Profile CAC_Login_Profile *
	* Identity Source AD:AD
	Save Reset

- 5. Click Save.
- 6. Os serviços ISE em todos os nós na implantação são reiniciados.

·

Verificar

Verifique o acesso à GUI do ISE depois que o status do serviço **do Servidor de Aplicativos** for alterado para **em execução**.

Usuário Super Admin: verifique se o usuário é solicitado a escolher um certificado para fazer login na GUI do ISE e se recebe privilégios Super Admin se o certificado for de um usuário do grupo de Identidade Externa do Super Admin.





Usuário Admin Somente Leitura: Verifique se o usuário é solicitado a escolher um certificado para

fazer login na GUI do ISE e recebe privilégios Admin Somente Leitura se o certificado for de um usuário do grupo Identidade Externa Admin Somente Leitura.

(<-) (<>) (</>
 https://ise2.mydomain.com/





Note: Se o Cartão de Acesso Comum (CAC) estiver em uso, o Smartcard apresenta o certificado do usuário ao ISE depois que o usuário digitar seu super pino válido.

Troubleshoot

1. Use o comando application start ise safe para iniciar o Cisco ISE em um modo seguro que

permite desativar temporariamente o controle de acesso ao portal Admin e Corrija a configuração e reinicie os serviços do ISE com o comando **application stop ise** seguido pelo **application start ise**.

2. A opção de segurança fornece um meio de recuperação se um administrador bloqueia inadvertidamente o acesso ao portal do administrador do Cisco ISE para todos os usuários. Este evento pode ocorrer se o administrador tiver configurado uma lista de acesso IP incorreta na página Administração > Acesso de administrador > Configurações > Acesso. A opção safe também ignora a autenticação baseada em certificado e reverte para a autenticação de nome de usuário e senha padrão para fazer login no portal Cisco ISE Admin.