# 为ISE管理配置基于证书或智能卡的身份验证

## 目录

简介 先决条件 要求 使用的组件 配置 网络图 <u>将ISE加入Active Directory</u> 选择目录组 为管理访问启用基于密码的Active Directory身份验证 将外部身份组映射到管理员组 导入受信任证书 配置证书身份验证配置文件 启用基于客户端证书的身份验证 验证 故障排除

# 简介

本文档介绍如何为身份服务引擎(ISE)管理访问配置基于客户端证书的身份验证。在本示例中 ,ISE管理员根据用户证书进行身份验证,以获得对思科身份服务引擎(ISE)管理GUI的管理员访问 权限。

# 先决条件

#### 要求

思科建议了解以下主题:

- 密码和证书身份验证的ISE配置。
- Microsoft Active Directory(AD)

## 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科身份服务引擎(ISE)版本2.6
- Windows Active Directory(AD)Server 2008版本2
- 证书

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果网络处于活动状态,请确保了解任何配置的潜在影响。

配置

使用此部分将客户端证书或智能卡配置为外部身份,用于管理访问思科ISE管理GUI。

#### 网络图



## 将ISE加入Active Directory

- 1. 选择管理> 身份管理>外部身份源> Active Directory。
- 2. 在Cisco ISE中创建具有加入点名称和AD域的Active Directory实例。
- 3. 单击"Submit"。

•i[+i]         •i]         •i]	Operations      Policy      Administration      Work Centers	License Warning 🔺	O,	0	0	<b>\$</b>
System      Identity Management     Network Resources     Dev	≠ Portal Management pxGrid Services → Feed Service → Threat Centric NAC					
Identities Groups External Identity Sources Identity Source	quences + Settings					
External Identity Sources Connection	I		*			
Certificate Authentication Profile     Solution	it Name AD ①					
Active Directory     Active Directory     Active Directory	Domain mydomain.com					
RADIUS Token			Ŧ			
RSA SecurID Submit Canc						
Social Login						

4. 在提示符中使用适当的用户名和密码加入所有节点。

Syste	cisco Identity Services Engine Home )	Context Visibility      Operations      Policy      Administration      Work Centers	License Warning 🔺 🔍 🚳 😆 🌣
Identities @roops External Identity Sources Identity Sources & bettings     Identity Sources (Identity Sources & Advanced Settings)     Identity Sources (Identity Sources Advanced Settings)     Identity Sources     Ide	System      Identity Management      Network	Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC	
External Identity Sources         Image: Control on Adhenication Profile         Control on Adhenication Profile         Active Directory         Advanced Settings         In Dark         Advanced Settings         Control on Adhenication Profile         Advanced Settings         Advanced Settings         Control on Adhenication Profile         Advanced Settings         Control on Advanced Settings         Cont on Advanced Settings         Cont on Advanced Settings         Cont on Advanced Settings         Cont on Advanced Settings	+ Identities Groups External Identity Sources	s Identity Source Sequences + Settings	
	External Identity Sources	Connection       Whitelated Domains       PassiveID       Groups       Attributes       Advanced Settings         • Join Point Name       AD       I       I         • Active Directory Domain       mydemain.com       I         Image: Status       Image: Status       Image: Status       Image: Status         Image: Status       Image: Status       Image: Status       Image: Status       Image: Status         Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status         Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status       Image: Status	

5. Click Save.

## 选择目录组

1. 创建外部管理员组并将其映射到Active Directory组。

2. 选择管理>身份管理>外部身份源> Active Directory >组>从目录选择组。

3. 至少检索一个管理员所属的AD组。

25	Identity Source Sequences		
	Select Directory Groups		×
	This dialog is used to select groups from the Directo	ny.	
	Domain mydomain.com	Ŧ	
	Name Filter *ISE-* SID	Filter * Type Filter ALL	<b>*</b>
	Retrieve Groups 2 Groups Retrieve	.d.	
	Vame 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
			OK Cancel

### 为管理访问启用基于密码的Active Directory身份验证

- 1. 启用active directory实例作为之前加入ISE的基于密码的身份验证方法。
- 2. 选择管理>系统>管理员访问>身份验证,如图所示。

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 + Certific	cates → Logging → Maintenance Upgrade → Backup & Restore ▼Admin Access → Settings
2 Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
▶ Authorization	Authentication Type
Administrators	Password Based     * Identity Source AD:AD     *
<ul> <li>Settings</li> </ul>	
	O Client Certificate Based
	Save Reset

3. Click Save.

**注意:**启用基于证书的身份验证需要基于密码的身份验证配置。此配置应在成功配置基于证书 的身份验证后恢复。

#### 将外部身份组映射到管理员组

在本例中,外部AD组映射到默认管理员组。

- 1. 选择管理>系统>管理员访问>管理员>管理员组>超级管理员。
- 2. 选中"Type as External(类型为外部)",然后在"External groups(外部组)"下选择AD组。

System > Identity Management     Deployment Licensing > Certificate     Authentication     Authorization	Network Resources      tes      Logging      M  Admin Groups > System  Admin Groups	Device Portal Management aintenance Upgrade + Bac	pxGrid Services → Fe ckup & Restore →Admin	ed Service 🕨 TI Access 🕨 Settin	nreat Centric NAC ngs		
Deployment Licensing + Certificate Authentication	tes → Logging → M Admin Groups > <b>Syster</b> Admin Group	aintenance Upgrade ⊧Ba	ckup & Restore →Admin	Access ▶ Settin	ngs		
Authentication	Admin Groups > <b>Syster</b> Admin Group	n Admin					
	numin aroup						
	* Name	System Admin					
- Administrators	Description	Access permission for Operations	: tab. Includes System and	data access permis	sion for Admin Gro	ups.	
Admin Users	Type	External					
Admin Groups	External Identity Source	e					
<ul> <li>Settings</li> </ul>	External Groups						
,	* External Groups * mydomain.com Member Users Users	/ISE-Admin 📀 🕂					
	🕂 Add 👻 🗶 Delete						
	Status	🔺 Email	Username	First Name	Last Name		
	Save Reset				No data avail	able	

- 3. Click Save.
- 4. 选择Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin。
- 5. 选中"Type as External(类型)",然后在"External groups(外部组)"下选择AD组,如图所示。

disco Identity Services Engine	Home + Context Vi	sibility + Operations	Policy ▼Administ	ration 🔹 Work Cen	iters		License W
▼System → Identity Managemen	t 🕨 Network Resources	Device Portal Manag	gement pxGrid Services	Feed Service	Fhreat Centric NAC		
Deployment Licensing + Certi	icates ⊧Logging ⊧N	laintenance Upgrade	▶ Backup & Restore ▼A	dmin Access + Sett	lings		
Authentication	Admin Groups > Read Admin Group	Only Admin					
	* 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					
<ul> <li>Settings</li> </ul>	Name: AD						
	External Groups     Member Users     Users	1) h/Users/ISE-RO 🛛 🖓 🕂					
	🕂 Add 👻 🗙 Delete						
	Status	🔺 Email	Username	First Name	Last Name		
	Save Reset				No data avai	lable	

6. Click Save.

## 导入受信任证书

- 1. 导入签署客户端证书的证书颁发机构(CA)证书。
- 2. 选择 管理员>系统>证书>受信任证书>导入。
- 3. 点击浏览并选择CA证书。
- 4. 如图所示,选中Trust for client authentication和Syslog复选框。

Identity Services Engine	Home + Context Visibility + Operations + Policy  Administration + Work Centers	License Warning 🔺	<u>م</u>	Θ	0	•	
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						
0							
▼ Certificate Management	Import a new Certificate into the Certificate Store						
System Certificates	* Certificate File Choose File DCcomDCmymainW.pem						
Trusted Certificates	Friendly Name 🛛 🕖						
OCSP Client Profile	To stad For-						
Certificate Signing Requests	□ Tarté for válkozátí stor válko 150						
Certificate Periodic Check Setti							
Certificate Authority	Trut for client authentication and Systog						
	Trust for authentication of Cisco Services						
	Validate Certificate Extensions						
	Description						
	Submit						

5. 单击"Submit"。

#### 配置证书身份验证配置文件

- 1. 要为基于客户端证书的身份验证创建证书身份验证配置文件,请选择管理>身份管理>外部身份 源>证书身份验证配置文件>添加。
- 2. 添加配置文件名称。
- 3. 选择在证书属性中包含管理员用户名的适当属性。
- 4. 如果用户的AD记录包含用户的证书,并且想将从浏览器收到的证书与AD中的证书进行比较 ,请选中**始终执行二进制比**较复选框,并选择之前指定的Active Directory实例名称。

cisco Identity Services Engine Home	Context Visibility → Operations → Policy ▼Administration → Work Centers
System      Identity Management     Network	k Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
Identities Groups External Identity Source	es Identity Source Sequences + Settings
External Identity Sources	Certificate Authentication Profiles List > New Certificate Authentication Profile Certificate Authentication Profile

5. 单击"Submit"。

注意:也可使用相同的证书身份验证配置文件进行基于身份的终端身份验证。

#### 启用基于客户端证书的身份验证

1. 选择 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 1	Management pxGrid Services + Feed Service + Threat Centric NAC		
Deployment Licensing + Certificates + 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	Cancer		
▼ Administrators	O Paraward Parend			
Admin Users	C Passoond based	* Identity Source AD:AD *		
Admin Groups				
Settings	<ul> <li>Client Certificate Based</li> </ul>			
	Save			

- 2. Click OK.
- 3. 选择之前配置的证书身份验证配置文件。
- 4. 选择Active Directory实例名称。

CISCO Identity 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 <mark>→</mark> 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     * Certificate Authentication Profile     CAC_Login_Profile     *
	* Identity Source AD:AD
	Save Reset

- 5. Click Save.
- 6. 部署中所有节点上的ISE服务将重新启动。

cisco Identity Services Engine	Home → Context Visibility → Ope	rations + 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 🔒	The system will now restart.
0	Authorities Malhed	
Authentication	Autrentication Method	
Authorization	Authentication Type	
▼ Administrators	O Password Based	
Admin Users		
Admin Groups		
• Settings	Client Certificate Based	* Certificate Authentication Profile CAC_Login_Profile *
		* Identity Source AD:AD T
	Save Reset	

# 验证

验证在应用服务器服务状态更改为运行后对ISE GUI的访问。

Super Admin User: Verify该用户是否被提示选择证书以登录ISE GUI,并且如果证书是Super Admin External Identity组的用户部分,则会获得Super Admin权限。





**只读管理员用户**:如果证书是只读管理员外部身份组的用户部分,请验证是否提示用户选择证书以 登录ISE GUI并授予只读管理员权限。





注意:如果使用通用访问卡(CAC),智能卡在用户输入有效超级PIN后向ISE显示用户证书。

# 故障排除

- 使用application start ise safe 命令在安全模式下启动Cisco ISE,允许临时禁用对管理员门户 的访问控制,并使用命令application stop ise和application start ise更正ISE的配置并重新启动 ISE的服务。。
- 2. 如果管理员无意中锁定了所有用户对思科ISE管理员门户的访问,安全选项提供恢复方法。如

果管理员在"管理"(Administration)>"管理员访问"(Admin Access)>"设置"(Settings)>"访问 "(Access)页面中配置了错误的IP访问列表,则可能会发生此事件。safe 选项还绕过基于证书 的身份验证并恢复为默认用户名和密码身份验证,以便登录Cisco ISE管理员门户。