Configure Certificate or Smartcard Based authentication for ISE Administration

Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Join ISE to Active Directory Select Directory Groups Enable Active Directory Password-Based Authentication for Administrative Access Map External Identity Groups to Admin Groups Import Trusted Certificate Configure Certificate Authentication Profile Enable Client Certificate-based Authentication Verify Troubleshoot

Introduction

This document describes how to configure Client Certificate-based authentication for Identity Services Engine (ISE) management access. In this example, the ISE administrator authenticates against the User certificate to gain Admin access to the Cisco Identity Services Engine (ISE) management GUI.

Prerequisites

Requirements

Cisco recommends to have knowledge of these topics:

- ISE configuration for password and certificate authentication.
- Microsoft Active Directory (AD)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE) Version 2.6
- Windows Active Directory (AD) Server 2008 Release 2
- Certificate

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. If the network is live, make sure to understand the potential impact of any configuration.

Configure

Use this section to configure the Client certificate or Smart Card as an external identity for administrative access to the Cisco ISE management GUI.

Network Diagram



Join ISE to Active Directory

- 1. Choose Administration > Identity Management > External Identity Sources > Active Directory.
- 2. Create an Active Directory instance with Join Point name and AD domain in Cisco ISE.
- 3. Click Submit.



4. Join all the nodes with the appropriate **Username** and **Password** in the prompt.

cisco Identity Services Engine Home	→ Context Visibility → Ope	rations + Policy -Admin	nistration 🔹 Work Co	enters		License Warning 🔺	٩. (0 0	ø	
+ System →Identity Management → Network Resources → Device Portal Management pxSrid Service → Threat Centric NAC										
I dentities Groups External I dentity Sources I dentity Sources + Settings										
External Identity Sources	Connection	Whitelisted Domains Pas	siveID Groups	Attributes Advance	ced Settings					
	* Join Point Name									
Active Directory AD	* Active Directory Domain									
DDBC	👷 Join 🧛 Leave 🤦 Tes									
RADIUS Token	ISE Node	 ISE Node Role 								
RSA SecurID	ise2.mydomain.com	STANDALONE								
SAML Id Providers										
Social Login		Join Domain	and the late IOF of	defective the define Disertees Demois	×					
		Please specify the credentials	required to Join ISE no	de(s) to the Active Directory Domain						
		* AD User Name	e @							
* Password										

5. Click Save.

Select Directory Groups

- 1. Create an external Administrator group and map it to the active directory group.
- 2. Choose Administration >Identity Management > External Identity Sources > Active Directory > Groups > Select Groups from Directory.
- 3. Retrieve at least one AD Group to which the administrator belongs.

es l	dentity Source Sequences 🔹 Settings			
	Select Directory Groups			×
	This dialog is used to select groups from the Di	rectory.		
	Domain mydomain com	*		
	Name Filter #ICE_#	SID Filter *	*	
	Retrieve Groups 2 Groups Ret	ieved		
C	Name Name	Group SID	Group Type	
	✓ mvdomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1	GLOBAL	
	mydomain.com/Users/ISE-BD	8-1-5-21-4009324581-3850473582-821584990-11	GLOBAL	
	E mysonantoonrootaroerno	0 100 100 000 100 100 000 100 100 100 1		
2				
			Call	-

4. Click Save.

Enable Active Directory Password-Based Authentication for Administrative Access

- 1. Enable active directory instance as Password-based authentication method which has joined ISE earlier.
- 2. Choose Administration > System > Admin access > Authentication, as shown in the image.

disab. 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 + Certific	ates → Logging → Maintenance Upgrade → Backup & Restore <mark>→</mark> Admin Access → Settings
O 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.

Note: Password-Based authentication configuration is required to enable Certificate-Based authentication. This configuration should be reverted after a successful configuration of Certificate-Based authentication.

Map External Identity Groups to Admin Groups

In this example, the external AD group is mapped to the default Admin group.

- 1. Choose Administration >System >Admin Access >Administrators >Admin Groups > Super admin.
- 2. Check the Type as External and select the AD group under External groups.

cisco Identity Services Engine	Home + Context Vi	sibility + Operations (Policy -Administra	ition 🔹 Work Cer	nters		License W				
▼System → Identity Management	Network Resources	Device Portal Managemer	nt pxGrid Services 🕨	Feed Service 🔸	Threat Centric NAC	;					
Deployment Licensing + Certifi	cates → Logging → N	faintenance Upgrade 🕨	Backup & Restore 🛛 🕶 Ad	min Access → Set	tings						
Authentication + Authorization	Admin Groups > Syste Admin Group * Name	m Admin System Admin									
▼ Administrators	Description	Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.									
Admin Users	Туре	External									
Admin Groups	External Identity Sour	ce									
 Settings 	Name : AD										
	🕂 Add 👻 🗶 Delete	1= -4	1			1					
	Status	 Email 	Username	First Name	Last Name	ilabla					
	Save Reset				No data ava	i a di te					

- 3. Click Save.
- 4. Choose Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin.
- 5. Check the Type as **External** and select the AD group under **External groups**, as shown in the image.

cisco Identity Services Engine	Home + Context Visibility	♦ Operations ♦ Policy		Centers		License W					
▼ System → Identity Managemen	t 🕨 Network Resources 🕨 Devi	e Portal Management p×Grid	Services I Feed Service	▶ Threat Centric NAC							
Deployment Licensing + Certif	icates ⊧Logging ⊧Maintena	nce Upgrade ⊧Backup&F	Restore •Admin Access •	Settings							
C Authentication	Admin Groups > Read Only Ad Admin Group	min									
 Authorization 	Name Read C	Inlu Admin									
▼ Administrators	Description Access	Permission for admin with read-or	alv functionality								
Admin Users	Description Access	end administration of the second second	ny roncoortaixy								
Admin Groups	Type Exter	mai									
) Settings	External Identity Source Name : AD										
	▼ External Groups ④										
	* mydomain.com/Users/ISE-RO 🖸 🕂										
	Member Users Users										
	🕂 Add 👻 🗙 Delete										
	Status	Email Userna	me First Name	Last Name							
				No data available							
	Save										

6. Click Save.

Import Trusted Certificate

- 1. Import the Certificate authority(CA) certificate that signs the client certificate.
- 2. Choose Administrator > System > Certificates > Trusted Certificate > Import.
- 3. Click browse and choose the CA certificate.
- 4. Check the Trust for client authentication and Syslog checkbox, as shown in the image.

Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers	License Warning 🔺	<u>م</u>	0	0	•				
System > Identity Management > Network Resources > Device Portal Management px&id Services > Feed Service > Threat Centric NAC										
Deployment Licensing - Certifi	Deployment Licensing -Certificates +Logging +Maintenance Upgrade +Backup&Restore +AdminAccess +Settings									
0	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	Trusted For: ()									
Certificate Signing Requests	✓ Trust for authentication within ISE									
Certificate Periodic Check Setti	Trust for client authentication and Surlon									
Certificate Authority										
	 Trust for admenication or Caco Services 									
	Validate Certificate Extensions									
	Description									
	Submit Cancel									

5. Click Submit.

Configure Certificate Authentication Profile

 In order to create Certificate Authentication Profile for Client certificate-based authentication, Choose Administration >Identity Management > External Identity Sources > Certificate Authentication Profile > Add.

- 2. Add profile name.
- 3. Select the appropriate attribute that contains the administrator username in the certificate attribute.
- 4. If the AD record for the user contains the user's certificate, and want to compare the certificate that is received from the browser against the certificate in AD, check Always perform binary comparison checkbox, and select the Active Directory instance name that was specified earlier.

CISC	b lo	dentity	/ Servic	ces l	Engine		Home) C	ontext	∕isibilit	ty	♦ Ор	erations) F	Policy	▼Admin	istration	♦ Work	k Centers		
• 5	Syster	m	- Identii	ty M	anagen	nent	▶ Netwo	nk Re	sources)evice	Portal	l Manag	ement	p×G ri	d Services	▶ Feed	Service	Threat Centric NAC		
+ ا	denti	ties	Group	s	Externa	Ilden	tity Sourc	es	Identit	y Sourc	ce Se	quence	es ⊧S	Settings							
External Identity Sources				Certific Certifi	ate Aut cate A	thenti Autho	cation entica	Profiles ation Pr	List > New Certificate Authentication Profile ofile												
Certificate Authentication Profile Active Directory AD LDAP DBC						* Name Description						CAC_Login_Profile									
	RADIUS Token RSA SecurID SAML Id Providers SAML Id Providers							Identity Store						AD Ţ							
											Us	e Ideni	tity From	•	Certifica Any Sub	te Attribute ject or Alte	Subjec	t Alternati me Attrib	ive Name - Other Name 🛛 🕡 utes in the Certificate (for Active Directory Only) 🕡		
									Ma Ce	tch Clie rtificat	ient C te In I	ertifica dentity	ite Again r Store (j	ast D O	Never Only to Always) resolve ic	entity aml nary comp	biguity parison			
									Submi	it 🖸	Cancel										

5. Click Submit.

Note: The same Certificate authentication profile can be consumed for endpoint Identitybased authentication also.

Enable Client Certificate-based Authentication

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

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. Click **OK**.
- 3. Choose the **Certificate Authentication Profile** that is configured earlier.
- 4. Select the Active Directory instance name.

dialba 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	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 Certificate Authentication Profile CAC Login Profile T
	* Identity Source AD:AD
	Save Reset

- 5. Click Save.
- 6. ISE services on all the nodes in the deployment restarts.

cisco Identity Services Engine		erations + Policy -Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal	Management pxGrid Services + Feed Service + Threat Centric NAC
Deployment Licensing + Certific	cates + 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 	* Certificate Authentication Profile CAC_Login_Profile *
		* Identity Source AD:AD *
	Save Reset	

Verify

Verify access to the ISE GUI after the Application Server service status changes to running.

Super Admin User: Verify that the user is prompted to choose a certificate to login to the ISE GUI and is given Super Admin privileges if the certificate is of a user part of the Super Admin External Identity group.





Read-only Admin User: Verify that the user is prompted to choose a certificate to login to the ISE GUI and is given Read-only Admin privileges if the certificate is of a user part of Read-only Admin

() (https://ise2.mydomain.com/





Note: If Common Access Card (CAC) is in use, Smartcard presents the user certificate to ISE after the user enters their valid super pin.

Troubleshoot

1. Use the application start ise safe command to start Cisco ISE in a safe mode that allows to disable access control temporarily to the Admin portal and Correct the configuration and

restart the services of ISE with the command **application stop ise** followed by **application start ise**.

2. The safe option provides a means of recovery if an administrator inadvertently locks out access to the Cisco ISE Admin portal for all users. This event can happen if the administrator configured an incorrect IP Access list in the Administration > Admin Access > Settings > Access page. The safe option also bypasses certificate-based authentication and reverts to the default username and password authentication for logging into the Cisco ISE Admin portal.