ISE Administrationの証明書またはスマートカー ドベースの認証の設定

内容

概要
 前提条件
 要件
 使用するコンポーネント
 設定
 ネットワーク図
 ISEのActive Directoryへの参加
 ディレクトリグループの選択
 管理アクセスのためのActive Directoryパスワードベース認証の有効化
 外部IDグループの管理グループへのマッピング
 信頼できる証明書のインポート
 証明書認証プロファイルの設定
 クライアント証明書ベース認証の有効化
 確認
 トラブルシュート

概要

このドキュメントでは、Identity Services Engine(ISE)管理アクセス用にクライアント証明書ベー スの認証を設定する方法について説明します。この例では、ISE管理者がユーザ証明書に対して 認証を行い、Cisco Identity Services Engine(ISE)管理GUIへの管理者アクセスを取得します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- •パスワードおよび証明書認証のためのISE設定。
- Microsoft Active Directory(AD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)/ $(- \vec{v} = 2.6)$
- ・Windows Active Directory(AD)Server 2008リリース2
- •証明書

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響を十分に理解しておいてください 。

設定

このセクションでは、Cisco ISE管理GUIへの管理アクセス用の外部IDとしてクライアント証明書 またはスマートカードを設定します。

ネットワーク図



ISEのActive Directoryへの参加

- 1. Administration > [Identity Management] > [External Identity Sources] > [Active Directory]。
- 2. Cisco ISEで結合ポイント名とADドメイ**ンを持つActive Directory**イン**スタンスを**作成します。
- 3. [Submit] をクリックします。



4. プロンプトで、すべてのノードに適切なユーザ**名とパ**スワードを追加します。

ciaco Identity Services Engine Home I	ontext Visibility + Operations + Policy	Administration > Work Centers		License Warning 🔺	् 6	0	- ¢					
System Identity Management Network	sources	ervices										
+ Identities Groups External Identity Sources	Identities Groups External Identity Sources Identity											
Esternal Identity Sources	Connection Whitelisted Domains * Join Point Name AD * Active Directory Domain mydomain.com	PassiveID Groups Attributes	Advanced Settings				*					
COBC COBC	Join of Leave Viest User ODiagnostic Tool	Remesti i able	014									
RADIUS Token	ise2.mydomain.com STANDALC	ONE Operational WIN-58UQFTHFNIP.myd	omai Default-First-Site-Name									
🥁 svélu la providers 🚰 Social Login	Join Domain Please specify the crede * AD Use * © Specify Organization © Store Crede	entials required to Join ISE node(©) to the Active Directory r Name ⊕ [P assword al Unit ⊕ fentials ⊕	Domain.									

5. [Save] をクリックします。

ディレクトリ グループの選択

- 1. 外部の管理者グループを作成し、Active Directoryグループにマッピングします。
- 2. Administration >[Identity Management] > [External Identity Sources] > [Active Directory] > [Groups] > [Select Groups from Directory]。
- 3. 管理者が属する少なくとも1つのADグループを取得します。

es	Identity Source Sequences + Settings			
	Select Directory Groups		×	
	This dialog is used to select groups from the Directory.			
	Domain mydomain.com	*		
	Name Filter *ISE-* SID Filter *	Type Filter ALL	· ·	
	Retrieve Groups 2 Groups Retrieved.			
	C 🔽 Name 🔺 G	Froup SID	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	

4. [Save] をクリックします。

管理アクセスのためのActive Directoryパスワードベース認証の有効化

- 1. Active Directoryインスタンスを、以前にISEに参加したパスワードベースの認証方式として 有効にします。
- 2. 図に示すように、[Administration > [System] > [Admin access] > [Authentication]を選択しま す。

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Povice Portal Management pxGrid Services 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 * Identity Source AD:AD *
 Settings 	
	O Client Certificate Based
	Save Reset

3. [Save] をクリックします。

注:証明書ベースの認証を有効にするには、パスワードベースの認証設定が必要です。証明

書ベースの認証を正常に設定した後、この設定を元に戻す必要があります。

外部IDグループの管理グループへのマッピング

この例では、外部ADグループがデフォルトのAdminグループにマッピングされています。

- 1. [Administration] > [System] > [Admin Access] > [Administrators]の順に選択します。[Admin Groups] > [Super admin]。
- 2. [Type]を[External]に選択し、[External groups]の下のADグループを選択します。

cisco Identity Services Engine	Home + Context Visibility	Operations Policy	→Administration → Wor	k Centers	L	icense W
▼ System → Identity Management	Network Resources Dev	vice Portal Management p×Grid	Services + Feed Service	▶ Threat Centric NAC		
Deployment Licensing + Certifi	ates ⊧Logging ⊧Mainten	nance Upgrade ⊧Backupℜ	estore •Admin Access	 Settings 		
Authentication Authorization	Admin Groups > System Adm Admin Group * Name Syste	nin em Admin				
▼ Administrators	Description Acces	ss permission for Operations tab. Incl	udes System and data access	permission for Admin Gr	oups. //	
Admin Users	Type 🗹 Ext	ternal				
Admin Groups	External Identity Source					
 Settings 	Name : AD					
	🕂 Add 👻 🗙 Delete				·	
	Status	Email Usernan	ne First Name	e Last Name		
	Save Reset			No data ava	ilable	

- 3. [Save] をクリックします。
- 4. Administration > System > Admin Access > Administrators > Admin Groups > Read Only Adminの順に選択します。
- 5. 図に示すように、[Type]**に[External]**を選択し、[**External groups]の下の**ADグループを選択し ます。

cisco Identity Services Engine	Home	ibility + Operations	▶ Policy ▼Adminis	tration 🔹 Work Cen	nters		License W
▼System → Identity Managemen	t 🕨 Network Resources	Device Portal Manag	ement p×Grid Services	Feed Service	Threat Centric NAC		
Deployment Licensing + Certif	icates ⊧Logging ⊧N	laintenance Upgrade	▶ Backup & Restore 💌	Admin Access + Sett	tings		
Authentication + Authorization	Admin Groups > Read Admin Group * Name	Only Admin Read Only Admin					
▼ Administrators	Description	Access Permission for ac	min with read-only functiona	lity		1	
Admin Users	Type	External	,	,			
Admin Groups	Schemel Identify Cours	External					
) Settings	Name : AD	je					
	▼ External Groups	Ð					
	* I mydomain.com	/Users/ISE-RO 🛛 😔 🕂					
	Member Users						
	🕂 Add 👻 🗙 Delete						
	Status	🕳 Email	Username	First Name	Last Name		
					No data availa	ble	
	Save Reset						

6. [Save] をクリックします。

信頼できる証明書のインポート

- 1. クライアント証明書に署名する認証局(CA)証明書をインポートします。
- 2. 選択 Administrator > System > Certificates > Trusted Certificate > Import.
- 3. [browse]をクリックし、CA証明書を選択します。
- 4. 図に示すように、[Trust for client authentication and Syslog]チェックボックスをオンにしま す。

diale Identity Services Engine	Home → Context Visibility → Operations → Policy ▼Administration → Work Centers	License Warning 🔺	٩,	0 0) (
System → I dentify Management → Network Resources → Device Portal Management pxOrid Services → Feed Service → Threat Centric NAC											
Deployment Licensing -Certificates +Logging +Maintenance Upgrade +Backup&Restore +AdminAccess +Settings											
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests	Import a new Certificate into the Certificate Store * Certificate File Choose File DCcomDCmymainWpem Friendly Name Tusted For: ① Tusted For: ①										
Certificate Periodic Check Setti Certificate Authority	Trust for authentication within ISE Trust for client authentication and Syslog Trust for authentication of Cisco Services Validate Certificate Extensions										
	Description Submit Cancel										

5. [Submit] をクリックします。

証明書認証プロファイルの設定

1. クライアント証明書ベース認証用の証明書認証プロファイルを作成するには、 [Administration] > [Select]を選択します[Identity Management] > [External Identity Sources] > [Certificate Authentication Profile] > [Add]を選択します。

- 2. プロファイル名を追加します。
- 3. 証明書属性の管理者ユーザ名を含む適切な属性を選択します。
- ユーザのADレコードにユーザの証明書が含まれ、ブラウザから受信した証明書をADの証明書と比較する場合は、[Always perform binary comparison]チェックボックスをオンにして、 先に指定したActive Directoryインスタンス名を選択します。

clash 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
Identities Groups External Identity Sources	Identity Source Sequences + Settings
Identities Groups External Identity Sources External Identity Sources Certificate Authentication Profile AD DDAP ODBC RADIUS Token RSA SecurID SAML Id Providers Social Login	Identity Source Sequences
	Use Identity From 💿 Certificate Attribute Subject Alternative Name - Other Name 🝷 🛈
	O Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) 🕡
	Match Client Certificate Against Certificate In Identity Store 🕧 💿 Never
	 Only to resolve identity ambiguity
	Always perform binary comparison
	Submit Cancel

5. [Submit] をクリックします。

注:同じ証明書認証プロファイルをエンドポイントのIDベースの認証にも使用できます。

クライアント証明書ベース認証の有効化

1. 選択 [Administration] > [System] > [Admin Access] > [Authentication] > [Authentication Method Client Certificate Based]。

cisco Identity Services Engine	Home → Context Visibility → Oper	ations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal N	danagement 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
Ø	Authentication Method	nodes. This will result in significant downtime for the system.
Authentication	Authentication Type	Cancel
▼ Administrators	O Password Based	S Identity Source (AD-AD)
Admin Users		Identity Source Net Net :
Admin Groups	Client Certificate Based	
Settings		
	Save Reset	

- 2. [OK] をクリックします。
- 3. 先ほど設定した証明書認証プロファイルを選択します。
- 4. Active Directoryインスタンス名を選択します。

disco 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 - Admin Access + Settings	
O Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings	
Authorization	Authentication Type	
▼ Administrators Admin Users	O Password Based	
Admin Groups • Settings	Client Certificate Based * Certificate Authentication Profile CAC_Login_Profile *	
	* Identity Source AD:AD	
	Save Reset	

- 5. [Save] をクリックします。
- 6. 展開内のすべてのノードのISEサービスが再起動します。

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 The system will now restart.
3 Authentication	Authentication Method
Authorization	Authentication Type
▼ Administrators	O Password Based
Admin Users	
Admin Groups	Client Catificate Based
 Settings 	* Certificate Authentication Profile CAC_Login_Profile
	* Identity Source AD:AD T
	Save Reset



Application Serverサービスのステータスが**Running**に変わった後**に**、ISE GUI**へのア**クセスを確認 します。

スーパー管理者ユーザ:ISE GUIにログインするための証明書の選択を求めるプロンプトが表示 され、証明書がスーパー管理者外部IDグループのユーザ部分の場合はスーパー管理者権限が付与 されることを確認します。

C S Maiting for ise2.mydomain... ×





Read-only Admin User: ISE GUIにログインするための証明書の選択を求めるプロンプトが表示さ

れ、証明書がRead-only Admin External Identityグループのユーザ部分の場合は、Read-only Admin権限が付与されることを確認します。

Attps://ise2.mydomain.com/

P - × ○ Waiting for ise2.mydomain... ×



() (https://ise2.mydomain.com/admin/						,P − í	🔒 🖒 🏉 Identity	Services Engine ×				ሰ ደ	7 🛱 1
alı cıs	dentity Servi	ces Engine	Home	▶ Context Visibility	 Operations 	▶ Policy	Administration	 Work Centers 	Aread-O	lly License Warning 🔺	٩		• ^
	Summary	Endpoints	Guests	Vulnerability	Threat	+						\$	-
	METRICS											- ø	
	<	Total Endpo	oints	0	Active Endpoi	nts 🛛		lejected Endpoints ()	0	nomalous Behavior 🖲	0	>	
	Identity Store Identity Group Network Device Failure Reason		Failure Reason	III NETWORK DEVICES I Image: Constraint of the second se			ENDPOINTS Type Profile			σx			
		No data a	vailable.		No data available. No data available.								
	# BYOD EN	IDPOINTS (>	ΒQΧ	# ALAR	MS 🛛		eσx	# SYSTEM S	JMMARY [©]	ø	σx	
	Type Profile				Severity	Name	0	ccu Last Occi	1 node(s)		All -	24HR -	
		No data a	vailable.		V				🗹 📄 ise2				~

注: Common Access Card(CAC)が使用中の場合、ユーザが有効なスーパーピンを入力する と、スマートカードはユーザ証明書をISEに提示します。

トラブルシュート

1. application start ise safeコマンドを使用して、Cisco ISEを安全モードで起動します。これに

より、管理ポータルへのアクセス制御を一時的に無効にし、設定を修正し、application stop iseコマンドを使用してISEのサービスを再起動できます.

 [safe]オプションを使用すると、管理者が誤ってすべてのユーザのCisco ISE Adminポータル へのアクセスをロックアウトした場合の回復方法が提供されます。このイベントは、管理者 が[Administration] > [Admin Access] > [Settings] > [Access]ページで誤ったIPアクセスリスト を設定した場合に発生することがあります。safeオプションは証明書ペースの認証をバイパ スし、Cisco ISE Adminポータルにログインするためのデフォルトのユーザ名とパスワード 認証に戻ります。