H3Cアクセスコントローラ

Cisco ISEサーバーによるアクセス認証の設定例

Copyright©2022 New H3C Technologies Co.,Ltd.無断転載を禁ず。 本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の承諾なく、いかなる形式または手段によっても複 製または譲渡することはできません。 New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登

録商標です。 このドキュメントの情報は、予告なしに変更されることがあります。

内容

Cisco ISEサーバーによるアクセス認証の設定例	1
はじめに	
使用されているソフトウェアバージョン	
例:Cisco ISEベースの802.1X PEAP認証の設定	
ネットワーク構成	
手順	
 設定の確認	9
構成ファイル	
dot1x authentication-method eap	
例:Cisco ISEベースのMAC認証の設定	
ネットワーク構成	
手順	
設定の確認	
構成ファイル	
例:Cisco ISEベースのポータル認証の設定	
ネットワーク構成	
制約事項とガイドライン	
手順	
設定の確認	
構成ファイル	
ネットワーク構成	
手順	
設定の確認	
構成ファイル	

はじめに

次に、Cisco ISEサーバーを使用して無線クライアントを認証するようにH3Cアクセスコントローラを設定 する例を示します。この例には、Cisco ISEベースの802.1X認証、MAC認証、ポータル認証、および SSHログインHWTACACS認証の設定が含まれます。

使用されているソフトウェアバージョン

次の設定例が作成され、次のハードウェアおよびソフトウェアバージョンで確認されています。

- 2.3.0.298を実行しているCisco ISEサーバー。
- R5428以降を実行しているH3Cアクセスコントローラ。

例:Cisco ISEベースの802.1X PEAP認証の設 定

ネットワーク構成

図1に示すように、APはスイッチを介してACに接続され、クライアントはAPを介してワイヤレスネットワークにアクセスします。

次の要件を満たすようにデバイスとサーバーを設定します。

- クライアントがワイヤレスネットワークにアクセスするには、802.1X PEAP認証を通過する必要があります。
- クライアントが802.1X PEAP認証を通過すると、ISEサーバーはクライアントに認可ACLと認可 VLANを割り当てます。

図1 ネットワーク図



手順

()重要:

この設定例では、Cisco ISEサーバーでの802.1X認証によるクライアントの認証に関連する主な設定だけを示します。ネットワーク接続設定の詳細については、デバイスおよびサーバーのマニュアルを参照してください。

デバイスとサーバーがネットワーク接続されていることを確認します。

ACの 設定

- EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。
 <AC> system-view
 [AC] dot1x authentication-method eap
- 2. RADIUSスキームを設定します。

RADIUS scheme iseを作成します。

[AC] radius scheme ise

#8.1.1.18にあるISEサーバーをプライマリ認証サーバーとして指定し、サーバーとの安全な通信の ための共有キーを指定します。共有キーが、ISEサーバーで構成されている共有シークレットと同じ であることを確認してください。

[AC-radius-ise] primary authentication 8.1.1.18 key cipher \$c\$3\$FpBySjKd6TF17QmPAQ83vNM+mNuZHUw=

#ISEサーバーに送信されるユーザー名からドメイン名を除外します。

[AC-radius-ise] user-name-format without-domain

#ISEサーバーに送信されるRADIUSパケットのNAS IPアドレスとして191.120.1.56を指定します。 NAS IPアドレスが、ISEサーバーでACに対して指定されたものと同じであることを確認します。 [AC-radius-ise] nas-ip 191.120.1.56

[AC-radius-ise] quit

3. ISPドメインを構成します。

#ISPドメインiseを作成します。

[AC] domain ise

#LANユーザーの認証と認可にRADIUSスキームiseを使用するようにISPドメインを設定します。 [AC-isp-ise] authentication lan-access radius-scheme ise [AC-isp-ise] authorization lan-access radius-scheme ise [AC-isp-ise] quit

4. サービステンプレートを構成します。

#サービステンプレートiseを作成します。

[AC] wlan service-template ise

#サービステンプレートのSSIDを000AAA-MACAUに設定します。

[AC-wlan-st-ise] ssid 000AAA-MACAU

#サービステンプレートを介してオンラインになるクライアントをVLAN 71に割り当てます。

[AC-wlan-st-ise] vlan 71

#AKMモードを802.1Xに設定します。

[AC-wlan-st-ise] akm mode dot1x

#AES-CCMP暗号スイートを指定し、ビーコンおよびプローブ応答でRSN IEをイネーブルにします。

[AC-wlan-st-ise] cipher-suite ccmp

[AC-wlan-st-ise] security-ie rsn

#認証モードを802.1X認証に設定し、認証ドメインiseを指定します。 [AC-wlan-st-ise] client-security authentication-mode dot1x

[AC-wlan-st-ise] dot1x domain ise

#サービステンプレートを有効にします。 [AC-wlan-st-ise] service-template enable

[AC-wlan-st-ise] quit

5. 手動APを設定します。

```
#axという名前のAPを設定し、そのモデルとシリアルIDを指定します。
[AC] wlan ap ax model WA6528
```

[AC-wlan-ap-ax] serial-id 219801A1LH8188E00011

#radio 1を有効にし、サービステンプレートiseを無線にバインドします。 [AC-wlan-ap-ax] radio 1 [AC-wlan-ap-ax-radio-1] radio enable [AC-wlan-ap-ax-radio-1] service-template ise [AC-wlan-ap-ax-radio-1] quit [AC-wlan-ap-ax] quit

- 高度なACL 3100と、クライアントが8.1.1.5にアクセスすることを拒否する規則を設定します。 [AC] acl advanced 3100 [AC-acl-ipv4-adv-3100] rule 1 deny ip destination 8.1.1.5 0 [AC-acl-ipv4-adv-3100] guit
- 7. 許可VLANを設定します。

#VLAN 4094およびVLAN-interface 4094を作成し、VLANインターフェイスにIPアドレスを割り当 てます。 [AC] vlan 4094 [AC-vlan4094] quit [AC] interface vlan-interface 4094 [AC-Vlan-interface4094] ip address 191.94.0.1 24

[AC-Vlan-interface4094] quit

#vlan4094のDHCPアドレスプールvlan4094を設定します。 [AC] dhcp server ip-pool vlan4094 [AC-dhcp-pool-vlan4094] network 191.94.0.0 mask 255.255.255.0 [AC-dhcp-pool-vlan4094] gateway-list 191.94.0.1 [AC-dhcp-pool-vlan4094] dns-list 191.94.0.1

[AC-dhcp-pool-vlan4094] quit

ISEサーバーの構成

- 1. ユーザーグループを作成します。
 - a. トップナビゲーションバーでAdministration > Identity Management > Groupsを選択します。
 - b. 左側のナビゲーションペインで、User Identity Groupsを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をLDFに設定します。
 - e. Submitをクリックします。

図2 ユーザーグループの作成

dentity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۹. 😝
System Identity Management Network R Identities Groups External Identity Sources	kesources		
Identity Groups Image: Compart Lendty Lendty Lendty Image: Compart Lendty Image: Comp	Use Identify Groups > New User Identify Group *Name LDP × Description		

- 2. ネットワークアクセスユーザーを作成します。
 - a. 上部ナビゲーションバーで、Administration > Identity Management > Identitiesを選択しま す。
 - b. 左側のナビゲーションペインで、Usersを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をldf00001に、パスワードをLdf123456に設定し、ユーザーをユーザ ーグループLDFにバインドします。

パスワードに大文字、小文字、および数字が含まれていることを確認します。

e. Submitをクリックします。

図3 ネットワークアクセスユーザーの作成

dentity Services Engine Hon	me Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	
System ✓ Identity Management Net	twork Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC		
- Identities Groups External Identity Sol	urces Identity Source Sequences		
•	laturati Aranan Harri Latu Men Metersek Arana Harr		
Users	emula Autoso Usera Las 2 new network Autoso User * Network Auroso Hisor		
Latest Manual Network Scan Results			
	Name dououu		
	Status Enabled •		
	Email		
	▼ Passwords		
	Password Type: Internal Users v		
	Password Re-Enter Password		
	* Login Password Generate Password (i)		
	Enable Password		
	▼ User Information		
	First Name		
	Last Name		
	Account Options		
	Account Disable Policy		
	▼ User Groups		
	LDF 📀 🕂		
	Submit Cancel		

- 3. ACをネットワークアクセスデバイスとしてサーバーに追加します。
 - a. 上部のナビゲーションバーで、Administration > Network Resources > Network Devicesを選択します。
 - b. Addをクリックします。
 - c. 名前をACに設定し、IPアドレス191.120.1.56を指定して、RADIUS Authentication Settingsを選択し、共有秘密をH3ccに設定します。

IPアドレスがAC上のRADIUSパケットのNAS IPアドレスと同じであることを確認します。 共有秘密がACIに設定された共有キーと同じであることを確認します。

d. 設定を保存します。

図4 サーバーへのAC電源の追加

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🛕 🔍 📵 💿 🌣
System Identity Management	Network Resources Herice Portal Management pxGrid Service Feed Service Threat Centric NAC	
Network Devices Network Device 0	Sroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
0	Notwork Devices Lists an	
Network Devices	Network Devices	
Default Device	* Nome AC	
Device Security Settings	Description	
	IP Address * * IP : 191.120.1.56 / 32	@ .
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected	
	* Device Profile data Olsco 💌 🕀	
	Model Name 💌	
	Software Version	
	* Naturni: Davisa Grain	
	Televis Corosp	
	Location All Locations Set. To Default	
	IPSEC No Set To Default	
	Device Type All Device Types 📀 Set To Default	
	✓ RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	

- 4. 認証プロトコルを設定します。
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Results を選択します。
 - b. 左側のナビゲーションペインで、Authentication > Allowed Protocolsを選択します。
 - **c. 1xという**名前の許可されたプロトコルサービスを作成し、**Allow EAP-TLS**およびAllow PEAPを選択します。
 - d. 設定を保存します。

図5 許可されたプロトコルサービスの作成

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	0	0	
Policy Sets Profiling Posture C	lient Provisioning Policy Elements				
Dictionaries + Conditions - Resul	15				
Authentication	Allowed Protocols Services List > New Allowed Protocols Service Allowed Protocols				
Allowed Protocols	Name 1x				
Authorization	Description				
Profiling					
	Allowed Protocols				
▶ Posture	Authentication Bypass				
Client Provisioning	Process Host Lookup (j)				
	Authentication Protocols				
	Allow PAP/ASCII				
	Allow CHAP				
	Allow MS-CHAPv1				
	Allow MS-CHAPv2				
	Allow EAP-MD5				
	Allow EAP-TLS				
	Allow LEAP				
	Allow PEAP				
	Allow EAP-FAST				
	Allow EAP-TTLS				
	Preferred EAP Protocol LEAP				

- 5. 許可ACLの設定:
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
 - b. 左側のナビゲーションペインで、Authorization > Authorization Profilesを選択します。
 - c. Addをクリックします。
 - d. Authorization Profile領域で、名前をacl_3100に設定し、Network Device Profileフィー

ルドからCiscoを選択します。Advanced Attributes Settings領域で、アトリビュート Radius:Filter-IDを選択し、アトリビュート値を3100(ACL番号)に設定します。

e. 設定を保存します。

図6 認可ACLの設定

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🕓	2 0 0 0
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements		
Dictionaries + Conditions - Result			
0	Authorization Profiles > ad_3100		
Authentication	Authorization Profile		
- Authorization	* Name acL_3100 Description		
Authorization Profiles			
Downloadable ACLs	* Access Type ACCESS_ACCEPT *		
▶ Profiling	Network Device Profile and Cisco V 🕒		
Posture	Service Template		
Client Provisioning	Track Movement		
	Passive Identity Tracking 🗌 🕖		
	▶ Common Tasks		
	▼ Advanced Attributes Settings		
	Radus-Filter-ID ◯ = 100 = +		
	▼ Attributes Details		
	Access Type = ACCESS_ACCEPT Filter-ID = 3100		

- 6. 許可VLANの設定:
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
 - b. 左側のナビゲーションペインで、Authorization > Authorization Profilesを選択します。
 - c. Addをクリックします。
 - Authorization Profile領域で、名前をvlan_4094に設定し、Network Device Profileフィ ールドからCiscoを選択します。Custom Tasks領域で、VLANオプションを選択し、 ID/Nameフィールドに4094と入力します。
 - e. 設定を保存します。

図7 認可VLANの設定

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	٩	0	• •
Policy Sets Profiling Posture C	ient Provisioning Policy Elements				
Dictionaries + Conditions - Result	5				
0	Authorization Profiles > vlan 4094				
Authentication	Authorization Profile				
- Authorization	* Name [klan_4004 ×				
Authorization Profiles	Description				
Downloadable ACLs					
Profiling	* Access Type ACCESS_ACCEPT *				
Posture	Network Device Profile 🛛 📾 Cisco 🔹 🕀				
Client Provisioning	Service Template				
	Track Movement				
	Passive Identity Tracking				
					~
	✓ VLAN Tag ID 1 Edit.Tag ID/Name 4094				
	Voice Domain Permission				
	Web Redirection (CWA, MDM, NSP, CPP)				
	Auto Smart Port				~

- 7. 認証および認可ポリシーセットを設定します。
 - a. トップナビゲーションバーで、Policy > Policy Setsを選択します。

- b. Policy Setsの下にあるプラスアイコン+をクリックします。
- c. ポリシーセット名を1xに設定します。条件名を1xに設定し、条件としてWired_Dot1xまたはWireless Dot1xを選択し、Allowed Protocols/Server Sequenceリストから1xを選択します。

|--|

Policy Sets		Réset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
⊘ tx	E tx	tx * * + 1 🗘 >
Default Default Default		Default Network Access × + 2 🗘 🕻

- d. 認証および認可ポリシーセットのViewカラムにあるアイコンをクリックします。
- e. Authorization Policy領域で、acl_vlanという名前の認可ポリシーを追加します。認可 ポリシーのResults > Profilesカラムで、プロファイルacl_3100およびvlan_4094を選択 します。

	ala tata	otă: Con	it on Engine			_							
- C	Policy Se	ts Profil	ices Engline Home	Context Visibility Operations	* Policy	Administration	 Work Centers 			License Warning 🔺	٩	Θ	• •
	oncy de	e	1X	rooming Proncy crements	🖬 1x					Lietault Network Access	×	Т	0
-	✓ Authe	entication	Policy (1)										
	(\bullet)	Status	Rule Name	Conditions						Use		Hits	Actions
							+						
		-								All_User_ID_Stores	× *		
		0	Default							> Options		0	¢
	Authorization	prization F	Policy - Local Exceptions										
1	Autho	prization F	olicy - Global Exception	5									
	✓ Author	orization F	Policy (2)										
								Results					
	+	Status	Rule Name	Conditions				Profiles		Security Groups		Hits	Actions
		Ø	acl_vlan	tx 1x				×acl_3100 ×vtan_4094	+	Select from list	+	0	٥
		0	Default					× DenvAccess	+	Select from list *	+	0	ò
		9	C. C. Galari										*

図9 許可ポリシーの構成

f. 設定を保存します。

設定の確認

1. 上部のナビゲーションバーで、Operations > RADIUS > Live Logsを選択します。オ ンラインクライアントのライブログ情報を表示します。

図10 オンラインクライアントのライブログ情報の表示

deale Identity Services Engine	Home + Conte	oxt Visibility	· Operations	Policy Admin	istration + Work Centers	6				License Warnin	a 🗛 😐	0 0
RADIUS Threat-Centric NAC Live	ve Logs + TACACS	+ Troublesh	hoot + Adaptive	Network Control Repo	orts							
Live Logs Live Sessions												
Misc	configured Supplicants	0	Misconfigured	Network Devices 0	RADIUS Dro	ps O	Client Stopp	ed Responding C	9	Repeat Counter 0		
	0			0	0			0		3		
								Refresh Never	v	how Latest 20 records] Within Last 3 hou	rs 💟
C Refresh O Reset Repeat Co	unts										▼ Fib	er• •••
Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorizati	IP Address	Network Device	Device P
×	~									v		
Sep 14, 2019 08:58:36 426 AN	•	à	0	10100001	88:D7:AF:12:42:EB	Unknown	1x >> Default	1x >> acl_vlan	acl_3100,vla			01000000
Sep 14, 2019 08:58:36.426 AM		0		ldf00001	88:D7:AF:12:42:EB	Unknown	1x >> Default	1x >> acl_vlan	acl_3100,vla		AC	01000000

トップナビゲーションバーで、Operations > RADIUS > Live Sessionsを選択します。オンラインクラ イアントのライブセッション情報を表示します。

図11 オンラインクライアントのライブセッション情報の表示

disto Identi	ity Services Engine	Home Context Visibili	y • Operations	Policy	Administration 🔹 🕨					Licer	nse Warning 🔺 🔍	e 0
▼ RADIUS	Threat-Centric NAC Live	Logs + TACACS + Trou	eleshoot + Adapti	ve Network Control	Reports							
Live Logs	Live Sessions											
									Refresh Every 1 minute	Show Latest 2	20 records 💌 Within	Last 24 hours 🔽
2 Refresh												▼ Filter • • • •
Initial	ted	Updated	Session S	Action	Endpoint ID	Identity	Server	Auth Met	Authentication Protocol	Authentication	Authorization Policy	Authorization Pr
Sep 1	4, 2019 08:58:36.426	Sep 14, 2019 08:58:36.426 AM	Authenticated	Show CoA Actions	B8:D7:AF:12:42:EB	ldf00001	ISE	dot1x	PEAP (EAP-MSCHAPv2)	1x >> Default	1x >> acl_vlan	acl_3100,vlan_409
Sep 1	4, 2019 08:47:55.629	Sep 14, 2019 08:47:55.629 AM	Authenticated	Show CoA Actions	E8:E8:87:98:43:8D	Idf00001	ISE	dot1x	PEAP (EAP-MSCHAPv2)	1x >> Default	1x >> acl_vlan	aci_3100,vlan_409
<												>
Last Update	d: Sat Sep 14 10:54:27 U	TC+0800 2019										Records Shown: 2

構成ファイル

```
#
vlan 4094
#
dhcp server ip-pool vlan4094
  network 191.94.0.0 mask 255.255.255.0
  gateway-list 191.94.0.1
  dns-list 191.94.0.1
#
interface vlan-interface 4094
  ip address 191.94.0.1 24
#
acl advanced 3100
  rule 1 deny ip destination 8.1.1.5 0
#
radius scheme ise
  primary authentication 8.1.1.19 key cipher
  $c$3$FpBySjKd6TF17QmPAQ83vNM+mNuZHUw=
  user-name-format without-domain
  nas-ip 191.120.1.56
#
domain ise
  authentication lan-access radius-scheme ise
  authorization lan-access radius-scheme ise
#
wlan service-template ise
  ssid 000AAA-MACAU
  vlan 71
  akm mode dot1x
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode dot1x
  dot1x domain ise
  service-template enable
#
wlan ap ax model WA6528
  serial-id 219801A1LH8188E00011
  radio 1
  radio enable
  service-template ise
#
```

dot1x authentication-method eap

例:Cisco ISEベースのMAC認証の設定

ネットワーク構成

図12に示すように、APはスイッチを介してACに接続され、クライアントはAPを介してワイヤレスネットワークにアクセスします。

クライアントのネットワークリソースへのアクセスを制御するには、次の要件を満たすようにデバイスとサ ーバーを設定します。

- クライアントがワイヤレスネットワークにアクセスするには、MAC認証を通過する必要があります。
- クライアントとAPは、PSK AKMモードを使用して、両者間のデータパケットを保護します。
- クライアントがMAC認証を通過すると、ISEサーバーは許可ACLと許可VLANをクライアントに割り 当てます。

図12 ネットワーク図



手順

()重要:

この設定例では、Cisco ISEサーバーでのMAC認証によるクライアントの認証に関連する主な設定だけを説明します。ネットワーク接続設定の詳細については、デバイスおよびサーバーのマニュアルを参照してください。

デバイスとサーバーがネットワーク接続されていることを確認します。

ACの設定

1. RADIUSスキームを設定します。#RADIUSスキームを作成します。

<AC> system-view [AC] radius scheme ise #8.1.1.18にあるISEサーバーをプライマリ認証サーバーとして指定し、サーバーとの安全な通信の ための共有キーを指定します。共有キーが、ISEサーバーで構成されている共有シークレットと同じ であることを確認してください。

[AC-radius-ise] primary authentication 8.1.1.18 key cipher \$c\$3\$FpBySjKd6TF17QmPAQ83vNM+mNuZHUw= #ISEサーバーに送信されるユーザー名からドメイン名を除外します。

[AC-radius-ise] user-name-format without-domain

#ISEサーバーに送信されるRADIUSパケットのNAS IPアドレスとして191.120.1.56を指定します。 NAS IPアドレスが、ISEサーバーでACに対して指定されたものと同じであることを確認します。 [AC-radius-ise] nas-ip 191.120.1.56

[AC-radius-ise] quit

2. ISPドメインを構成します。

#ISPドメインiseを作成します。

[AC] domain ise

#ユーザー認証と認可のデフォルト方式としてRADIUSスキームiseを使用するようにISPド メインを設定します。

[AC-isp-ise] authentication default radius-scheme ise [AC-isp-ise] authorization default radius-scheme ise

[AC-isp-ise] quit

3. サービステンプレートを設定します。

#サービステンプレートisemac2を作成します。

[AC] wlan service-template isemac2

#サービステンプレートのSSIDを指定します。

[AC-wlan-st-isemac2] ssid 000AAAMACAU-MAC-CCMP-WPA

#サービステンプレートを介してオンラインになるクライアントをVLAN 71に割り当てます。

[AC-wlan-st-isemac2] vlan 71

#PSK AKMモードを設定し、PSKを指定します。

[AC-wlan-st-isemac2] akm mode psk

[AC-wlan-st-isemac2] preshared-key pass-phrase cipher

\$c\$3\$XYqokG6l8YoOymuklyvxoJuzFoB+oVJD6exoqw==

#AES-CCMP暗号スイートを指定し、ビーコンおよびプローブ応答でRSN IEをイネーブルにします。

[AC-wlan-st-isemac2] cipher-suite ccmp

[AC-wlan-st-isemac2] security-ie rsn

#アクセス認証モードをMAC認証に設定し、認証ドメインiseを指定します。

[AC-wlan-st-isemac2] client-security authentication-mode mac

[AC-wlan-st-isemac2] mac-authentication domain ise

#サービステンプレートを有効にします。

[AC-wlan-st-isemac2] service-template enable

[AC-wlan-st-isemac2] quit

4. 手動APを設定します。

#axという名前のAPを設定し、そのモデルとシリアルIDを指定します。 [AC] wlan ap ax model WA6528

[AC-wlan-ap-ax] serial-id 219801A1LH8188E00011

#APのVLAN 1を指定します。

[AC-wlan-ap-ax] vlan 1

#radio 1を有効にし、サービステンプレートisemac2を無線にバインドします。 [AC-wlan-ap-ax] radio 1 [AC-wlan-ap-ax-radio-1] radio enable [AC-wlan-ap-ax-radio-1] service-template isemac2 [AC-wlan-ap-ax-radio-1] guit [AC-wlan-ap-ax] quit

- 高度なACL 3100と、クライアントが8.1.1.5にアクセスすることを拒否する規則を設定します。 [AC] acl advanced 3100
 [AC-acl-ipv4-adv-3100] rule 1 deny ip destination 8.1.1.5 0
 [AC-acl-ipv4-adv-3100] guit
- 6. 許可VLANを設定します。

#VLAN 4094およびVLAN-interface 4094を作成し、VLANインターフェイスにIPアドレスを割り当 てます。 [AC] vlan 4094 [AC-vlan4094] quit [AC] interface vlan-interface 4094 [AC-Vlan-interface4094] ip address 191.94.0.1 24

[AC-Vlan-interface4094] quit

#vlan4094のDHCPアドレスプールvlan4094を設定します。 [AC] dhcp server ip-pool vlan4094 [AC-dhcp-pool-vlan4094] network 191.94.0.0 mask 255.255.255.0 [AC-dhcp-pool-vlan4094] gateway-list 191.94.0.1 [AC-dhcp-pool-vlan4094] dns-list 191.94.0.1 [AC-dhcp-pool-vlan4094] guit

ISEサーバーの構成

- 1. ユーザーグループを作成します。
 - a. トップナビゲーションバーで、Administration > Identity Management > Groupsを選択しま す。
 - b. 左側のナビゲーションペインで、User Identity Groupsを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をLDFに設定します。
 - e. Submitをクリックします。

図13 ユーザーグループの作成

Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۲
System Identity Management Network	Resources		
Identities Groups External Identity Sources	Identity Source Sequences + Settings		
Identity Groups Image: Control Series Control Contro Control Control Control Control Control Control Control Control	User Identify Group *Name DFF		

- 2. ネットワークアクセスユーザーを作成します。
 - a. 上部ナビゲーションバーで、Administration > Identity Management > Identitiesを選択しま す。
 - b. 左側のナビゲーションペインで、Usersを選択します。
 - c. Addをクリックします。

d. 開いたページで、名前をldf00001に、パスワードをLdf123456に設定し、ユーザーをユーザ ーグループLDFにバインドします。

パスワードに大文字、小文字、および数字が含まれていることを確認します。

e. Submitをクリックします。

図14 ネットワークアクセスユーザーの作成

dentity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🔍 🐵
System Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC	
- Identities Groups External Identi	ty Sources Identity Source Sequences	
•	Network Access Users List > New Network Access User	
Users	Network Access User	
Latest Manual Network Scan Results	* Name df000001	
	Status 🔽 Enabled 👻	
	Email	
	▼ Passwords	
	Password Type: Internal Users +	
	Password Re-Enter Password	
	* Login Password ••••••• • Generate Password (i)	
	Enable Password Generate Password	
	▼ User Information	
	First Name	
	Last Name	
	Account Options	
	Account Disable Policy	
	▼ User Groups	
	LDF 🗢 🕂	
	Submit Cancel	

- 3. ACをネットワークアクセスデバイスとしてサーバーに追加します。
 - a. 上部のナビゲーションバーで、Administration > Network Resources > Network Devicesを選択します。
 - b. Addをクリックします。
 - c. 表示されたページで、名前をACに設定し、IPアドレス191.120.1.56を指定してRADIUS Authentication Settingsを選択し、共有秘密をH3cclこ設定します。
 IPアドレスがAC上のRADIUSパケットのNAS IPアドレスと同じであることを確認します。
 共有秘密がACに設定された共有キーと同じであることを確認します。
 - d. 設定を保存します。

図15 サーバーへのAC電源の追加

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 💿 🌣				
System Identity Management	Network Resources Device Portal Management px/Grid Services Feed Service Threat Centric NAC					
▼ Network Devices Network Device G	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services					
Network Devices	Network Devices List > AC					
Default Device	Network Devices					
Device Security Settings	* Name (AC Description					
	IP Address * 19: 191.120.1.56 / 32	@ .				
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected * Device Profile					
	* Network Device Group					
	Location Al Locations Set. To Default. IPSEC No Set. To Default. Device Type Al Device Types Set. To Default.					
	✓ RADIUS Authentication Settings					
	RADIUS UDP Settings Protocol RADIUS					

4. 認証プロトコルを設定します。

- a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
- b. 左側のナビゲーションペインで、Authentication > Allowed Protocolsを選択します。
- c. mabという名前の許可されたプロトコルサービスを作成します。Authentication Bypass 領域で、Process Host Lookupを選択します。Authentication Protocols領域で、 Allow PAP/ASCIIおよびAllow CHAPを選択します。
- **d.** 設定を保存します。

図16 認証プロトコルの構成

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	License Warning 🔺 🔍 🐵 🚽 🗘
Policy Sets Profiling Posture C	Sent Provisioning + Policy Elements	Click here to do wireless setup and visibility setup Do not show this again.
Dictionaries + Conditions - Resul	15	
0	the set of the set of the set	
✓ Authentication	Allowed Protocols	
Allowed Protocols	Name mab	
+ Authorization	Description	
Profiling		
+ Posture	✓ Allowed Protocols	
Client Provisioning	Authentication Bypass	
	Process Host Lookup (j)	
	Authentication Protocols	
	Allow PAP/ASCII	
	Allow CHAP	
	Allow MS-CHAPv1	
	Allow MS-CHAPv2	
	Allow EAP-MD5	
	Allow EAP-TLS	
	Allow LEAP	
	Allow PEAP	- CE 🖬 🔮
	Allow EAP-FAST	
	Allow EAP-TTLS	
	Preferred EAP Protocol	
	EAP-TLSL-DR ()	

- 5. 許可ACLの設定:
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
 - b. 左側のナビゲーションペインで、Authorization > Authorization Profilesを選択します。
 - c. Addをクリックします。
 - Authorization Profile領域で、名前をacl_3100に設定し、Network Device Profileフィー ルドからCiscoを選択します。Advanced Attributes Settings領域で、アトリビュート Radius:Filter-IDを選択し、アトリビュート値を3100(ACL番号)に設定します。
 - e. 設定を保存します。

図17 認可ACLの設定

dentity Services Engine	Home	Operations Policy		License Warning 🔺 🔍 🐵 🔿 🌣
Policy Sets Profiling Posture C	Client Provisioning Policy Elen	ients		
Dictionaries + Conditions - Result	Its			
0	Authorization Profiles > ad_3	100		
Authentication	Authorization Profile			
- Authorization	* Name	acl_3100		
Automination Destitue	Description			
Authorization Profiles	L			
DOWINDatiable AGES	* Access Type	ACCESS_ACCEPT *		
Profiling	Network Device Profile	ដ Cisco 👻 🕀		
Posture	Popiso Tomplato	1		
Client Provisioning	Track Movement	10		
	Passive Identity Tracking	30		
	Common Tasks			
	 Advanced Attributes 	Settings		
	Radius:Filter-ID	3100	- +	
		0		
	 Attributes Details 			
	Access Type = ACCESS_AC Filter-ID = 3100	LEPT		

- 6. 許可VLANの設定:
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
 - b. 左側のナビゲーションペインで、Authorization > Authorization Profilesを選択します。
 - c. Addをクリックします。
 - d. Authorization Profile領域で、名前をvlan_4094に設定し、Network Device Profileフィ ールドからCiscoを選択します。Custom Tasks領域で、VLANオプションを選択し、 ID/Nameフィールドに4094と入力します。
 - e. 設定を保存します。

図18 認可VLANの設定

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	٩,	0	• •
Policy Sets Profiling Posture Cl	ient Provisioning + Policy Elements				
Dictionaries + Conditions - Result	5				
0	Authorization Profiles > vlan_4094				
Authentication	Authorization Profile				
* Authorization	* Name Man_4094 ×				
Authorization Profiles	Description				
Downloadable ACLs					
Profiling	ACCESS TYPE ACCESS_ACCEPT *				
Posture	Network Device Profile 🛛 📾 Cisco 💌 🕀				
Client Provisioning	Service Template				
	Track Movement				
	Passive Identity Tracking 🗌 🕧				
	Common Tasks Jecurry Group				
	S VLAN Tag ID 1 Edk.Tag. ID/Name 4094				
	Voice Domain Permission				- 1
	Web Redirection (CWA, MDM, NSP, CPP) (j)				
	Auto Smart Port				~

- 7. 認証および認可ポリシーセットを設定します。
 - a. トップナビゲーションバーで、Policy > Policy Setsを選択します。
 - b. Policy Setsの下にあるプラスアイコン+をクリックします。
 - c. ポリシーセット名をmablc設定し、条件名をmablc設定してAllowed Protocols/Server Sequenceリストからmabを選択します。

図19 認証および許可ポリシーセットの構成

cisco Identity	Services Engine Home	Fontext Visibility Ope	rations Policy Administration Work Centers	License Warning 🔺	۹. 0	5 0
Policy Sets Pi	ofiling Posture Client Pro	visioning + Policy Elements		Click here to do wireless setup and visibility setup	Do not show th	s again. ×
Policy Sets					Reset	Save
+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits Action	s View
Search						
0	mab		mab	mab * * +	24 🗘	>
0	tx		🗖 1x	1x * * +	24 0	>
0	Default	Default policy set		Default Network Access * * +	• •	>

d. 条件としてWired_MABまたはWireless_MABを選択します。

図20条件の構成

Con	ditions Studio							0×
Libra	ry		Editor					
Sea	irch by Name				Wireless_MAB			°° *
Q E		O t 🕈		_				۲
	1x		OR ¥		Wired_MAB			
	Catalyst_Switch_Local_Web_Authenticat ion	(1)				+ New AND OR		
	d	0		Set to 'Is	not		Duplicate	Save
	mab	()						

- e. 認証および認可ポリシーセットのViewカラムにあるアイコンをクリックします。
- f. Authorization Policy領域で、Authorization Rule 1という名前の許可ポリシーを追加します。
 許可ポリシーのResults > Profiles列で、プロファイルacl_3100およびvlan_4094を選択します。

	ervices Engine Home	Context Visibility Op	verations · Policy	 Administration 	 Work Centers 			CLicense Warr	ning 🔺 🔍	•	9 0
Policy Sets Pro	fling Posture Client Provision	ing + Policy Elements					Click he	re to do wireless setup and vis	ibility setup Do n	ot show th	is again, >
olicy Sets +	mab									Reset	Savo
Status	Policy Set Name	Description	Conditions					Allowed Prote	ocols / Server S	Sequenci	e Hits
Bearch											
0	mab		🖀 mab					mab		× * +	- 24
Authentication	n Policy (1)										
Authorization	Policy - Local Exceptions										
	Total Clarket Freedom										
 Authorization 	Policy - Global Exceptions										
Authorization Authorization	Policy (2)										
Authorization Authorization	Policy (2)					Results					
Authorization Authorization (+) Status	Policy (2) Rule Name	Conditions				Results Profiles		Security Groups		Hits	Actions
Authorization Authorization (+) Status Search	Policy - Global Exceptions Policy (2) Rule Name	Conditions				Results Profiles		Security Groups		Hits	Actions
Authorization Authorization + Status Search	Policy - Global Exceptions Policy (2) Rule Name Authorization Rule 1	Conditions				Results Profiles (*aci_3100) (*vian_4094)	+	Security Groups		Hits 22	Actions

図21 許可ポリシーの追加

g. 設定を保存します。

設定の確認

- 1. クライアントで、ワイヤレスネットワークに接続し、設定されたユーザー名とパスワードを 入力します(詳細は表示されません)。
- 2. ACで、ユーザーがオンラインになり、サーバーが認可ACLおよびVLANをユーザーに割り当てた ことを確認します。

図22 オンラインユーザー情報の表示

[H3C]dis wlan client ser isemac2	-			
Total number of clients: 1				
MAC address User name		AP name	R IP address	VLAN
e8e8-b79b-438d e8e8b79b438d		ax	1 191.94.0.2	4094
[H3C]dis ma				
[H3C]dis mac-address				
[H3C]dis mac-authentication co				
[H3C]dis mac-authentication conn	iecti	ion		
Total connections: 1				
User MAC address		: e8e8-b79b-438d		
AP name		ax ax		
Radio ID		: 1		
SSID		: 000AAAMACAU-MAC-CCMP	-WPA	
BSSID		: dcda-8004-6362		
Username		: e8e8b79b438d		
Authentication domain		: ise		
Initial VLAN		: 71		
Authorization VLAN		: 4094		
Authorization ACL number		: 3100		
Authorization user profile		: N/A		
Authorization CAR		: N/A		
Authorization URL		: N/A		
Termination action		: N/A		
Session timeout last from		: N/A		
Session timeout period		: N/A		
Online from		: 2019/09/10 18:08:38		
Online duration		: Oh Om 42s		

構成ファイル

```
#
vlan 4094
#
dhcp server ip-pool vlan4094
  network 191.94.0.0 mask 255.255.255.0
  gateway-list 191.94.0.1
  dns-list 191.94.0.1
#
interface vlan-interface 4094
  ip address 191.94.0.1 24
#
acl advanced 3100
  rule 1 deny ip destination 8.1.1.5 0
#
radius scheme ise
  primary authentication 8.1.1.19 key cipher
  $c$3$FpBySjKd6TF17QmPAQ83vNM+mNuZHUw=
  user-name-format without-domain
  nas-ip 191.120.1.56
#
domain ise
  authentication default radius-scheme ise
17
authorization default radius-scheme ise
#
wlan ap ax model WA6528
serial-id 219801A1LH8188E00011
#
wlan service-template isemac2
```

ssid 000AAAMACAU-MAC-CCMP-WPA vlan 71 akm mode psk preshared-key pass-phrase cipher \$c\$3\$XYqokG6I8YoOymuklyvxoJuzFoB+oVJD6exoqw== cipher-suite ccmp security-ie rsn client-security authentication-mode mac mac-authentication domain ise service-template enable # wlan ap ax model WA6528 serial-id 219801A1LH8188E00011 vlan 1 radio 1 radio enable service-template isemac2

例:Cisco ISEベースのポータル認証の設定

ネットワーク構成

図23に示すように、APはスイッチを介してACに接続され、クライアントはAPを介してワイヤレスネットワークにアクセスします。

次の要件を満たすようにデバイスとサーバーを設定します。

- クライアントがワイヤレスネットワークにアクセスするには、直接ポータル認証を通過する必要があり ます。
- ISEサーバーは、ポータルサーバーおよびRADIUSサーバーとして機能します。

図23 ネットワーク図



制約事項とガイドライン

ファイルise_h3c.zipがAC上のストレージメディアのルートディレクトリに保存されていることを確認します。

手順

(!)重要:

この設定例では、Cisco ISEサーバーでのポータル認証によるクライアントの認証に関連する主な設定 だけを示します。ネットワーク接続設定の詳細については、デバイスおよびサーバーのマニュアルを参 照してください。

デバイスとサーバーがネットワーク接続されていることを確認します。

ACの設定

1. ISPドメインを設定します:

#ISPドメインiseを作成します。

<H3C> system-view [H3C] domain ise

#ポータルユーザーの認証、認可、アカウンティングにRADIUSスキームiseを使用するようにISPドメ インを設定します。

[H3C-isp-ise] authentication portal radius-scheme ise [H3C-isp-ise] authorization portal radius-scheme ise

[H3C-isp-ise] accounting portal radius-scheme ise

[H3C-isp-ise] quit

2. RADIUSスキームを設定します。

RADIUS スキーム iseを作成します。

[H3C]radius scheme ise

#100.18.0.200にあるISEサーバーをプライマリ認証およびアカウンティングサーバーとして指定し、 ISEサーバーとの安全な通信のための共有キーを指定します。共有キーが、ISEサーバーで構成 されている共有シークレットと同じであることを確認してください。

[H3C-radius-ise]primary authentication 100.18.0.200 key simple 12345678

[H3C-radius-ise]primary accounting 100.18.0.200 key simple 12345678

#ISEサーバーに送信されるユーザー名からドメイン名を除外します。

[H3C-radius-ise]user-name-format without-domain

3. ポータル認証を設定します。

#ワイヤレスポータルユーザーの自動ログアウトを有効にします。

[H3C] portal user-logoff after-client-offline enable

#サードパーティ認証中にクライアントがアクセスするためのAC上のVLANインターフェイス1000 を指定します。

[H3C] portal client-gateway interface vlan-interface 1000

#AC宛てのパケットを許可します。

[H3C] portal free-rule 2 destination ip 6.6.4.10 255.255.255.255

#RADIUSサーバー宛てのパケットを許可します。

[H3C] portal free-rule 5 destination ip 100.18.0.200 255.255.255.255

#Webサーバーを設定します。

注:

WebサーバーのURLの詳細については、「ISEサーバーの構成」のポータル設定を参照してください。

[H3C] portal web-server ise [H3C-portal-websvr-ise] url https://100.18.0.200:8443/portal/PortalSetup.action?portal=f0ae43f0-7159-11e7-a35 5-005056aba474

[H3C-portal-websvr-ise] server-type ise

#HTTPベースのローカルポータルWebサービスとHTTPSベースのローカルポータルWebサービスを作成します。ローカルポータル認証のデフォルトの認証ページファイルとしてファイル ise_h3c.zipを指定します。ファイルがAC上の記憶域メディアのルートディレクトリに格納されていることを確認します。 [H3C] portal local-web-server http [H3C-portal-local-websvr-http] default-logon-page ise_h3c.zip [H3C] portal local-web-server https [H3C] portal local-web-server https

- [H3C-portal-local-websvr-https] default-logon-page ise_h3c.zip
- サービステンプレートを設定して有効にします。

[H3C] wlan service-template iseportal
[H3C-wlan-st-iseportal] ssid h3c-ise-portal
[H3C-wlan-st-iseportal] portal enable method direct
[H3C-wlan-st-iseportal] portal domain ise
[H3C-wlan-st-iseportal] portal bas-ip 6.6.4.10
[H3C-wlan-st-iseportal] portal apply web-server ise
[H3C-wlan-st-iseportal] service-template enable

[H3C-wlan-st-iseportal] quit

 手動APを設定し、サービステンプレートをAPのradio 1にバインドします。 [H3C] wlan ap ap1 model WA6330 [H3C-wlan-ap-ap1] serial-id 219801A23V8209E0043Y [H3C-wlan-ap-ap1] radio 1 [H3C-wlan-ap-ap1-radio-1] service-template iseportal vlan 234 [H3C-wlan-ap-ap1-radio-1] radio enable [H3C-wlan-ap-ap1-radio-1] quit [H3C-wlan-ap-ap1] quit

ISEサーバーの構成

- 1. デバイスプロファイルを作成します。
 - a. トップナビゲーションバーで、Administration > Network Resources > Network Device Profilesを選択します。
 - b. Addをクリックします。
 - c. デバイスプロファイル名をH3Cに設定し、ベンダーとしてOtherを選択しSupported Protocols領域でRADIUSを選択します。
 - d. 設定を保存します。

図24 デバイスプロファイルの作成

dentity Services E	ngine _{Home}	Context Visibility	Operations Polic	- Administration			
♦ System ♦ Identity Mana	agement v Netwo	rk Resources	Portal Management pxGr	d Services + Feed Se	ervice + Threat Centric I	NAC	
Network Devices Netwo	ork Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequ	uences NAC Managers	External MDM	Location Services
Natwork Davisa Profile List >	1120						
Network Device Profile	e				Save	Reset	
* Nome							
Description	НЗС						
Description							
				/			
Icon	Change icon.	. Set To Default (i)					
Vendor	Other	÷					
Supported Protocols							
TACACE+							
TrustSec							
Tusidec							
RADIUS Dictionaries							
Templates							
Expand All / Collapse All							
Authentication/Au	thorization						
Permissions							
Change of Authorit	zation (CoA)						
Redirect							
Advanced							
r Auvanced							
Summary	he following are over	ortod:					
Services: Rad	fius, TACACS, Trusts	Gec					
CoA: Not	Supported						
Native URL Redirect: Not	Supported (i)						
Save Reset							

- 2. ACをネットワークアクセスデバイスとしてサーバーに追加します。
 - a. 上部のナビゲーションバーで、Administration > Network Resources > Network Devicesを選択します。
 - **b.** Addをクリックします。
 - c. 表示されたページで、名前をACに設定し、デバイスプロファイルH3Cを選択して、IPアドレス 6.6.4.10を指定し、RADIUS Authentication Settingsを選択して、共有秘密を12345678に 設定します。

IPアドレスがAC上のRADIUSパケットのNAS IPアドレスと同じであることを確認します。

共有秘密がACに設定された共有キーと同じであることを確認します。

d. Submitをクリックします。

図25 サーバーへのAC電源の追加

dulle 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
▼ Network Devices Network Device Gro	oups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	Network Davison List & New Network Device
Network Devices	Network Devices List > New Network Device
Default Device	* Name AC
Device Security Settings	Description
	IP Address * IP: 6.6.4.10 / 32
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	* Device Profile I H3C + A
	Model Name
	Software Version
	* Network Device Group
	IPSEC Is topic Device
	Device Type All Device Type (Contra Default
	Sono nyo Ali Device rypes 🥥 Set to Derault
	RADIUS Authentication Settions
	• To broot numerine due to dungo
	RADIUS UDP Settings
	Protocol RADIUS
	* Shared Secret 12345678 Hide
	CoA Port Set To Default
	RADIUS DTLS Settings (j)
	DTLS Required 🔲 🛞
	Shared Secret radius/dtls
	CoA Port Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional)
	DNS Name
	General Settings
	Enable KeyWrap
	* Key Encryption Key Show
	* Message Authenticator Code Key Show
	Key Input Format ASCII HEXADECIMAL
	TACACS Authentication Settings
	└ → SIMP Settings
	Advanced TrustSec Settings
	Submit Cancel

- 3. ユーザーグループを作成します。
 - a. トップナビゲーションバーでAdministration > Identity Management > Groupsを選択します。
 - b. 左側のナビゲーションペインで、User Identity Groupsを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をH3Cに設定します。
 - e. Submitをクリックします。

図26 ユーザーグループの作成

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
► System - Identity Management	Network Resources
Identities Groups External Iden	/ Sources Identity Source Sequences
Identity Groups ▼ Image: Second Sec	User Identity Groups > New User Identity Group Identity Group * Name H3C Description Submit Cancel (It) uit) ault)

- 4. ネットワークアクセスユーザーを作成します。
 - a. 上部ナビゲーションバーで、Administration > Identity Management > Identitiesを選択しま す。
 - b. 左側のナビゲーションペインで、Usersを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をh3c001に、パスワードをH3c123456に設定し、ユーザーをユーザー グループH3Cにバインドします。

パスワードに大文字、小文字、および数字が含まれていることを確認します。

e. [Submit]をクリックします。

図27 ネットワークアクセスユーザーの作成

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
✓Identities Groups External Iden	tity Sources Identity Source Sequences + Settings
G	
Users	Network Access Users List > New Network Access User
Latest Manual Network Scan Results	Network Access User
	* Name h3c001
	Status 🔽 Enabled 💌
	Email
	▼ Passwords
	Password Type: Internal Users
	Password Re-Enter Password
	* Login Password Generate Password ()
	Enable Password Generate Password ()
	▼ User Information
	First Name
	Last Name
	▼ Account Options
	Description
	Change password on next login
	▼ Account Disable Policy
	Disable account if date exceeds 2022-07-04 (yyyy-mm-dd)
	▼ User Groups
	Нзс 🔍 — 🕂
	Submit Cancel

- 5. 認証プロトコルを設定します。
 - a. 上部ナビゲーションバーで、Policy > Policy Elements > Resultsを選択します。
 - b. 左側のナビゲーションペインで、Authentication > Allowed Protocolsを選択します。
 - c. Default Network Accessをクリックし、Allow CHAPを選択します。
 - d. 設定を保存します。

図28 認証プロトコルの構成

cisco Iden	tity Service	s Engine	Home	Contex	t Visibility)	Operations	▼Policy	► Administratio	on Vork Centers
Policy Sets	Profiling	Posture	Client Provisio	ning 🔻 F	olicy Elements	_			
Dictionaries	Conditi	ons -Re	sults						
			Allowed	Protocols S	ervices List > D	efault Netwo	rk Access		
 Authentical 	tion		Allowe	d Protoc	ols				
Allowed Pr	otocols		N	ame De	fault Network A	ccess			
Authorization	on		Descrij	otion De	fault Allowed Pr	otocol Service			
Profiling									
Posture			✓ Allov	ed Protoc	ols				
				Authentie	cation Bypass				
Client Prov	isioning			Proc	ess Host Looku	p (j)			
				Authentio	cation Protocol	s			
				Allov	w PAP/ASCII				
				Allov	W CHAP				
				Allow	w MS-CHAPv1				
				Allow	w MS-CHAPv2				
				Allow	v EAP-MD5				
				Allov	WEAP-TLS				
					Allow Authent	lication of expir	ed certificate:	s to allow certificat	e renewal in Authorization Policy
					Enable Statel	ess Session Re	esume		
					Session ticke	t time to live	2	Hours	*
					Proactive ses	sio <mark>n ticket up</mark> da	ate will occur	after 90 % o	of Time To Live has expired
				Allow	w LEAP				
			•	Allov	V PEAP				
			•		WEAP-FAST				
				Allow	WEAP-TTLS				
				Pref	erred EAP Proto	col LEAP	*		
				EAP	-TLS L-bit (i)				
				Allow	w weak ciphers f	or EAP (j)			
				C Req	uire Message-Ai	uthenticator for	all RADIUS F	Requests (j)	
			Save	Reset					

- 6. ポータル設定を構成します。
 - a. 上部ナビゲーションバーで、Work Centers > Guest Access > Portals & Componentsを 選択します。
 - b. 左側のナビゲーションペインで、Guest Portalsを選択します。
 - c. 表示されたページで、Self-Registered Guest Portal(デフォルト)をクリックします。デフォルト 設定を使用して、URL Portal test URLをクリックします。表示されたウィンドウのアドレスバ ーにあるアドレスは、Webサーバーのアドレスです。

図29 ポータル設定の構成

	e ► Context Visibility ► Operations ► Policy ► Administration Work Centers
Network Access Guest Access Trust	Sec + BYOD + Profiler + Posture + Device Administration + PassiveID
Overview + Identities Identity Groups E	xt Id Sources 🕨 Administration Network Devices 🔷 Portais & Components 🛛 Manage Accounts 🕨 Policy Elements Policy Sets Reports Custom Portal Files 🕨 Settings
Ø	
Guest Portals	user Portale
Guest Types	
Sponsor Groups	noose one or the three pre-delined portal types, which you can edit, customize, and authorize for guest access.
Sponsor Portals	
	Create Edit Duplicate Delete
	Hotspot Guest Portal (default) Guest do not require userame and acessiver credentials to access the network, but you can optionally require an access code
	A Authorization setup required
	portal
	Authorization setup required
	Self-Registered Guest Portal (default) Guests may create their own accounts and be assigned a username and password, or use their social login to access the network
	S Used in 1 rules in the Authorization policy
	To authorize a portal for use, you must create an Authorization profile for it and then reference that profile in a rule in the Authorization policy
	To create an authorization profile
	Go to Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles
	To proste an authorization policy
	to create an autorization policy
	Go to Work Centers > Guest Access > Policy Sets
	G create an autorization poincy Go to Work Centers > Guest Access > Policy Sets
Tento Bortily Sorvices Erigine Hana Casted Vadeby	Constant and automization poincy Go to Work Centers - Guast Access > Policy Sets
Matching Notify Services Engine None Control Washing > Metauri Access = Over Access + TradSec + TradSec > Verview + Settions Soletty Oruga Exist Soletty Access + TradSec	Create an aduminization pointy Go to Vork Centers - Guest Access > Policy Sets Contain - Deck Administration - Printe@ Prints - Deck Administration - Printe@ Thints - Deck Administration - Printe@ Thints - Deck Administration - Printe@
design energy Monthly Strivton Lruger None + Context Values/ + Tuttors Access - Context Values/ + Tuttors - Values/ - Context Values/ + Stripton Ourseive + Months/ + Stripton + Stripton + Stripton + Stripton Ourseive + Months/ + Stripton + Portals Stripton + Stripton + Stripton Ourseit + Portals + Portals Stripton + Stripton + Stripton	Contacte and administration poincy Go to Vork Centers - SQuest Access - Policy Sets ··Operate: +New +Americation - *New Centers ··Operate: +New +Americation - *New +Americation - *New Centers ··Operate: +New +Americation - *New +Americat
Testing Monthly Services Engine None + Context Vesility + Nieters Access - Ownet occes - Transition - Transition Overview - Nieters - Transition - Advected Owerst Proteins - Portices Sectiongs and Clust - Portices Sectiongs and Clust Owerst Proteins - Portices Neetings and Clust - Portices Neetings and Clust	Containe and autoinization poincy Go to Verice Centers - S Guest Access > Policy Sets Poince
Control Normal Control Normal + Metalisk Access - Ownet Access - Ownet Access - Access - Ownet Access - Ownet Access - Access - Access - Ownet Access - Ownet Access - Access - Access - Ownet Access - Ownet Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access - Ownet Access - Access - Access - Access	Create all aduitionization pointy Create all aduitionization Create all aduitionizationization Create all aduitionization Create all aduitionizationization Create all aduitionizationization Create all aduitionizationizationizationization Create all aduitionizationizationizationizationizationizationizationizationizationizationizationizationizationizationizationizationin Create all aduitionizationizationizationizationizationizat
Condet Statistics Access - A condet Mathematic Overview - A condet Access + Training: + STOCO + Training: + STOCO Overview - Statistics + Training: + STOCO + Training: + STOCO + Training: + STOCO Overview - Statistics - Statistics + Training: + STOCO + Training: + STOCO Overview - Statistics - North Access - North Access - North Access Overview - Statistics - North Access - North Access - North Access Statistics - North Access - North Access - North Access - North Access	Contents and automicitation poincy Go to eater and automicitation poincy content and automicitation
* Newly Services Drame texe • Control Maker * Newly Services Drame * Tastice # 2000 * Point Ourset Prioritie * Date Services # 2000 * Point Geast Prioritie * Point Sectlings and Casting Services Portals Sectlings and Casting Services Portals Sectlings and Casting Services Geast Prioritie * Portals Sectlings and Casting Services Portals Sectlings and Casting Services Geast Prioritie * Portals Sectlings and Casting Services Portals Sectlings and Casting Services Geast Prioritie * Portals Sectlings and Casting Services Portals Sectlings and Casting Services Geast Prioritie * Point Sectlings Point Sectlings Point Sectlings Sectors Prioritie * Point Sectlings Point Sectlings Point Sectlings	Contains and automization poincy Go to Work Centers > Guast Access > Policy Sets Contains and automization poincy contains and automization poincy contains and automization contains and automization contains
Table Monthly Services Ergan None • Conduct Weaker • Nieder Access - Outer Access • Single Access • Single Access • Single Access • Nieder Access • Outer Access • Nieder Access Nieder Acc	lo create al aduaticitation pointy lo create al aduaticitation p
Finder Northly StrivkOS Ergin North Northly StrivkOS Ergin North -> Control Value + Nieterika Strike -> Ount Access -> Strike -> Port -> Port Ount Access -> Ount Access -> Ount Access -> Port -> Port Ount Arrows -> Portals Settlings and Cust -> Portals Settlings and Cust -> Portals Settlings and Cust Ount Types -> Portals Settlings and Cust -> Portals Settlings and Cust -> Portals Settlings and Cust Description -> Ount Access -> Portals Settlings and Cust -> Ount Access Description -> Ount Access -> Ount Access -> Ount Access Description -> Ount Access -> Ount Access -> Ount Access Description -> Ount Access -> Ount Access -> Ount Access Description -> Ount Access -> Ount Access -> Ount Access	Contraine and automicitation pointy Contraine and automicitation Contraine and automicitation Contraine and automicitation Contrained automicitation
Statistics Name Control Volume + Nation Access - Quart Access + Nation Statistics + Nation Statistics - Volume + National Statistics + National Statistics + National Statistics + National Statistics - Outer Access - Portable Statistics + National Statistics + National Statistics - Outer Access - Portable Statistics + National Statistics + National Statistics - Outer Access - Portable Statistics + National Statistics + National Statistics - Outer Access - Portable Statistics + National Statistics + National Statistics - Outer Access - Portable Statistics + Portable Statistics + Portable Statistics - Outer Access - Portable Statistics - Portable Statistics + Portable Statistics	O Create all addronation pointy Go to Work Centers > Guest Access > Policy Sets • Opcode: • Note Centers • Note Centers • Note Centers
Binding Name of Control Stratutes Name Control Control • Mitteria Alcossi - Quartitic Control • Name of Control • Name of Control • Outprice Alcossi - Quartitic Control • Name of Control • Name of Control • Outprice Alcossi - Quartitic Control • Name of Control • Portal Stratutes • Outprice Alcossis - Quartitic Control • Portal Stratutes • Control Name of Control • Outprice Alcossis • Portal Stratutes • Portal Stratutes • Outprice Alcossis • Outprice Alcossis • Outprice Alcossis • Portal Stratutes • Outprice Alcossis • Outprice Alcossis • Outprice Alcossis • Portal Stratutes • Outprice Alcossis	Contents and addressing of points Contents
• Northy Services Forper Nore • Control Market • Norther Vectors • Control Market • Elicitio • Protein Outer Transis • Portal Sectings and Custo • Portal Sectings • Portal Sectings Outer Transis • Portal Sectings • Portal Sectings • Portal Sectings Beneror Proteits • Portal Sectings • Portal Sectings • Portal Sectings • Portal Sectings • Portal Sectings • Portal Sectings • Portal Sectings	Outstale all all autorization points Go teale all all autorization points So teale all all autorization points ************************************
* Newly Servers Depres text • Central challers * Newly Servers Depres * Tables * 2000 C * 1000 C	Outlete all aduancement property Go to Work Centers > Guast Access > Policy Sets ************************************
Baseling Source / Source Scrippe Baseling Conduct Musice • Maintan Access - Guard Access - Final Baseling • Maintan Access - Guard Access - Final Baseling Custal Trunces Custal Trunces Partial Secttings and Class Scontor Oruge Scontor Pricisis Partial Reserver Custal Trunces Datation Datation Scontor Pricisis Partial Reserver Datation Datation - Acceptable true Price - Acceptable true Price	lo create al autorization pointy Bo to Work Centers > Guest Access > Policy Sets + Neares + Seesa Access > Policy Sets + Neares + Seesa Access → Policy Sets + Neares + Seesa Access + Seesa Access + Neares + Seesa Access + Ne
Owner Notice Strate Note: • Coded Volation ** Netline Access - Owner Volation * Netline Volation ** Netline Access - Owner Volation * Netline Volation Outsit Thruss * Portal Sectifyings Portal Sectifyings Development Privates * Portal Sectifyings Portal Sectifyings Development Privates * Portal Sectifyings Portal Sectifyings Portal Sectifyings * Portal Sectifyings * Portal Sectifyings * Accepatible there Polityings * Accepatible there Polityings * Accepatible there Polityings	lo cetele al autorization pointy lo cet
Result South (Strict) South (Strict) <thstrict)< th=""></thstrict)<>	lo cleate al autorization point G cleate al autorization point Point here > Guest Access > Policy Sets * More + More - * More - * More + Content - * More Denote: Note Set Rept: Custom Policy Firs + Settres entration point here and barrouge a women al autorization policy First + Settres entration point here and barrouge a women al autorization policy First + Settres entration entration - * Content + Content + Policy Beerster - * Content + * Policy Beerster - * Content + * Policy Beerster - * Contend + * Policy Beerster - * Contend + * Policy Beerster
• North Services Form: • North Sectors • Control Mathem • Part Sectors • Control Mathem • Part Sectors • Sectors • Part Sectors • Sectors • Sectors • Part Sectors • Sectors • Sectors • Sectors • Sectors • Part Sectors • Sectors	lo create al autorization points Go to tale al autorization points So to tale al autorization points set setes a decense al control points set setes a set
2000 Monthly Terretors Depart Interline > Consert charling 2 Monthly Access - Consert of Lines 2 Monthly 2 Monthly Court Protein Portale Settlings and Court Portale Settlings Portale Settlings and Court Settlings Portale Settlings Portale Settlings Portale Settlings Notein Protein Settlings Settlings	lo create al autorization pointy Go to Work Centers > Guest Access > Policy Sets
Standy Journee Dryne two • Conduct Values// • Heider Allessin • Conduct Values// • Subject Values// • Ourset Profile • Subject Values// • Subject Values// Guart Truitis • Partial Sectilings and Claub • Partial Sectilings and Claub Guart Truitis • Partial Sectilings and Claub • Partial Sectilings and Claub Guart Truitis • Partial Sectilings and Claub • Partial Sectilings and Claub Guart Truitis • Partial Sectilings and Claub • Partial Sectilings Borner Drottis • Partial Sectilings • Partial Sectilings • Partial Sectilings </td <th>lo create al autorization points lo create al autorization points lo to treate al autorization points lo treate al autorization points lo treate al autorization points lo treate al autorization points lo to treate al autorization points lo to treate al autorization points lo treate al autorization poi</th>	lo create al autorization points lo create al autorization points lo to treate al autorization points lo treate al autorization points lo treate al autorization points lo treate al autorization points lo to treate al autorization points lo to treate al autorization points lo treate al autorization poi
Baserie / Stander Access Descent / Stander Access <thdescent access<="" stander="" th=""> <thdescent <="" td=""><th>lo cetele al autorization pointy lo cetele al autorization pointy lo cetele al autorization pointy lo tetele al autorization pointy lo te</th></thdescent></thdescent>	lo cetele al autorization pointy lo cetele al autorization pointy lo cetele al autorization pointy lo tetele al autorization pointy lo te
Anorthy Services Engine Anorthy Services Engine Anorthy Services Engine Anorthy Services Engine Anorthy Services	lo cleale al autorization points B to Verke Centers > Quest Access > Policy Sets ************************************

設定の確認

#携帯電話で、SSID h3c-ise-portalを使用してワイヤレスサービスに接続します。Cisco認証ログインページが開いたら、正しいユーザー名とパスワードを入力し、Sign Onをクリックします。開いたページで、 Continueをクリックします。ログインが成功することを確認します。

図30 設定の確認

내 中国电信 🗢	10:53	ð 100% 🗩)	.ul 中国电信 穼	10:53	2 100% 📟
AА	₿ 10.249.56.169	C	AA	€ 10.249.56.169	C
	Foxconn Guest Port	tal		Foxconn Guest Portal	
Welcome Sign on for g Userna Passw	guest access. inne: ord:		Welcome N Click Contin You're very	lessage nue to connect to the networ close to gaining network acc Continue	k. æss.
	Sign On				
<	> û	<u>ш</u>	<	> ĉ m	G

#ACで、オンラインポータルのユーザー情報を表示します。 [H3C] display portal user all Total portal users: 1 Username: h3c001 AP name: ap1 Radio ID: 1 SSID: h3c-ise-portal Portal server: N/A State: Online VPN instance: N/A IP MAC 9cbc-f0e7-50f0 10.249.56.169 234 Authorization information: DHCP IP pool: N/A User profile: N/A Session group profile: N/A ACL number: N/A Inbound CAR: N/A Outbound CAR: N/A Web URL: N/A

VLAN Interface WLAN-BSS1/0/4

構成ファイル

#
vlan 234
#
vlan 1000
#
wlan service-template iseportal ssid h3c-ise-portal portal enable method direct portal domain ise portal bas-ip 6.6.4.10 portal apply web-server ise

```
service-template enable
#
interface Vlan-interface1000
  ip address 6.6.4.10 255.255.255.0
#
radius scheme ise
  primary authentication 100.18.0.200 key cipher $c$3$oTPE3ir9uYI718iL9tFmRoaoDu7
  DmtlZ2gZC
  primary accounting 100.18.0.200 key cipher $c$3$/Vcna21JU94hHKqWvBTrACCGhUm8iPi
  B5Vp7
  user-name-format without-domain
  nas-ip 6.6.4.10
#
domain ise
  authentication portal radius-scheme ise
  authorization portal radius-scheme ise
  accounting portal radius-scheme ise
#
portal user-logoff after-client-offline enable
portal client-gateway interface Vlan-interface1000
portal free-rule 2 destination ip 6.6.4.10 255.255.255.255
portal free-rule 5 destination ip 100.18.0.200 255.255.255.255
#
portal web-server ise
  url
  https://100.18.0.200:8443/portal/PortalSetup.action?portal=f0ae43f0-7159-11e7-a355-00
  5056aba474
  server-type ise
#
portal local-web-server http
  default-logon-page ise_h3c.zip
#
portal local-web-server https
  default-logon-page ise h3c.zip
#
wlan ap ap1 model WA6330
  serial-id 219801A23V8209E0043Y
  radio 1
  radio enable
  service-template iseportal vlan 234
  radio 2
  radio 3
```

```
#
```

例:Cisco ISEベースの設定 SSHログイン用のHWTACACS認証

ネットワーク構成

図31に示すように、コンピュータはスイッチを介してACに接続されています。クライアントがSSHを介して ACにログインすると、ISEサーバーはクライアントのHWTACACS認証を実行します。

クライアントは、SSHを使用してACにログインした後、次の権限を持ちます。

- レベル1ユーザーロールの権限を持ちます。
- display cpu-usageコマンドにアクセスできません。

図31 ネットワーク図



手順

(!)重要:

この設定例では、Cisco ISEサーバーでのHWTACACS認証によるSSHログインの認証に関連する主要な設定だけを説明します。ネットワーク接続設定の詳細については、デバイスおよびサーバーのマニュアルを参照してください。

デバイスとサーバーがネットワーク接続されていることを確認します。

ACの設定

1. HWTACACSスキームを設定します。#HWTACACSスキームtacを作成します。

<AC> system-view

[AC] hwtacacs scheme tac

#8.1.1.19にあるISEサーバーをプライマリ認証、認可、アカウンティングサーバーとして指定し、
 ISEサーバーとの安全な通信のための共有キーを指定します。共有キーは、ISEサーバーで構成
 されている共有シークレットと同じであることを確認してください。
 [AC-hwtacacs-tac] primary authentication 8.1.1.19 key cipher
 \$c\$3\$8zfqwa07HmNhvjWvEeixw5NGEGo82r/htRg=
 [AC-hwtacacs-tac] primary authorization 8.1.1.19 key cipher
 \$c\$3\$fARZu6PskfKoULCy46SHq0hVbNHakBUPleE=
 [AC-hwtacacs-tac] primary accounting 8.1.1.19 key cipher

\$c\$3\$tBnfBlfHnO9YHBko2ZjMpzpuRqSyN3wdDPA=

#ISEサーバーに送信されるユーザー名からドメイン名を除外します。

[AC-hwtacacs-tac] user-name-format without-domain

#ISEサーバーに送信されるHWTACACSパケットのNAS IPアドレスとして191.2.1.56を指定します。 NAS IPアドレスが、ISEサーバーでACに対して指定されているものと同じであることを確認します。 [AC-hwtacacs-tac] nas-ip 191.2.1.56

[AC-hwtacacs-tac] quit

2. ISPドメインを構成します。

#ISPドメインシステムを作成します。

[AC] domain system

#ログインユーザーの認証と認可にHWTACACSスキームtacを使用し、ログインユーザーのアカウンティングを実行しないように、ISPドメインを設定します。

[AC-isp-system] authentication login hwtacacs-scheme tac

[AC-isp-system] authorization login hwtacacs-scheme tac

[AC-isp-system] accounting login none

#コマンドの認可とアカウンティングにHWTACACSスキームtacを使用するようにISPドメインを設定します。

[AC-isp-system] authorization command hwtacacs-scheme tac [AC-isp-system] accounting command hwtacacs-scheme tac

[AC-isp-system] quit

ローカルRSAおよびDSAキーペアを作成し、SSHサーバーをイネーブルにします。
 [AC] public-key local create rsa
 [AC] public-key local create dsa

[AC] ssh server enable

- デフォルトロール機能をイネーブルにします。
 [AC] role default-role enable
- コマンド認可およびアカウンティングをイネーブルにします。 [AC] line vty 0 31 [AC-line-vty0-31] authentication-mode scheme [AC-line-vty0-31] command authorization [AC-line-vty0-31] command accounting [AC-line-vty0-31] quit

ISEサーバーの構成

- 1. ネットワークアクセスユーザーを作成します。
 - a. 上部のナビゲーションバーで、Work Centers > Device Administration > Identitiesを選択 します。
 - b. 左側のナビゲーションペインで、Usersを選択します。
 - c. Addをクリックします。
 - d. 開いたページで、名前をldfloginに、パスワードをLdf654321に設定します。パスワードに大文 字、小文字および数字が含まれていることを確認します。
 - e. Submitをクリックします。

図32 ネットワークアクセスユーザーの作成

Network Access Guest Access TrustSec BYOD Profiler Posture Posture Posture Posture Posture	Clink here to do wireless seture and visibility seture Do not show this anain
Overview Viewentities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings	click here to do microso detap and meening being be not brow and again.
Network Access Users List > Millogin	
vers ▼ Network Access User	
* Name Idflogin	
Status 🥑 Enabled 👻	
Email	
▼ Passwords	
Password Type: Internal Users *	
Password Re-Enter Password	
* Login Password	
Enable Password Generate Password	
▼ User Information	
First Name	
Last Name	
* Account Options	
Description	
Change password on next login	
▼ Account Disable Policy	
Disable account if date exceeds 2019-11-18 (yyy-mm-dd)	
▼ User Groups	

- 2. ACをネットワークアクセスデバイスとしてサーバーに追加します。
 - a. トップナビゲーションバーで、Work Centers > Device Administration > Network Resourcesを選択します。
 - b. 左側のナビゲーションペインで、Network Devicesを選択します。
 - c. Addをクリックします。
 - d. 表示されたページで、名前をAC2に設定し、IPアドレス191.2.1.56を指定してTACACS Authentication Settingsを選択し、共有秘密をH3cclこ設定します。
 IPアドレスがAC上のHWTACACSパケットのNAS IPアドレスと同じであることを確認します。
 共有秘密がACIに設定された共有キーと同じであることを確認します。
 - e. 設定を保存します。
 - 図33 サーバーへのAC電源の追加

dentity Services Engine Home	Context Visibility Operations Policy Administration Vork Centers License Warning	A 9 0 . A
Network Access Guest Access TrustSec Overview Identities User Identity Groups	BYOD Profiler Posture -Device Administration PassvelD Click here to do wireless setup and valible Ext la Sources Policy Elements Device Admin Policy Sets Reports Settings	ty setup Do not show this again. $ imes$
Network	rk Devices	
Network Devices	* Name AC2	
Network Device Groups	Description	
Default Devices		
TACACS External Servers	IP Address 🔹 "IP: 191.2.1.56 / 32	
TACACS Server Sequence		
O IPv6	is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected	
	* Device Profile 📄 Alcate/Wired 💌 🕀	
	Model Name v	
	Software version	
* Ne	etwork Device Group	
	Incation All Leasting Cost to Default	
	IPREC IV.	
Devi		
	All Device Types Visit to Default	
	DADITO Adhestication Californi	
	Rectors Authentication Sectings	
	TACACS Authentication Settings	
	Shared Secret Show Retire	
	Enable Single Connect Mode	
	 Legacy Clasco Device TACACS Draft Compliance Single Connect Support 	

- 3. 認証プロトコルを設定します。
 - a. 上部のナビゲーションバーで、Work Centers > Device Administration > Policy Elementsを選択します。
 - b. 左側のナビゲーションペインで、Results > Allowed Protocolsを選択します。

- c. Default Device Adminという名前のデフォルトの許可プロトコルサービスを使用しま
- す。図34 認証プロトコルの構成

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 🐵 😓 🔅
Network Access Guest Access	TrustSec + BYOD + Profiler + Posture Device Administration + PassiveID	Click here to do wireless setup and visibility setup Do not show this again. ×
Overview Identities User Identit	y Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings	
Conditions	Allowed Protocols Services List > Default Device Admin Allowed Protocols	
Network Conditions	Name Default Device Admin	
	Description Default Allowed Protocol Service Admin	
Allowed Protocols	4	
TACACS Command Sets	✓ Allowed Protocols	
TACACS Profiles	Authentication Protocols	
	Only Authentication Protocols relevant to TACACS are displayed.	
	Allow PAP/ASCII	
	Allow CHAP	
	Allow MS-CHAPy1	
	Same Reset.	

- 4. TACACSプロファイルを設定します。
 - a. 上部のナビゲーションバーで、Work Centers > Device Administration > Policy Elementsを選択します。
 - b. 左側のナビゲーションペインで、Results > TACACS Profilesを選択します。
 - **c.** Addをクリックします。
 - d. 表示されたページで、名前をldftacasに設定し、**Default Privilege**を選択して、デフォルト 権限をレベル1に設定します。
 - e. 設定を保存します。

図35 TACACSプロファイルの設定

dentity Services Engine	Home	is → Policy → Administration 💌	/ork Centers	License Warning 🔺 🔍 🐵 🍃 🌣
Network Access Guest Access	TrustSec + BYOD + Profiler + Postu	re		Click here to do wireless setup and visibility setup Do not show this again. X
Overview Identities User Identity	Groups Ext Id Sources Network Resources	urces - Policy Elements Device Admin F	Policy Sets Reports Settings	
Conditions	TACACS Profiles > Idftacas			
Network Conditions	TACACS Profile			
	Name	Idftacas		
✓ Kesults	Description			
Allowed Protocols	Description			
TACACS Command Sets				
TACACS Profiles	Task Attribute View Raw	View		
	Common Tasks			
	Common Task Type Shell *			
	Default Privilege	0	(Select 0 to 15)	
	Maximum Privilege	0	(Select 0 to 15)	
	Access Control List	0		
	- Auto Command			
		•		
	No Escape	0	(Select true or false)	
	Timeout	0	Minutes (0-9999)	
	Idle Time	0	Minutes (0-9999)	
	Custom Attributes			

- 5. TACACSコマンドセットを設定します。
 - a. 上部のナビゲーションバーで、Work Centers > Device Administration > Policy Elementsを選択します。
 - b. 左側のナビゲーションペインで、Results > TACACS Command Setsを選択します。
 - c. Addをクリックします。
 - **d.** 開いたページで、名前をldftacacsに設定します。Commands領域で、**Permit any command that not listed at below**を選択し、display cpu-usageコマンドを拒否します。
 - e. 設定を保存します。

図36 TACACSコマンドセットの設定

cisco Identity Services Engine	Home + Context Visibility + Operations	Policy Administration Work Centers	License Warning 🔺 🔍	0 2 0
Network Access Guest Access	TrustSec BYOD Profiler Posture	Device Administration PassiveID	Click here to do wireless setup and visibility setup Do not	show this again. X
Overview Identities User Identit	y Groups Ext Id Sources + Network Resources	Policy Elements Device Admin Policy Sets Reports Settings		
Conditions	TACACS Command Sets > Idflacacs Command Set			
Network Conditions	Name	loftacacs		
Allowed Protocols	Description			
TACACS Command Sets				
	Permit any command that is not listed below	8		
	🕇 Add 🍵 Trash 🕶 🖾 Edit 🕴	love Up 4 Move Down	o-	
	Grant Comma	ad Arguments		
	DENY display	cpu-usage	С fi	
	4			
			Cancel Save	

- 6. 認証および認可ポリシーセットを設定します。
 - a. 上部のナビゲーションバーで、Work Centers > Device Administration > Device Admin Policy Setsを選択します。
 - b. Policy Setsの下にあるプラスアイコン+をクリックします。
 - c. ポリシーセット名を a に設定します。

図37 認証および許可ポリシーセットの構成

cisco Ide	entity Services En	gine Home	Context Visibility	Operations	Policy Admin	stration · Work Center	5		Licen	se Warning 🔺	<u>q</u>	0	0
 Network Overview 	Access + Guest	Access + TrustSec User Identity Groups	BYOD Profiler Ext Id Sources Network	Posture rk Resources	Device Administration Policy Elements	PassiveID Device Admin Policy Sets	Reports Settings	s	Click here to do wireless setup	and visibility setu	up Do not	show this a	igan. ×
Policy Se	ets										R	eset	Save
+ s	Status Policy Se	st Name	Description	C	Conditions				Allowed Protocols / Serve	r Sequence	Hits	Actions	View
Search													
	⊘ a			1	a a				Default Device Admin	× * +	17	0	>
	Default		Tacacs Default policy se	et					Default Device Admin	×= +	14	•	>
													Save

- d. という名前の認証および許可ポリシーセットのView列にあるアイコンをクリックします。 a.
- e. Authorization Policy領域で、Authorization Ruleという名前の許可ポリシーを追加します。
 1. 許可ポリシーのResults > Command Sets列で、コマンドセットIdftacacsを選択します。
 許可ポリシーのResults > Shell Profiles列で、TACACSプロファイルIdftacasを選択します。

図38 許可ポリシーの追加

Network	k Access	Guest Access TrustSe	Ic BYOD Profiler Posture	Device Administration	 PassiveID 			Taxa and taxa		1012002-00100-0000		
Overvie	ew 🕨 Idi	lentities User identity Groups	Ext Id Sources + Network Resour	ces + Policy Elements	Device Admin Policy Sets	Reports Settings		Click he	re to do wireless setup and	insibility setup Do n	tot show th	is again.
olicy S	Sets +	a									Reset	Save
	Status	Policy Set Name	Description	Conditions					Allowed Pr	otocols / Server !	Sequenc	e Hits
Bearch												
	0	a		a a					Default De	vice Admin	x.v. 4	17
Authe	entication	n Policy (1)										
Authe	entication orization	n Policy (1) Policy - Local Exceptions										
Authe Autho	entication orization orization	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions										
 Authe Autho Autho Autho Autho 	entication orization orization orization	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2)										
Authe Autho Autho Autho Autho	entication orization orization	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2)					Results					
Autho Autho Autho Autho	entication orization orization orization Status	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2) Rule Name	Conditions				Results Command Sets		Shell Profiles		Hits	Actions
Authe Authe Authe Authe Authe Authe Search	entication orization orization orization Status	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2) Rule Name	Conditions				Results Command Sets		Shell Profiles		Hits	Actions
Authe Authe Authe Authe Authe Search	entication orization orization orization Status	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2) Rule Name Authorization Rule 1	Conditions				Results Command Sets	*	Shell Profiles	** #	Hits	Actions
 Authe Autho Autho Autho Autho Autho Search 	entication orization orization orization Status © @	n Policy (1) Policy - Local Exceptions Policy - Global Exceptions Policy (2) Rule Name Authorization Rule 1 Default	Conditions				Results Command Sets Instacces	*	Shell Profiles Isthaces Deny Al Shell Profile	** *	Hits 11	Actions ©

- **f.** 設定を保存します。
- 7. デバイスアクセス認証サービスを有効にする:
 - a. トップナビゲーションバーで、Administration > System > Deploymentを選択します。
 - b. ISEノードを選択し、Editをクリックします。

図39 ISEノードの選択とEditのクリック

- System + Identity Management + Network Resources + Device Portal Management pxGrid Services + Feed Service + Thread Centric NAC					Clinity beauty in the second	Much have be do unabled when that which and a first statements when	
eployment Licensing + Certi	ficates + Logging	g Maintenance Upgra	de Backup & Restore Admin Access S	ettings			
Deployment		Deployment Nodes					
Deployment	@ .	Deployment Nodes				Selected 1	1 Total 1 🚸 🙀
Deployment	.	Deployment Nodes	Syncup			Selected Show All	1 Total 1 🎄 🙀
Deployment Qui * Hz * * Deployment PAN Failover	÷.	Edit Register Hostname	Syncup Deregister	Role(s)	Services	Selected Show All Node Status	1 Total 1 😵 🤮

c. 表示されたページで、Enable Device Admin Serviceオプションを選択し、設定を保存します。

図40 ISEノードの編集

tite Identity Services Engine Home	Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🧠 🕘 🥥 🌣
System + Identity Management + Network Re Deployment Licensing + Certificates + Loggi	sources + Device Portal Management pxGind Services + Feed Service + Thread Centric NAC ng + Maintenance Upgrade + Backup & Restore + Admin Access + Settings	Click here to do wireless setup and visibility setup Do not show this again. \times
Deployment → YE * * Concornent * PAN Falover		

設定の確認

- 1. クライアントが正しいユーザー名とパスワードを入力した後、SSHを使用してACにログインできることを確認します(詳細は省略)。
- 2. クライアントがレベル1の役割で許可されたコマンドのみにアクセスできることを確認します。たとえ ば、クライアントはdisplay memoryコマンドにアクセスできます。クライアントがdisplay cpu-usage コマンドにアクセスできないことを確認します。

図41 アクセス権の検証

```
(H3C>ssh2 191.120.1.56
Username: ldflogin
Press CTRL+C to abort.
Connecting to 191.120.1.56 port 22.
Ldflogin@191.120.1.56's password:
Enter a character ~ and a dot to abort.
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
 Without the owner's prior written consent,
 no decompiling or reverse-engineering shall be allowed.
 <H3C>disp
<H3C>display cpu
<H3C>display cpu-usage
Permission denied.
<H3C>disp
<H3C>display me
<H3C>display memory
Memory statistics are measured in KB:
Slot 1:
          Total
                   Used
                            Free
                                    Shared Buffers
                                                     Cached
                                                             FreeRatio
      32537652 9064916 23472736
Mem:
                                                     179300
                                                                 72.1%
-/+ Buffers/Cache: 8885540 23652112
Swap:
Slot 2:
          Total
                  Used
                             Free
                                    Shared
                                           Buffers
                                                     Cached
                                                             FreeRatio
                5749824 26787828
5573024 26964628
      32537652
Mem:
                                               136
                                                     176664
                                                                82.3%
/+ Buffers/Cache:
Swap:
<H3C>di
<H3C>display hi
<H3C>display history-command al
<H3C>display history-command al
Permission denied.
<H3C>
```

構成ファイル

#

hwtacacs scheme tac

primary authentication 8.1.1.19 key cipher \$c\$3\$8zfqwa07HmNhvjWvEeixw5NGEGo82r/htRg= primary authorization 8.1.1.19 key cipher \$c\$3\$fARZu6PskfKoULCy46SHq0hVbNHakBUPleE= primary accounting 8.1.1.19 key cipher \$c\$3\$tBnfBlfHnO9YHBko2ZjMpzpuRqSyN3wdDPA= user-name-format without-domain nas-ip 191.2.1.56

#

domain system

authentication login hwtacacs-scheme tac authorization login hwtacacs-scheme tac accounting login none authorization command hwtacacs-scheme tac accounting command hwtacacs-scheme tac # public-key local create rsa # public-key local create dsa # ssh server enable # role default-role enable # line vty 0 31 authentication-mode scheme command authorization command accounting