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

内容

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

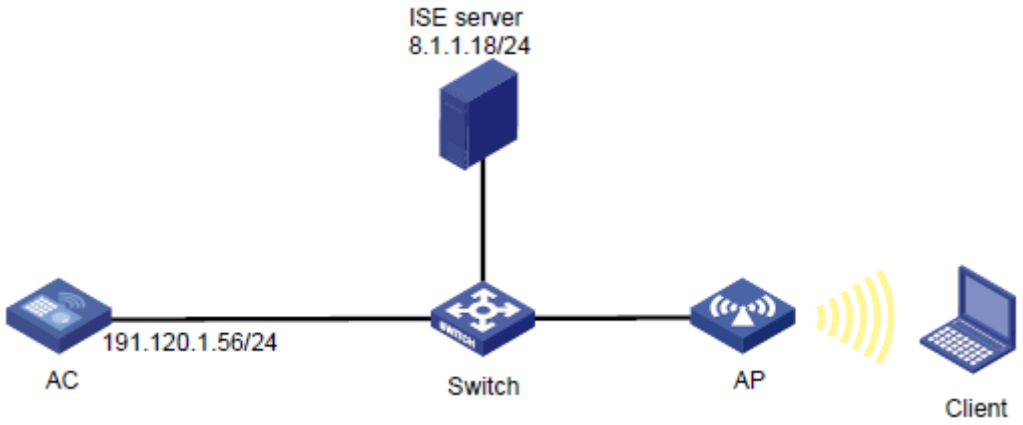
ネットワーク構成

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

1. 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
   c3$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

6. 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] quit

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。

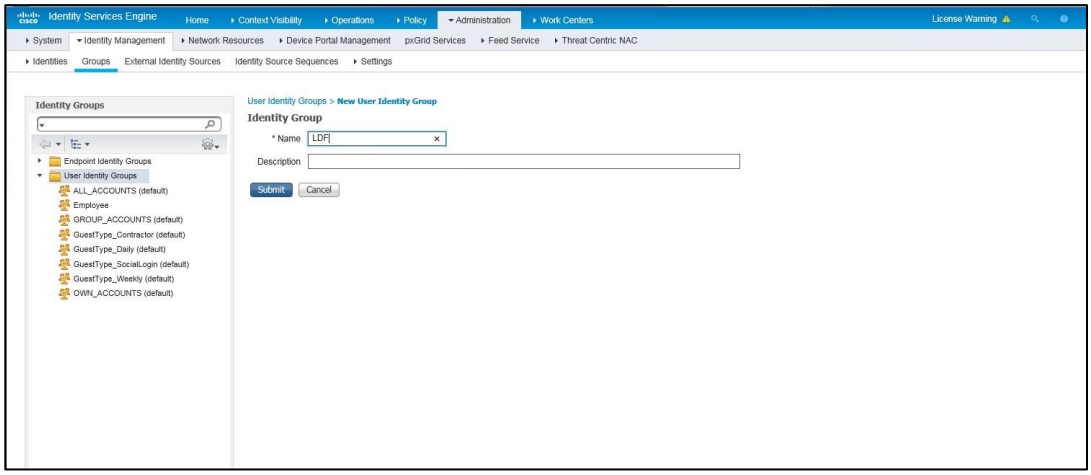
b. 左側のナビゲーションペインで、**User Identity Groups**を選択します。

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。

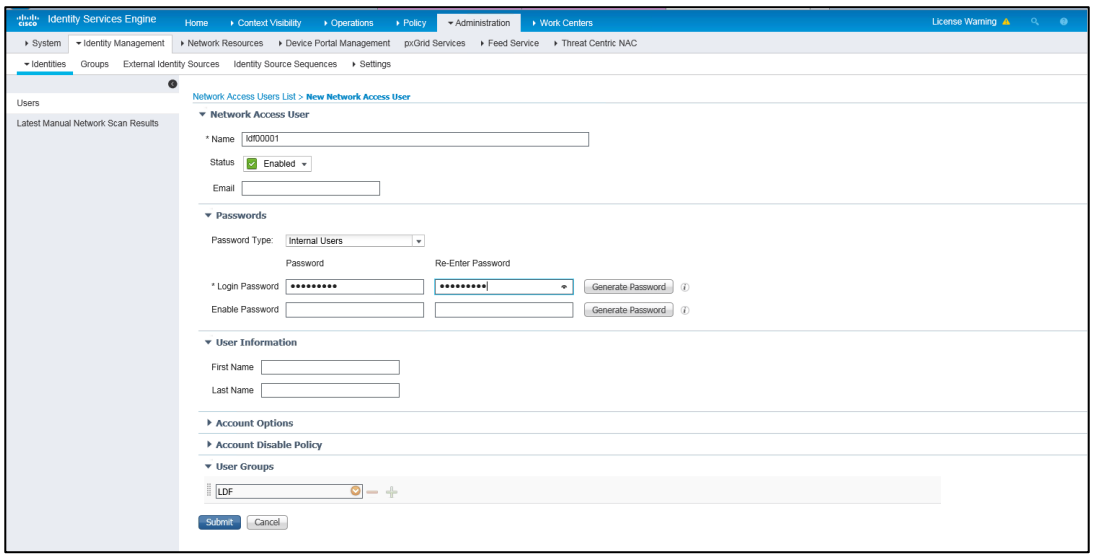
図2 ユーザーグループの作成



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**Idf00001**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

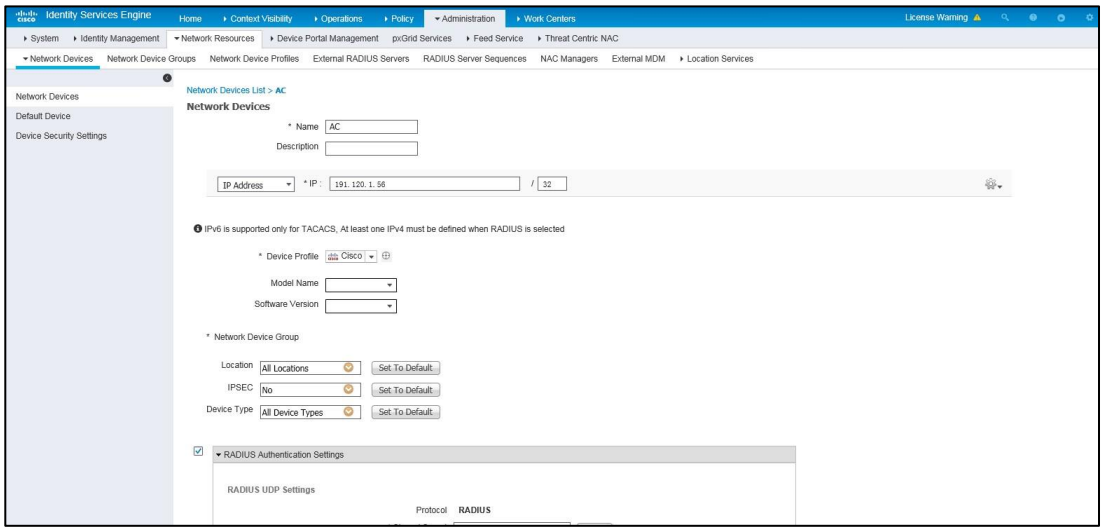


3. ACをネットワークアクセスデバイスとしてサーバーに追加します。
   a. 上部のナビゲーションバーで、**Administration > Network Resources > Network Devices**を選択します。
   b. **Add**をクリックします。
   c. 名前をACに設定し、IPアドレス191.120.1.56を指定して、**RADIUS Authentication Settings**を選択し、共有秘密を**H3cc**に設定します。

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4 サーバーへのAC電源の追加



4. 認証プロトコルを設定します。

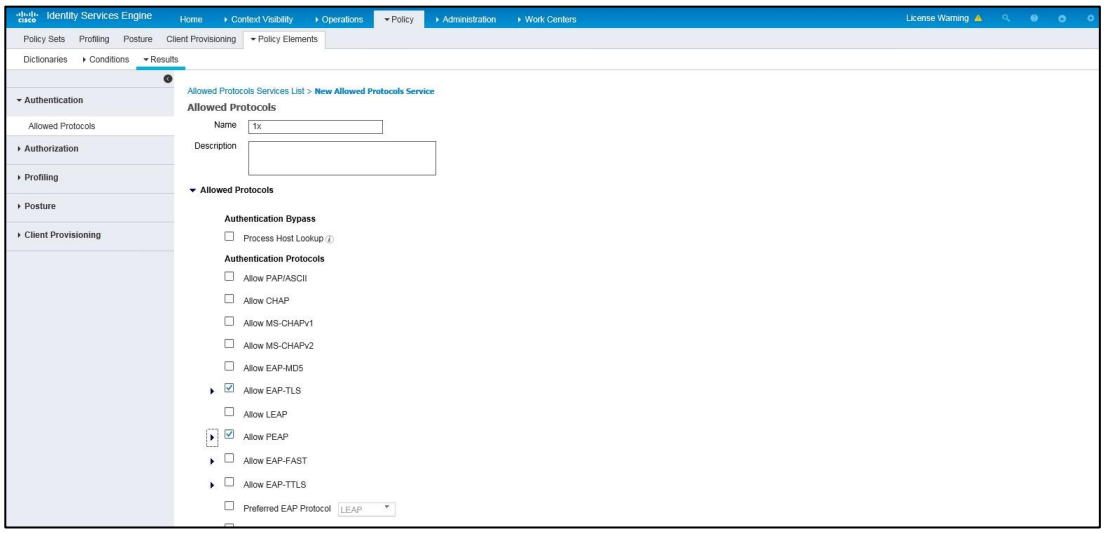
a. 上部ナビゲーションバーで、**Policy > Policy Elements > Results** を選択します。

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



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。

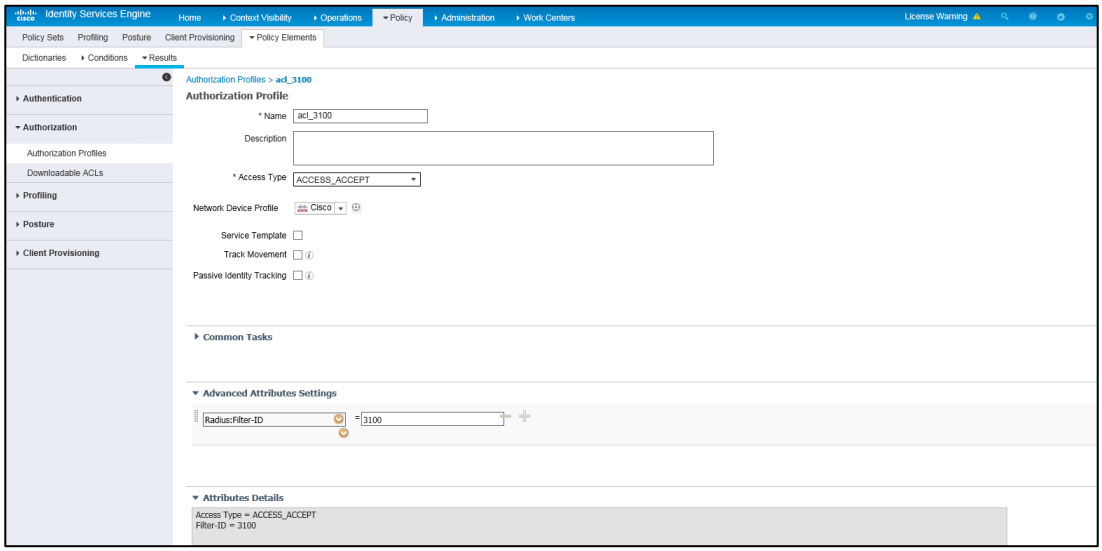
c. **Add**をクリックします。

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



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。

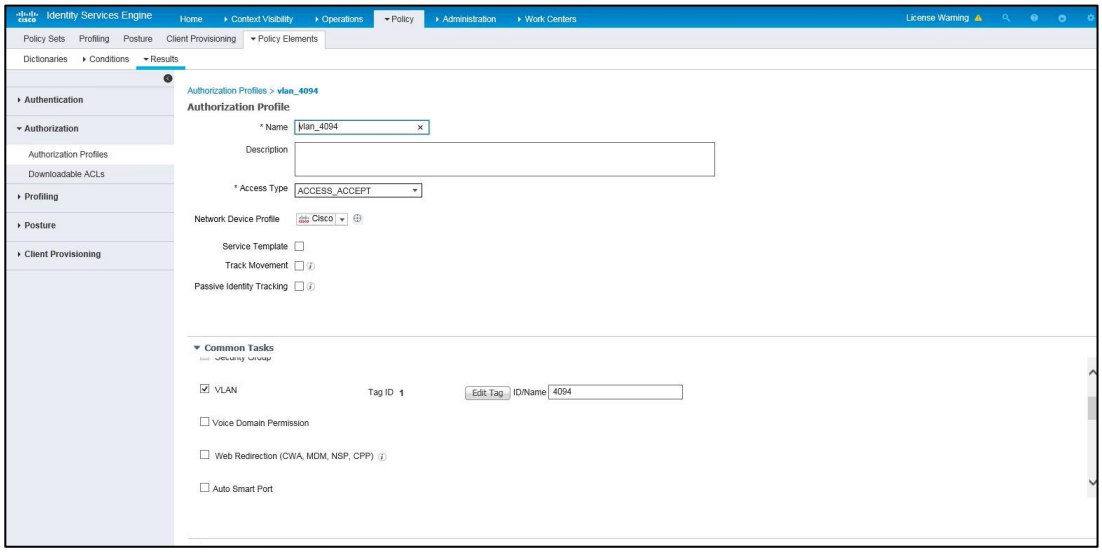
b. 左側のナビゲーションペインで、**Authorization > Authorization Profiles**を選択します。

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7 認可VLANの設定



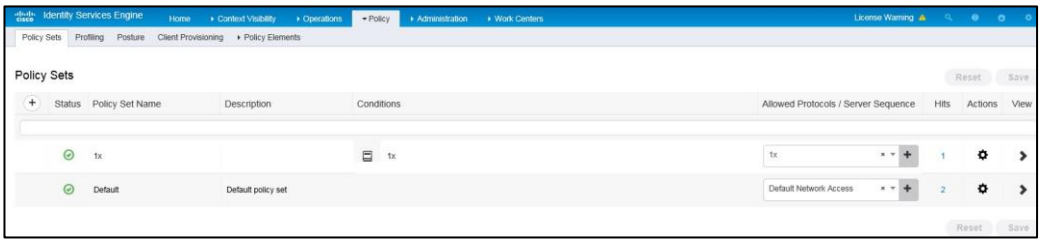
7. 認証および認可ポリシーセットを設定します。

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。

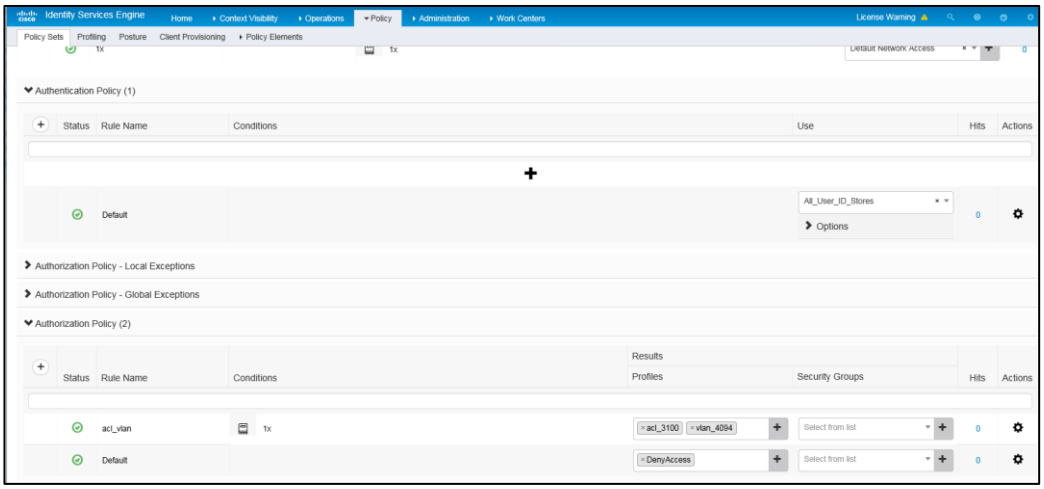
図8 認証および許可ポリシーセットの構成



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。

図9 許可ポリシーの構成

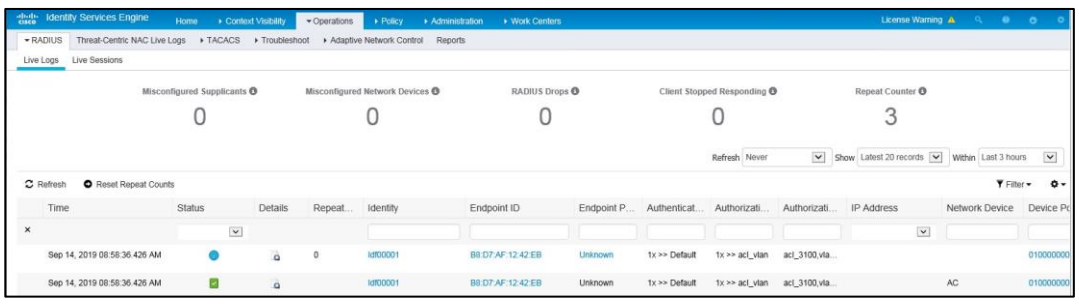


f. 設定を保存します。

設定の確認

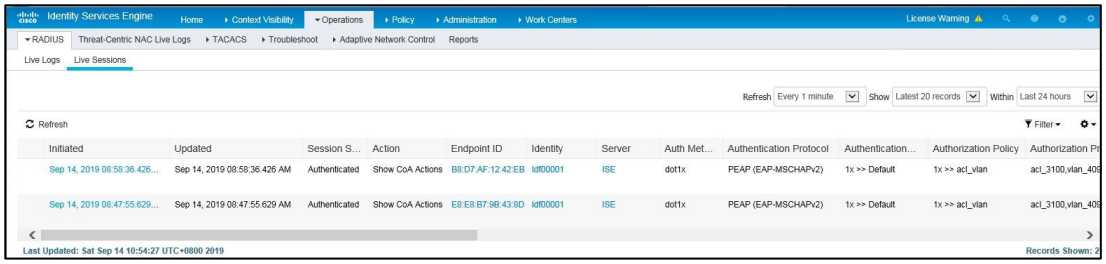
1. 上部のナビゲーションバーで、**Operations > RADIUS > Live Logs**を選択します。オンラインクライアントのライブログ情報を表示します。

図10 オンラインクライアントのライブログ情報の表示



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



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

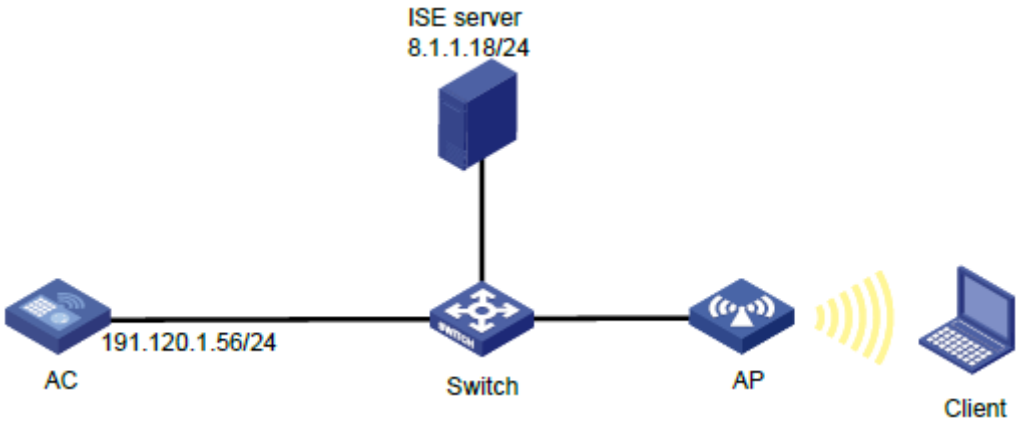
ネットワーク構成

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

   c3$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
c3$XYqokG6I8YoOymukIyvxoJuzFoB+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] quit

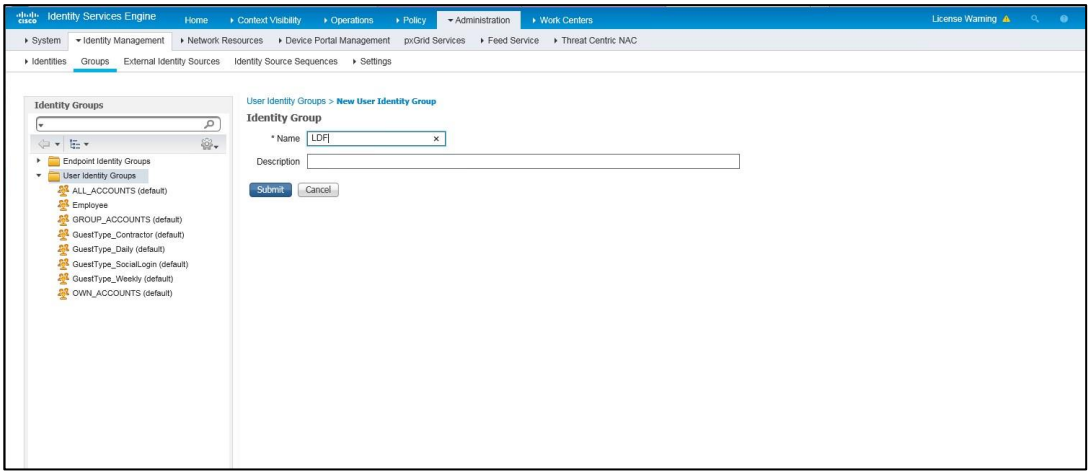
[AC-wlan-ap-ax] quit

5. 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] quit
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] 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13 ユーザーグループの作成



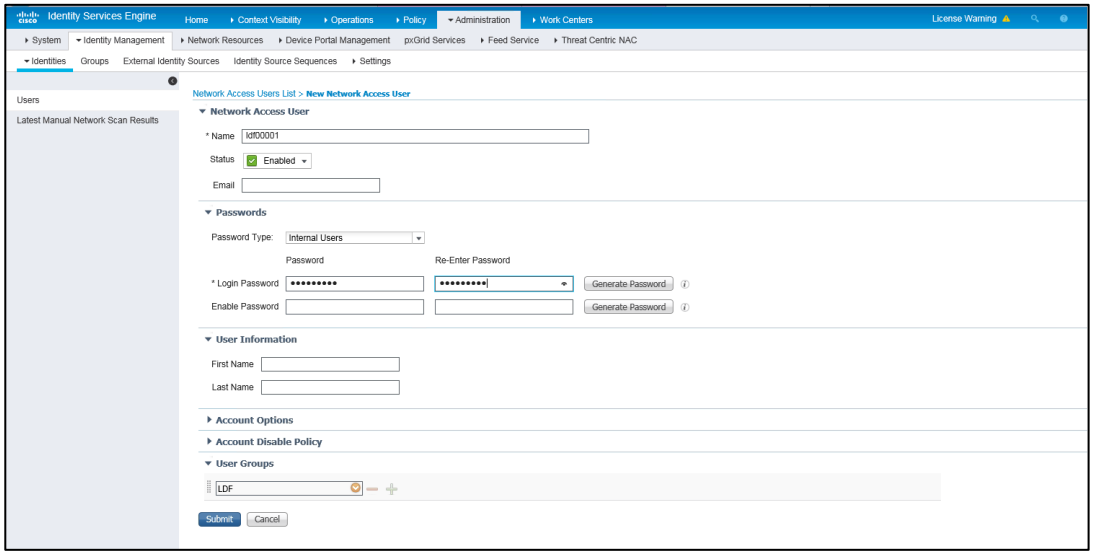
2. ネットワークアクセスユーザーを作成します。
   a. 上部ナビゲーションバーで、**Administration > Identity Management > Identities**を選択します。
   b. 左側のナビゲーションペインで、**Users**を選択します。
   c. **Add**をクリックします。

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



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。

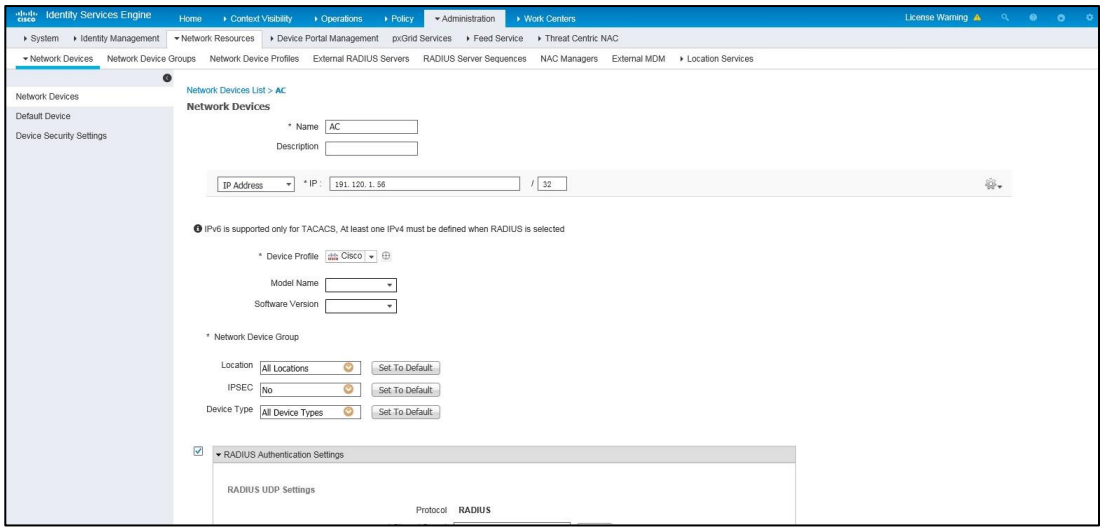
c. 表示されたページで、名前をACに設定し、IPアドレス191.120.1.56を指定して**RADIUS Authentication Settings**を選択し、共有秘密をH3ccに設定します。

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



4. 認証プロトコルを設定します。

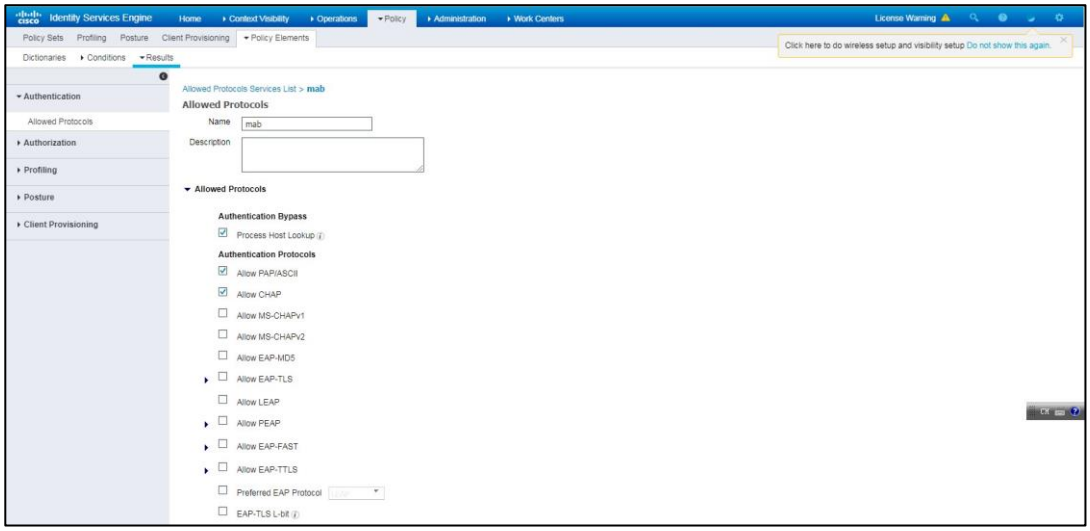
a. 上部ナビゲーションバーで、**Policy > Policy Elements > Results**を選択します。

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



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。

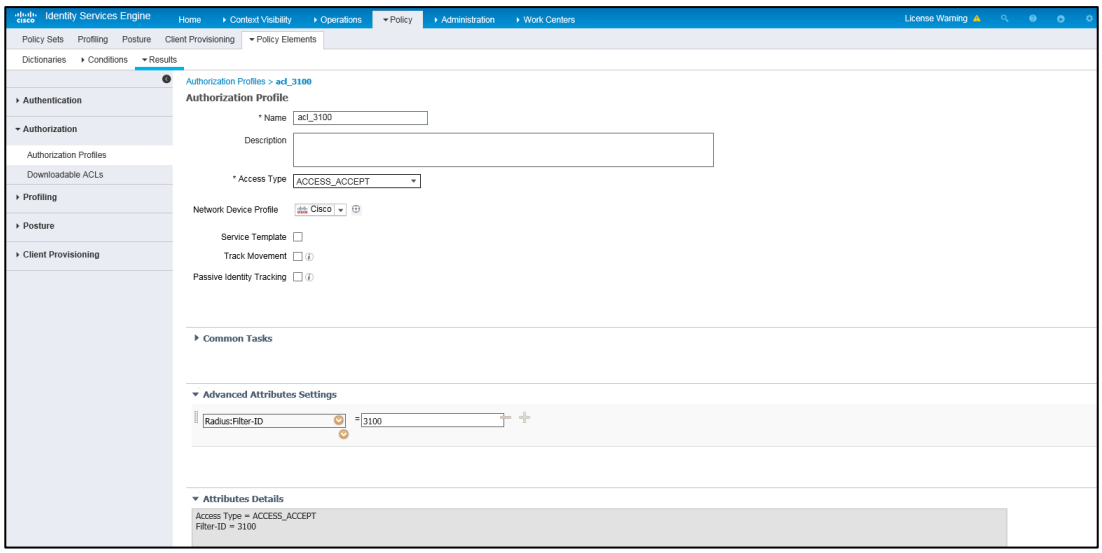
b. 左側のナビゲーションペインで、**Authorization > Authorization Profiles**を選択します。

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。

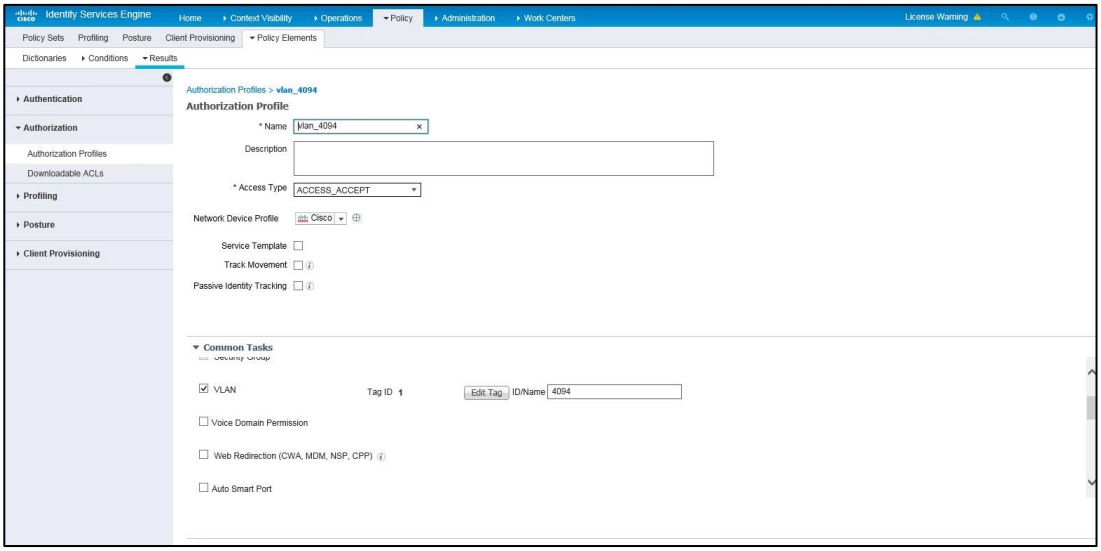
e. 設定を保存します。

図17 認可ACLの設定



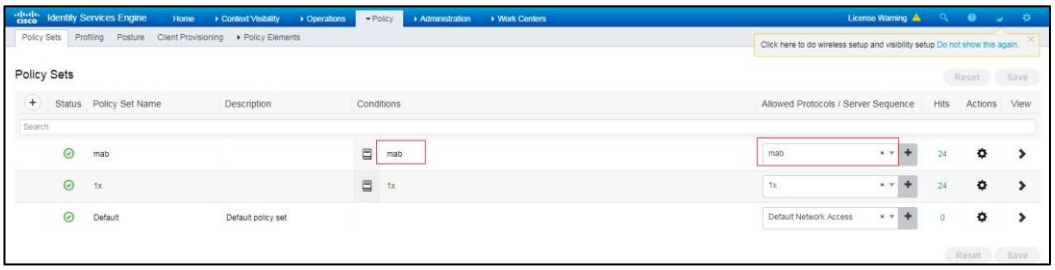
6. 許可VLANの設定:
   a. 上部ナビゲーションバーで、**Policy > Policy Elements > Results**を選択します。
   b. 左側のナビゲーションペインで、**Authorization > Authorization Profiles**を選択します。
   c. **Add**をクリックします。
   d. **Authorization Profile**領域で、名前をvlan_4094に設定し、**Network Device Profile**フィールドから**Cisco**を選択します。**Custom Tasks**領域で、**VLAN**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



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mabに設定し、条件名をmabに設定して**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



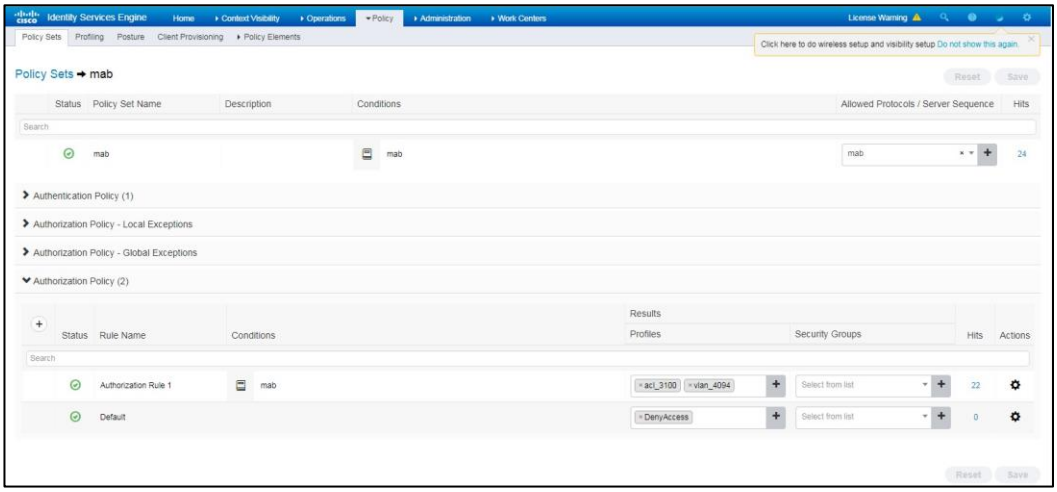
   d. 条件として**Wired_MAB**または**Wireless_MAB**を選択します。

図20 条件の構成

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。

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 connection
Total connections: 1
User MAC address                  : e8e8-b79b-438d
AP name                           : 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                   : 0h 0m 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$3$XYqokG6I8YoOymukIyvxoJuzFoB+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

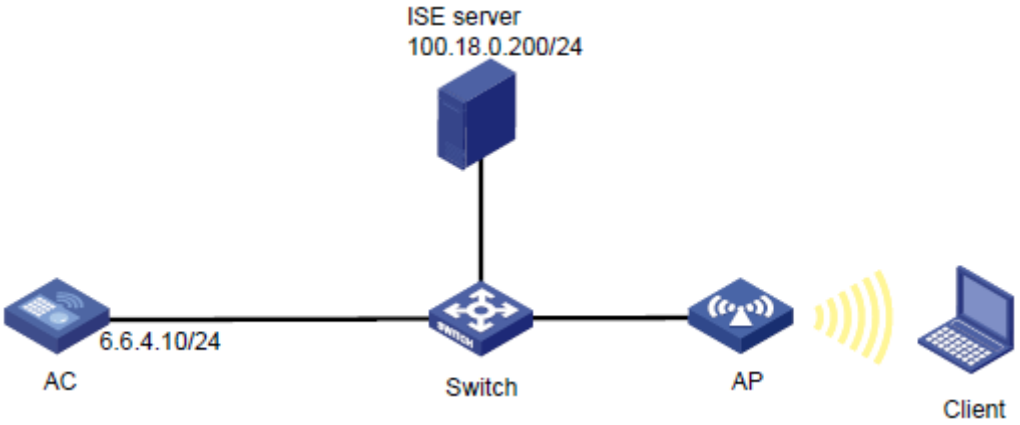
ネットワーク構成

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-a355-005056aba474
[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-websvr-https] default-logon-page ise_h3c.zip
```

4. 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
```

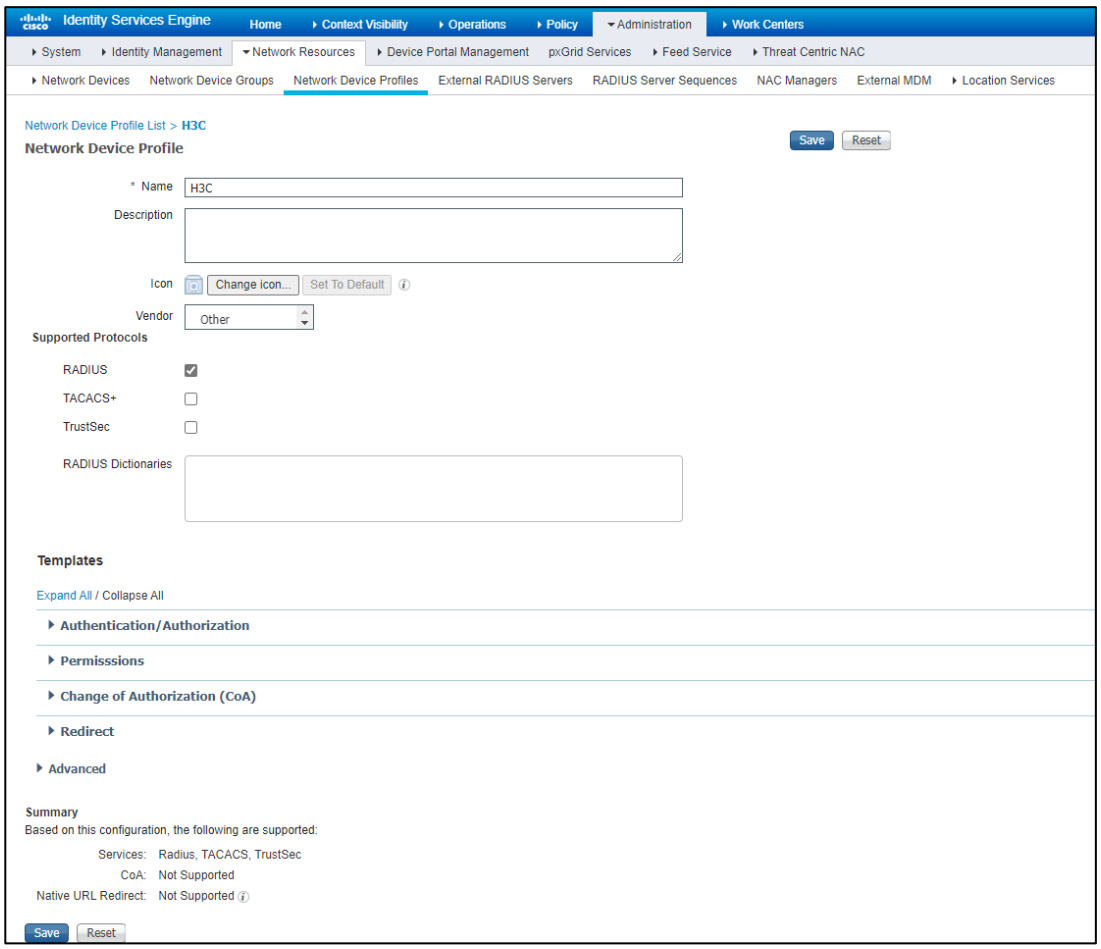
5. 手動APを設定し、サービステンプレートをAPのradio 1にバインドします。

```
[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

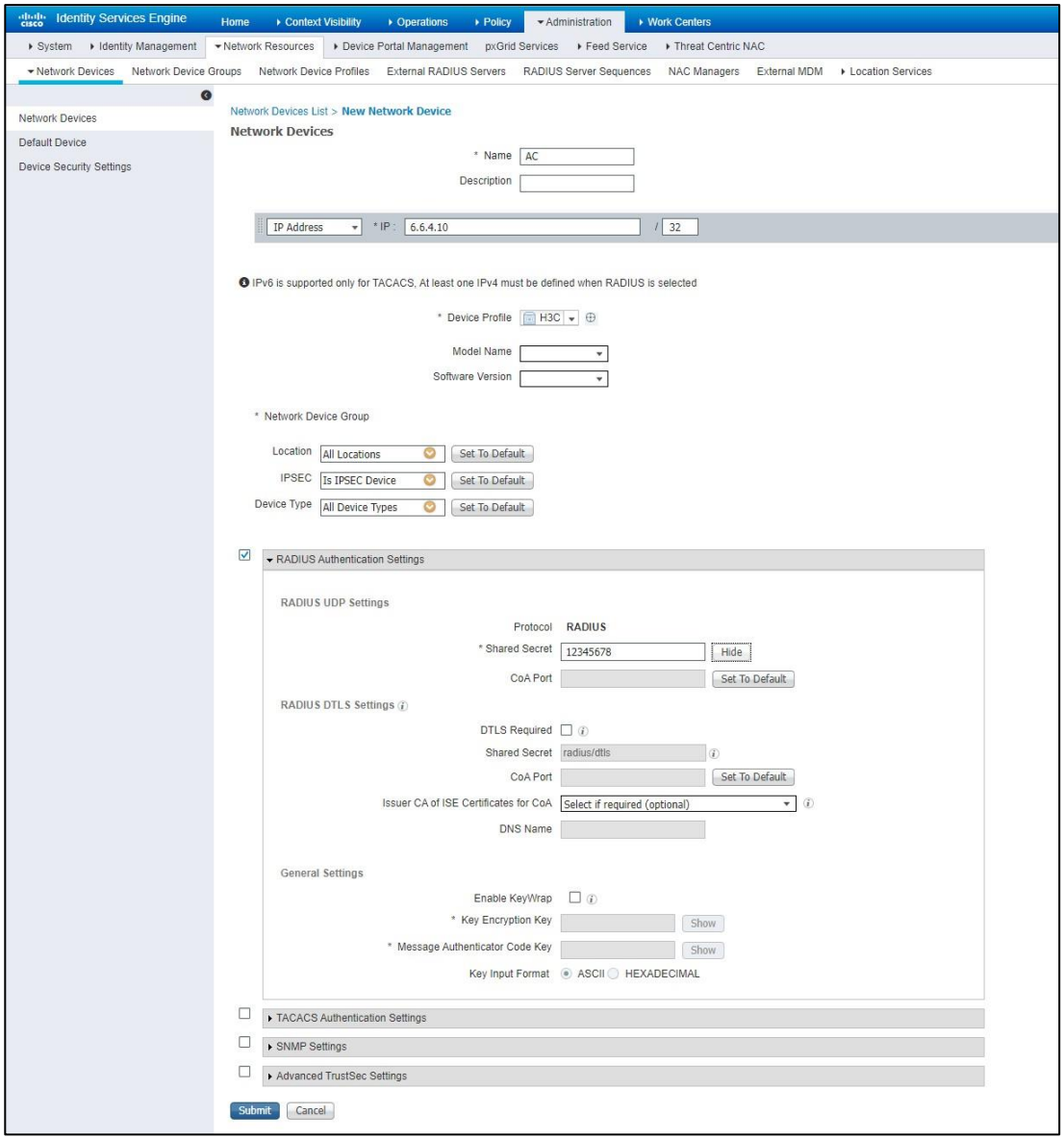


2. ACをネットワークアクセスデバイスとしてサーバーに追加します。
   a. 上部のナビゲーションバーで、**Administration > Network Resources > Network Devices**を選択します。
   b. **Add**をクリックします。
   c. 表示されたページで、名前を**AC**に設定し、デバイスプロファイル**H3C**を選択して、IPアドレス6.6.4.10を指定し、**RADIUS Authentication Settings**を選択して、共有秘密を**12345678**に設定します。

      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。

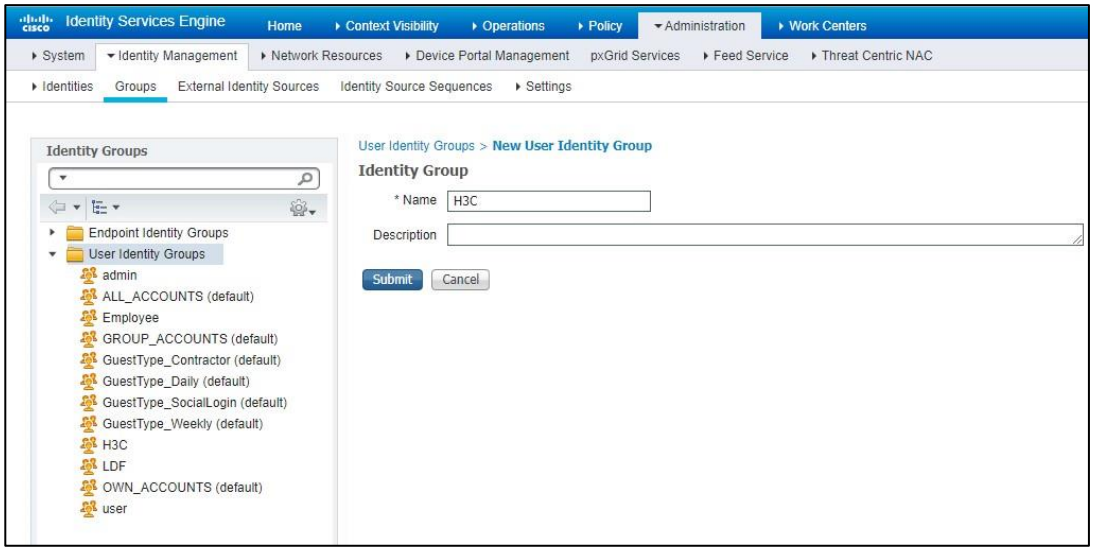
      共有秘密がACに設定された共有キーと同じであることを確認します。
   d. **Submit**をクリックします。

図25 サーバーへのAC電源の追加



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。

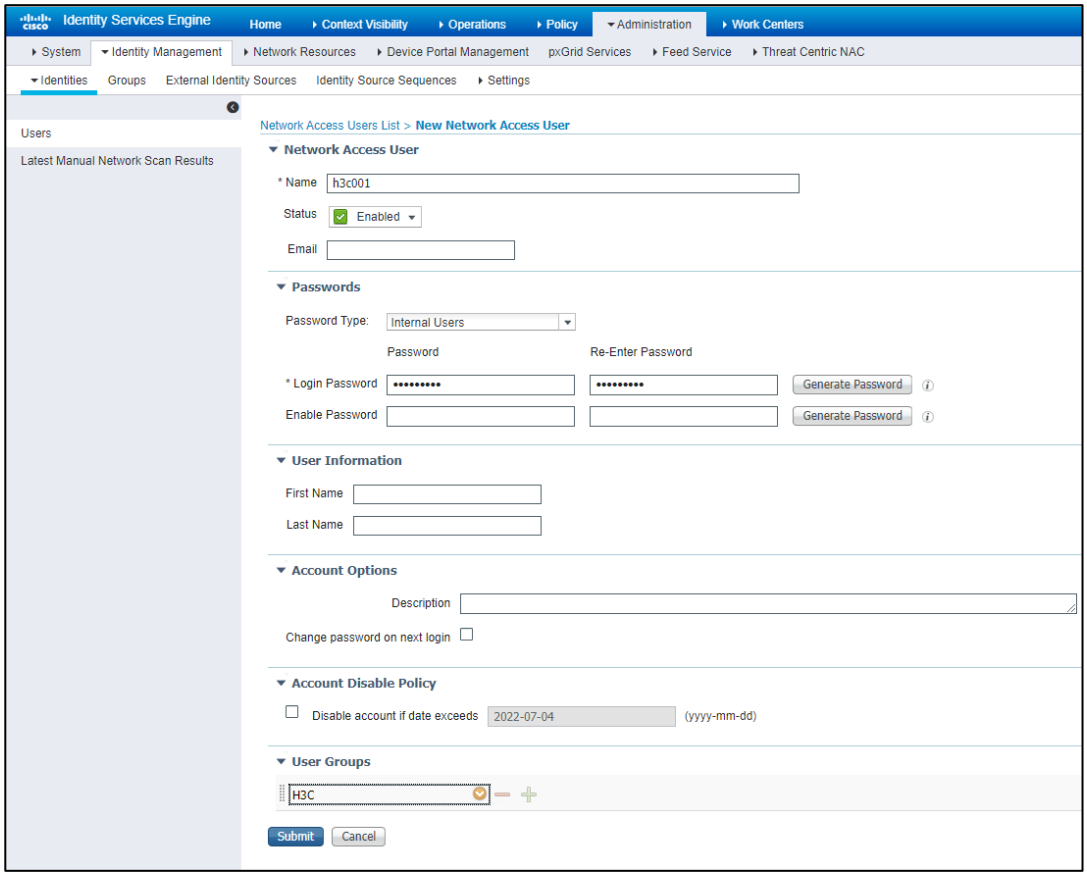
図26 ユーザーグループの作成



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。

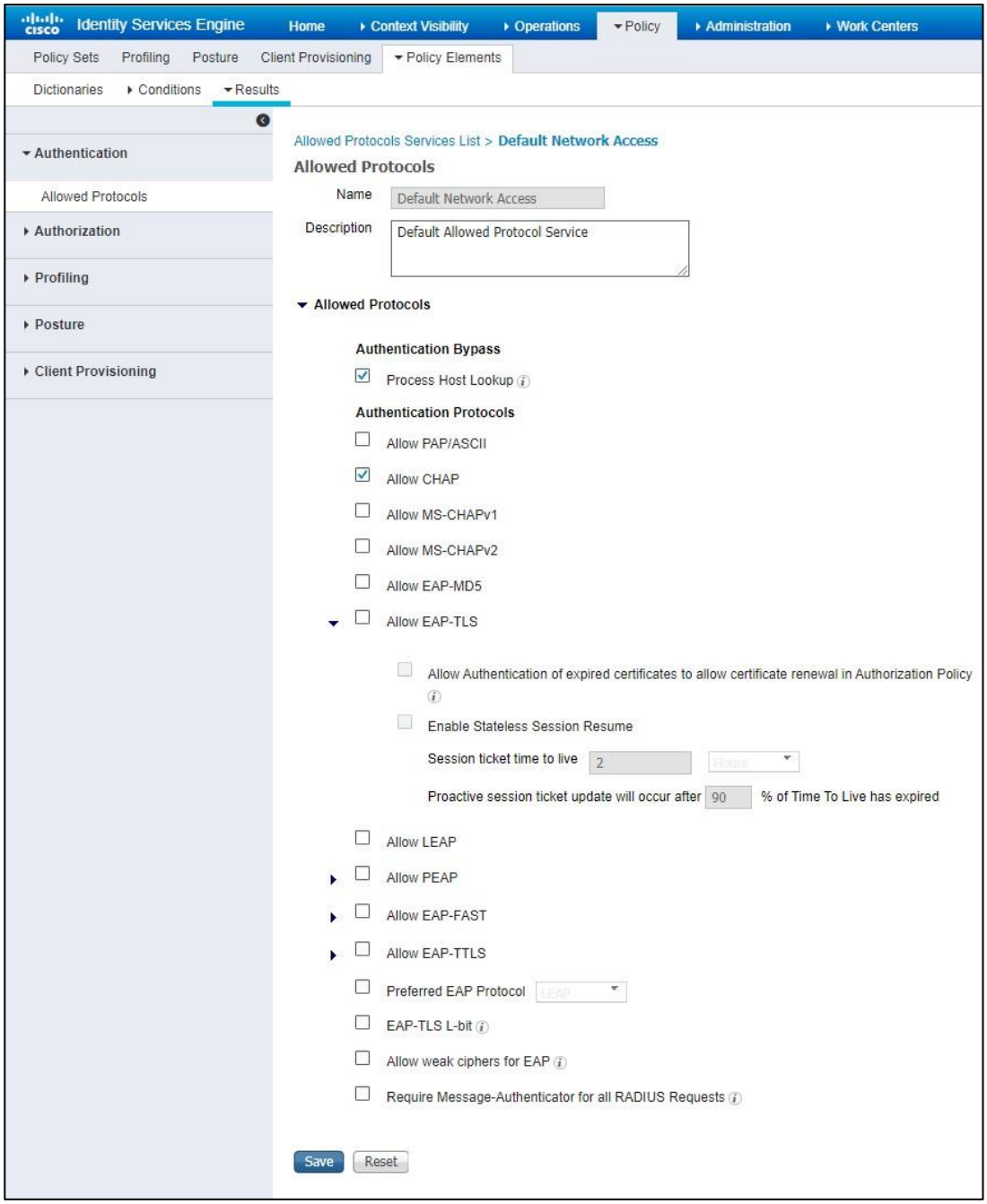
      パスワードに大文字、小文字、および数字が含まれていることを確認します。
   e. [Submit]をクリックします。

図27 ネットワークアクセスユーザーの作成



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



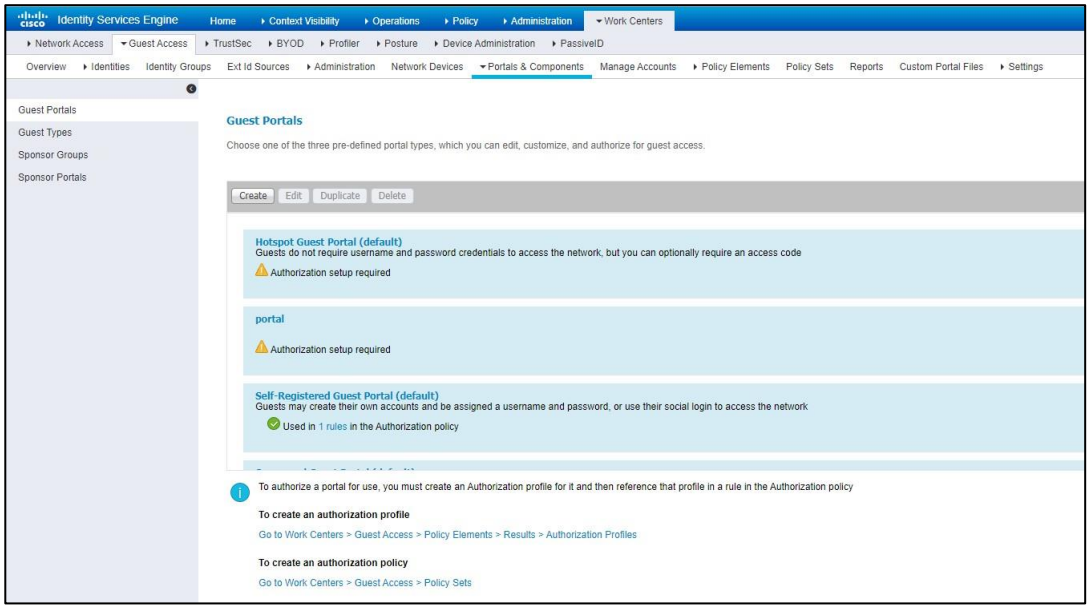
6. ポータル設定を構成します。

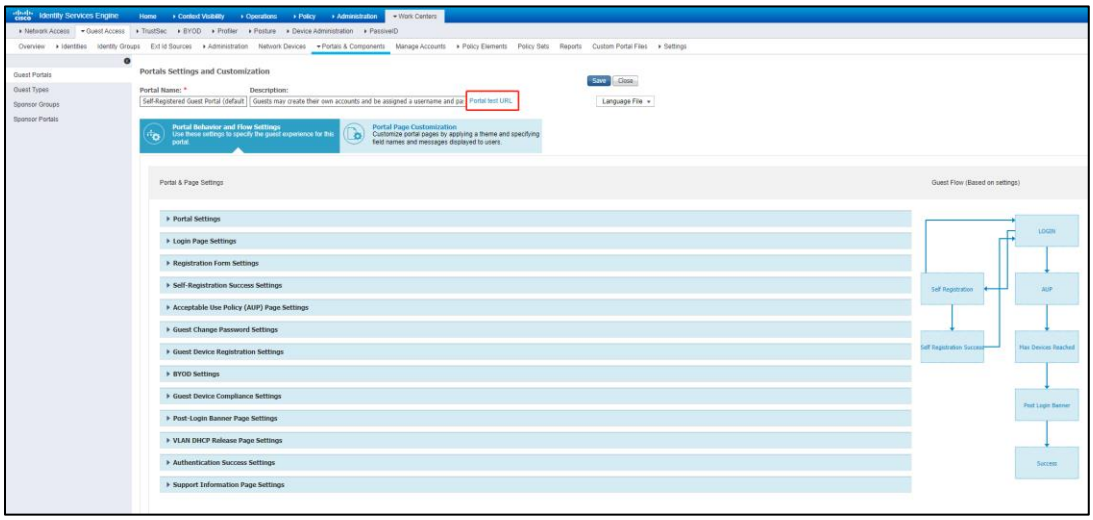
   a. 上部ナビゲーションバーで、**Work Centers > Guest Access > Portals & Components**を選択します。

   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

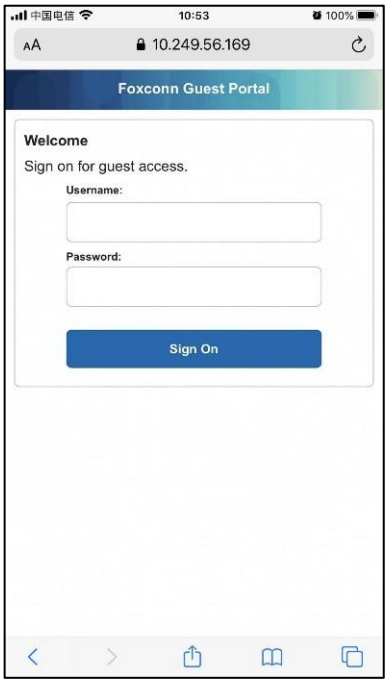


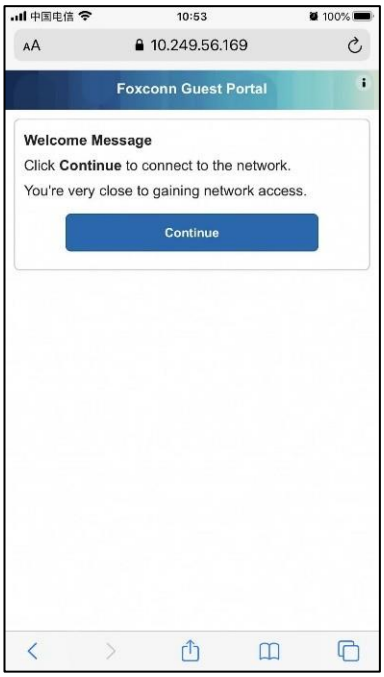


設定の確認

#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





#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
   MAC                    IP                    VLAN   Interface
   9cbc-f0e7-50f0   10.249.56.169  234      WLAN-BSS1/0/4
   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
```

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

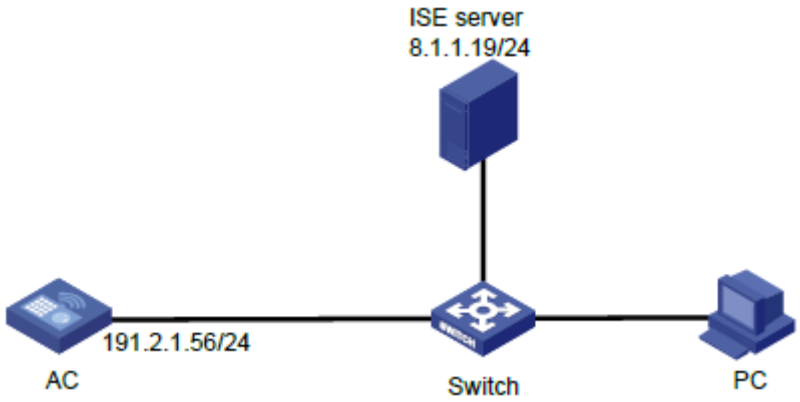
ネットワーク構成

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 c3$8zfqwa07HmNhvjWvEeixw5NGEGo82r/htRg=

   [AC-hwtacacs-tac] primary authorization 8.1.1.19 key cipher c3$fARZu6PskfKoULCy46SHq0hVbNHakBUPleE=

   [AC-hwtacacs-tac] primary accounting 8.1.1.19 key cipher

c3$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

3. 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

4. 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

5. 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。

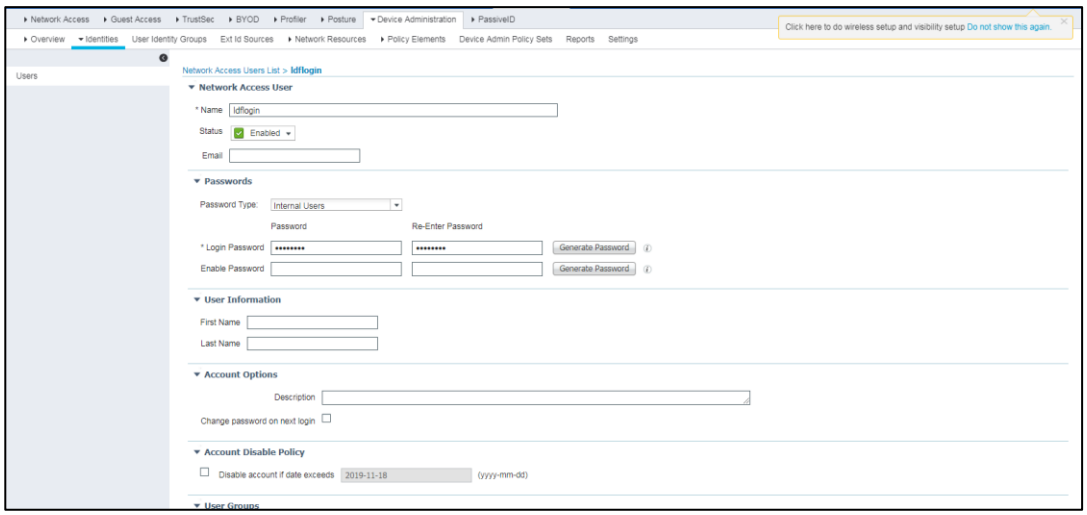
b. 左側のナビゲーションペインで、**Users**を選択します。

c. **Add**をクリックします。

d. 開いたページで、名前を**Idflogin**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

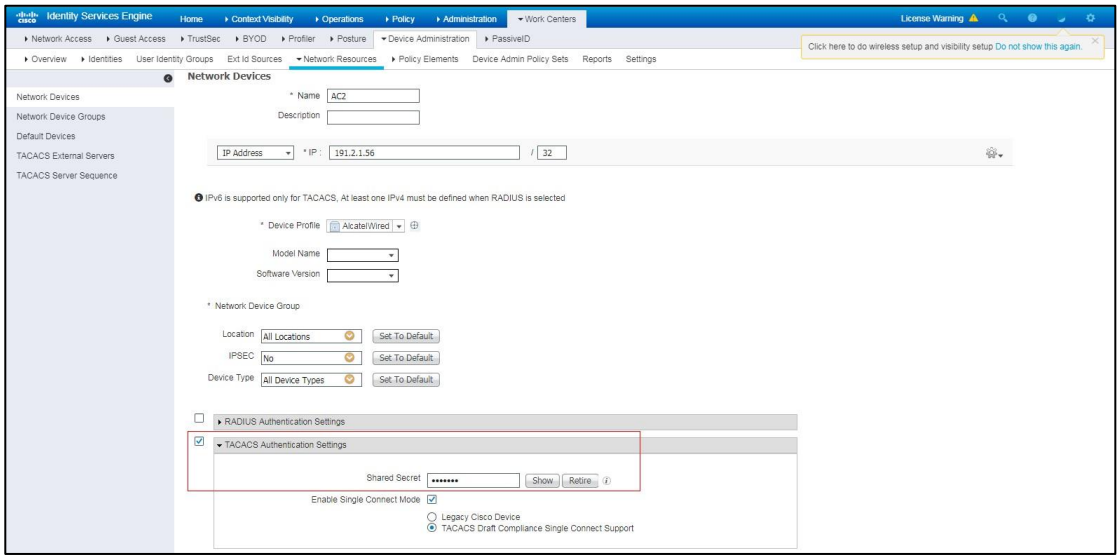


2. ACをネットワークアクセスデバイスとしてサーバーに追加します。
   a. トップナビゲーションバーで、**Work Centers > Device Administration > Network Resources**を選択します。
   b. 左側のナビゲーションペインで、**Network Devices**を選択します。
   c. **Add**をクリックします。
   d. 表示されたページで、名前をAC2に設定し、IPアドレス191.2.1.56を指定して**TACACS Authentication Settings**を選択し、共有秘密をH3ccに設定します。

      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。

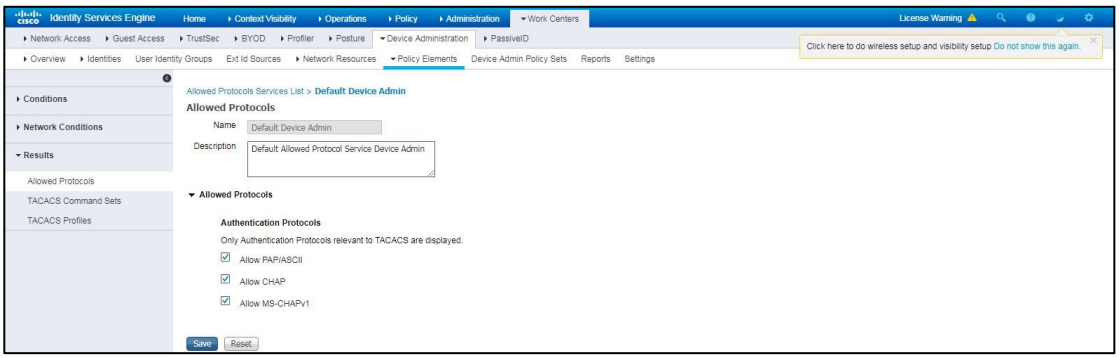
      共有秘密がACに設定された共有キーと同じであることを確認します。
   e. 設定を保存します。

図33 サーバーへのAC電源の追加



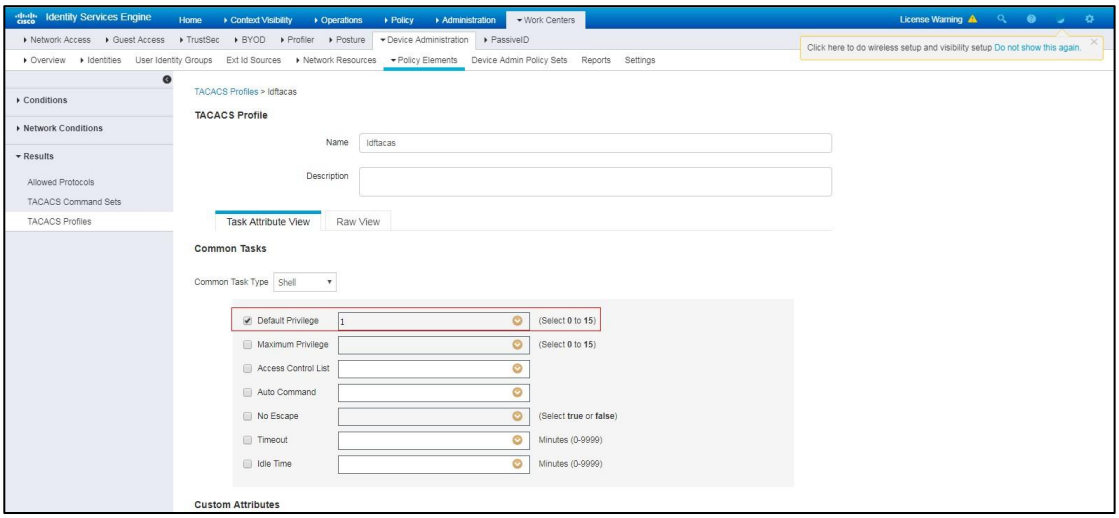
3. 認証プロトコルを設定します。
   a. 上部のナビゲーションバーで、**Work Centers > Device Administration > Policy Elements**を選択します。
   b. 左側のナビゲーションペインで、**Results > Allowed Protocols**を選択します。

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**



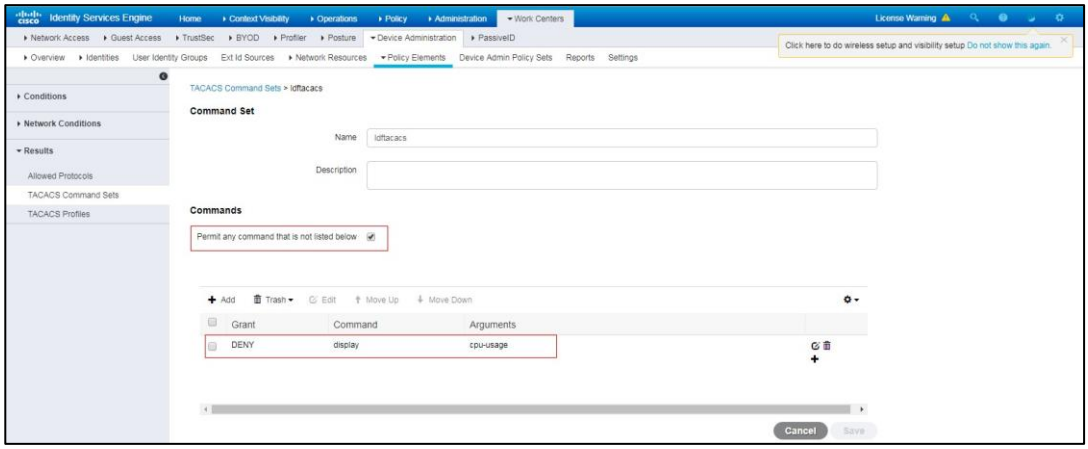
4. TACACSプロファイルを設定します。
   a. 上部のナビゲーションバーで、**Work Centers > Device Administration > Policy Elements**を選択します。
   b. 左側のナビゲーションペインで、**Results > TACACS Profiles**を選択します。
   c. **Add**をクリックします。
   d. 表示されたページで、名前をldftacasに設定し、**Default Privilege**を選択して、デフォルト権限をレベル1に設定します。
   e. 設定を保存します。

図35 TACACSプロファイルの設定



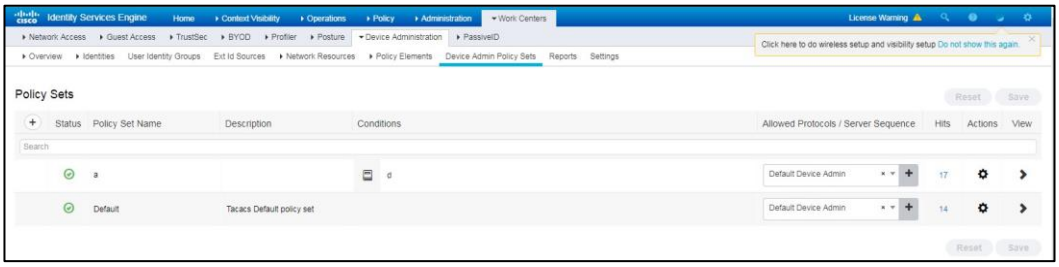
5. TACACSコマンドセットを設定します。
   a. 上部のナビゲーションバーで、**Work Centers > Device Administration > Policy Elements**を選択します。
   b. 左側のナビゲーションペインで、**Results > TACACS Command Sets**を選択します。
   c. **Add**をクリックします。
   d. 開いたページで、名前をldftacacsに設定します。Commands領域で、**Permit any command that not listed at below**を選択し、display cpu-usage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



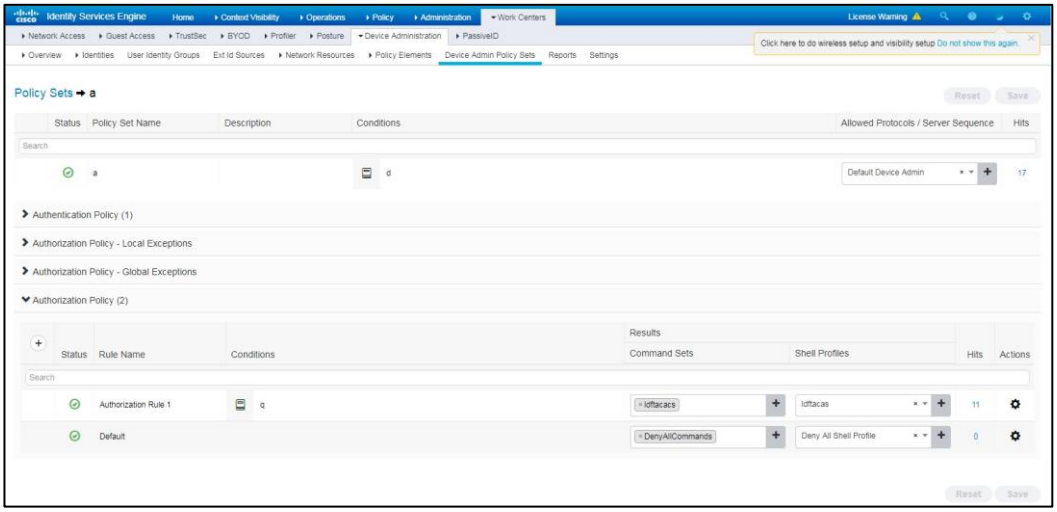
6. 認証および認可ポリシーセットを設定します。
   a. 上部のナビゲーションバーで、**Work Centers > Device Administration > Device Admin Policy Sets**を選択します。
   b. **Policy Sets**の下にあるプラスアイコン**+**をクリックします。
   c. ポリシーセット名を **a** に設定します。

図37 認証および許可ポリシーセットの構成



   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**ldftacacs**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ldftacasを選択します。

図38 許可ポリシーの追加



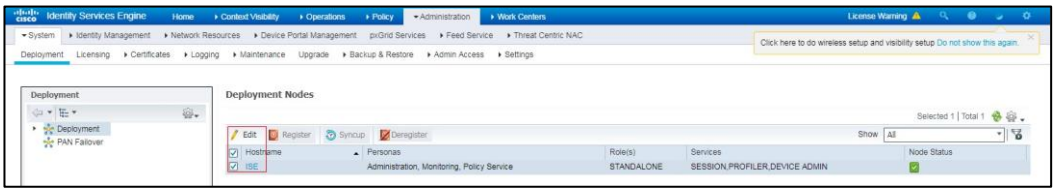
f. 設定を保存します。

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。

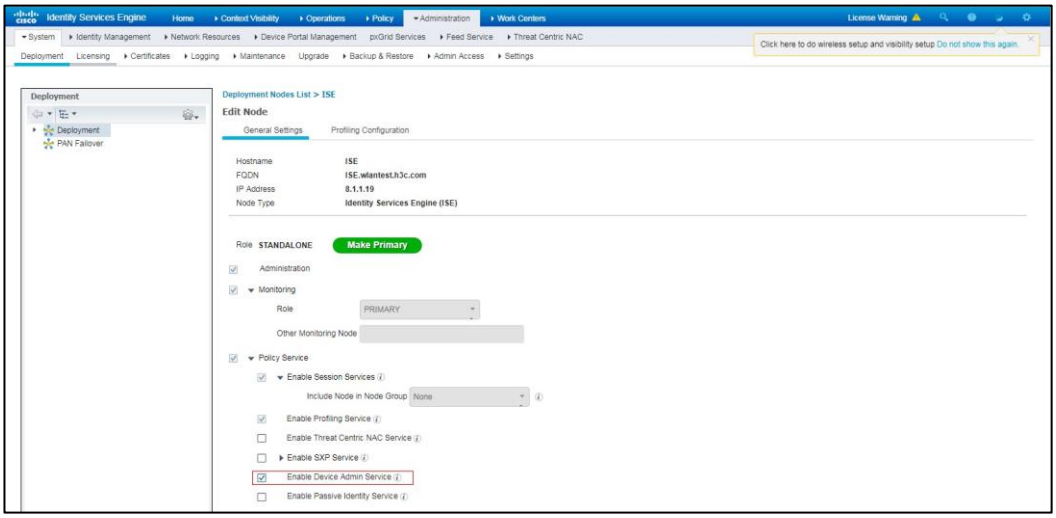
b. ISEノードを選択し、**Edit**をクリックします。

図39 ISEノードの選択とEditのクリック



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



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>
<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
Mem:      32537652   9064916  23472736         0        76    179300       72.1%
-/+ Buffers/Cache:   8885540  23652112
Swap:           0         0         0

Slot 2:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:      32537652   5749824  26787828         0       136    176664       82.3%
-/+ Buffers/Cache:   5573024  26964628
Swap:           0         0         0

<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
```