

Catalyst 9800でのアンカーを使用した中央Web認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[別のCatalyst 9800にアンカーされたCatalyst 9800の設定](#)

[ネットワーク図](#)

[両方の9800でのAAAの設定](#)

[WLCでのWLANの設定](#)

[外部WLCでポリシープロファイルとポリシータグを作成します](#)

[アンカーWLCでポリシープロファイルを作成します](#)

[両方の9800のリダイレクトACL設定](#)

[ISE の設定](#)

[AireOS WLCにアンカーされたCatalyst 9800の設定](#)

[Catalyst 9800の外部設定](#)

[アンカーAireOS WLCのAAA設定](#)

[AireOS WLCのWLAN設定](#)

[AireOS WLCでのリダイレクトACL](#)

[ISE の設定](#)

[AireOS WLCが外部で、Catalyst 9800がアンカーである場合の設定の違い](#)

[確認](#)

[トラブルシューティング](#)

[Catalyst 9800のトラブルシューティング情報](#)

[クライアント詳細](#)

[Embedded Packet Capture](#)

[RadioActiveトレース](#)

[AireOSのトラブルシューティング情報](#)

[クライアント詳細](#)

[CLIからのデバッグ](#)

[参考資料](#)

概要

このドキュメントでは、別のワイヤレスLANコントローラ(WLC)をモビリティアンカーとしてポイントするCatalyst 9800上で、AireOSまたは別の9800 WLCを使用した中央Web認証(CWA)を設定およびトラブルシューティングする方法方法について説明します。

前提条件

要件

9800 WLC、AireOS WLC、およびCisco ISEの基本的な知識があることが推奨されます。CWAアンカー設定を開始する前に、2台のWLC間のモビリティトンネルをすでに確立していることを前提としています。これは、この設定例の範囲外です。この問題に関するヘルプが必要な場合は、ドキュメント「[Catalyst 9800コントローラでのモビリティトンネルの構築](#)」を参照してください

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

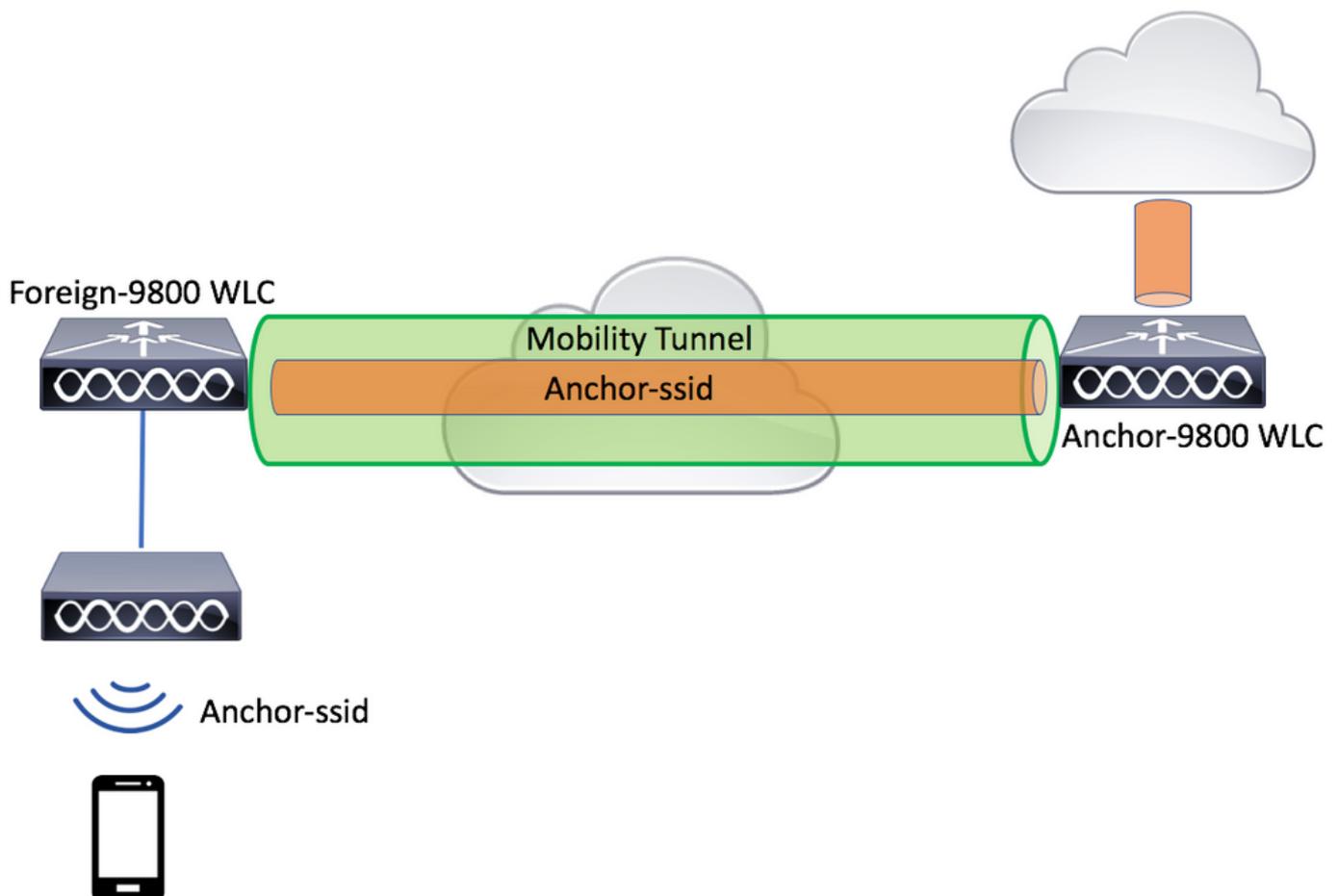
9800 17.2.1

5520 8.5.164 IRCMイメージ

ISE 2.4

別のCatalyst 9800にアンカーされたCatalyst 9800の設定

ネットワーク図



両方の9800でのAAAの設定

アンカーと外部の両方で、まずRADIUSサーバを追加し、CoAが有効になっていることを確認する必要があります。これはメニューで実行できます[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Servers]> [Add]ボタンをクリックします

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top reads 'Configuration > Security > AAA'. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'Servers / Groups' section with the 'RADIUS' tab active. A 'Create AAA Radius Server' dialog box is open, showing the following fields and values:

Field	Value
Name*	CLUS-Server
Server Address*	X.X.X.X
PAC Key	<input type="checkbox"/>
Key Type	Clear Text
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

The 'Support for CoA' field is highlighted with a red box. At the bottom of the dialog, there are 'Cancel' and 'Apply to Device' buttons.

ここで、サーバグループを作成し、設定したサーバをそのグループに配置する必要があります。これは、[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Server Groups] > [Add]で行います。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS Servers Server Groups

TACACS+

LDAP

Create AAA Radius Server Group

Name* CLUS-Server-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers Assigned Servers

CLUS-Server

Cancel Apply to Device

ここで、認証方式リストを作成します（CWAでは認証方式リストは不要です）。タイプがnetwork、グループタイプがgroupです。前のアクションのサーバグループをこのメソッドリストに追加します。

この設定は、[Configuration] > [Security] > [AAA] > [Servers/AAA Method List] > [Authorization] > [Add]で行います

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization + Add × Delete

Accounting

Quick Setup: AAA Authorization

Method List Name* CLUS-AuthZ-Meth-List

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups Assigned Server Groups

radius ldap tacacs+ ISE1

CLUS-Server-Group

Cancel Apply to Device

(オプション) 認可方式リストと同じサーバグループを使用して、アカウントリング方式リストを作成します。アカウントリングリストは、[Configuration] > [Security] > [AAA] > [Servers/AAA Method List] > [Accounting] > [Add]で作成できます

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar shows the navigation menu with "Configuration" selected. The main content area is titled "AAA Method List" and includes a "+ Add" button. A modal window titled "Quick Setup: AAA Accounting" is open, showing the following configuration details:

- Method List Name*: CLUS-Acct-Meth-List
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for "Cancel" and "Apply to Device" are visible at the bottom of the modal.

WLCでのWLANの設定

両方のWLCでWLANを作成し、設定します。WLANは両方で一致する必要があります。セキュリティタイプはMACフィルタリングで、前の手順の認可方式リストを適用する必要があります。この設定は、[Configuration] > [Tags & Profiles] > [WLANs>+Add]で行います

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Profile Name* CLUS-WLAN-Name Radio Policy All

SSID* CLUS-SSID Broadcast SSID ENABLED

WLAN ID* 2

Status ENABLED

Cancel Apply to Device

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None Lobby Admin Access

MAC Filtering Fast Transition Adaptive Enab...

OWE Transition Mode Over the DS

Authorization List* CLUS-AuthZ-Meth-l Reassociation Timeout 20

Cancel Apply to Device

外部WLCでポリシープロファイルとポリシータグを作成します

外部WLC Web UIに移動します。

ポリシープロファイルを作成するには、[Configuration] > [Tags & Profiles] > [Policy] > [Add]に移動します

アンカーするときは、中央スイッチングを使用する必要があります。

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller Web UI. The breadcrumb navigation is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog is open, showing the **General** tab. The **Status** field is set to **ENABLED** and highlighted. The **WLAN Switching Policy** section is highlighted, showing the following settings:

Policy Name	Status
Central Switching	ENABLED
Central Authentication	ENABLED
Central DHCP	ENABLED
Central Association	ENABLED
Flex NAT/PAT	DISABLED

[Advanced]タブでは、CWAにはAAAオーバーライドとRADIUS NACが必須です。ここでは、アカウントリング方式リストを作成するように選択した場合に、そのリストを適用することもできます。

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Client Exclusion Timeout (sec) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type RADIUS

Policy Name default-aaa-policy x

Accounting List CLUS-Acct-Meth-x

Fabric Profile Search or Select

mDNS Service Policy Search or Select

Hotspot Server Search or Select

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map Not Configured Clear

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

[Mobility]タブで、[export anchor]チェックボックスをオンにしないで、アンカーリストにアンカーWLCを追加します。[Apply to Device]を必ず押してください。この場合、2つのコントローラ間にモビリティトンネルがすでに設定されていることを前提としています

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility **DISABLED**

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

Anchor IP No anchors available

Selected (1)

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

Cancel Apply to Device

APがこのポリシープロファイルを使用するには、ポリスタグを作成し、使用するAPに適用する必要があります。

ポリシータグを作成するには、[Configuration] > [Tags & Profiles] > [Tags?Policy] > [Add]に移動します

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation path is Configuration > Tags & Profiles > Tags. The 'Policy' tab is selected, and the '+ Add' button is highlighted. The 'Add Policy Tag' dialog box is open, showing the following details:

- Name*: CLUS-Policy-Tag
- Description: Policy Tag for CLUS
- WLAN-POLICY Maps: 0
- WLAN Profile: CLUS-WLAN-Name
- Policy Profile: CLUS-Policy-Profile

The 'Map WLAN and Policy' section shows the mapping of the selected WLAN Profile and Policy Profile. The 'Apply to Device' button is highlighted at the bottom right of the dialog.

これを複数のAPに同時に追加するには、[Configuration] > [Wireless Setup] > [Advanced] > [Start Now]に移動します。[Tag APs]の横にある箇条書きバーをクリックし、選択したAPにタグを追加します。

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

<input type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	
<input checked="" type="checkbox"/>	Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local	E
<input checked="" type="checkbox"/>	Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local	E
<input checked="" type="checkbox"/>	AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local	D

1 10 items per page

Tag APs

Tags

Policy: CLUS-Policy-Tag

Site: Search or Select

RF: Search or Select

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

アンカーWLCでポリシープロファイルを作成します

アンカーWLC Web UIに移動します。アンカー9800の[Configuration] > [Tags & Profiles] > [Tags] > [Policy] > [+Add]でポリシープロファイルを追加します。これは、モビリティタブとアカウントングリストを除き、外部で行われたポリシープロファイルと一致していることを確認します。

ここではアンカーを追加しませんが、[Export Anchor]チェックボックスはオンにします。ここでアカウントングリストを追加しないでください。この場合、2つのコントローラ間にモビリティトンネルがすでに設定されていることを前提としています

注：このプロファイルをポリスタグ内のWLANに関連付ける理由はありません。これにより、問題が発生します。このWLC上のAPに同じWLANを使用する場合は、それに対して別のポリシープロファイルを作成します。

Configuration > Tags & Profiles > Policy

+ Add × Delete

Add Policy Profile

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)		Selected (0)	
Anchor IP		Anchor IP	Anchor Priority
192.168.160.16	→	Anchors not assigned	

Cancel Apply to Device

両方の9800のリダイレクトACL設定

次に、両方の9800でリダイレクトACL設定を作成する必要があります。ACLをトラフィックに適用するアンカー-WLCであるため、外部のエントリは重要ではありません。唯一の要件は、そこにエントリがあるということです。アンカー上のエントリは、ポート8443でISEへのアクセスを「拒否」し、それ以外はすべて「許可」する必要があります。このACLは、クライアントから「着信」するトラフィックにのみ適用されるため、リターントラフィックのルールは必要ありません。DHCPとDNSは、ACLのエントリなしでパススルーします。

Cisco Catalyst 9800-L Wireless Controller 17.2.1 Welcome admin
Last login None

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

+ Add - Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
<input type="checkbox"/> 100	permit	any		any		ip	None	None	None	Disabled

10 items per page 1 - 2 of 2 items

Cancel Apply to Device

ISE の設定

最後の手順は、CWA用にISEを設定することです。これには多くのオプションがありますが、この例では基本に従い、デフォルトの自己登録ゲストポータルを使用します。

ISEでは、認可プロファイル、認証ポリシーと認可プロファイルを使用する認可ポリシーを含むポリシーセットを作成し、9800 (外部) をネットワークデバイスとしてISEに追加し、ユーザ名とパスワードを作成してネットワークにログインする必要があります。

認可プロファイルを作成するには、**[Policy] > [Policy Elements] > [Authorization] > [Results] > [Authorization Profiles] > [Add]**をクリックします。返されるアクセスタイプが「access_accept」であることを確認し、返信するAVP (属性と値のペア) を設定します。CWAでは、リダイレクトACLとリダイレクトURLは必須ですが、VLAN IDやセッションタイムアウトなどの情報を返信することもできます。ACL名は、外部とアンカー9800の両方のリダイレクトACLの名前と一致することが重要です。

← → ↻ Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > test

Authorization Profile

* Name CLUS-AuthZ-Profile-ISE

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal

次に、作成した認可プロファイルをCWAを通過するクライアントに適用する方法を設定する必要があります。これを実現するには、MAB使用時に認証をバイパスするポリシーセットを作成し、着信側ステーションIDで送信されるSSID使用時に認証プロファイルを適用する方法があります。繰り返しになりますが、これを実現する方法は数多くありますので、より具体的な方法や、より安全な方法が必要な場合は、これが最も簡単な方法です。

ポリシーセットを作成するには、[Policy] > [Policy Sets]に移動し、画面の左側にある[+]ボタンをクリックします。新しいポリシーセットに名前を付け、「default network access」またはMABの「Process Host Lookup」を許可する許可されたプロトコルリスト（許可されたプロトコルリストを確認するには、[Policy] > [Policy Elements] > [Results] > [Authentication] > [Allowed Protocols]に移動）にします。作成した新しいポリシーセットの中央にある+記号をクリックします。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

License Warning

Click here to do visibility setup Do not show this again.

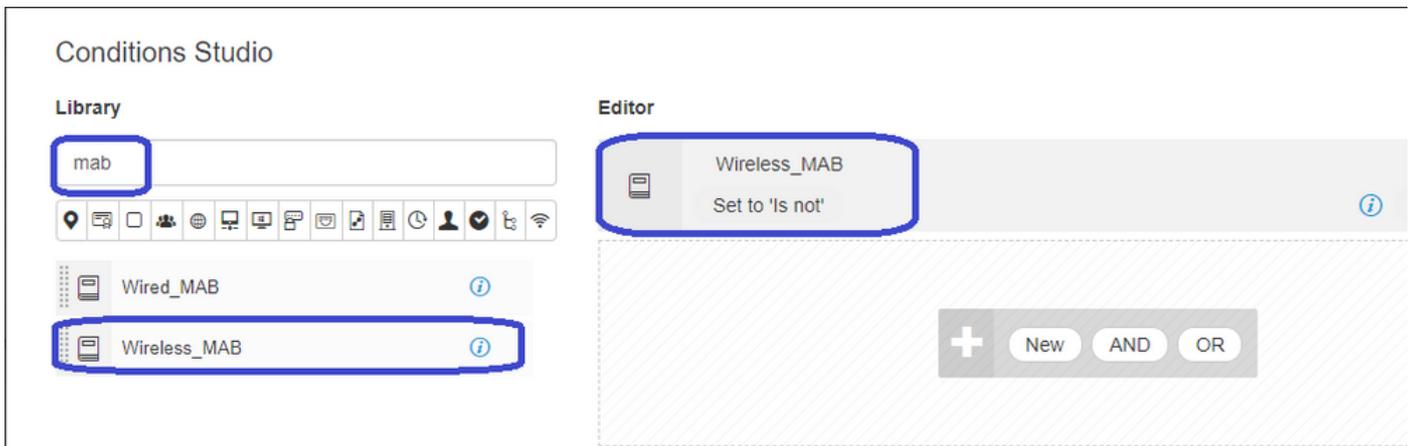
ResetAll Hitcounts Reset Save

Policy Sets

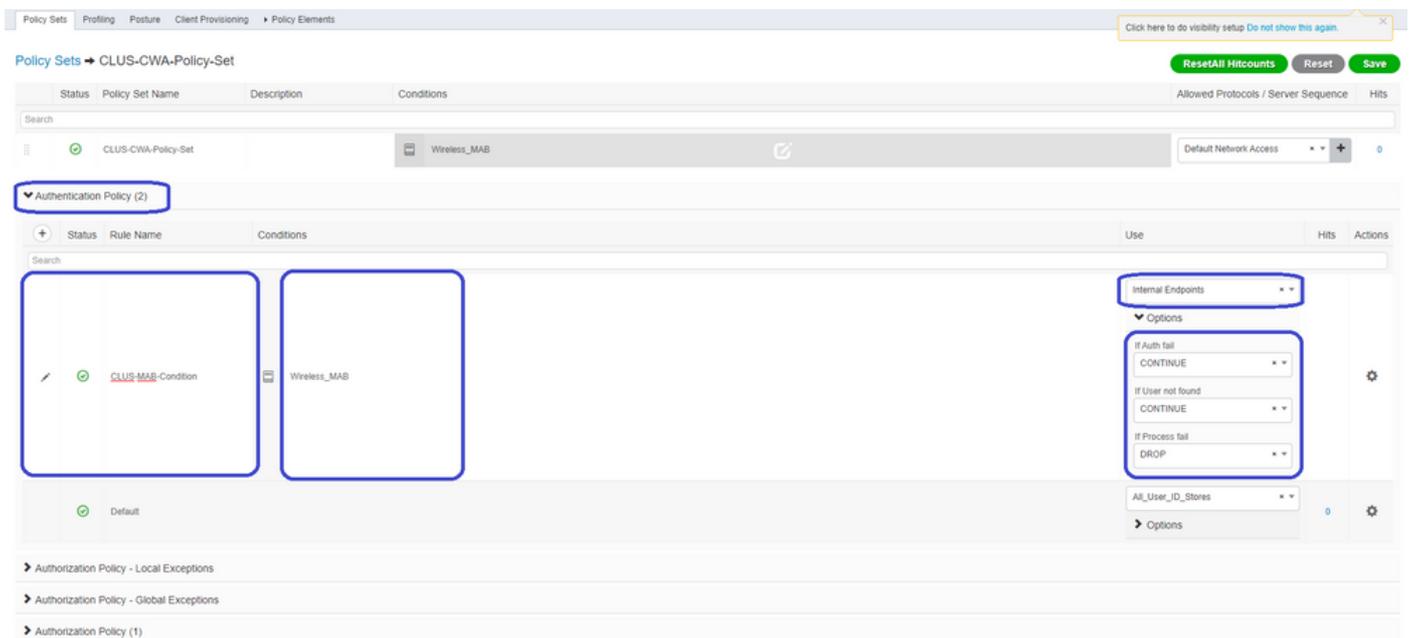
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	CLUS-CWA-Policy-Set			Default Network Access			
	Default	Default policy set		Default Network Access	0		

Reset Save

ISEでMABが使用されるたびに、このポリシーセットが通過します。後で、着信側ステーションIDに一致する認可ポリシーを作成して、使用されているWLANに応じて異なる結果を適用できます。このプロセスはカスタマイズ可能で、多くのものをマッチさせることができます。



ポリシーセット内で、ポリシーを作成します。認証ポリシーはMABで再度一致しますが、「内部エンドポイント」を使用するようにIDストアを変更し、認証が失敗してユーザが見つからない場合は、オプションを変更する必要があります。



認証ポリシーを設定したら、認可ポリシーに2つのルールを作成する必要があります。このポリシーはACLのように読み取られるので、順序の先頭にポスト認証ルール、末尾にプレ認証ルールが必要です。認証後ルールは、すでにゲストフローを通過したユーザと一致します。これは、すでにサインインしている場合は、ルールにヒットし、そこで停止するということです。ログインしていない場合は、リストをダウンし続け、リダイレクトを受け取る事前認証ルールをヒットします。認証ポリシールールをSSIDで終わる着信側ステーションIDと照合して、設定されたWLANのみにヒットすることをお勧めします。

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
🟢	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (4)

+	Status	Rule Name	Conditions	Results	Profiles	Security Groups
🟢	Post-CWA	AND	Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth		Select from list
🟢	MAB on WLAN	AND	Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE		Select from list
🟢	Flex AuthZ		Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA		Select from list
🟢	Default			DenyAccess		Select from list

ポリシーセットを設定したら、ISEがオーセンティケータとして信頼できるように、9800（外部）についてISEに通知する必要があります。これは、[Admin] > [Network Resources] > [Network Device] > [+]で実行できます。名前を付け、IPアドレス（この場合はadminサブネット全体）を設定し、RADIUSを有効にし、共有秘密を設定する必要があります。ISEの共有秘密は、9800の共有秘密と一致する必要があります。一致しないと、このプロセスは失敗します。設定を追加したら、送信ボタンを押して保存します。

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 Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices List > JaysNet

Network Devices

* Name: CLUS_Net-Device

Description: []

IP Address: * IP: 192.168.160.0 [24]

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

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

Shared Secret: [] [Show]

Use Second Shared Secret: [] [Show]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings []

最後に、クライアントがネットワークにアクセスできることを確認するために、クライアントがログインページに入力するユーザ名とパスワードを追加する必要があります。これは、[Admin] >

[Identity Management] > [Identity] > [Users] > [Add] で行います。追加した後で[submit]をクリックしてください。ISEと同様に、これはカスタマイズ可能で、ローカルに保存する必要はありませんが、もう一度は最も簡単な設定です。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name CLUS-User

Status Enabled

Email

Passwords

Password Type: Internal Users

Password

* Login Password

Re-Enter Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

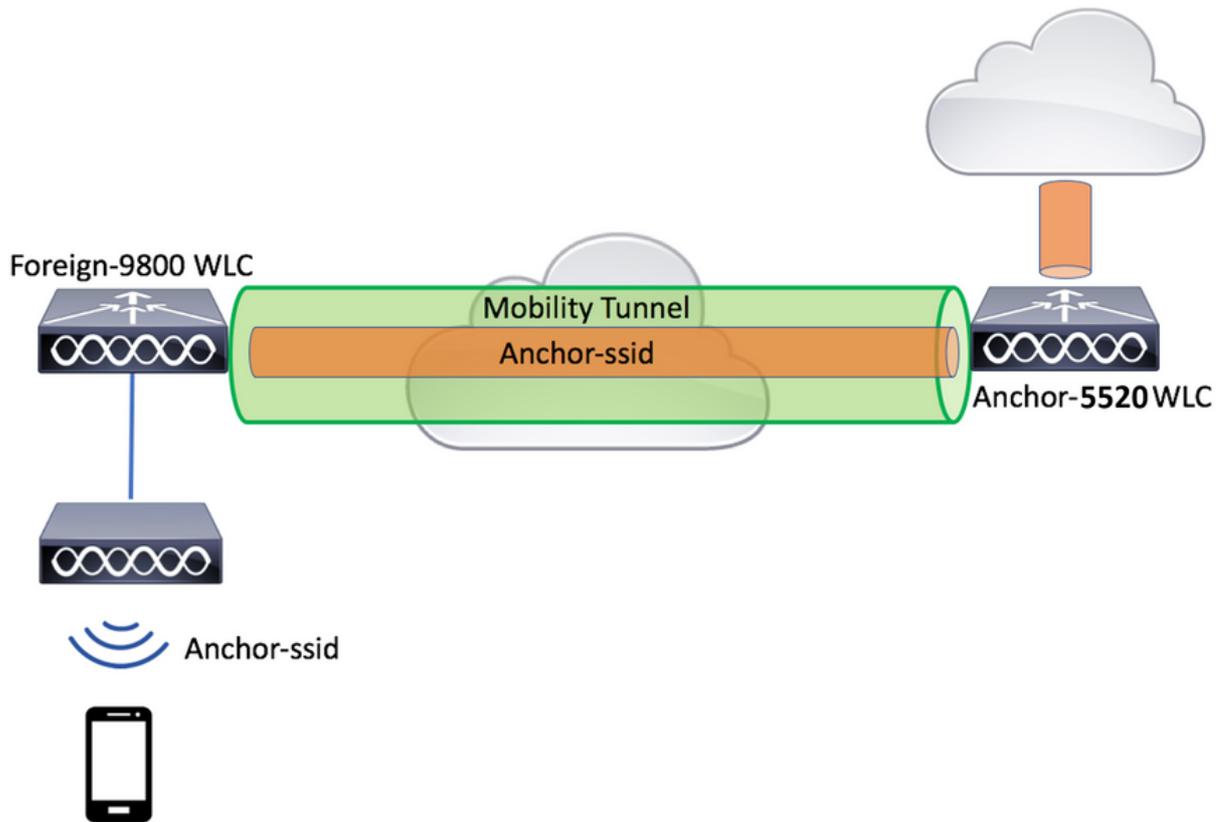
Disable account if date exceeds 2020-07-17 (yyyy-mm-dd)

User Groups

Select an item

Submit Cancel

AireOS WLCにアンカーされたCatalyst 9800の設定



Catalyst 9800の外部設定

「アンカーWLCでのポリシープロファイルの作成」セクションをスキップし、前述の手順と同じ手順に従ってください。

アンカーAireOS WLCのAAA設定

[Security] > [AAA] > [RADIUS] > [Authentication] > [New]の順に選択して、サーバをWLCに追加します。サーバのIPアドレス、共有秘密、およびCoAのサポートを追加します。

The top screenshot shows the 'RADIUS Authentication Servers' configuration page in the Cisco Catalyst GUI. The 'Auth Called Station ID Type' is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen' and the 'Framed MTU' is 1300. A table below lists the configuration for a new server.

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status

The bottom screenshot shows the 'New' configuration page for a RADIUS server. The 'Server Index (Priority)' is 1. The 'Server IP Address(Ipv4/Ipv6)' is 192.168.160.99. The 'Shared Secret Format' is ASCII and the 'Shared Secret' is masked with asterisks. The 'Confirm Shared Secret' is also masked. The 'Apply Cisco ISE Default settings' checkbox is checked. The 'Key Wrap' checkbox is unchecked. The 'Port Number' is 1812. The 'Server Status' is 'Enabled'. The 'Support for CoA' is 'Enabled'. The 'Server Timeout' is 5 seconds. The 'Network User' and 'Management' checkboxes are checked. The 'Management Retransmit Timeout' is 5 seconds. The 'Tunnel Proxy', 'PAC Provisioning', and 'IPSec' checkboxes are unchecked.

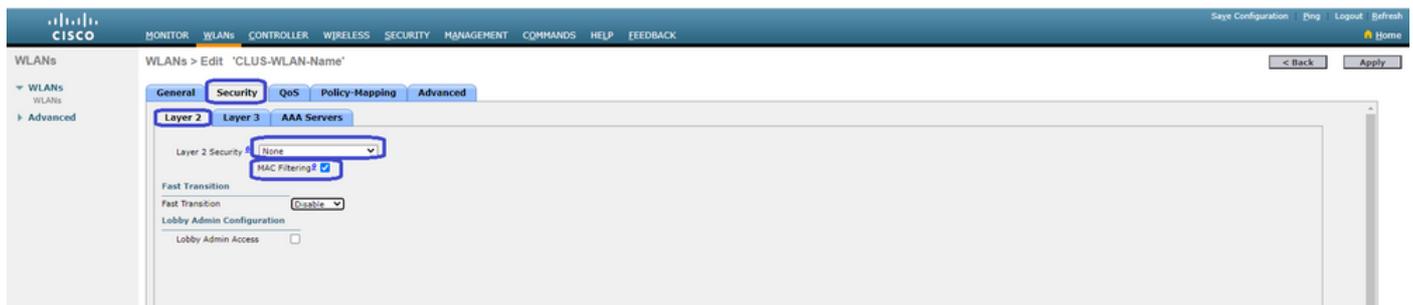
AireOS WLCのWLAN設定

WLANを作成するには、[WLANs] > [Create New] > [Go]に移動します。

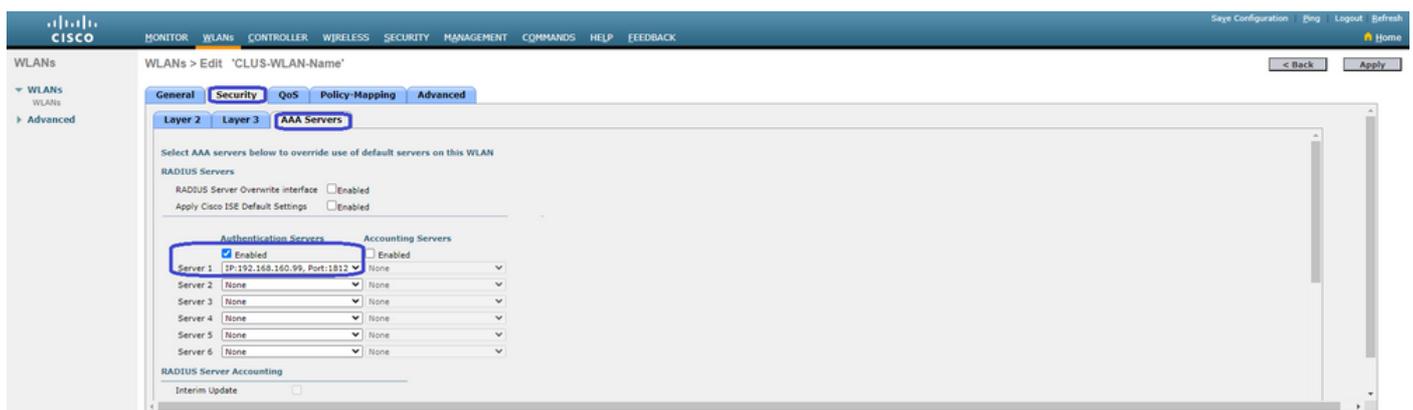
プロファイル名、WLAN ID、およびSSIDを設定し、[Apply]をクリックします。



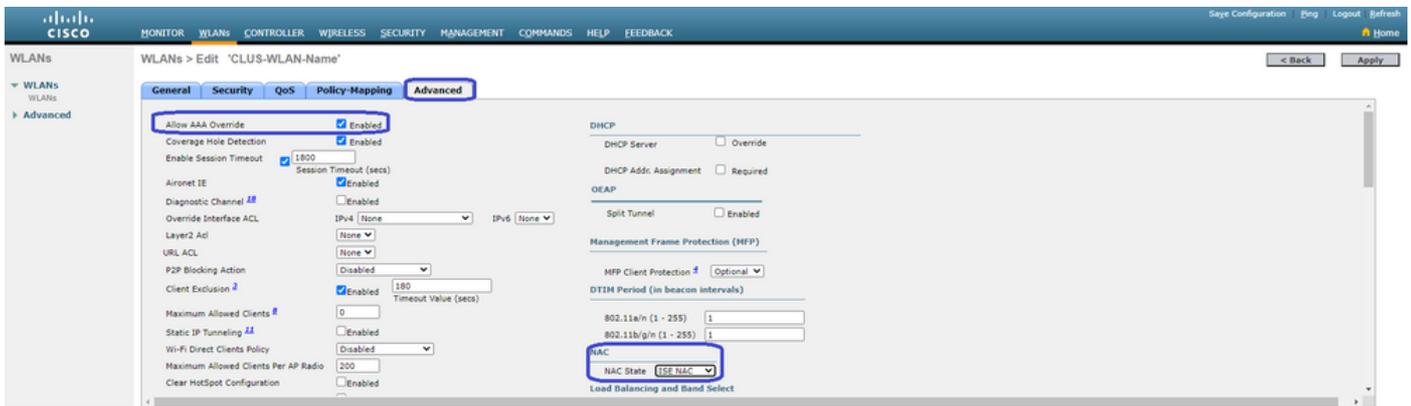
これにより、WLAN設定が表示されます。[General]タブでは、AVPでISEを送信するように設定しない場合に、クライアントで使用するインターフェイスを追加できます。次に、[Security] > [Layer2]タブに移動し、9800で使った[Layer 2 Security]設定と一致し、[MAC Filtering]を有効にします。



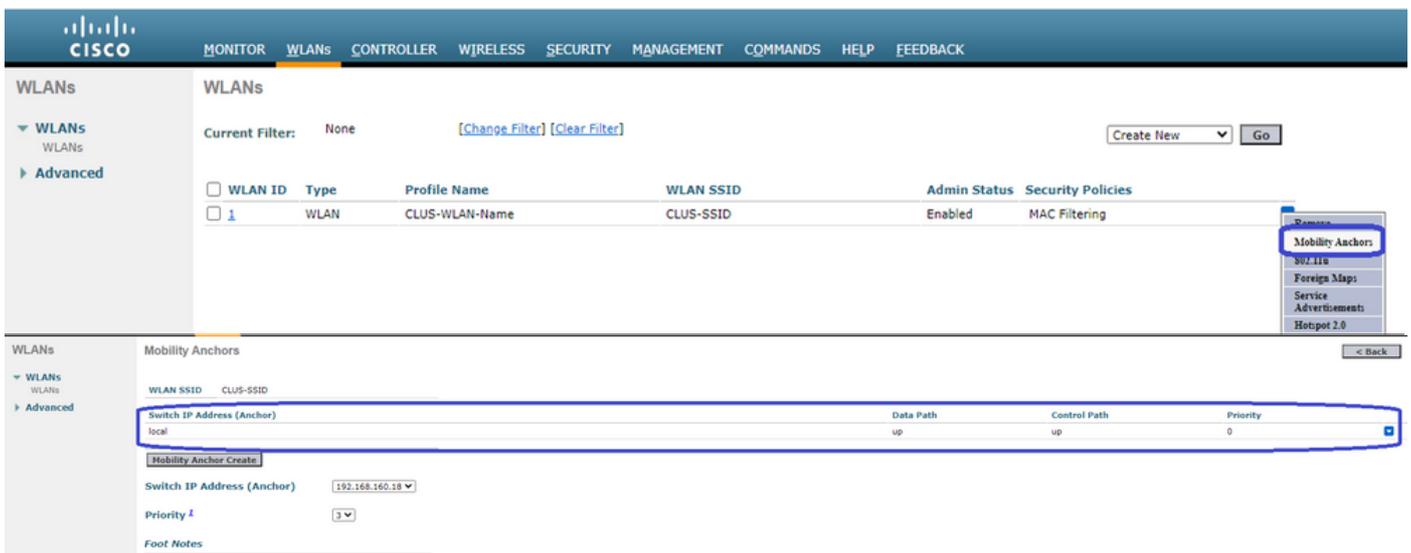
次に、[Security] > [AAA Servers]タブに移動し、ISEサーバを[Authentication Servers]に設定します。Accounting Serversには何も設定しないでください。アカウントングの[Enable]ボックスをオフにします。



WLANの設定を続けながら、[Advanced]タブに移動し、[Allow AAA Override]を有効にし、[NAC State]を[ISE NAC]に変更します



最後に、自分自身に固定します。これを行うには、[WLANs]ページに戻り、[WLAN] > [Mobility Anchors]の右側にある青いボックスにカーソルを合わせます。[Switch IP Address (Anchor)]を[local]に設定し、[Mobility Anchor Create]ボタンを押します。次に、プライオリティ0がアンカーされたローカルで表示されます。



AireOS WLCでのリダイレクトACL

これは、AireOS WLCに必要な最終的な設定です。リダイレクトACLを作成するには、[Security] > [Access Control Lists] > [Access Control Lists] > [New]に移動します。ACL名 (これはAVPで送信されるものと一致している必要があります) を入力し、[Apply]をクリックします。



作成したACLの名前をクリックします。[Add New Rule]ボタンをクリックします。9800コントローラとは異なり、AireOS WLCでは、リダイレクトされずにISEに到達できるトラフィックに対してpermit文を設定します。 DHCPとDNSはデフォルトで許可されています。

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Ping Logout Refresh Home

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists**
 - Access Control Lists
 - CPU Access Control

Access Control Lists > Edit

< Back Add New Rule

General

Access List Name CLUS-ACL

Deny Counters 5

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

ISE の設定

CWAISE

ISE9800ISE

[Policy] > [Policy Elements] > [Authorization] > [Results] > [Authorization Profiles] > [Add] access_acceptAVPCWAACLURLVLAN IDACLWLCWLCACL

← → ↻ Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > test

Authorization Profile

* Name CLUS-AuthZ-Profile-ISE

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL CLUS-ACL Value Self-Registered Guest Portal

CWAMABIDSSID

[Policy] > [Policy Set]+default network accessMABProcess Host Lookup[Policy] > [Policy Elements] > [Results] > [Authentication] > [Allowed Protocols] +

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Click here to do visibility setup Do not show this again.

Policy Sets

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	CLUS-CWA-Policy-Set			Default Network Access			
	Default	Default policy set		Default Network Access	0		

Reset Save

ISEMABIDWLAN

Conditions Studio

Library

mab

Wired_MAB

Wireless_MAB

Editor

Wireless_MAB

Set to 'Is not'

New AND OR

MABID

Policy Sets Profiling Posture Client Provisioning Policy Elements

Click here to do visibility setup Do not show this again.

Policy Sets → CLUS-CWA-Policy-Set

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access	0

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
	CLUS-MAB-Condition	Wireless_MAB	Internal Endpoints		
	Default		All_User_ID_Stores	0	

Options

- If Auth fail: CONTINUE
- If User not found: CONTINUE
- If Process fail: DROP

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

2ACLSSIDWLAN

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S
✓	CLUS-CWA-Policy-Set		Wireless_MAB	Default Network Access

Authentication Policy (2)						
Authorization Policy - Local Exceptions						
Authorization Policy - Global Exceptions						
Authorization Policy (4)						
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups
+	✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth		Select from list
+	✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE		Select from list
+	✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA		Select from list
+	✓	Default		DenyAccess		Select from list

ISE9800ISE[Admin] > [Network Resources] > [Network Device]>+.IPadminRADIUSISE9800

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 Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > JaysNet

Network Devices

* Name: CLUS_Net-Device

Description:

IP Address: * IP: 192.168.160.0 / 24

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

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

Shared Secret: [Show]

Use Second Shared Secret: [i]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings [i]

[Admin] > [Identity Management] > [Identity] > [Users] > [Add]submit ISE

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. The left sidebar shows 'Identities' > Users. The main content area is titled 'Network Access Users List > New Network Access User'. The form includes the following sections:

- Network Access User:** * Name (CLUS-User), Status (Enabled), Email.
- Passwords:** Password Type (Internal Users), * Login Password, Re-Enter Password, Enable Password, and Generate Password buttons.
- User Information:** First Name, Last Name.
- Account Options:** Description, Change password on next login (checkbox).
- Account Disable Policy:** Disable account if date exceeds (2020-07-17).
- User Groups:** Select an item dropdown.

The 'Submit' button is highlighted with a red box.

AireOS WLCが外部で、Catalyst 9800がアンカーである場合の設定の違い

AireOs WLCを外部コントローラにする場合、設定は以前と同じですが、2つの違いがあります。

1. AAAアカウントリングはアンカーで実行されないため、9800ではアカウントリング方式リストが作成されず、AireOS WLCではアカウントリングが有効になり、ISEを指します。
2. AireOSは、それ自身ではなく9800にアンカーする必要があります。[Policy Profile]では、9800のアンカーは選択されていませんが、[Export Anchor]ボックスはオンになっています。
3. AireOS WLCがクライアントを9800にエクスポートするときに、ポリシープロファイルの概念が存在しないことに注意してください。ポリシープロファイル名だけが送信されます。したがって、9800はAireOSから送信されたWLANプロファイル名をWLANプロファイル名とポリシープロファイル名の両方に適用します。つまり、AireOS WLCから9800 WLCへのアンカーの場合、両方のWLCのWLANプロファイル名と9800のポリシープロファイル名がすべて一致している必要があります。

確認

9800 WLC上の設定を確認するには、コマンドを実行します

- [AAA]

Show Run | section aaa|radius

- WLAN

Show wlan id <wlan id>

- ポリシープロファイル

Show wireless profile policy detailed <profile name>

- ポリシータグ

Show wireless tag policy detailed <policy tag name>

- ACL

Show IP access-list <ACL name>

- アンカーでモビリティがアップしていることを確認します

Show wireless mobility summary

AireOS WLCの設定を確認するには、次のコマンドを実行します

- [AAA]

Show radius summary

注：RFC3576はCoAの設定です

- WLAN

Show WLAN <wlan id>

- ACL

Show acl detailed <acl name>

- 外部サーバとのモビリティがアップしていることを確認します

Show mobility summary

トラブルシューティング

トラブルシューティングは、プロセスのどの時点でクライアントが停止するかによって異なります。たとえば、WLCがMABのISEから応答を受信しない場合、クライアントは「Policy Manager State:Associating」と入力すると、アンカーにエクスポートされません。この状況では、外部でのみトラブルシューティングを行い、WLCとISE間のトラフィックに対するRAトレースとパケットキャプチャを収集する場合があります。もう1つの例は、MABが正常に通過したが、クライアントがリダイレクトを受信しないことです。この場合、AVPで外部がリダイレクトを受信し、クライアントに適用していることを確認する必要があります。また、アンカーをチェックして、クライアントが正しいACLを持っているかどうかを確認する必要があります。このトラブルシュー

テイングの範囲は、このテクニカルドキュメントの設計の範囲外です（一般的なクライアントのトラブルシューティングガイドラインについては、参考資料を参照してください）。

9800 WLCでのCWAのトラブルシューティングの詳細については、Cisco Live!presentation DGTL-TSTOKEN-404

Catalyst 9800のトラブルシューティング情報

クライアント詳細

```
show wireless client mac-address
```

ここでは、[Policy Manager State]、[Session Manager]、[Auth Method]、[Mobility Role]を確認します。

この情報は、GUIの[Monitoring] > [Clients]で確認することもできます

Embedded Packet Capture

CLIからコマンドは#*monitor capture <capture name>*を起動し、その後にオプションが表示されます。

GUIから[Troubleshoot] > [Packet Capture] > [Add]に移動します

RadioActiveトレース

CLIを使用する場合

```
debug wireless mac/ip
```

コマンドのno形式を使用して停止します。これは、「ra_trace」という名前のブートフラッシュ内のファイルに記録されます。その後、クライアントのMACアドレスまたはIPアドレスと日時が記録されます。

GUIから[Troubleshoot] > [Radioactive Trace] > [Add]に移動します。クライアントのMACアドレスまたはIPアドレスを追加し、applyを押してからstartを押します。プロセスを数回実行した後、トレースを停止し、ログを生成して、デバイスにダウンロードします。

AireOSのトラブルシューティング情報

クライアント詳細

CLIから *show client details <client mac>*

GUIの[Monitor] > [Clients]から

CLIからのデバッグ

Debug client

Debug mobility handoff

Debug mobility config

参考資料

[9800コントローラによるモビリティトンネルの構築](#)

[9800でのワイヤレスデバッグとログ収集](#)