

Configuration de l'authentification Web centralisée avec ancrage sur Catalyst 9800

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configurer un Catalyst 9800 ancré à un autre Catalyst 9800](#)

[Diagramme du réseau](#)

[Configurer AAA sur les deux modèles 9800](#)

[Configurer les WLAN sur les WLC](#)

[Créer le profil de stratégie et la balise de stratégie sur le WLC étranger](#)

[Créer le profil de stratégie sur le WLC d'ancrage](#)

[Rediriger la configuration des listes de contrôle d'accès sur les deux modèles 9800](#)

[Configurer ISE](#)

[Configurer un Catalyst 9800 ancré à un WLC AireOS](#)

[Configuration étrangère du Catalyst 9800](#)

[Configurations AAA sur le WLC AireOS d'ancrage](#)

[Configuration WLAN sur le WLC AireOS](#)

[Rediriger l'ACL sur le WLC AireOS](#)

[Configurer ISE](#)

[Différences dans la configuration lorsque le WLC AireOS est étranger et que le Catalyst 9800 est l'ancrage](#)

[Vérification](#)

[Dépannage](#)

[Informations de dépannage du Catalyst 9800](#)

[Détails du client](#)

[Capture de paquets intégrée](#)

[Suivi RadioActive](#)

[Informations de dépannage AireOS](#)

[Détails du client](#)

[Débogues à partir de l'interface de ligne de commande](#)

[Références](#)

Introduction

Ce document décrit comment configurer et dépanner une authentification Web centrale (CWA) sur le Catalyst 9800 pointant vers un autre contrôleur de réseau local sans fil (WLC) comme point d'ancrage de mobilité, couvrant la destination avec AireOS ou un autre WLC 9800.

Conditions préalables

Conditions requises

Il est recommandé d'avoir une compréhension de base du WLC 9800, du WLC AireOS et de Cisco ISE. Il est supposé qu'avant de démarrer la configuration d'ancrage CWA, vous avez déjà monté le tunnel de mobilité entre les deux WLC. Cela ne fait pas partie de la portée de cet exemple de configuration. Si vous avez besoin d'aide, consultez le document intitulé "[Construire des tunnels de mobilité sur les contrôleurs Catalyst 9800](#)"

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

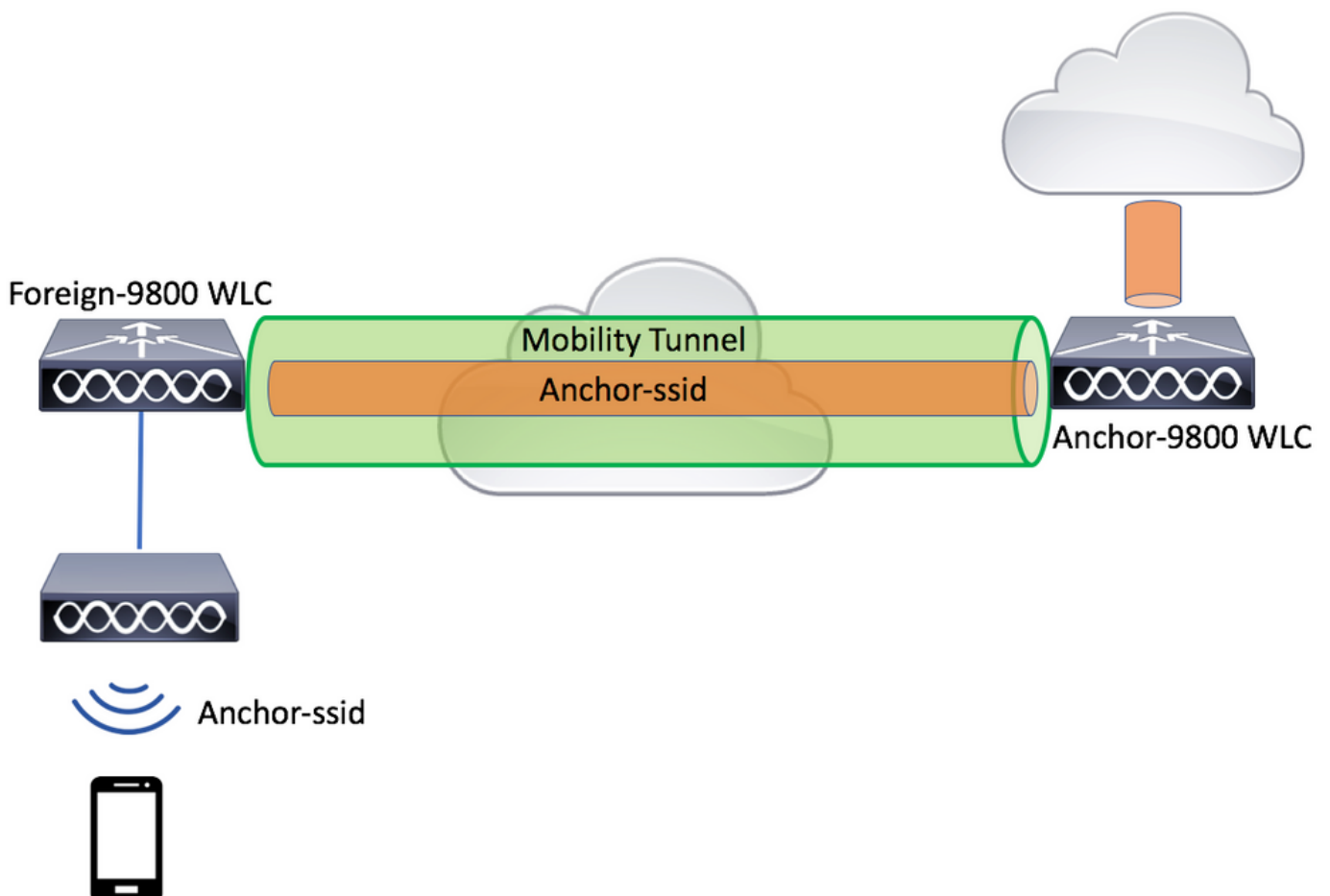
9 800 17,2,1

5520 image IRCM 8.5.164

ISE 2.4

Configurer un Catalyst 9800 ancré à un autre Catalyst 9800

Diagramme du réseau



Configurer AAA sur les deux modèles 9800

Sur l'ancrage et l'étranger, vous devez d'abord ajouter le serveur RADIUS et vous assurer que CoA est activé. Cela peut être fait dans le menu **Configuration > Security > AAA > Serveurs/Groupes** > cliquez sur le bouton **Add**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Security > AAA**. The current view is **Servers / Groups**. The **RADIUS** tab is selected, and the **Servers** sub-tab is active. A **Create AAA Radius Server** dialog box is open, with the following fields and values:

| | |
|--------------------------|---|
| 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 | <input checked="" type="checkbox"/> ENABLED |

The **Support for CoA** checkbox is checked and labeled **ENABLED**. The **Apply to Device** button is visible at the bottom right of the dialog box.

Vous devez maintenant créer un groupe de serveurs et placer le serveur que vous venez de configurer dans ce groupe. Ceci est fait ici **Configuration > Security > AAA > Serveurs/Groupes > Groupes de serveurs > +Add**.

Cisco Catalyst 9800-L Wireless Controller
17.2.1

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

Maintenant, créez une liste de méthodes **d'autorisation** (une liste de méthodes d'authentification n'est pas requise pour CWA) où le type est réseau et le type de groupe est groupe. Ajoutez le groupe de serveurs de l'action précédente à cette liste de méthodes.

Cette configuration est effectuée ici **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Security > AAA**. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the **AAA Method List** configuration page. The **Authorization** tab is selected, and the **+ Add** button is highlighted. A modal dialog titled **Quick Setup: AAA Authorization** is open, showing the following configuration details:

- Method List Name*: CLUS-AuthZ-Meth-List
- Type*: network
- Group Type: group
- Fallback to local:
- Authenticated:
- 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 dialog.

(Facultatif) Créez une liste de méthodes comptables en utilisant le même groupe de serveurs que la liste de méthodes d'autorisation. La liste de comptabilité peut être créée ici **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar contains menu items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the "AAA Method List" configuration page with tabs for "Servers / Groups", "AAA Method List", and "AAA Advanced". The "Accounting" tab is selected. A "Quick Setup: AAA Accounting" dialog box is open, showing the following configuration:

- 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 dialog.

Configurer les WLAN sur les WLC

Créez et configurez les WLAN sur les deux WLC. Les WLAN doivent correspondre sur les deux. Le type de sécurité doit être le filtrage mac et la liste des méthodes d'autorisation de l'étape précédente doit être appliquée. Cette configuration est effectuée sous **Configuration>Balises et profils>WLAN>+Add**

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

SSID* CLUS-SSID

WLAN ID* 2

Status ENABLED

Radio Policy All

Broadcast SSID 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

MAC Filtering

OWE Transition Mode

Authorization List* CLUS-AuthZ-Meth-l

Lobby Admin Access

Fast Transition Adaptive Enab...

Over the DS

Reassociation Timeout 20

Cancel Apply to Device

Créer le profil de stratégie et la balise de stratégie sur le WLC étranger

Accédez à l'interface utilisateur Web du WLC étranger.

Pour créer le profil de stratégie, accédez à **Configuration>Balises et profils>Stratégie>+Ajouter**

Lors de l'ancrage, vous devez utiliser la commutation centrale.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog box is open, showing the **General** tab. A warning message states: "Configuring in enabled state will result in loss of connectivity for clients associated with this profile." The **Name*** field is "CLUS-Policy-Profile" and the **Description** is "Policy Profile for CLUS". The **Status** is set to **ENABLED**. The **WLAN Switching Policy** section has **Central Switching**, **Central Authentication**, **Central DHCP**, and **Central Association** all set to **ENABLED**. The **CTS Policy** section has **Inline Tagging** and **SGACL Enforcement** set to **DISABLED**, and the **Default SGT** is "2-65519". The **Flex NAT/PAT** is set to **DISABLED**. The **Apply to Device** button is visible at the bottom right.

Dans l'onglet « Avancé », le remplacement AAA et RADIUS NAC sont obligatoires pour CWA. Ici, vous pouvez également appliquer la liste des méthodes comptables si vous avez choisi d'en faire une.

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

Accounting List CLUS-Acct-Meth-

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

Dans l'onglet « Mobilité », **NE** cochez **PAS** la case « Exporter l'ancre » mais ajoutez plutôt le WLC d'ancrage à la liste d'ancrages. Assurez-vous d'appuyer sur Appliquer au périphérique. Pour rappel, ceci suppose que vous avez déjà une configuration de tunnel de mobilité entre les deux contrôleurs

Cisco Catalyst 9800-L Wireless Controller

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 VLANs 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

Pour que les AP utilisent ce profil de stratégie, vous devez créer une balise de stratégie et

l'appliquer aux AP que vous souhaitez utiliser.

Pour créer la balise de stratégie, accédez à **Configuration>Balises et profils>Balises?Stratégie>Ajouter**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. 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 fields:

- 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 WLAN Profile to the Policy Profile. The 'Apply to Device' button is highlighted at the bottom right.

Pour l'ajouter à plusieurs points d'accès en même temps, accédez à **Configuration>Wireless Setup>Advanced>Start Now**. Cliquez sur les barres de puces en regard de « Tag APs » et ajoutez la balise aux AP que vous choisissez.

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

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

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

Créer le profil de stratégie sur le WLC d'ancrage

Accédez à l'interface utilisateur Web du WLC d'ancrage. Ajoutez le profil de stratégie sur le point d'ancrage 9800 sous **Configuration>Balises et profils>Balises>Stratégie>Ajouter**. Assurez-vous que cela correspond au profil de stratégie établi sur l'étranger, à l'exception de l'onglet Mobilité et de la liste de comptabilisation.

Ici, vous n'ajoutez pas d'ancrage mais vous cochez la case « Exporter l'ancrage ». N'ajoutez pas la liste de comptabilisation ici. Pour rappel, ceci suppose que vous avez déjà une configuration de tunnel de mobilité entre les deux contrôleurs

Note: Il n'y a aucune raison d'associer ce profil à un WLAN dans une balise de stratégie. Cela créera des problèmes si vous le faites. Si vous voulez utiliser le même WLAN pour les AP sur ce WLC, créez un autre profil de stratégie pour lui.

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

Rediriger la configuration des listes de contrôle d'accès sur les deux modèles 9800

Ensuite, vous devez créer la configuration de la liste de contrôle d'accès de redirection sur les deux modèles 9800. Les entrées sur l'étranger n'ont pas d'importance car il s'agira du WLC d'ancrage appliquant la liste de contrôle d'accès au trafic. La seule condition est qu'il y en ait et qu'il y ait une entrée. Les entrées de l'ancre doivent refuser l'accès à ISE sur le port 8443 et autoriser tout le reste. Cette liste de contrôle d'accès est appliquée uniquement au trafic entrant en provenance du client, de sorte que les règles pour le trafic de retour ne sont pas nécessaires. DHCP et DNS passent sans entrée dans la liste de contrôle d'accès.

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

| 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

Configurer ISE

La dernière étape consiste à configurer ISE pour CWA. Il y a une tonne d'options pour cela, mais cet exemple s'en tiendra aux bases et utilisera le portail invité auto-enregistré par défaut.

Sur ISE, vous devez créer un profil d'autorisation, un jeu de stratégies avec une stratégie d'authentification et une stratégie d'autorisation qui utilise le profil d'autorisation, ajouter le 9800(étranger) à ISE en tant que périphérique réseau et créer un nom d'utilisateur et un mot de passe pour vous connecter au réseau.

Pour créer le profil d'autorisation, accédez à **Policy>Policy>Policy Elements>Authorization>Results>Authorization Profiles>**, puis cliquez sur **Add**. Assurez-vous que le type d'accès retourné est « access_accept », puis définissez les AVP(attribute-value paires) que vous voulez renvoyer. Pour CWA, la liste de contrôle d'accès de redirection et l'URL de redirection sont obligatoires, mais vous pouvez également renvoyer des éléments tels que l'ID de VLAN et le délai d'attente de session. Il est important que le nom de la liste de contrôle d'accès corresponde au nom de la liste de contrôle d'accès de redirection sur l'adresse étrangère et l'ancre 9800.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements > Results. The left sidebar shows the navigation menu with 'Authorization' and 'Authorization Profiles' highlighted. The main content area is titled 'Authorization Profiles > test' and 'Authorization Profile'. The configuration fields are:

- * Name: CLUS-AuthZ-Profile-ISE
- Description: (empty)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: (checkbox)
- Track Movement: (checkbox)
- Passive Identity Tracking: (checkbox)

 Under the 'Common Tasks' section, the 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is checked. Below it, the configuration is:

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

Vous devez ensuite configurer un moyen d'appliquer le profil d'autorisation que vous venez de créer aux clients qui passent par CWA. Pour ce faire, une méthode consiste à créer un jeu de stratégies qui ignore l'authentification lors de l'utilisation de MAB et applique le profil d'autorisation lors de l'utilisation du SSID envoyé dans l'ID de station appelée. Encore une fois, il y a beaucoup de façons d'y parvenir, donc si vous avez besoin de quelque chose de plus spécifique ou de plus sûr, cette bonne, c'est juste la façon la plus simple de le faire.

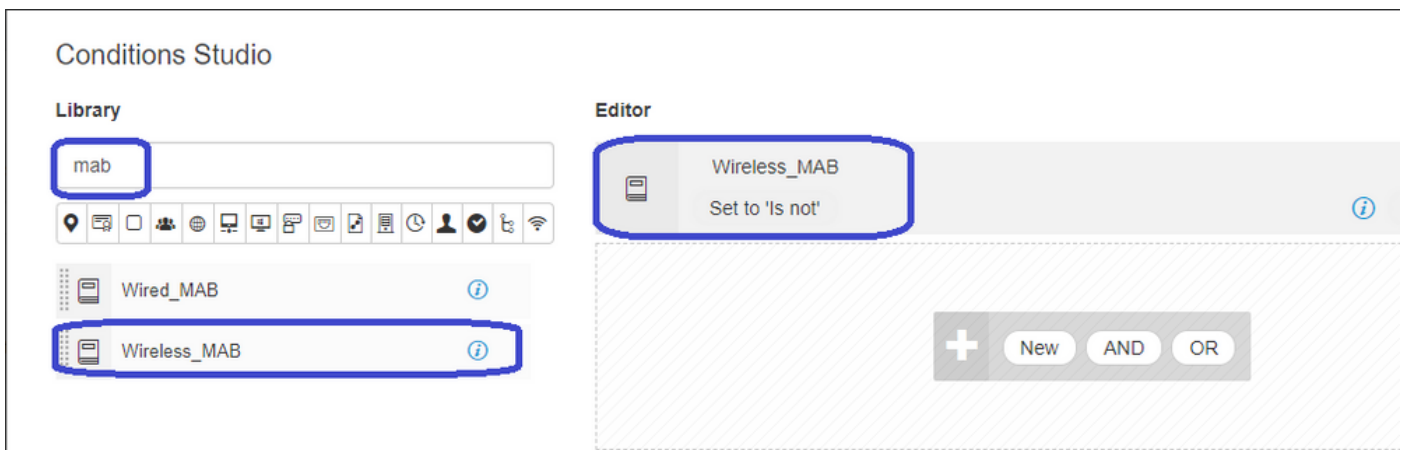
Pour créer le jeu de stratégies, accédez à **Policy>Policy Sets** et cliquez sur le bouton + à gauche de l'écran. Nommez le nouveau jeu de stratégies et assurez-vous qu'il est défini sur « accès réseau par défaut » ou toute liste de protocoles autorisée qui autorise « Traiter la recherche d'hôte » pour MAB(pour vérifier la liste de protocoles autorisés, accédez à Policy>Policy Elements>Policy>Results>Authentication>Allowed Protocols). Maintenant, cliquez sur le signe + au milieu du nouvel ensemble de stratégies que vous avez créé.

The screenshot shows the 'Policy Sets' configuration page in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements. The page displays a table of policy sets:

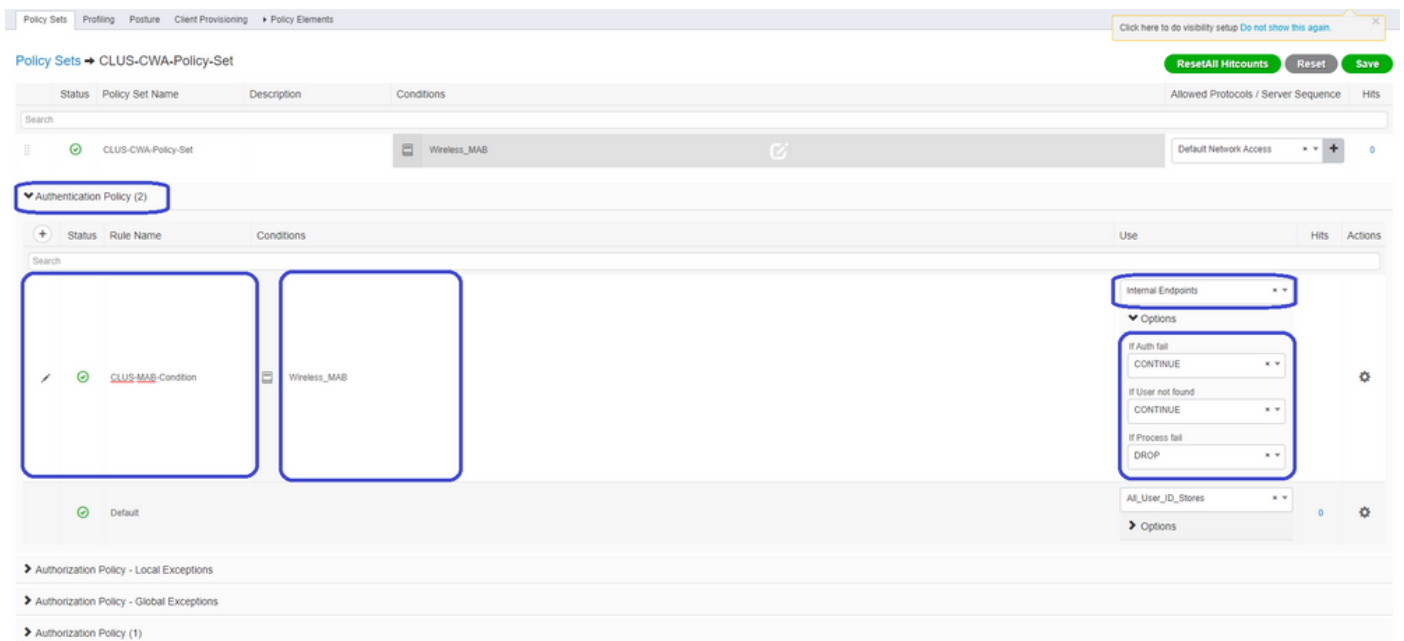
| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|-----------------------|--------------------|------------|-------------------------------------|------|---------|------|
| + | CLUS-AuthZ-Policy-Set | | | Default Network Access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

 The '+' button in the 'Allowed Protocols / Server Sequence' column for the 'CLUS-AuthZ-Policy-Set' row is highlighted with a blue box.

Pour ce jeu de stratégies, chaque fois que MAB est utilisé dans ISE, il passe par ce jeu de stratégies. Plus tard, vous pouvez définir des stratégies d'autorisation qui correspondent à l'ID de station appelée afin que différents résultats puissent être appliqués en fonction du WLAN utilisé. Ce processus est très personnalisable avec beaucoup de choses que vous pouvez mettre en correspondance.



Dans le jeu de stratégies , créez les stratégies. La stratégie d'authentification peut à nouveau correspondre sur MAB, mais vous devez modifier le magasin d'ID pour utiliser des « terminaux internes » et modifier les options pour continuer l'échec d'authentification et l'utilisateur introuvable.



Une fois la stratégie d'authentification définie, vous devez créer deux règles dans la stratégie d'autorisation. Cette stratégie se lit comme une liste de contrôle d'accès, de sorte que l'ordre doit avoir la règle post-authentification en haut et la règle pré-authentification en bas. La règle post-authentification correspond aux utilisateurs qui ont déjà passé par le flux d'invités. En d'autres termes, s'ils se sont déjà connectés, ils vont appliquer cette règle et s'arrêter là. S'ils ne se sont pas connectés, ils poursuivront dans la liste et accéderont à la règle pré-authentification en obtenant la redirection. Il est recommandé de faire correspondre les règles de stratégie d'autorisation avec l'ID de station appelée se terminant par le SSID afin qu'il ne touche que les WLAN configurés pour le faire.

| Status | Policy Set Name | Description | Conditions | Results | 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 | 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 |

Maintenant que le jeu de stratégies est configuré, vous devez informer ISE sur le 9800 (étranger) afin que ISE puisse lui faire confiance en tant qu'authentificateur. Pour cela, consultez **Admin > Network Resources > Network Device > +**. Vous devez lui donner un nom, définir l'adresse IP (ou dans ce cas l'ensemble du sous-réseau d'administration), activer RADIUS et définir le secret partagé. Le secret partagé sur ISE doit correspondre au secret partagé sur le 9800, sinon ce processus échouera. Une fois la configuration ajoutée, cliquez sur le bouton Envoyer pour l'enregistrer.

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: [REDACTED] (Show)

Use Second Shared Secret: (Show)

CoA Port: 1700 (Set To Default)

RADIUS DTLS Settings

Enfin, vous devez ajouter le nom d'utilisateur et le mot de passe que le client va entrer dans la

page de connexion afin de valider qu'il doit avoir accès au réseau. Cela se fait sous **Admin>Identity Management>Identity>Users>+Add** et assurez-vous d'appuyer sur soumettre après l'avoir ajouté. Comme tout le reste avec ISE, il est personnalisable et n'a pas besoin d'être un utilisateur stocké localement, mais encore une fois, c'est la configuration la plus facile.

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

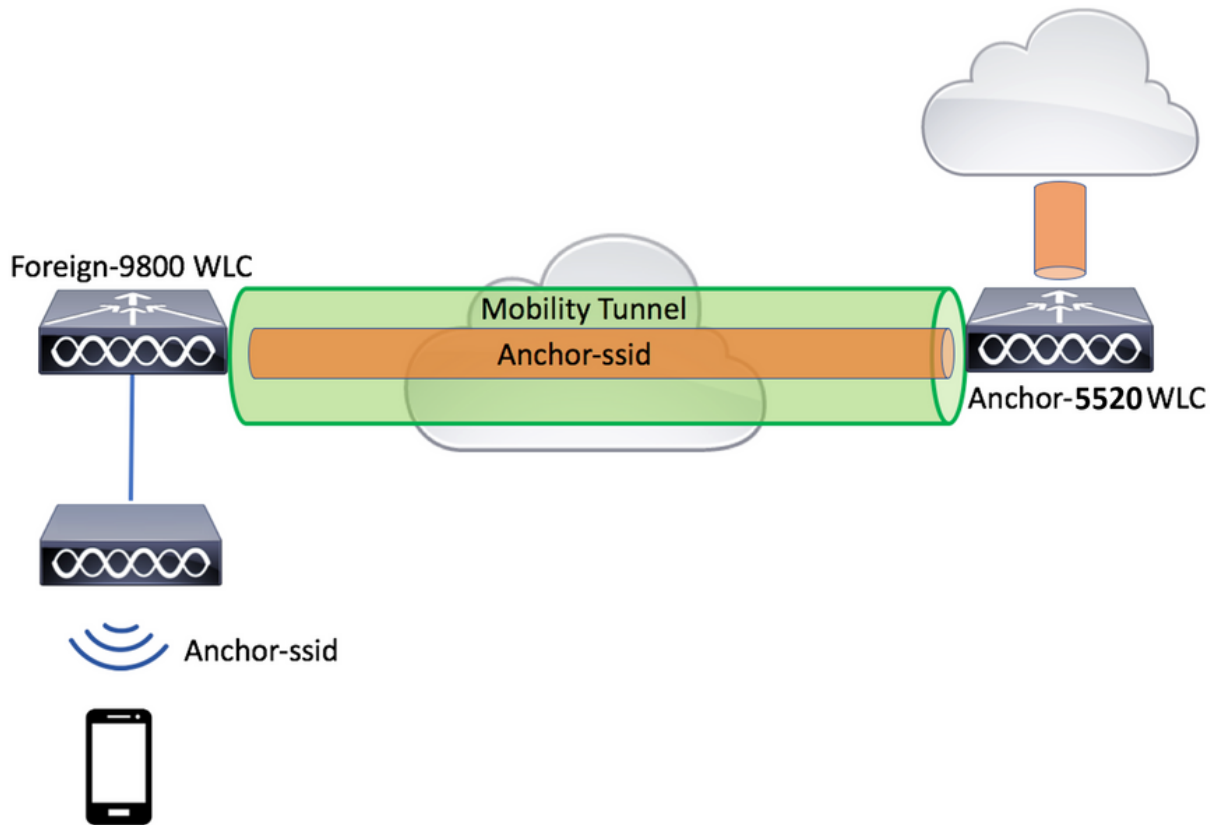
Disable account if date exceeds 2020-07-17 (yyyy-mm-dd)

User Groups

Select an item

Submit Cancel

Configurer un Catalyst 9800 ancré à un WLC AireOS



Configuration étrangère du Catalyst 9800

Suivez les mêmes étapes que celles décrites précédemment, en ignorant la section "Créer le profil de stratégie sur le WLC d'ancrage".

Configurations AAA sur le WLC AireOS d'ancrage

Ajoutez le serveur au WLC en accédant à **Security>AAA>RADIUS>Authentication>New**. Ajoutez l'adresse IP du serveur, le secret partagé et la prise en charge de CoA.

The top screenshot shows the 'RADIUS Authentication Servers' configuration page in the Cisco AireOS 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 RADIUS server.

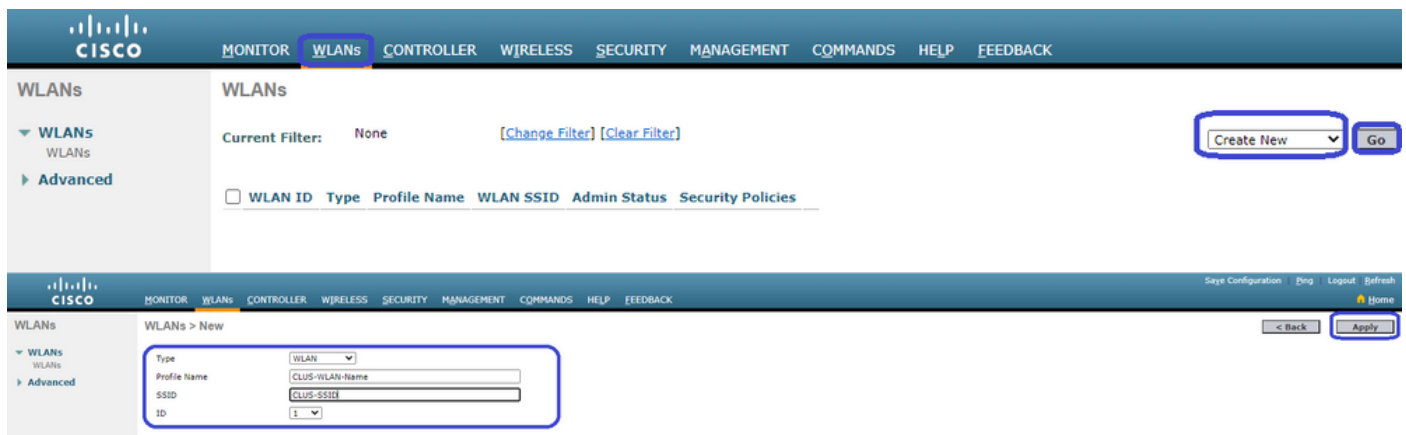
| Network User | Management | Tunnel Proxy | Server Index | Server Address(Ipv4/Ipv6) | Port | IPSec | Admin Status |
|--------------|------------|--------------|--------------|---------------------------|------|-------|--------------|
| | | | | | | | |

The bottom screenshot shows the 'RADIUS Authentication Servers > New' configuration page. Several fields are highlighted in blue: 'Server Index (Priority)' is set to 1; 'Server IP Address(Ipv4/Ipv6)' is 192.168.160.99; 'Shared Secret Format' is ASCII; 'Shared Secret' and 'Confirm Shared Secret' are masked with asterisks; 'Apply Cisco ISE Default settings' is checked; 'Key Wrap' is unchecked; 'Port Number' is 1812; 'Server Status' is Enabled; 'Support for CoA' is Enabled; 'Server Timeout' is 5 seconds; 'Network User' and 'Management' are checked; 'Management Retransmit Timeout' is 5 seconds; 'Tunnel Proxy', 'PAC Provisioning', and 'IPSec' are unchecked.

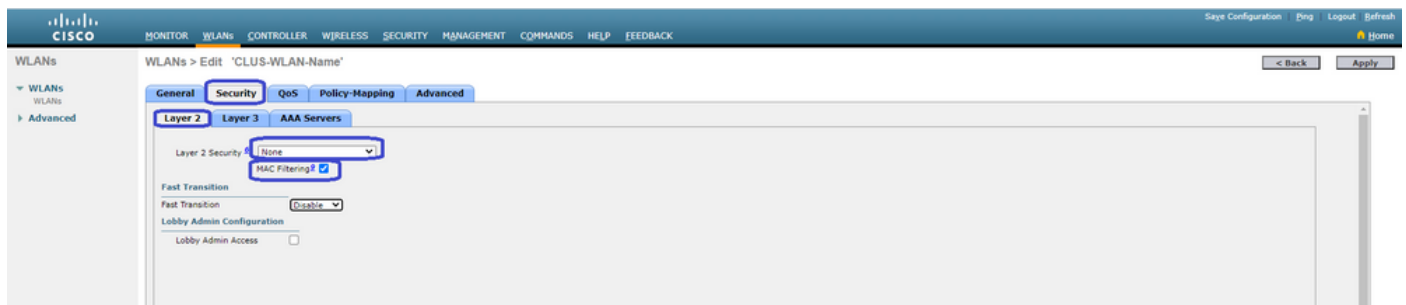
Configuration WLAN sur le WLC AireOS

Pour créer le WLAN, accédez à **WLANs>Create New>Go**.

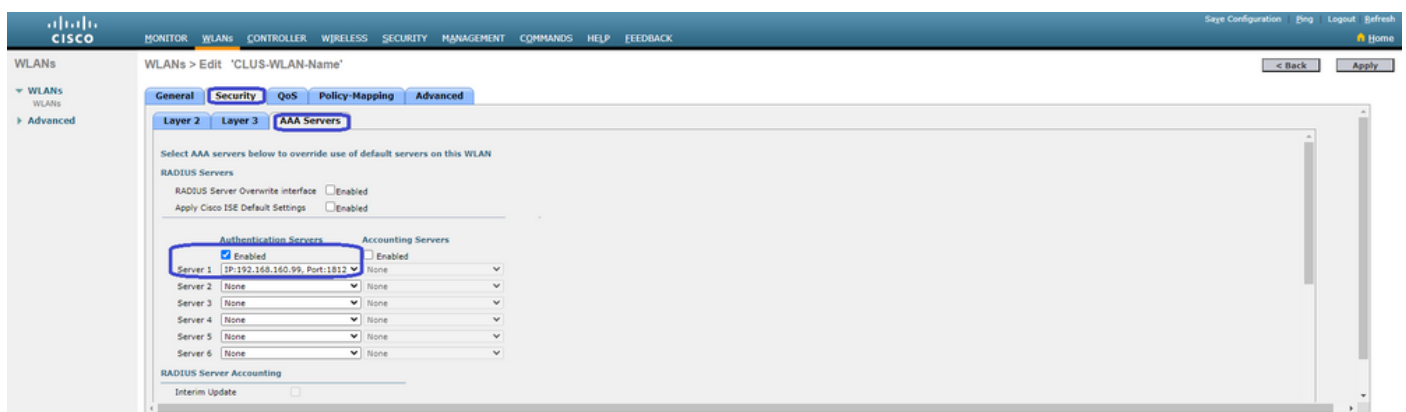
Configurez le nom du profil, l'ID WLAN et le SSID, puis appuyez sur « Apply ».



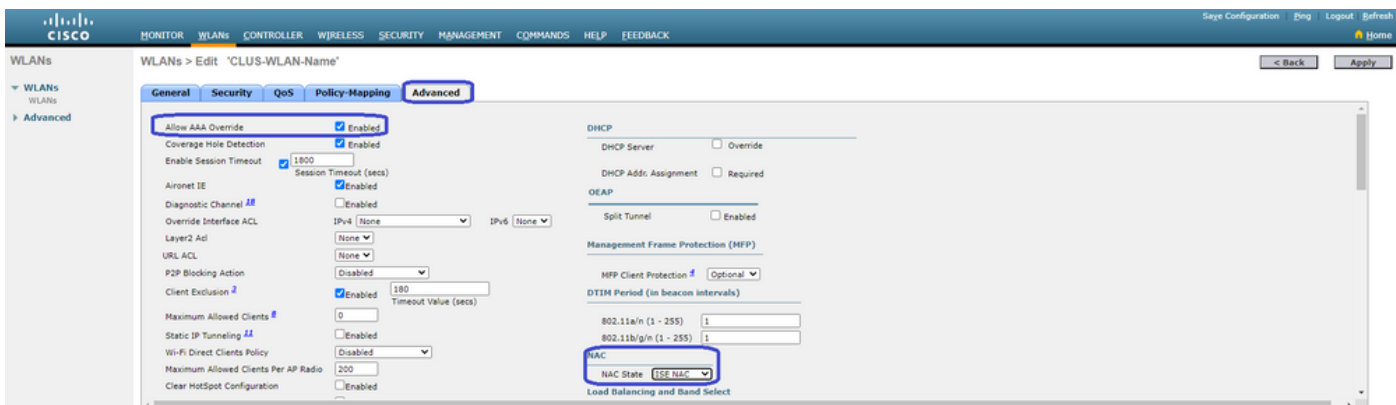
Ceci devrait vous conduire à la configuration WLAN. Dans l'onglet « Général », vous pouvez ajouter l'interface que vous voulez que les clients utilisent si vous n'allez pas configurer ISE pour l'envoyer dans les AVP. Ensuite, accédez à l'onglet **Security>Layer2** et faites correspondre la configuration de sécurité de couche 2 que vous avez utilisée sur le 9800 et activez le filtrage MAC.



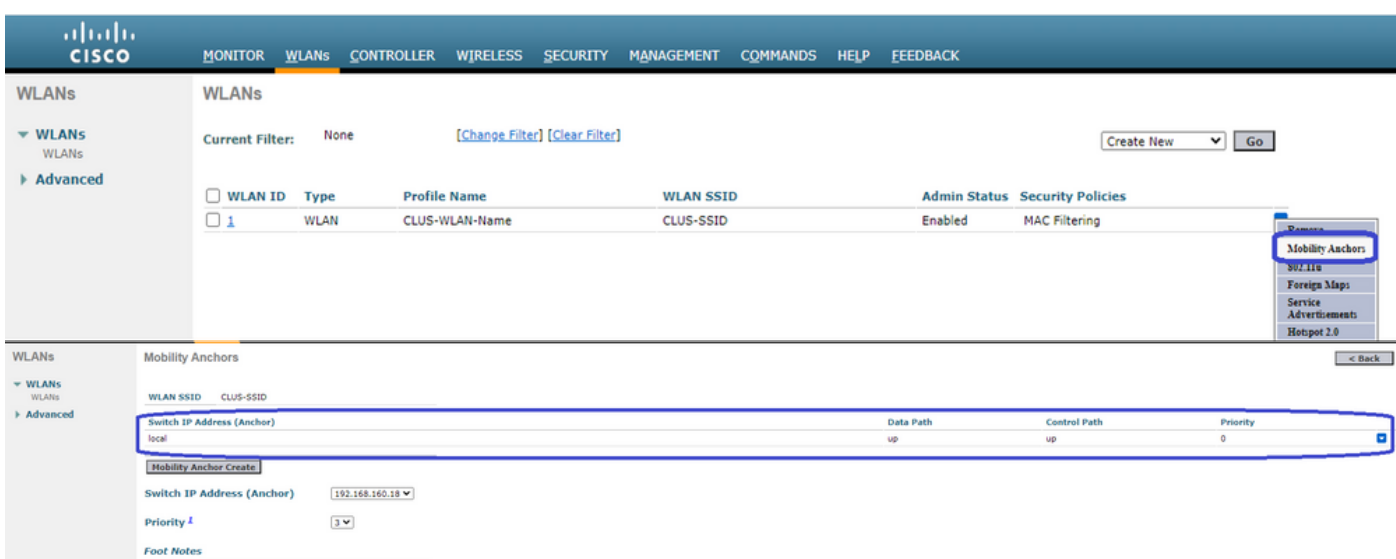
Passez maintenant à l'onglet **Security>AAA Servers** et définissez le serveur ISE comme « Authentication Servers ». **Ne** définissez rien pour les serveurs de comptabilité. Décochez la case Activer pour la comptabilité.



Toujours dans les configurations WLAN, passez à l'onglet « Advanced » et activez « Allow AAA Override » et changez « NAC State » en « ISE NAC »

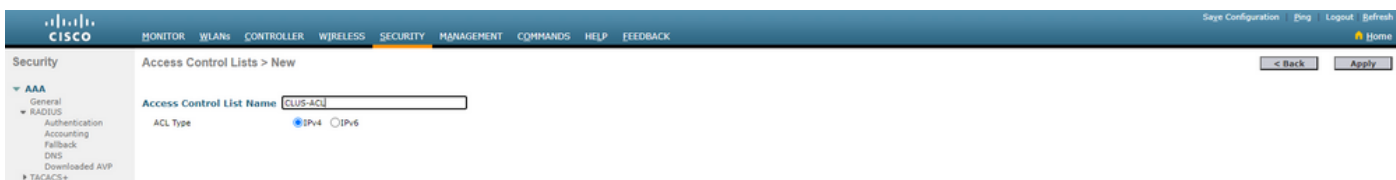


La dernière chose est de l'ancrer à lui-même. Pour cela, revenez à la page **WLAN** et placez le pointeur de la souris sur la case bleue située à droite de **WLAN>Mobility Anchors**. Définissez l'option Switch IP Address (Ancre) sur local et cliquez sur le bouton Mobility Anchor Create. Il doit ensuite apparaître avec la priorité 0 ancrée local.



Rediriger l'ACL sur le WLC AireOS

Il s'agit de la configuration finale requise sur le WLC AireOS. Pour créer la liste de contrôle d'accès de redirection, accédez à **Sécurité>Listes de contrôle d'accès>Listes de contrôle d'accès>Nouveau**. Saisissez le nom de la liste de contrôle d'accès (qui doit correspondre à ce qui est envoyé dans les AVP) et appuyez sur Appliquer.



Cliquez maintenant sur le nom de la liste de contrôle d'accès que vous venez de créer. Cliquez sur le bouton Ajouter une nouvelle règle. Contrairement au contrôleur 9800, sur le WLC AireOS, vous configurez une instruction permet pour le trafic autorisé à atteindre ISE sans être redirigé. DHCP et DNS sont autorisés par défaut.

Security

Access Control Lists > Edit

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 |

Configurer ISE

La dernière étape consiste à configurer ISE pour CWA. Il y a une tonne d'options pour cela, mais cet exemple s'en tiendra aux bases et utilisera le portail invité auto-enregistré par défaut.

Sur ISE, vous devez créer un profil d'autorisation, un jeu de stratégies avec une stratégie d'authentification et une stratégie d'autorisation qui utilise le profil d'autorisation, ajouter le 9800(étranger) à ISE en tant que périphérique réseau et créer un nom d'utilisateur et un mot de passe pour vous connecter au réseau.

Pour créer le profil d'autorisation, accédez à **Policy>Policy>Policy Elements>Authorization>Results>Authorization Profiles>+Add**. Assurez-vous que le type d'accès retourné est « access_accept », puis définissez les AVP(attribute-value paires) que vous voulez renvoyer. Pour CWA, la liste de contrôle d'accès de redirection et l'URL de redirection sont obligatoires, mais vous pouvez également renvoyer des éléments tels que l'ID de VLAN et le délai d'attente de session. Il est important que le nom de la liste de contrôle d'accès corresponde au nom de la liste de contrôle d'accès de redirection sur le WLC étranger et le WLC d'ancrage.

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionary > Conditions > Results

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

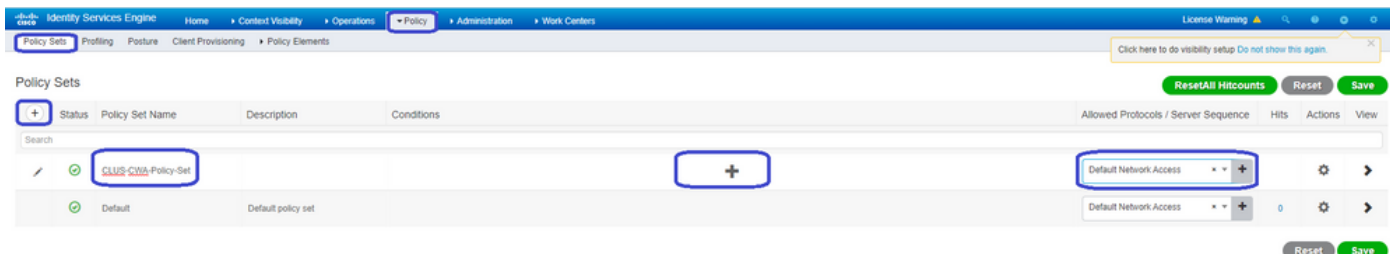
Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

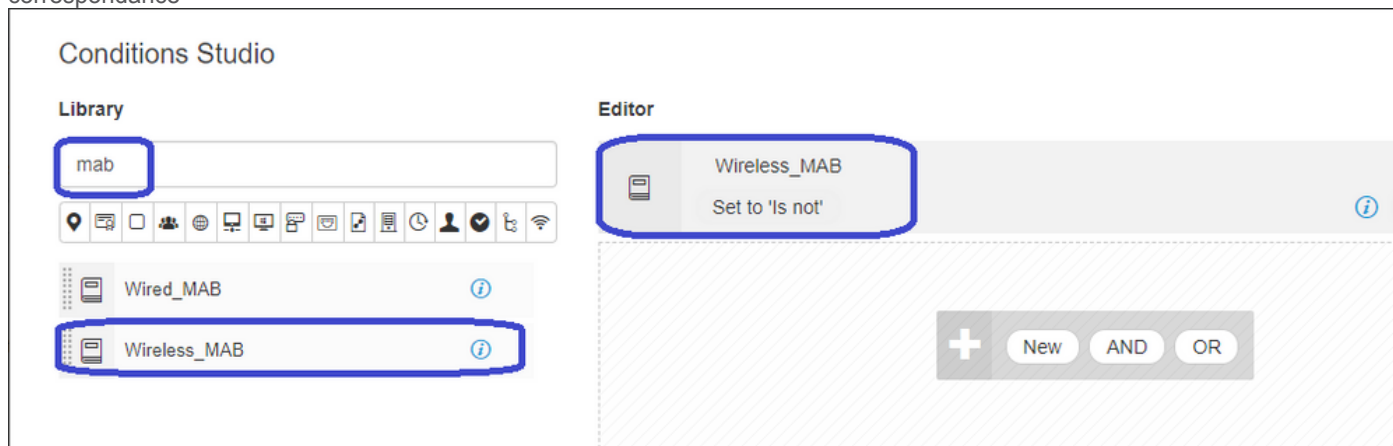
Centralized Web Auth ACL: CLUS-ACL Value: Self-Registered Guest Portal

Vous devez ensuite configurer un moyen d'appliquer le profil d'autorisation que vous venez de créer aux clients qui passent par CWA. Pour ce faire, une méthode consiste à créer un jeu de stratégies qui ignore l'authentification lors de l'utilisation de MAB et applique le profil d'autorisation lors de l'utilisation du SSID envoyé dans l'ID de station appelée. Encore une fois, il y a beaucoup de façons d'y parvenir, donc si vous avez besoin de quelque chose de plus spécifique ou de plus sûr, cette bonne, c'est juste la façon la plus simple de le faire.

Pour créer le jeu de stratégies, accédez à **Policy>Policy Settings** et appuyez sur le bouton + à gauche de l'écran. Nommez le nouveau jeu de stratégies et assurez-vous qu'il est défini sur « accès réseau par défaut » ou toute liste de protocoles autorisée qui autorise « Traiter la recherche d'hôte » pour MAB(pour vérifier la liste de protocoles autorisés, accédez à Policy>Policy Elements>Policy>Results>Authentication>Allowed Protocols). Maintenant, cliquez sur le signe + au milieu du nouvel ensemble de stratégies que vous avez créé.



Pour ce jeu de stratégies, chaque fois que MAB est utilisé dans ISE, il passe par ce jeu de stratégies. Plus tard, vous pouvez définir des stratégies d'autorisation qui correspondent à l'ID de station appelée afin que différents résultats puissent être appliqués en fonction du WLAN utilisé. Ce processus est très personnalisable avec beaucoup de choses que vous pouvez mettre en correspondance



Dans le jeu de stratégies , créez les stratégies. La stratégie d'authentification peut à nouveau correspondre sur MAB, mais vous devez modifier le magasin d'ID pour utiliser des « terminaux internes » et modifier les options pour continuer l'échec d'authentification et l'utilisateur introuvable.

Une fois la stratégie d'authentification définie, vous devez créer deux règles dans la stratégie d'autorisation. Cette stratégie se lit comme une liste de contrôle d'accès, de sorte que l'ordre doit avoir la règle post-authentification en haut et la règle pré-authentification en bas. La règle post-authentification correspond aux utilisateurs qui ont déjà passé par le flux d'invités. En d'autres termes, s'ils se sont déjà connectés, ils vont appliquer cette règle et s'arrêter là. S'ils ne se sont pas connectés, ils poursuivront dans la liste et accéderont à la règle pré-authentification en obtenant la redirection. Il est recommandé de faire correspondre les règles de stratégie d'autorisation avec l'ID de station appelée se terminant par le SSID afin qu'il ne touche que les WLAN configurés pour le faire.

Maintenant que le jeu de stratégies est configuré, vous devez informer ISE sur le 9800(étranger) afin que ISE puisse lui faire confiance en tant qu'authentificateur. Cela peut être fait à l'adresse suivante : **Admin>Ressources réseau>Périphérique réseau>+**. Vous devez lui donner un nom, définir l'adresse IP (ou dans ce cas l'ensemble du sous-réseau d'administration), activer RADIUS et définir le secret partagé. Le secret partagé sur ISE doit correspondre au secret partagé sur le 9800, sinon ce processus échouera. Une fois la configuration ajoutée, cliquez sur le bouton Envoyer pour l'enregistrer.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the navigation tree with 'Network Resources' expanded to 'Network Devices'. The main configuration area is titled 'Network Devices List > JaysNet' and 'Network Devices'. The configuration fields are as follows:

- * Name: CLUS_Net-Device
- Description: (empty)
- IP Address: 192.168.160.0
- Subnet: 24
- * Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- * Network Device Group:
 - Location: All Locations
 - IPSEC: No
 - Device Type: All Device Types
- RADIUS Authentication Settings
 - RADIUS UDP Settings
 - Protocol: RADIUS
 - Shared Secret: (masked)
 - Use Second Shared Secret:
 - CoA Port: 1700
 - RADIUS DTLS Settings: (empty)

Enfin, vous devez ajouter le nom d'utilisateur et le mot de passe que le client va entrer dans la page de connexion afin de valider qu'il doit avoir accès au réseau. Ceci est fait sous **Admin>Gestion des identités>Identité>Utilisateurs>Ajouter** et assurez-vous d'appuyer sur soumettre après l'avoir ajouté. Comme tout le reste avec ISE, il est personnalisable et n'a pas besoin d'être un utilisateur stocké localement, mais encore une fois, c'est la configuration la plus facile.

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 configuration 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.

Différences dans la configuration lorsque le WLC AireOS est étranger et que le Catalyst 9800 est l'ancrage

Si vous voulez que le WLC AireOS soit le contrôleur étranger, la configuration est la même que précédemment avec seulement deux différences.

1. La comptabilité AAA n'est jamais effectuée sur l'ancre, de sorte que le 9800 n'aurait pas de liste de méthodes comptables et que le WLC AireOS aurait activé la comptabilité et pointerait vers ISE.
2. L'AireOS devrait s'ancrer au 9800 plutôt qu'à lui-même. Dans le profil de stratégie, le 9800 n'aurait pas d'ancrage sélectionné, mais la case « Exporter l'ancrage » serait cochée.
3. Il est important de noter que lorsque les WLC AireOS exportent le client vers le 9800, il n'y a pas de concept de profils de stratégie, il envoie seulement le nom de profil WLAN. Par conséquent, le 9800 appliquera le nom de profil WLAN envoyé par AireOS au nom de profil WLAN et au nom de profil de stratégie. Cela dit, lors de l'ancrage d'un WLC AireOS à un WLC 9800, le nom du profil WLAN sur les deux WLC et le nom du profil de stratégie sur le 9800 doivent tous correspondre.

Vérification

Pour vérifier les configurations sur le WLC 9800 exécutez les commandes

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Profil de stratégie

```
Show wireless profile policy detailed <profile name>
```

- Étiquette de stratégie

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Vérifier que la mobilité est activée avec l'ancrage

```
Show wireless mobility summary
```

Pour vérifier les configurations sur le WLC AireOS, exécutez les commandes

- AAA

```
Show radius summary
```

Note: RFC3576 est la configuration CoA

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Vérifier que la mobilité fonctionne avec les

```
Show mobility summary
```

Dépannage

Le dépannage est différent selon le point dans lequel le client s'arrête. Par exemple, si le WLC n'obtient jamais de réponse d'ISE sur MAB, le client sera coincé dans l'état du Gestionnaire de stratégies : Associant » et ne serait pas exporté vers l'ancrage. Dans cette situation, vous ne

dépanneriez que sur l'étranger et vous pourriez collecter une trace RA et une capture de paquets pour le trafic entre le WLC et ISE. Un autre exemple est que MAB a réussi mais que le client ne reçoit pas la redirection. Dans ce cas, vous devez vous assurer que l'étranger a reçu la redirection dans les AVP et l'a appliquée au client. Vous devez également vérifier l'ancrage pour vous assurer que le client est bien présent avec la liste de contrôle d'accès correcte. Cette portée du dépannage ne se trouve pas dans la conception de ce document technique (consultez les références pour obtenir des instructions de dépannage client génériques).

Pour obtenir de l'aide sur le dépannage de CWA sur le WLC 9800, reportez-vous au Cisco Live ! présentation DGTL-TSCENT-404

Informations de dépannage du Catalyst 9800

Détails du client

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

Ici, vous devez regarder « Policy Manager State », « Session Manager>Auth Method », « Mobility Role ».

Vous pouvez également trouver ces informations dans l'interface utilisateur graphique sous Surveillance > Clients

Capture de paquets intégrée

À partir de l'interface de ligne de commande, la commande démarre *#monitor capture <nom de capture>* puis les options viennent après.

À partir de l'interface graphique, accédez à Dépannage>Capture de paquets>+Ajouter

Suivi RadioActive

À partir de l'interface de ligne de commande

```
debug wireless mac/ip
```

Utilisez la forme no de la commande pour l'arrêter. Il sera enregistré dans un fichier bootflash nommé « ra_trace », puis l'adresse MAC ou IP du client et la date et l'heure.

À partir de l'interface utilisateur graphique, accédez à Dépannage>Suivi radioactif>+Ajouter. Ajoutez l'adresse MAC ou ip du client, appuyez sur Apply, puis appuyez sur start. Une fois le processus terminé, arrêtez à plusieurs reprises la trace, générez le journal et téléchargez-le sur votre périphérique.

Informations de dépannage AireOS

Détails du client

À partir de l'interface de ligne de commande *show client details <client mac>*

À partir de l'interface graphique utilisateur Monitor>Clients

Débogues à partir de l'interface de ligne de commande

Debug client

Debug mobility handoff

Debug mobility config

Références

[Construction de tunnels de mobilité avec des contrôleurs 9800](#)

[Débogage sans fil et collecte de journaux sur 9800](#)