

Configuration de la position sur les WLC et ISE Catalyst 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration AAA sur un contrôleur WLC 9800](#)

[Configuration d'un réseau local sans fil \(WLAN\)](#)

[Configuration du profil des politiques](#)

[Configuration des balises des politiques](#)

[Affectation des balises des politiques](#)

[Configuration d'une liste de contrôle d'accès de redirection](#)

[Configuration ACL de stratégie](#)

[Configuration et réglage de la position AAA sur ISE](#)

[Exemples](#)

[Vérifier](#)

[Dépannage](#)

[Liste de vérification](#)

[Collecter les débogages](#)

[Références](#)

Introduction

Ce document décrit comment configurer un WLAN de posture sur un WLC et ISE Catalyst 9800 via l'interface graphique utilisateur (GUI).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration générale du WLC 9800
- Configuration des profils et des politiques ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 9800 WLC Cisco IOS® XE Cupertino v17.9.5
- Identity Service Engine (ISE) v3.2
- Ordinateur portable Windows 10 Entreprise

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.

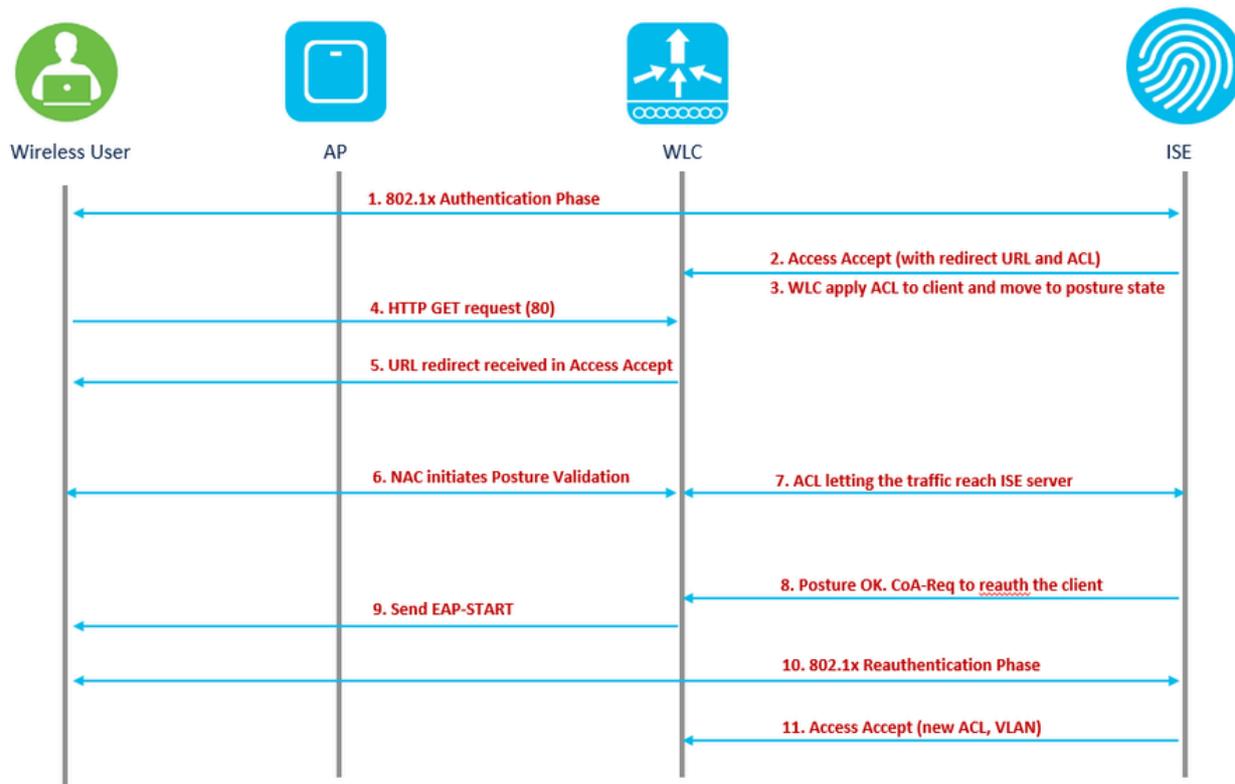
Informations générales

Flux de fonctionnalités RADIUS NAC et CoA du contrôleur LAN sans fil

1. Le client s'authentifie en utilisant l'authentification dot1x.
2. RADIUS Access Accept transporte l'URL redirigée pour le port 80 et les ACL de pré-authentification qui inclut l'autorisation des adresses IP et des ports, ou le VLAN de quarantaine.
3. Le client est redirigé vers l'URL fournie dans access accept, et placé dans un nouvel état jusqu'à ce que la validation de position soit effectuée. Le client dans cet état parle au serveur ISE et se valide par rapport aux stratégies configurées sur le serveur NAC ISE.
4. L'agent NAC sur le client lance la validation de position (trafic vers le port 80) : L'agent envoie une requête de détection HTTP au port 80, que le contrôleur redirige vers l'URL fournie dans access accept. L'ISE sait que le client tente d'atteindre et répond directement au client. De cette façon, le client apprend l'adresse IP du serveur ISE et, à partir de maintenant, le client communique directement avec le serveur ISE.
5. Le WLC autorise ce trafic, car la liste de contrôle d'accès est configurée pour autoriser ce trafic. En cas de remplacement du VLAN, le trafic est ponté de manière à atteindre le serveur ISE.
6. Une fois que le client ISE a terminé l'évaluation, une demande de certificat d'authenticité RADIUS avec le service Reauth est envoyée au WLC. Ceci lance la ré-authentification du client (en envoyant EAP-START). Une fois la ré-authentification réussie, l'ISE envoie l'acceptation d'accès avec une nouvelle liste de contrôle d'accès (le cas échéant) et aucune redirection d'URL, ou VLAN d'accès.
7. Le WLC prend en charge CoA-Req et Disconnect-Req conformément à la RFC 3576. Le WLC doit prendre en charge CoA-Req pour le service de ré-authentification, conformément à la RFC 5176.
8. Au lieu de listes de contrôle d'accès téléchargeables, des listes de contrôle d'accès préconfigurées sont utilisées sur le WLC. Le serveur ISE envoie simplement le nom de la liste de contrôle d'accès, qui est déjà configurée dans le contrôleur.

9. Cette conception fonctionne à la fois pour les VLAN et les ACL. Dans le cas d'une substitution de VLAN, nous redirigeons simplement le port 80 qui est redirigé et autorise (le pont) le reste du trafic sur le VLAN de quarantaine. Pour la liste de contrôle d'accès, la liste de contrôle d'accès de pré-authentification reçue dans access accept est appliquée.

Cette figure fournit une représentation visuelle de ce flux de fonctions :



workflow de fonction

Pour cet exemple d'utilisation, un SSID utilisé uniquement pour les utilisateurs d'entreprise est activé pour la position. Aucun autre cas d'utilisation, tel que BYOD, Invité ou tout autre, n'existe sur ce SSID.

Lorsqu'un client sans fil se connecte au SSID de posture pour la première fois, il doit télécharger et installer le module de posture sur le portail redirigé de l'ISE, puis l'appliquer avec les listes de contrôle d'accès appropriées en fonction du résultat du contrôle de posture (conforme/non conforme).

Configurer

Diagramme du réseau

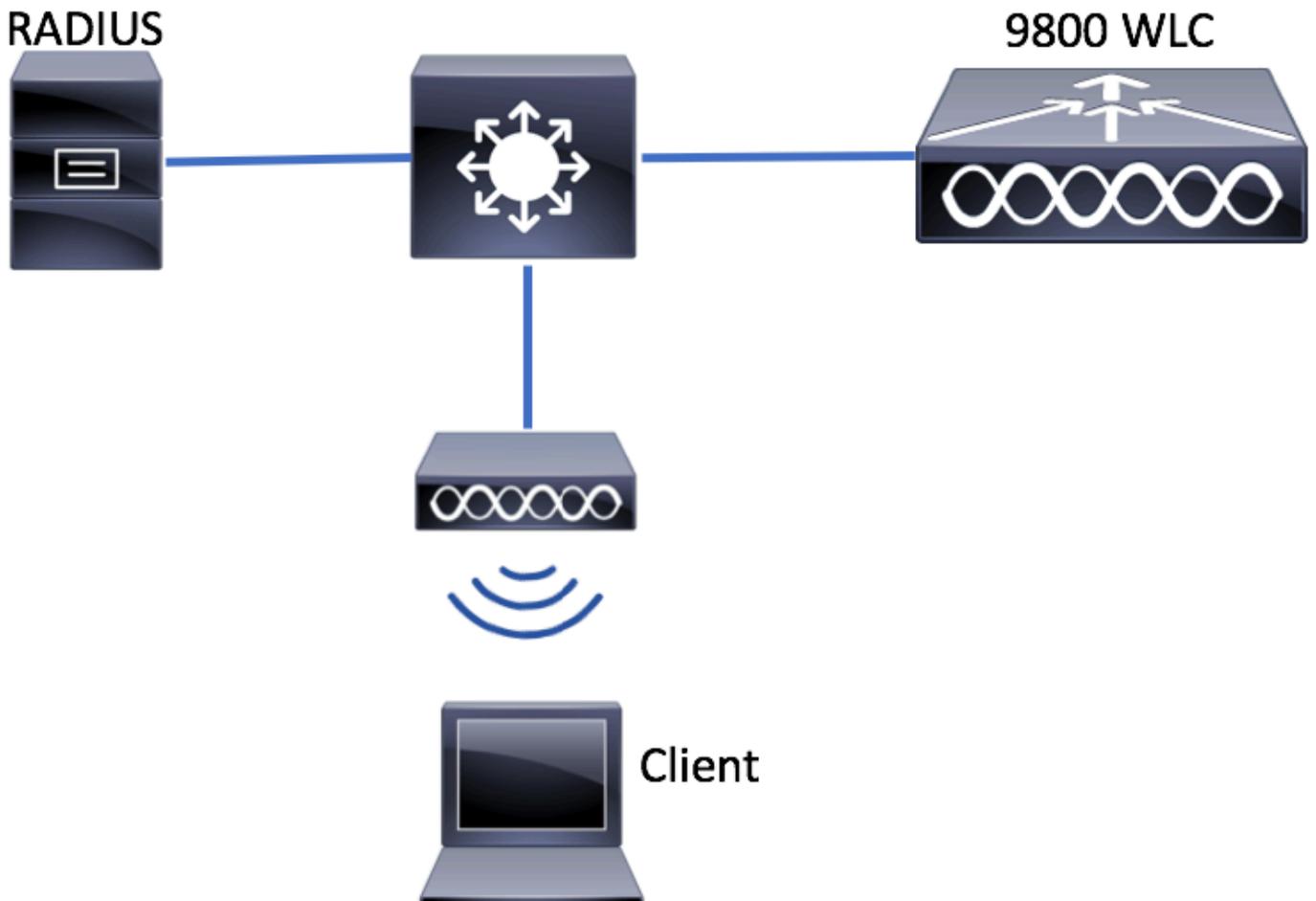
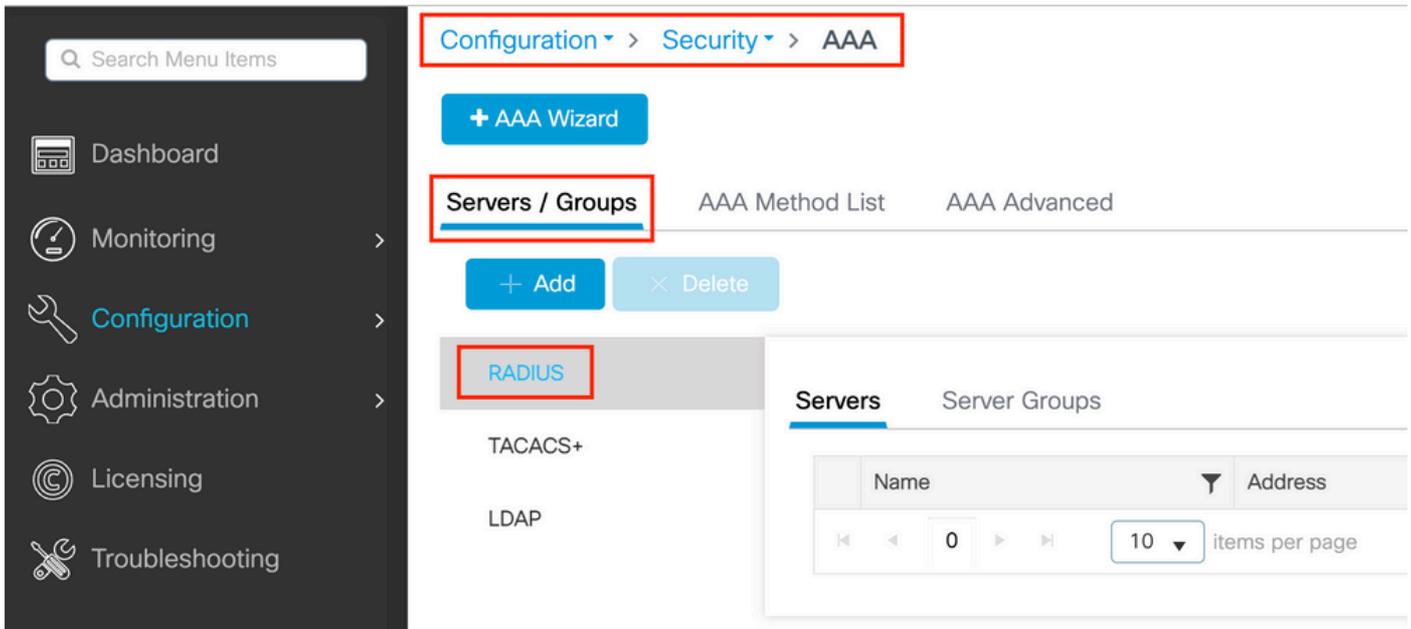


Diagramme du réseau

Configuration AAA sur un contrôleur WLC 9800

Étape 1 : ajout du serveur ISE à la configuration du WLC 9800 Accédez à Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add et entrez les informations du serveur RADIUS comme indiqué dans les images. Assurez-vous que la prise en charge CoA est activée pour NAC de posture.



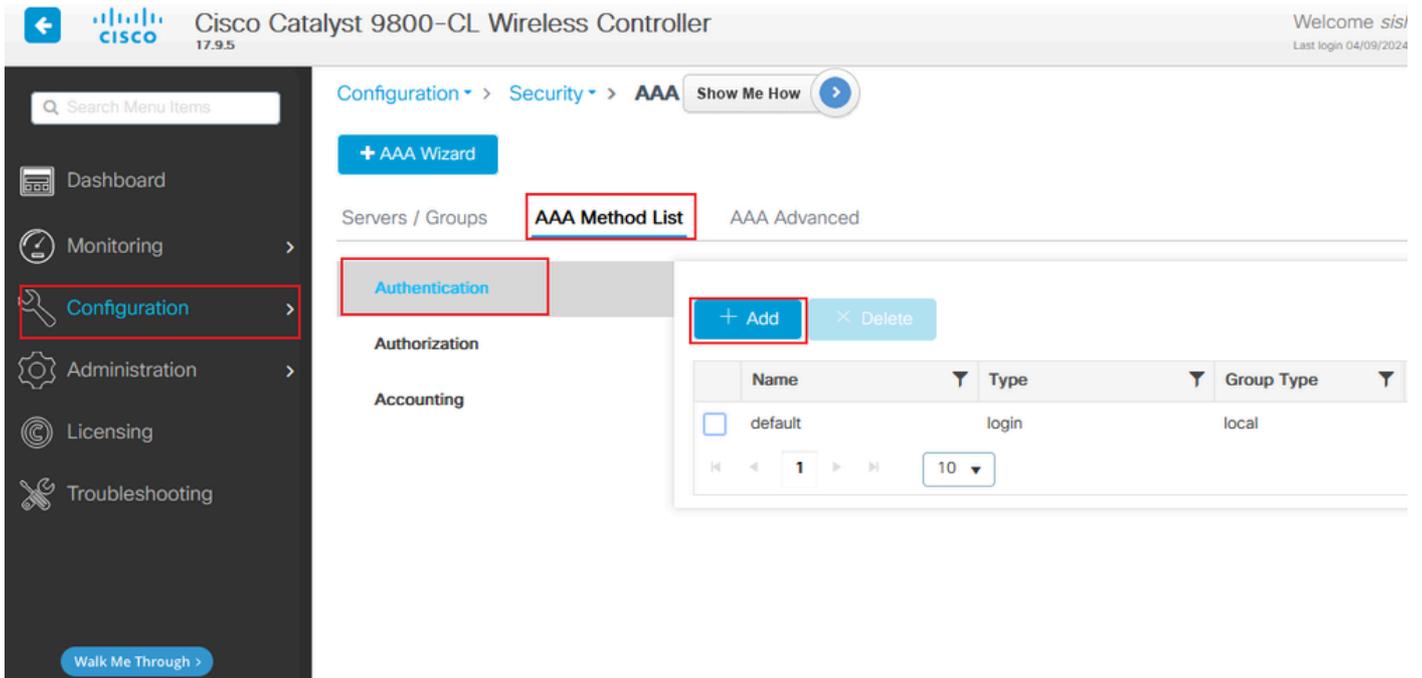
9800 créer un serveur radius

Create AAA Radius Server

Name*	posture-radius	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	10.124.57.141	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	•••••
Key Type	Clear Text ▼	Confirm CoA Server Key	•••••
Key* ⓘ	•••••	Automate Tester	<input type="checkbox"/>
Confirm Key*	•••••		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

9800 créer les détails du rayon

Étape 2 : création d'une liste de méthodes d'authentification Accédez à Configuration > Security > AAA > AAA Method List > Authentication > + Add comme indiqué dans l'image :



9800 ajouter une liste d'authentification

Quick Setup: AAA Authentication

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

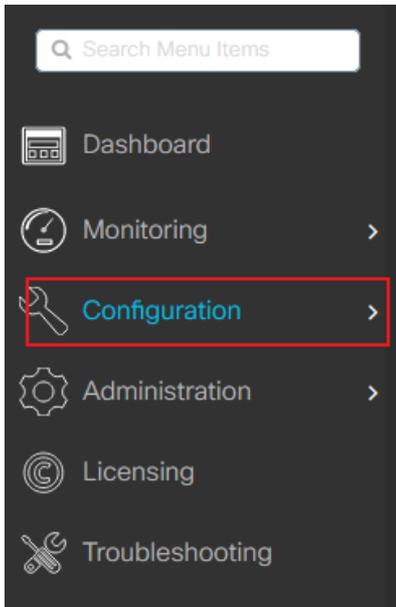
ldap
tacacs+

Assigned Server Groups

radius

9800 créer les détails de la liste d'authentification

Étape 3. (Facultatif) Créez une liste de méthodes de comptabilisation comme indiqué dans l'image :



Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

Name	Type
0	

Navigation: << < 0 > >> 10

9800 ajouter une liste de comptes

Quick Setup: AAA Accounting

Method List Name*

Type* ⓘ

Available Server Groups: ldap, tacacs+

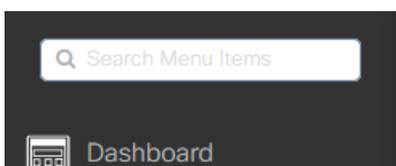
Assigned Server Groups: radius

Buttons: Cancel, Apply to Device

9800 créer une liste de comptes - détails

Configuration d'un réseau local sans fil (WLAN)

Étape 1 : création du WLAN Accédez à Configuration > Tags & Profiles > WLANs > + Add and configure the network as needed :



Configuration > Tags & Profiles > **WLANs**

+ Add × Delete

Clone

Enable WLAN

Disable WLAN

Ajout WLAN 9800

Étape 2. Entrez les informations générales du WLAN.

Add WLAN



General

Security

Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Broadcast SSID ENABLED

Radio Policy

[Show slot configuration](#)

6 GHz

Status ENABLED

- WPA2 Disabled
- WPA3 Enabled
- Dot11ax Enabled

5 GHz

Status ENABLED

2.4 GHz

Status ENABLED

802.11b/g Policy

Cancel

Apply to Device

9800 créer un WLAN général

Étape 3. Accédez à l'onglet Sécurité et choisissez la méthode de sécurité requise. Dans ce cas, choisissez '802.1x' et la liste d'authentification AAA (que vous avez créée à l'étape 2. dans la section Configuration AAA) sont nécessaires :

Add WLAN



General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize OSEN Policy

WPA2 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Protected Management Frame

PMF

Fast Transition

Status

Over the DS

Reassociation Timeout *

Auth Key Mgmt

802.1x PSK
Easy-PSK CCKM
FT + 802.1x FT + PSK
802.1x-SHA256 PSK-SHA256

Cancel

Apply to Device

9800 créer une sécurité WLAN L2

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 **AAA**

Authentication List

Local EAP Authentication

9800 créer une sécurité WLAN AAA

Configuration du profil des politiques

Dans un profil de stratégie, vous pouvez décider d'attribuer les clients à quel VLAN, entre autres paramètres (comme la liste de contrôle d'accès (ACL), la qualité de service (QoS), l'ancrage de mobilité, les minuteurs, etc.). Vous pouvez soit utiliser votre profil de politique par défaut, soit en créer un nouveau.

Étape 1. Créer un nouveau profil de stratégie. Accédez à Configuration > Tags & Profiles > Policy et créez-en une nouvelle :

Configuration > Tags & Profiles > Policy

+ Add Delete Clone

	Admin Status	Associated Policy Tags	Policy Profile Name
<input type="checkbox"/>	✓		posture_demo_pp
<input type="checkbox"/>	✓		default-policy-profile

1 10

9800 ajouter un profil de stratégie

Assurez-vous que le profil est activé.

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name* posture_demo_pp

Description Enter Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT 2-65519

9800 créer un profil de stratégie général

Étape 2 : sélection du VLAN Accédez à l'onglet Access Policies et choisissez le nom de VLAN dans la liste déroulante ou tapez manuellement l'ID de VLAN. Ne configurez pas de liste de contrôle d'accès dans le profil de politique:

Edit Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

9800 créer un profil de stratégie VLAN

Étape 3 : configuration du profil de stratégie pour accepter les remplacements ISE (autoriser le remplacement AAA) et la modification de l'autorisation (état NAC) Vous pouvez également définir une méthode de gestion des comptes:

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

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

WLAN Timeout

Session Timeout (sec) ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name ✕ ▾ ⓘ

Accounting List ✕ ▾ ⓘ

WGB Parameters

Fabric Profile ▾ ⓘ

Link-Local Bridging

mDNS Service Policy ▾ ⓘ
[Clear](#)

Hotspot Server ▾ ⓘ

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map ▾ ⓘ
[Clear](#)

Flex DHCP Option for DNS **ENABLED**

Flex DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL ▾ ⓘ

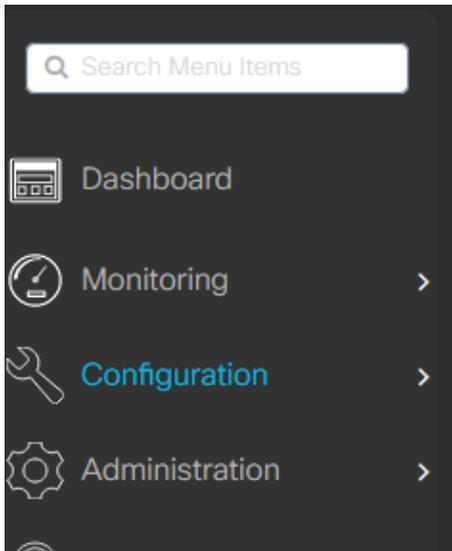
Air Time Fairness Policies

9800 créer un profil de stratégie Avancé

Configuration des balises des politiques

Vous pouvez associer votre SSID à votre profil de politiques dans la balise de politiques. Vous pouvez soit créer une nouvelle balise de politiques, soit utiliser la balise de politique par défaut.

Accédez à Configuration > Tags & Profiles > Tags > Policy et ajoutez-en un nouveau si nécessaire, comme indiqué dans l'image :



Policy Site RF AP

+ Add × Delete Clone

Policy Tag Name
<input type="checkbox"/> default-policy-tag

1 10

9800 policy tag add

Liez votre profil de réseau WLAN au profil de politiques souhaité:

Edit Policy Tag ✕

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* posture-policy-tag

Description Enter Description

▼ WLAN-POLICY Maps: 1

+ Add × Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> posture_demo	posture_demo_pp

1 10 1 - 1 of 1 items

Détails de la balise de stratégie 9800

Affectation des balises des politiques

Affectez la balise de politiques aux points d'accès nécessaires. Accédez à Configuration > Wireless > Access Points > AP Name > General Tags , effectuez l'affectation nécessaire, puis cliquez sur Update & Apply to Device .

Edit AP ✕

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy

Site

RF

Affectation de balise de stratégie 9800

Configuration d'une liste de contrôle d'accès de redirection

Rendez-vous à Configuration > Security > ACL > +Add (configuration > sécurité > liste de contrôle d'accès > +ajouter) afin de créer une nouvelle liste de contrôle d'accès.

La liste de contrôle d'accès utilisée pour la redirection de Posture Portal a les mêmes exigences que la CWA (authentification Web centrale).

Vous devez refuser le trafic vers vos nœuds PSN ISE, refuser le DNS et autoriser tout le reste. Cette liste de contrôle d'accès de redirection n'est pas une liste de contrôle d'accès de sécurité, mais une liste de contrôle d'accès ponctuelle qui définit le trafic acheminé vers le processeur (en cas d'autorisation) pour un traitement ultérieur (comme la redirection) et le trafic restant sur le plan de données (en cas de refus) et qui évite la redirection. La liste de contrôle d'accès doit ressembler à ceci (remplacez 10.124.57.141 par votre adresse IP ISE dans cet exemple) :

Edit ACL ✕

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		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/>	20	deny	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/>	30	deny	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/>	40	deny	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/>	50	permit	any		any		tcp	None	eq www	None	Disa

Détails ACL de redirection 9800

Configuration ACL de stratégie

Dans ce cas, vous devez définir des listes de contrôle d'accès distinctes sur le WLC 9800 pour ISE afin d'autoriser les scénarios Conforme et Non-Conforme en fonction du résultat du contrôle de position.

[Configuration](#) > [Security](#) > **ACL**

	ACL Name	ACL Type
<input type="checkbox"/>	POSTURE_COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_NON-COMPLIANT_ACL	IPv4 Extended
<input type="checkbox"/>	POSTURE_REDIRECT_ACL	IPv4 Extended

« 1 » 10 ▾

9800 ACL général

Pour le scénario Conforme, utilisez simplement permit all dans ce cas. Comme autre configuration courante, vous pouvez également demander à ISE de ne pas autoriser de liste de contrôle d'accès dans le résultat conforme, ce qui équivaut à autoriser tout du côté 9800 :

Edit ACL ✕

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	permit	any		any		ip	None	None	None	Disable

1 - 1 of 1 items

9800 ACL - Conforme

Dans un scénario non conforme, le client autorise uniquement l'accès à certains réseaux, généralement le serveur de conversion (ISE lui-même dans ce cas) :

Edit ACL ✕

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	permit	10.124.57.141		any		ip	None	None	None	Disa
<input type="checkbox"/> 20	permit	any		10.124.57.141		ip	None	None	None	Disa
<input type="checkbox"/> 30	permit	any		any		udp	None	eq domain	None	Disa
<input type="checkbox"/> 40	permit	any		any		udp	eq domain	None	None	Disa
<input type="checkbox"/> 50	deny	any		any		ip	None	None	None	Disa

1 - 5 of 5 items

ACL 9800 - Non conforme

Configuration et réglage de la position AAA sur ISE

Condition de posture : Dans cet exemple, l'exigence de déterminer la conformité consiste à détecter si un fichier de test spécifique existe sur le bureau utilisé pour tester le PC Windows.

Étape 1 : ajout du WLC 9800 en tant que NAD sur l'ISE Accédez à Administration > Ressources réseau > Périphériques réseau > Ajouter à :

The screenshot shows the Cisco ISE Administration interface for configuring a Network Device. The breadcrumb trail is Administration > Network Resources > Network Devices > WLC9800. The configuration fields are as follows:

- Name: WLC9800
- Description: (empty)
- IP Address: 10.124.60.41 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: All Device Types (Set To Default)

Ajouter un périphérique réseau 01

The screenshot shows the RADIUS Authentication Settings configuration page in Cisco ISE. The breadcrumb trail is Administration > Network Resources > Network Devices > RADIUS Authentication Settings. The configuration fields are as follows:

- Protocol: RADIUS
- Shared Secret: (masked with dots) (Show)
- Use Second Shared Secret: (unchecked)
- Second Shared Secret: (empty) (Show)
- CoA Port: 1700 (Set To Default)
- RADIUS DTLS Settings: (info icon)
- DTLS Required: (unchecked)
- Shared Secret: radius/dtls (info icon)
- CoA Port: 2083 (Set To Default)
- Issuer CA of ISE Certificates for CoA: Select if required (optional) (info icon)
- DNS Name: (empty)

Ajouter un périphérique réseau 02

Étape 2. Téléchargez le package de déploiement et le module de conformité Cisco Secure Client Headend sur le site Web Cisco Software CCO.

Accédez à Cisco Secure Client et effectuez des recherches :

Cisco Secure Client Headend Deployment Package (Windows) 06-Feb-2024 111.59 MB
cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg
[Advisories](#)

Client sécurisé 5.1.2.42

ISE Posture Compliance Library - Windows / Head-end deployment (PKG). This image can be used with AnyConnect version 4.3 and later along with ISE 2.1 and later. Cisco Secure Client 5.x along with ISE 2.7 and later.
cisco-secure-client-win-4.3.3335.6146-isecompliance-webdeploy-k9.pkg
[Advisories](#)

Module de conformité ISE 4.3

Étape 3 : chargement du package de déploiement et du module de conformité Cisco Secure Client Headend vers ISE Client Provisioning Accédez à Work Centers> Posture> Client Provisioning> Resources . Cliquez sur Add, choisissez Agent resources from local disk dans la liste déroulante :

Overview	Network Devices	Client Provisioning	Policy Elements
Client Provisioning Policy			
Resources			
Client Provisioning Portal			
[Edit] [Add] [Duplicate] [Delete]			
<input type="checkbox"/>	Agent resources from Cisco site		
<input type="checkbox"/>	Agent resources from local disk		
<input type="checkbox"/>	Native Supplicant Profile		
<input type="checkbox"/>	Agent Configuration		
<input type="checkbox"/>	Agent Posture Profile		
<input type="checkbox"/>	AMP Enabler Profile		

Télécharger le client sécurisé

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

Selected 0 Total 13

Edit + Add Duplicate Delete Quick Filter

Name	Type	Version	Last Update	Description
CiscoTemporalAgentOSX 4.10.02051	CiscoTemporalAgentOSX	4.10.2051.0	2021/08/10 03:12:31	With CM: 4.3.1858.4353
CiscoSecureClientComplianceModuleWindows 4.3.3335.6146	CiscoSecureClientComplianceModuleWindows	4.3.3335.6146	2024/03/30 19:28:34	Cisco Secure Client Win...
Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
CiscoAgentlessOSX 4.10.02051	CiscoAgentlessOSX	4.10.2051.0	2021/08/10 03:12:36	With CM: 4.3.1858.4353
bloomtest-Posture for Windows	AgentProfile	Not Applicable	2024/03/30 19:31:40	test windows PC for con...
AnyConnectDesktopWindows 4.10.7073.0	AnyConnectDesktopWindows	4.10.7073.0	2024/03/30 19:47:18	AnyConnect Secure Mob...
MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2021/08/10 03:12:27	Supplicant Provisioning ...
CiscoAgentlessWindows 4.10.02051	CiscoAgentlessWindows	4.10.2051.0	2021/08/10 03:12:33	With CM: 4.3.2227.6145
Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/10/07 04:01:12	Pre-configured Native S...
WLC9800-windows	AgentConfig	Not Applicable	2024/04/01 17:44:50	Test for WLC9800 Wirele...
WinSPWizard 3.0.0.3	WinSPWizard	3.0.0.3	2021/08/10 03:12:27	Supplicant Provisioning ...
CiscoTemporalAgentWindows 4.10.02051	CiscoTemporalAgentWindows	4.10.2051.0	2021/08/10 03:12:28	With CM: 4.3.2227.6145
CiscoSecureClientDesktopWindows 5.1.2.042	CiscoSecureClientDesktopWindows	5.1.2.42	2024/03/30 19:20:54	Cisco Secure Client for ...

Téléchargement du client sécurisé et du module de conformité réussi

Étape 4. Créer un profil de position d'agent Accédez à Centres de travail> Position> Approvisionnement client> Ressources> Ajouter> Profil de position d'agent :

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy Resources Client Provisioning Portal

ISE Posture Agent Profile Settings > bloomtest-Posture for Windows

Agent Posture Profile

Name *
bloomtest-Posture for Windows

Description:
test windows PC for connecting WLC9800

Agent Behavior

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	Agent can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled	Display user notifications even when in Stealth mode.

Profil de posture de l'agent

Étape 5. Créer une configuration d'agent Accédez à Centres de travail> Position> Approvisionnement client> Ressources> Ajouter> Configuration d'agent :

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1

* Configuration Name: WLC9800-windows

Description: Test for WLC9800 Wireless dot1x

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleW

Cisco Secure Client Module Selection

ISE Posture

VPN

Zero Trust Access

Network Access Manager

Secure Firewall Posture

Network Visibility

Umbrella

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture bloomtest-Posture for Windows

Ajouter une configuration d'agent

Étape 6. Confirmez que le portail d'approvisionnement du client, utilisez le portail par défaut pour le test est OK. (Générez un CSR et demandez un certificat SSL à partir du serveur AC, et remplacez la balise Groupe de certificats sur ce portail Paramètres. Sinon, un avertissement de certificat non approuvé se produit pendant le processus de test.)

Accédez à Work Centers> Posture> Client Provisioning> Client Provisioning Portals :

Cisco ISE Work Centers - Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Client Provisioning Portals

You can edit and customize the default Client Provisioning portal and create additional ones

Create Edit Duplicate Delete

Client Provisioning Portal (default)

Default portal and user experience used to install the posture agents and verify compliance on user's devices

Sélectionnez Client Provisioning Portal 01

Client Provisioning Policy
Resources
Client Provisioning Portal

Portal Behavior and Flow Settings Portal Page Customization

Portal & Page Settings

Portal Settings

HTTPS port:* **8443** (8000 - 8999)

Bidirectional port:* **8449** (8000 - 8999)

Allowed Interfaces:*

For PSNs Using Physical Interfaces	For PSNs with Bonded Interfaces Configured
<input checked="" type="checkbox"/> Gigabit Ethernet 0	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
<input type="checkbox"/> Gigabit Ethernet 1	<input type="checkbox"/> Bond 1 Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
<input type="checkbox"/> Gigabit Ethernet 2	<input type="checkbox"/> Bond 2 Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
<input type="checkbox"/> Gigabit Ethernet 3	
<input type="checkbox"/> Gigabit Ethernet 4	
<input type="checkbox"/> Gigabit Ethernet 5	

Certificate group tag: * **Test-CPP** ▼
Configure certificates at:
[Administration > System > Certificates > System Certificates](#)

Authentication method: * **Certificate_Request_Sequence** ▼
Configure authentication methods at:
[Administration > Identity Management > Identity Source Sequences](#)

Sélectionnez Client Provisioning Portal 02

Étape 7 : création d'une politique de provisionnement client Accédez à Work Centers> Posture> Client Provisioning> Client Provisioning Policy > Edit> insert new policy above.

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> WLC9800-Windows	If Any	and Windows All	and Condition(s)	then WLC9800-windows Edit ▼
<input checked="" type="checkbox"/> IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP Edit ▼
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit ▼
<input checked="" type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.10.02051 And WinSPWizard 3.0.0.3 And Cisco-ISE-NSP Edit ▼
<input checked="" type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 4.10.02051 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP Edit ▼
<input checked="" type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP Edit ▼

Créer une politique de provisionnement client

Étape 8. Création de conditions de fichier Accédez à Centres de travail> Position> Éléments de stratégie> Conditions> Fichier> Conditions de fichier> Ajouter :

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Conditions List > WLC9800-Posture-demo

File Condition

Name * WLC9800-Posture-demo

Description test for WLC9800

* Operating System Windows All

Compliance Module Any version

* File Type FileExistence

* File Path USER_DESKTOP WLC9800-Posture-Demo.txt

* File Operator Exists

Créer une condition de fichier

Étape 9. Créer des mesures correctives Accédez à Centres de travail> Position> Éléments de stratégie> Mesures correctives > Fichier> Ajouter :

≡ Cisco ISE Work Centers · Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

File Remediations List > WLC9800-Posture-Demo

File Remediation

* Name WLC9800-Posture-Demo

Description your PC must have file named WLC9800-Posture-

Compliance Module Any version

Version 1.0

File Uploaded WLC9800-Posture-Demo.txt

Créer une correction de fichier

Étape 10. Création du besoin Accédez à Centres de travail> Position> Éléments de stratégie> Exigences> Insérer une nouvelle exigence :

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

Remediations

- Application
- Anti-Malware
- Anti-Spyware
- Anti-Virus
- File
- Firewall
- Launch Program
- Link
- Patch Management
- Script
- USB
- Windows Server Update Servi...
- Windows Update

Requirements

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst then	Message Text Only Edit
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win then	Select Remediations Edit
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac then	Select Remediations Edit
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations Edit
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check then	Select Remediations Edit
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win then	Default_Firewall_Remediation_Win Edit
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac then	Default_Firewall_Remediation_Mac Edit
WLC9800-Posture-Demo	for Windows All	using Any version	using Agent	met if WLC9800-Posture-demo then	WLC9800-Posture-Demo Edit

Note:
 Remediation Action is filtered based on the operating system and stealth mode selection.
 Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
 Remediations Actions are not applicable for Agentless Posture type.

Créer une condition de posture

Étape 11. Créer une politique de posture Accédez à Work Centers> Posture> Insérer une nouvelle stratégie :

Cisco ISE Work Centers - Posture

Overview Network Devices Client Provisioning **Posture Policy** Policy Sets Troubleshoot Reports Settings

Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions. WLC9800

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Policy Options	WLC9800-Posture-Demo	If Any	and Windows All	and Any version	and Agent	and	with WLC9800-Posture-Demo Edit

Créer une politique de posture

Étape 12. Créez trois profils d'autorisation : L'état de la posture est Inconnu ; le statut de la posture est Non conforme ; L'état de posture est Conforme. Accédez à Stratégie> Éléments de stratégie> Résultats> Autorisation> Profils d'autorisation> Ajouter :

Dictionaries Conditions **Results**

Authentication

- Allowed Protocols

Authorization

- Authorization Profiles
- Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)

Name	Profile	Description
WLC9800	×	
<input type="checkbox"/> WLC9800-Posture-Compliant	Cisco	
<input type="checkbox"/> WLC9800-Posture-NonCompliant	Cisco	
<input type="checkbox"/> WLC9800-Posture-Unknown	Cisco	

Créer des profils d'autorisation 01

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles > Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > WLC9800-Posture-Unknown

Authorization Profile

* Name

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) POSTURE_REDIRECT_ACL Value

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Créer des profils d'autorisation 02

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles > Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > WLC9800-Posture-Compliant

Authorization Profile

* Name

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

Interface Template

Web Authentication (Local Web Auth)

Airespace ACL Name

Airespace IPv6 ACL Name

Créer des profils d'autorisation 03

Dictionarys Conditions Results

Authorization Profile

* Name: WLC9800-Posture-NonComp

Description: [Empty text box]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

Common Tasks

Interface Template

Web Authentication (Local Web Auth)

Airespace ACL Name: POSTURE_NON-COMPLIANT_

Airespace IPv6 ACL Name

Advanced Attributes Settings

Étape 13. Créer des ensembles de stratégies Accédez à Policy> Policy

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	WLC9800-Posture-Demo		AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture_demo	Default Network Access	0	⚙️ ▶️	
✔	Default	Default policy set		Default Network Access	0	⚙️ ▶️	

Reset Save

Créer des jeux de stratégies

Ensembles> Ajouter une icône :

Étape 14. Créer une stratégie d'authentification Accédez à Stratégie> Jeux de stratégies> Développez « WLC9800-Posture-Demo »> Stratégie d'authentification> Ajouter :

Cisco ISE Policy - Policy Sets

WLC9800-Posture-Demo AND Network Access Device IP Address EQUALS 10.124.60.41 Normalised Radius-SSID CONTAINS posture_demo Default Network Access

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Wireless-dot1x	Wireless_802.1X	Internal Users	0	Options
●	Default		All_User_ID_Stores	0	Options

Créer une stratégie d'authentification

Étape 15. Créer une stratégie d'autorisation Accédez à Stratégie> Jeux de stratégies> Développez « WLC9800-Posture-Demo »> Stratégie d'autorisation> Ajouter :

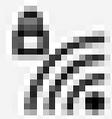
Authorization Policy (4)

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Posture-Compliant	Session PostureStatus EQUALS Compliant	WLC9800-Posture-Co...	Select from list	0
●	Posture-Noncompliant	Session PostureStatus EQUALS NonCompliant	WLC9800-Posture-No...	Select from list	0
●	Posture-Unknown	Session PostureStatus EQUALS Unknown	WLC9800-Posture-Unk...	Select from list	0
●	Default		DenyAccess	Select from list	0

Créer une stratégie d'autorisation

Exemples

1. Test du SSID connecté posture_demo avec les informations d'identification 802.1X correctes.



posture_demo
Secured

Enter your user name and password

wlc9800-user

••••••••

OK

Cancel

Network & Internet settings

Change settings, such as making a connection metered.



- Si le navigateur a été redirigé vers l'URL du portail ISE, mais que la page ne peut pas être chargée, vérifiez si le nom de domaine ISE n'est pas ajouté au serveur DNS. Par conséquent, le client ne peut pas résoudre l'URL du portail. Pour résoudre rapidement ce problème, vérifiez l'adresse IP statique/nom d'hôte/nom de domaine complet sous le profil d'autorisation pour fournir l'adresse IP dans l'URL de redirection. Cependant, cela peut constituer un problème de sécurité car cela expose l'adresse IP de l'ISE.

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▾

ACL

POSTURE_REDIRECT_ACL ▾

Value Client Provisioning Portal (def: ▾

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Auto Smart Port

Collecter les débogages

[Activer les débogages sur C9800](#)

[Activer les débogages sur ISE](#)

Références

- [Configuration de CWA sur WLC et ISE Catalyst 9800 - Cisco](#)
- [BYOD sans fil avec Identity Services Engine](#)
- [Déployer la position ISE](#)
- [Dépannage de la gestion et de la position des sessions ISE](#)
- [Comparer le flux de redirection de position ISE au flux sans redirection de position ISE](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.