

Configuración de la posición en Catalyst 9800 WLC e ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de AAA en WLC 9800](#)

[Configuración de WLAN](#)

[Configuración del perfil de la política](#)

[Configuración de etiquetas de políticas](#)

[Asignación de etiquetas de políticas](#)

[Configuración de ACL de redireccionamiento](#)

[Configuración de ACL de políticas](#)

[Configuración AAA y parámetro de estado en ISE](#)

[Examples](#)

[Verificación](#)

[Troubleshoot](#)

[Lista de Verificación](#)

[Recopilar depuraciones](#)

[Referencias](#)

Introducción

Este documento describe cómo configurar una WLAN de estado en un WLC Catalyst 9800 e ISE a través de la interfaz gráfica de usuario (GUI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración general del 9800 WLC
- Configuración de perfiles y políticas de ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

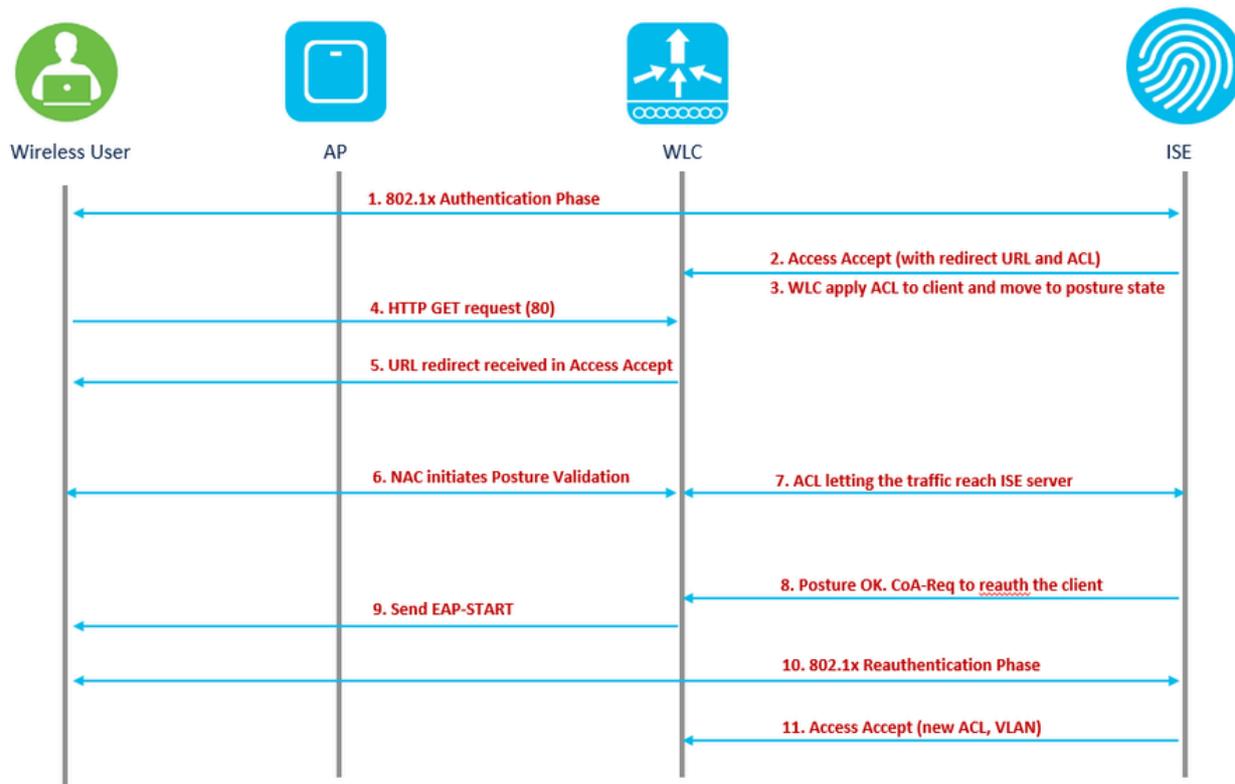
Antecedentes

Flujo de funciones de RADIUS NAC y CoA del controlador de LAN inalámbrica

1. El cliente autentica usando la autenticación dot1x.
2. La aceptación de acceso de RADIUS transporta la URL redirigida para el puerto 80 y las ACL previas a la autenticación que incluyen permitir direcciones IP y puertos, o poner en cuarentena VLAN.
3. El cliente se redirige a la URL proporcionada en access accept, y se pone en un nuevo estado hasta que se realice la validación de estado. El cliente en este estado se comunica con el servidor ISE y se valida con las políticas configuradas en el servidor ISE NAC.
4. El agente NAC del cliente inicia la validación de estado (tráfico al puerto 80): El agente envía la solicitud de detección HTTP al puerto 80, que el controlador redirige a la URL proporcionada en la aceptación de acceso. El ISE sabe que el cliente está intentando ponerse en contacto con él y responde directamente. De esta manera, el cliente aprende acerca de la IP del servidor ISE y, a partir de ahora, el cliente habla directamente con el servidor ISE.
5. El WLC permite este tráfico porque la ACL está configurada para permitir este tráfico. En caso de anulación de VLAN, el tráfico se puentea de modo que llegue al servidor ISE.
6. Una vez que el cliente de ISE completa la evaluación, se envía una petición de CoA de RADIUS con el servicio de reautenticación al WLC. Esto inicia la reautenticación del cliente (mediante el envío de EAP-START). Una vez que la reautenticación se realiza correctamente, ISE envía la aceptación de acceso con una nueva ACL (si la hay) y sin redirección de URL ni acceso a VLAN.
7. El WLC tiene soporte para CoA-Req y Disconnect-Req según RFC 3576. El WLC necesita soportar CoA-Req para el servicio de reautenticación, según RFC 5176.
8. En lugar de ACL descargables, las ACL preconfiguradas se utilizan en el WLC. El servidor ISE envía simplemente el nombre de ACL, que ya está configurado en el controlador.

9. Este diseño funciona para ambos casos de VLAN y ACL. En caso de anulación de VLAN, simplemente redirigimos el puerto 80 y permite el resto (bridge) del tráfico en la VLAN de cuarentena. Para la ACL, se aplica la ACL previa a la autenticación recibida en la aceptación de acceso.

Esta figura proporciona una representación visual de este flujo de funciones:



flujo de trabajo de funciones

Para este caso práctico, un SSID que solo se utiliza para usuarios corporativos está habilitado para el estado. No existen otros casos prácticos, como BYOD, Invitado o cualquier otro en este SSID.

Cuando un cliente inalámbrico se conecta al SSID de postura por primera vez, debe descargar e instalar el módulo de postura en el portal redirigido de ISE y, por último, debe aplicarse con las ACL relevantes en función del resultado de la comprobación de postura (Conforme/No conforme).

Configurar

Diagrama de la red

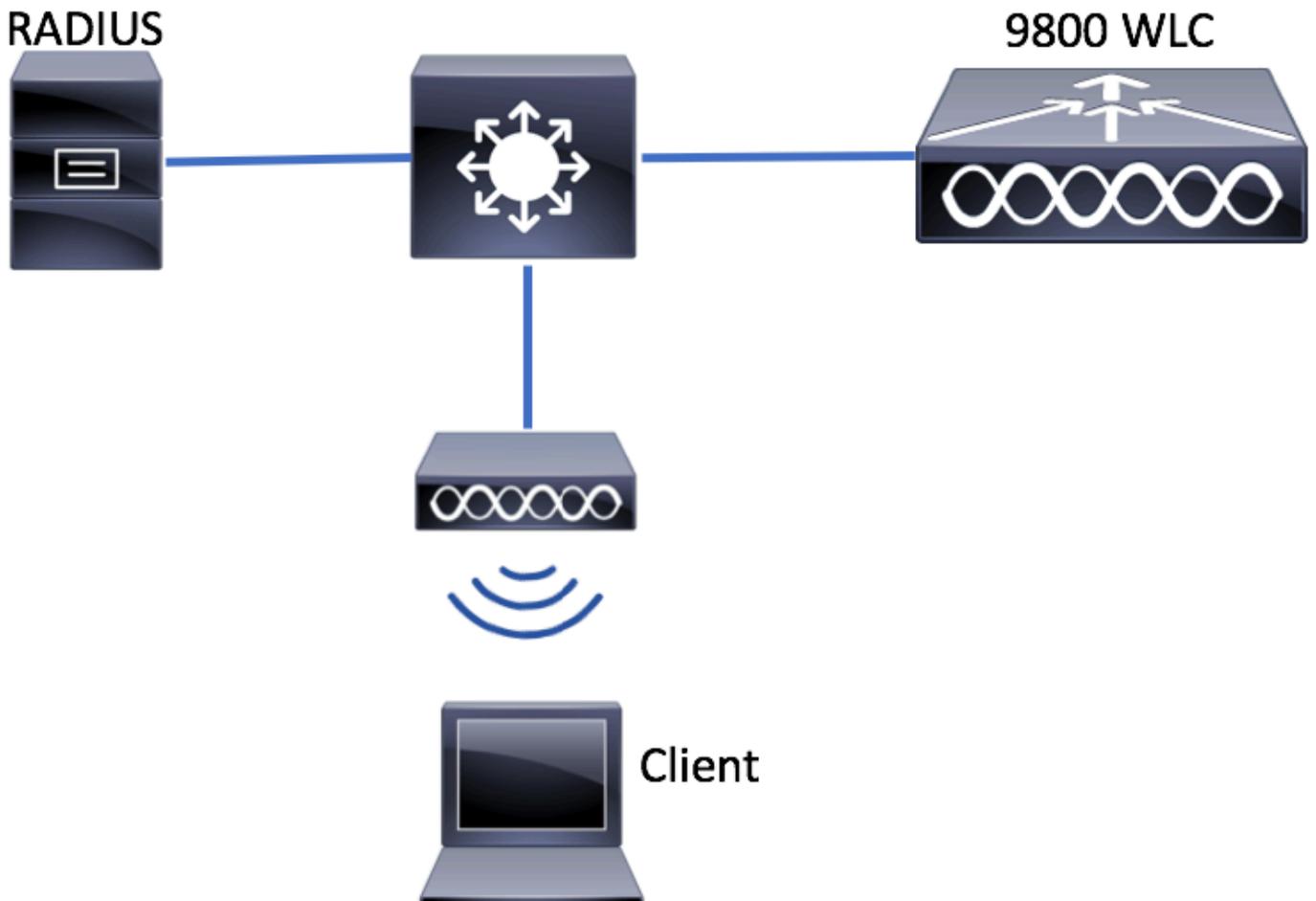
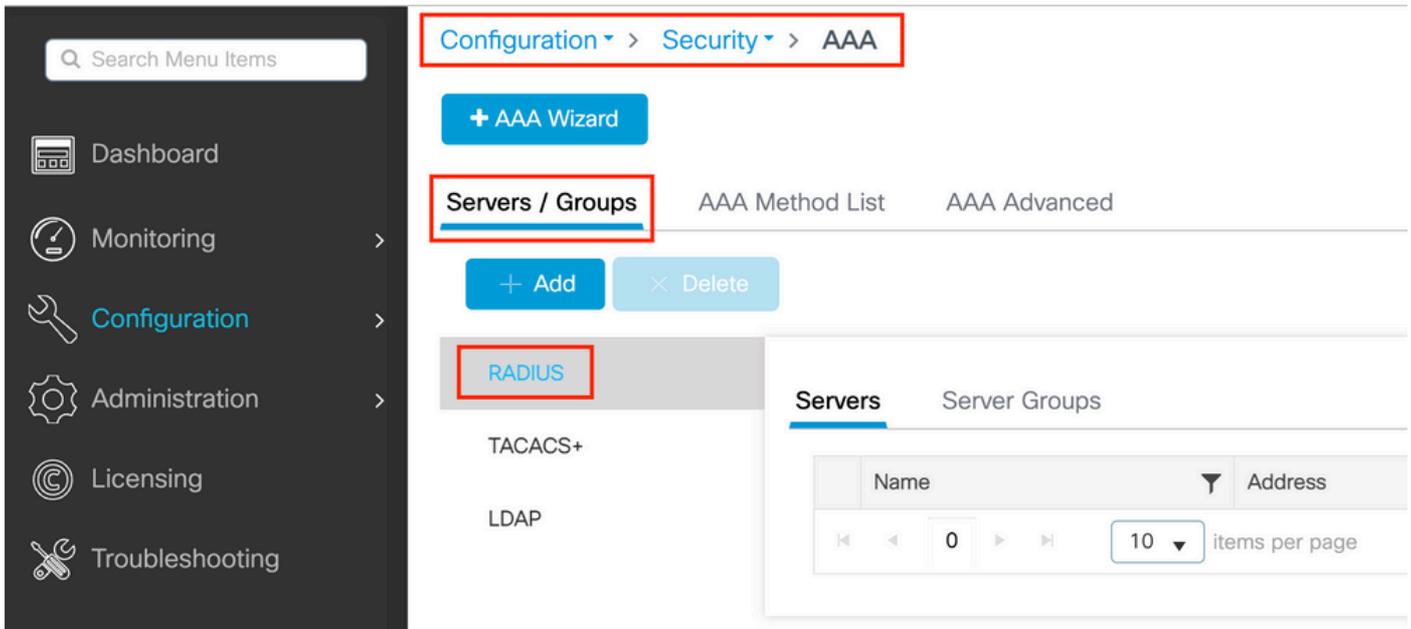


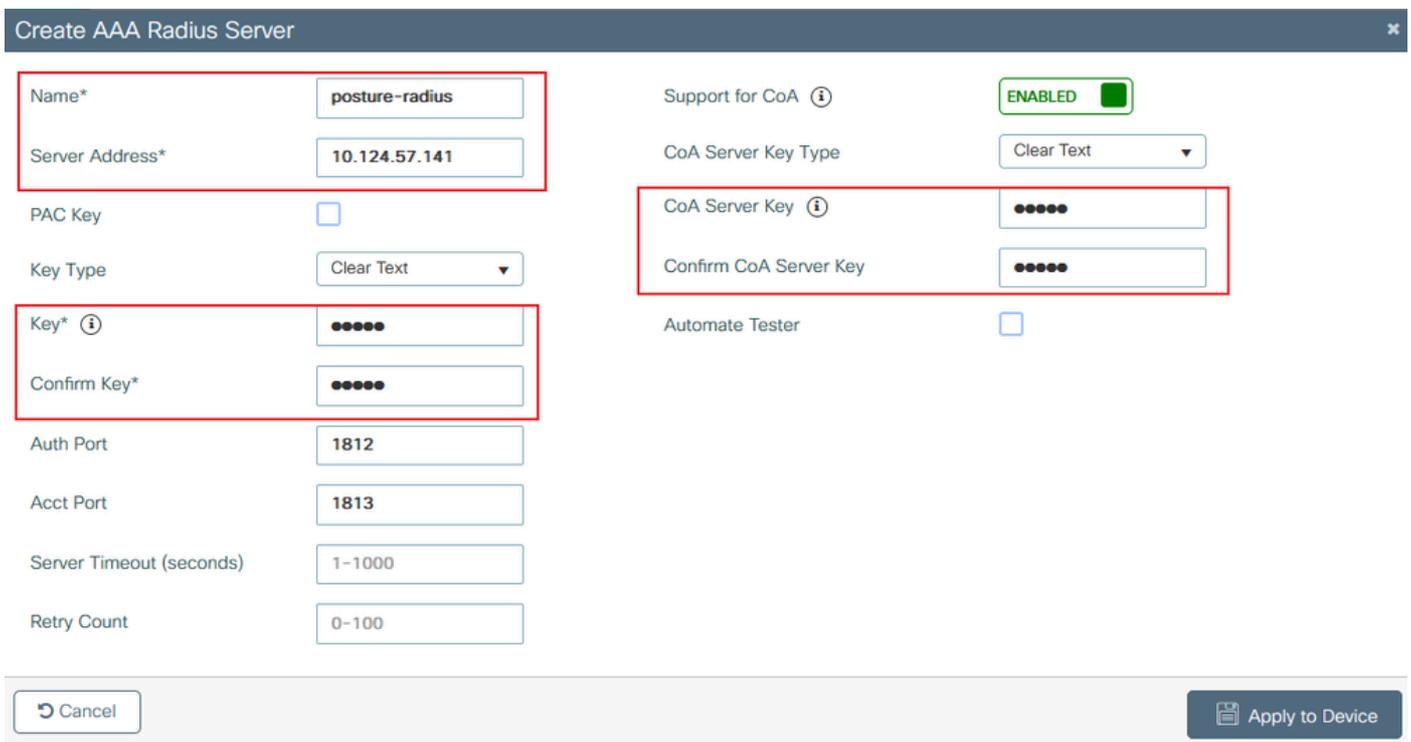
Diagrama de la red

Configuración de AAA en WLC 9800

Paso 1. Agregue el servidor ISE a la configuración del WLC 9800. Navegue hasta Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add e ingrese la información del servidor RADIUS como se muestra en las imágenes. Asegúrese de que la compatibilidad con CoA está habilitada para NAC de estado.

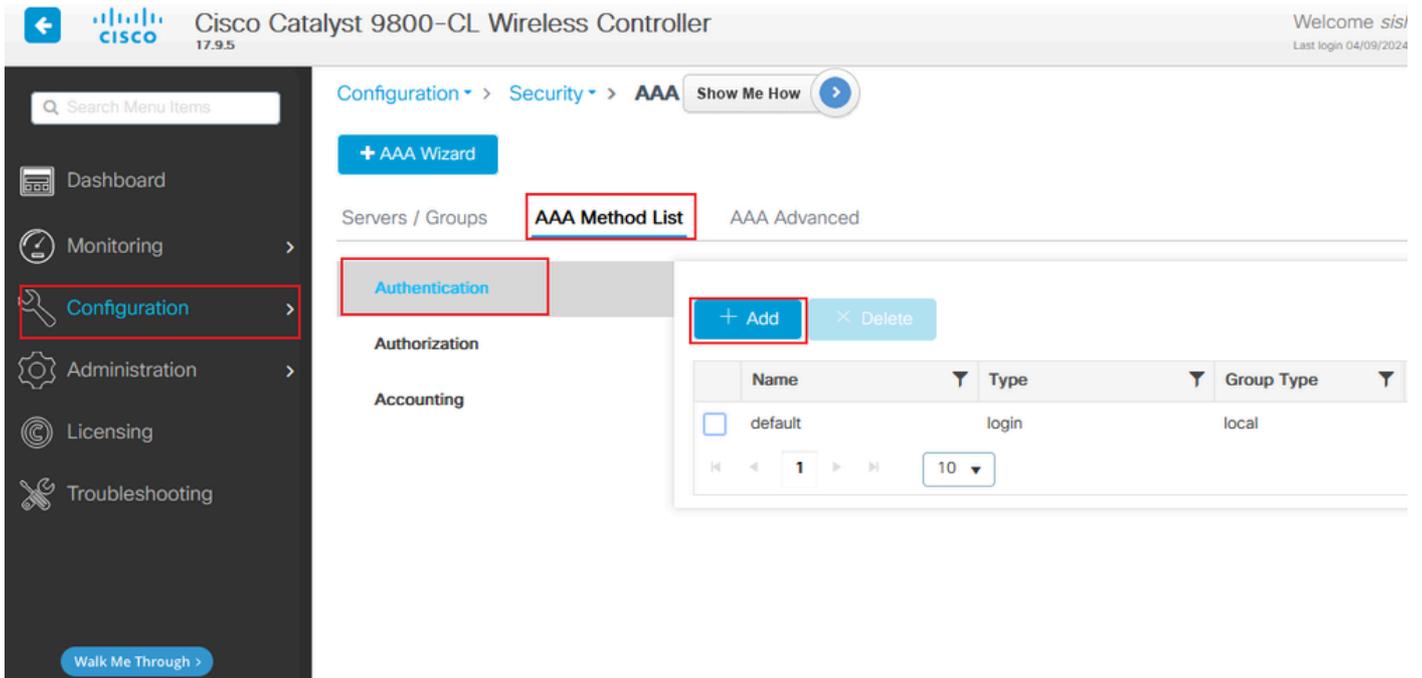


9800 crear servidor RADIUS

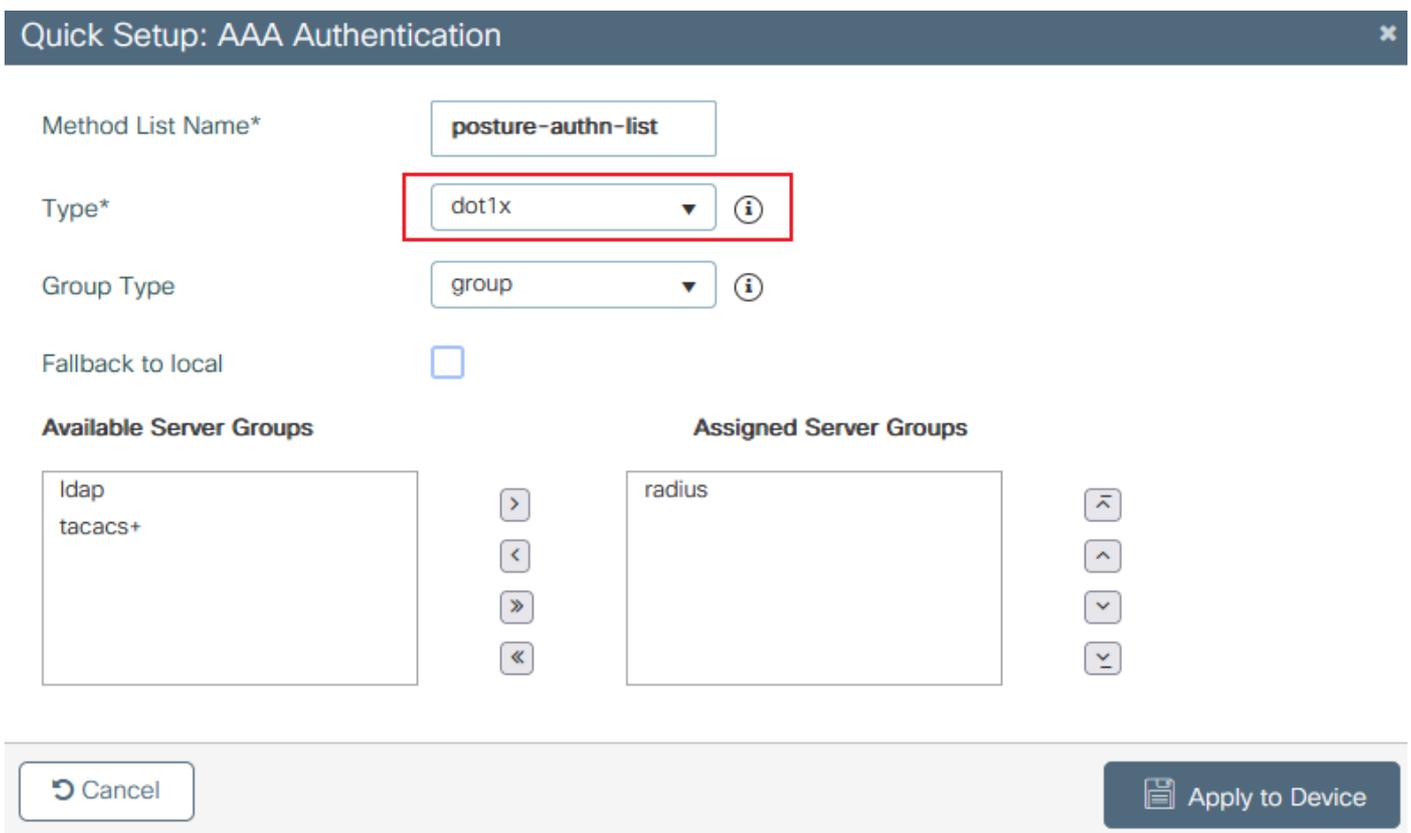


9800 crear detalles de RADIUS

Paso 2. Cree una lista de métodos de autenticación. Vaya a Configuration > Security > AAA > AAA Method List > Authentication > + Add como se muestra en la imagen:

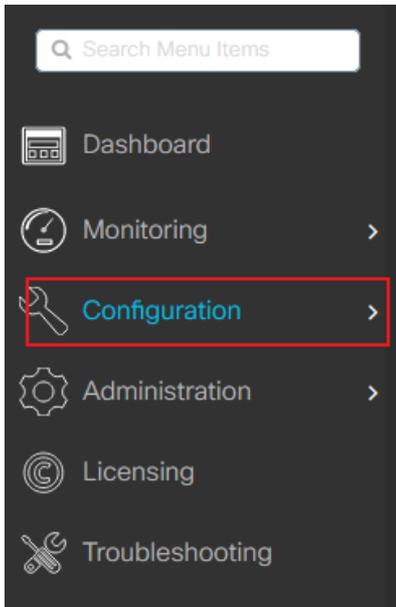


9800 agregar lista de autenticación



9800 crear detalles de lista de autenticación

Paso 3. (Opcional) Cree una lista de métodos de contabilidad como se muestra en la imagen:



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 agregar lista de cuentas

Quick Setup: AAA Accounting

Method List Name*

Type*

Available Server Groups: ldap, tacacs+

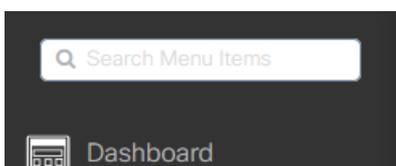
Assigned Server Groups: radius

Buttons: Cancel, Apply to Device

9800 crear detalles de la lista de cuentas

Configuración de WLAN

Paso 1. Cree la WLAN. Vaya a Configuration > Tags & Profiles > WLANs > + Add y configure la red según sea necesario:



Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN

9800 WLAN add

Paso 2. Introduzca la información general de 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 crear WLAN general

Paso 3. Navegue hasta la pestaña Seguridad y elija el método de seguridad necesario. En este caso, elija '802.1x' y la lista de autenticación AAA (que creó en el Paso 2. en la sección Configuración AAA) son necesarias:

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 crear seguridad 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

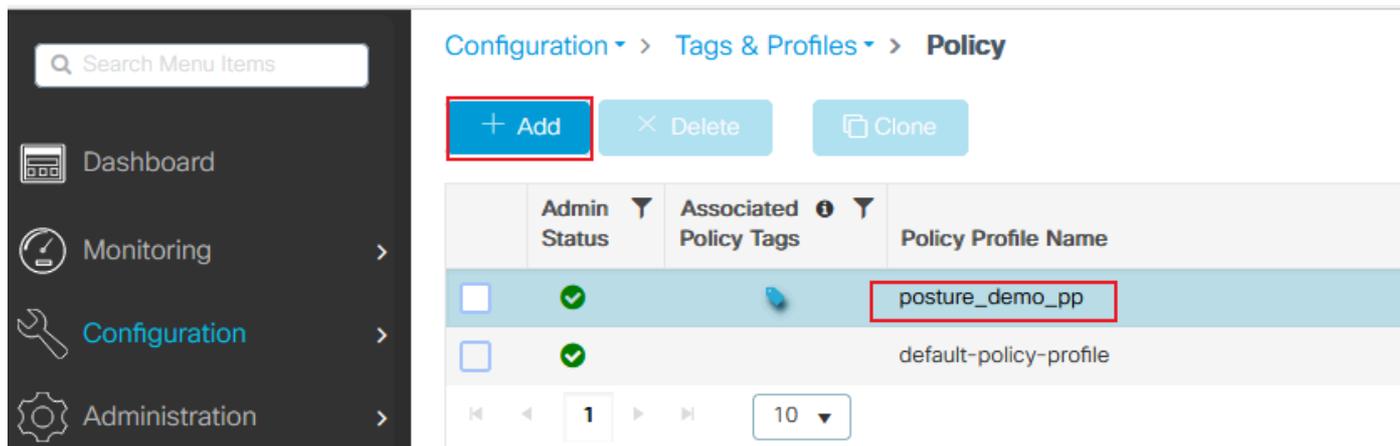
Local EAP Authentication

9800 crear seguridad WLAN AAA

Configuración del perfil de la política

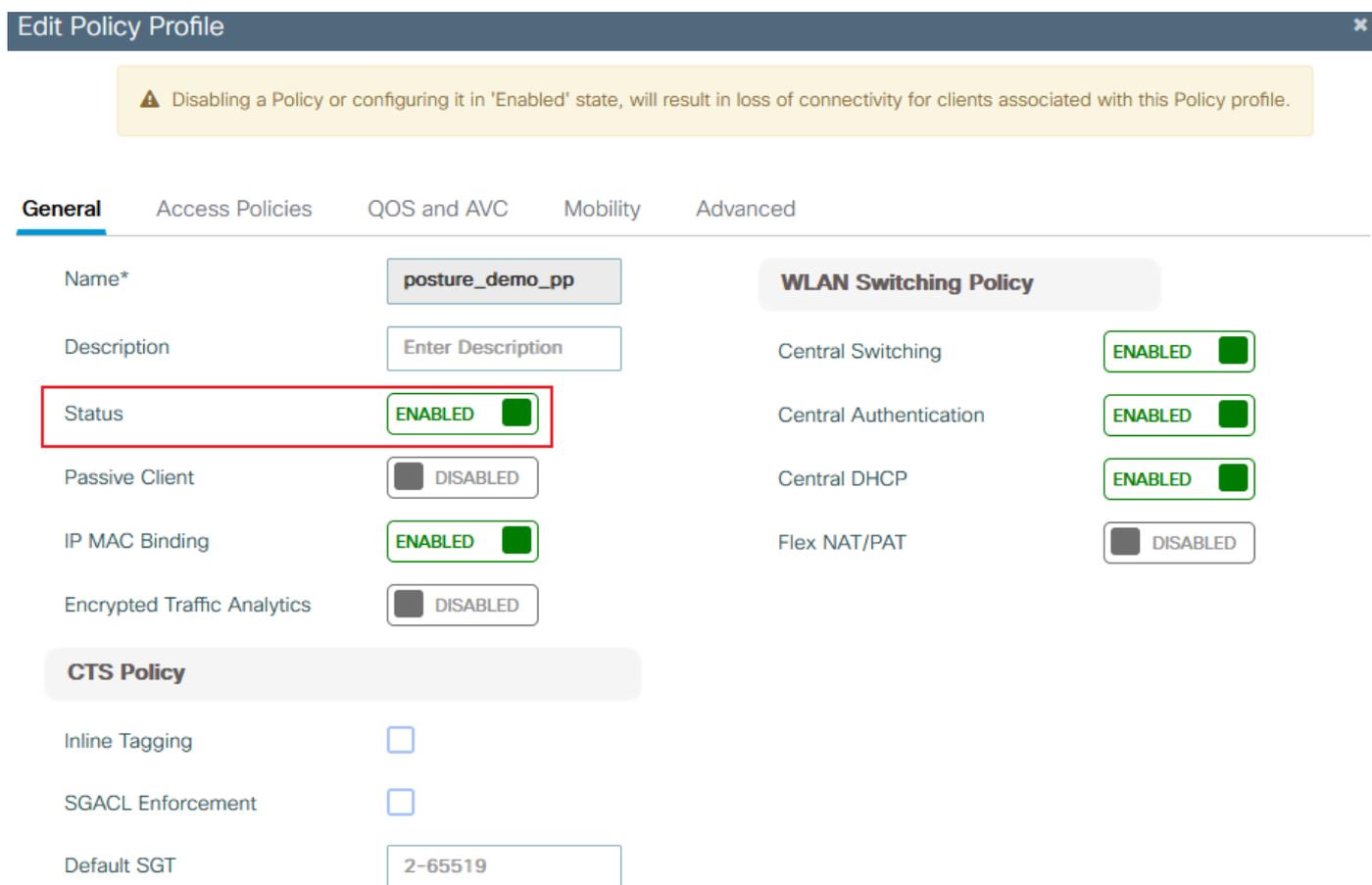
Dentro de un perfil de política, puede decidir asignar los clientes a los que se aplicará la VLAN, entre otras configuraciones (como la lista de controles de acceso (ACL), la calidad de servicio (QoS), el ancla de movilidad, los temporizadores, etc.). Puede utilizar su perfil de política predeterminado o puede crear uno nuevo.

Paso 1. Crear un nuevo perfil de política. Navegue hasta Configuration > Tags & Profiles > Policy y cree uno nuevo:



9800 agregar perfil de directiva

Asegúrese de que el perfil esté habilitado.



9800 crear perfil de políticas general

Paso 2. Elija la VLAN. Navegue hasta la pestaña Access Policies y elija el nombre de la VLAN en la lista desplegable o escriba manualmente el VLAN-ID. No configure una ACL en el perfil de política:

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 crear perfil de política VLAN

Paso 3. Configure el perfil de políticas para aceptar anulaciones de ISE (permitir la sustitución de AAA) y el cambio de autorización (CoA) (estado de NAC). Opcionalmente, también puede especificar un método de contabilidad:

⚠ 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

Cancel

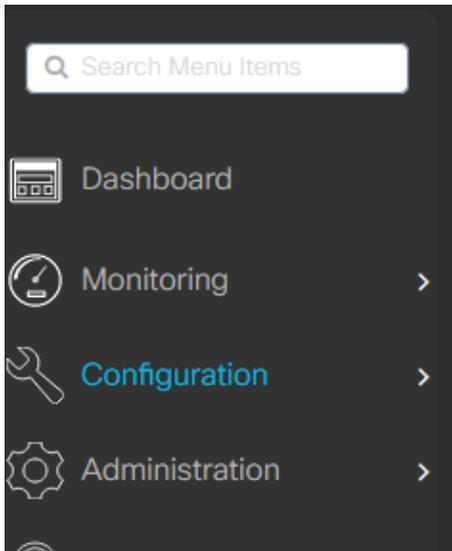
Update & Apply to Device

9800 crear perfil de políticas Avance

Configuración de etiquetas de políticas

Dentro de la etiqueta de política se encuentra el enlace del SSID con el perfil de política. Puede crear una nueva etiqueta de política o utilizar la etiqueta de política predeterminada.

Navegue hasta Configuration > Tags & Profiles > Tags > Policy y agregue uno nuevo si es necesario, como se muestra en la imagen:



Policy Site RF AP

+ Add Delete Clone

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

1 10

9800 etiqueta de política add

Vincule su perfil de WLAN con el perfil de política deseado:

Edit Policy Tag

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

Name*

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

Detalles de la etiqueta de política 9800

Asignación de etiquetas de políticas

Asigne la etiqueta de política a los AP necesarios. Navegue hasta Configuration > Wireless > Access Points > AP Name > General Tags , realice la asignación necesaria y luego haga clic en 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 ⌵

Asignación de etiqueta de directiva 9800

Configuración de ACL de redireccionamiento

Vaya a Configuración > Seguridad > ACL > + Agregar para crear una nueva ACL.

La ACL utilizada para la redirección del portal de postura tiene los mismos requisitos que la CWA (autenticación web central).

Debe denegar el tráfico a los nodos de PSN de ISE, así como también debe denegar el DNS y permitir el resto. Esta ACL de redirección no es una ACL de seguridad, sino una ACL de punt que define qué tráfico va a la CPU (en permisos) para un tratamiento adicional (como la redirección) y qué tráfico permanece en el plano de datos (en negación) y evita la redirección. La ACL debe verse de la siguiente manera (reemplace 10.124.57.141 con su dirección IP de ISE en este ejemplo):

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

Detalles de ACL de redirección 9800

Configuración de ACL de políticas

En este caso, debe definir ACL separadas en el WLC 9800 para ISE para autorizar los escenarios de cumplimiento y no cumplimiento según el resultado de la verificación de estado.

[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 general

Para el escenario de conformidad, simplemente utilice permit all en este caso. Como otra configuración común, también puede hacer que ISE no autorice ninguna ACL en el resultado conforme, lo que equivale a permitir todo en el lado 9800:

Edit ACL ✕

ACL Name* ACL Type

Rules

Sequence*

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

Compatible con 9800 ACL

En el caso de no conformidad, el cliente solo permite el acceso a determinadas redes, normalmente el servidor de corrección (ISE en este caso):

Edit ACL ✕

ACL Name* ACL Type

Rules

Sequence*

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

9800 ACL: no conforme

Configuración AAA y parámetro de estado en ISE

Requisito de condición: En este ejemplo, el requisito para determinar la conformidad es detectar si existe un archivo de prueba específico en el escritorio utilizado para probar Windows PC.

Paso 1. Agregue el WLC 9800 como NAD en el ISE. Vaya a Administración > Recursos de red > Dispositivos de red > Agregar:

The screenshot shows the Cisco ISE Administration interface for adding a Network Device. The page title is "Administration - Network Resources" and the breadcrumb is "Network Devices List > WLC9800". The "Network Devices" section is active, showing the configuration for a device named "WLC9800". The "IP Address" is set to "10.124.60.41 / 32". The "Device Profile" is set to "Cisco". The "Model Name", "Software Version", "Location", "IPSEC", and "Device Type" are all set to their default values: "All Locations", "No", "All Device Types", and "All Locations".

Agregar dispositivo de red 01

The screenshot shows the "RADIUS Authentication Settings" configuration page in Cisco ISE. The "RADIUS Authentication Settings" section is highlighted with a red box. The "RADIUS UDP Settings" section is also visible, with the "Shared Secret" field highlighted in red. The "CoA Port" is set to "1700". The "RADIUS DTLS Settings" section is also visible, with the "Shared Secret" field set to "radius/dtls" and the "CoA Port" set to "2083".

Agregar dispositivo de red 02

Paso 2. Descargue el paquete de implementación de cabecera y el módulo de cumplimiento de Cisco Secure Client en el sitio web de Cisco Software CCO.

Acceda y busque en Cisco Secure Client:

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

Secure Client 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	30-Jan-2023	19.59 MB
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------	----------

Módulo de cumplimiento de ISE 4.3

Paso 3. Cargue el paquete de implementación de cabecera de Cisco Secure Client y el paquete del módulo de cumplimiento en ISE Client Provisioning. Navegue hasta Centros de trabajo> Postura> Aprovisionamiento del cliente> Recursos . Haga clic en Agregar, Elija Recursos de agente del disco local en el cuadro desplegable:

Overview Network Devices **Client Provisioning** Policy Elements

Client Provisioning Policy

Resources

Client Provisioning Portal

Edit + Add ^ Duplicate Delete

- Agent resources from Cisco site
- Agent resources from local disk**
- Native Supplicant Profile
- Agent Configuration
- Agent Posture Profile
- AMP Enabler Profile

Cargar cliente seguro

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 ...

Carga de Secure Client y Compliance Module correctamente

Paso 4. Crear perfil de postura del agente Navegue hasta Centros de trabajo> Postura> Aprovisionamiento del cliente> Recursos> Agregar> Perfil de postura del agente:

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.

Perfil de postura del agente

Paso 5. Crear configuración de agente Navegue hasta Centros de trabajo> Estado> Aprovisionamiento de cliente> Recursos> Agregar> Configuración de agente:

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	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostics and Reporting Tool	<input checked="" type="checkbox"/>

Profile Selection

* ISE Posture bloomtest-Posture for Windows

Agregar configuración de agente

Paso 6. Confirme el portal de aprovisionamiento de clientes; utilice el portal predeterminado para probar que es correcto. (Genere CSR y solicite un certificado SSL del servidor de la CA y sustituya la etiqueta Grupo de certificados en esta configuración del portal. De lo contrario, se producirá una advertencia de certificado no fiable durante el proceso de prueba.)

Vaya a Centros de trabajo> Estado> Aprovisionamiento de clientes> Portales de aprovisionamiento de clientes:

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

Selecione 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](#)

Seleccione Client Provisioning Portal 02

Paso 7. Crear política de aprovisionamiento de clientes. Vaya a Centros de trabajo > Estado > Aprovisionamiento de cliente > Directiva de aprovisionamiento de cliente > Editar > insertar nueva directiva arriba.

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
WLC9800-Windows	If Any	and Windows All	and Condition(s)	then WLC9800-windows Edit
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP Edit
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit
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
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
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP Edit

Crear directiva de aprovisionamiento de clientes

Paso 8. Crear condiciones de archivo. Vaya a Centros de trabajo > Condición > Elementos de

directiva> Condiciones> Archivo> Condiciones de archivo> Agregar:

The screenshot shows the Cisco ISE Policy Elements configuration page for a File Condition. The breadcrumb trail is "File Conditions List > WLC9800-Posture-demo". The configuration fields are as follows:

- 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

Crear condición de archivo

Paso 9. Crear Remediaciones Vaya a Centros de Trabajo> Postura> Elementos de Política> Remediaciones > Archivo> Agregar:

The screenshot shows the Cisco ISE Policy Elements configuration page for a File Remediation. The breadcrumb trail is "File Remediations List > WLC9800-Posture-Demo". The configuration fields are as follows:

- * 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

Crear remediación de archivo

Paso 10. Crear Requisito. Vaya a Centros de trabajo> Condición> Elementos de directiva>

Requisitos> Insertar nuevo requisito:

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.

Crear requisito de estado

Paso 11. Crear política de estado. Vaya a Centros de trabajo> Estado> Insertar nueva directiva:

Cisco ISE Work Centers - Posture

Overview Network Devices Client Provisioning Policy Elements **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

Crear política de estado

Paso 12. Crear tres perfiles de autorización: El estado es Desconocido; El estado es No conforme; El estado de condición es compatible. Vaya a Directiva> Elementos de directiva> Resultados> Autorización> Perfiles de autorización> Agregar:

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](#)

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

Crear perfiles de autorización 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/Port name/FQDN

Suppress Profiler CoA for endpoints in Logical Profile

Crear perfiles de autorización 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

Crear perfiles de autorización 03

Dictionaries Conditions **Results**

Authorization Profile

* Name: WLC9800-Posture-NonComp

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: POSTURE_NON-COMPLIANT_

Airespace IPv6 ACL Name

Advanced Attributes Settings

Paso 13. Creación de Juegos de Políticas. Vaya a Directiva > Directiva

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	WLC9800-Posture-Demo		AND <ul style="list-style-type: none"> 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

Crear conjuntos de políticas

Conjuntos > Agregar icono:

Paso 14. Crear política de autenticación Navegue hasta Política > Conjuntos de políticas > Expanda "WLC9800-Posture-Demo" > Política de autenticación > Agregar:

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

Crear política de autenticación

Paso 15. Crear política de autorización Vaya a Política> Conjuntos de políticas> Expandir "WLC9800-Posture-Demo"> Política de autorización> Agregar:

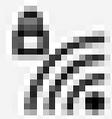
Authorization Policy (4)

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

Crear directiva de autorización

Examples

1. Demostración de estado de SSID de prueba conectada con credenciales 802.1X correctas.



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 el navegador se ha redirigido a la URL del portal de ISE pero no se puede cargar la página, compruebe si el nombre de dominio de ISE no se agrega al servidor DNS, por lo que el cliente no puede resolver la URL del portal. Para resolver rápidamente este problema, verifique Static IP/Host name/FQDN bajo el Perfil de autorización para proporcionar la dirección IP en la URL de redirección. Sin embargo, esto puede suponer un problema de seguridad, ya que expone la dirección IP de 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

Recopilar depuraciones

[Habilitar depuraciones en C9800](#)

[Habilitar depuraciones en ISE](#)

Referencias

- [Configuración de CWA en Catalyst 9800 WLC e ISE - Cisco](#)
- [BYOD inalámbrico con Identity Services Engine](#)
- [Implementar el estado de ISE](#)
- [Solución de problemas de administración y estado de sesiones de ISE](#)
- [Comparación del flujo de redirección de postura de ISE con el flujo sin redirección de postura de ISE](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).