

# Ejemplo fuera de banda de la configuración de red inalámbrica NAC (OOB)

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Descripción de Cisco NAC](#)

[Modo virtual del gateway \(modo del puente\)](#)

[Modo fuera de banda](#)

[Inicio de Sesión Único](#)

[Configure la solución de red inalámbrica NAC OOB](#)

[Configuración del switch del catalizador](#)

[Pasos para configurar NAC OOB en el encargado WLC y NAC](#)

[El configurar solo Muestra-en \(SSO\) con la solución de red inalámbrica OOB](#)

[Pasos para configurar SSO en el encargado NAC](#)

[Pasos para configurar SSO en el regulador LAN de la Tecnología inalámbrica](#)

[Verificación](#)

[Comandos CLI de CISCO WLC para la verificación](#)

[Verificación del estado del cliente del GUI WLC](#)

[Verificación de solo Muestra-en el servidor NAC con WLC](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona una guía para el diseño para el despliegue de seguridad de punto final para dispositivos Cisco Network Admission Control (NAC) Out of Band (OOB) en una implementación de Cisco Unified Wireless Network. Estas recomendaciones de la mejor práctica asumen que una red inalámbrica unificada Cisco se ha desplegado de acuerdo con las guías de consulta proporcionadas en el [3.0 de la guía de diseño de la movilidad de la empresa](#).

El diseño recomendado es el gateway virtual (modo del puente) y solución central del despliegue OOB con el RADIUS solo Muestra-en. El regulador Lan de la Tecnología inalámbrica (WLC) debe ser L2 colocado adyacente al servidor NAC. El cliente se asocia al WLC, y WLC autentica al usuario. Una vez que se completa la autenticación, el tráfico de usuarios pasa con el VLA N de la cuarentena del WLC al servidor NAC. El proceso de la evaluación y de la corrección de la postura

ocurre. Una vez que certifican al usuario, el VLAN de usuario cambia de la cuarentena para tener acceso al VLAN en el WLC. El tráfico desvía el servidor NAC cuando está movido para tener acceso al VLAN.

## prerrequisitos

### Requisitos

Esta configuración del documento es específica a la versión NAC 4.5 y WLC 5.1

### Componentes Utilizados

Este documento es restringido a las versiones de software y hardware específicas.

- Servidor 3350 4.5 NAC
- Encargado 3350 NAC 4.5
- WLC 2106 5.1

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Antecedentes

### Descripción de Cisco NAC

Cisco NAC utiliza la infraestructura de red para aplicar la conformidad de la política de seguridad en todos los dispositivos que busquen a los recursos de computación de la red de acceso. Con el dispositivo NAC de Cisco, los administradores de la red pueden autenticar, autorizar, evaluar, y remediar atado con alambre, Tecnología inalámbrica, y los usuarios remotos y sus máquinas antes del acceso a la red. El dispositivo NAC de Cisco identifica si los dispositivos conectados a la red tales como computadoras portátiles, Teléfonos IP, o videoconsolas son obedientes con las políticas de seguridad de la red, y repara cualquier vulnerabilidad antes de que permita el acceso a la red.

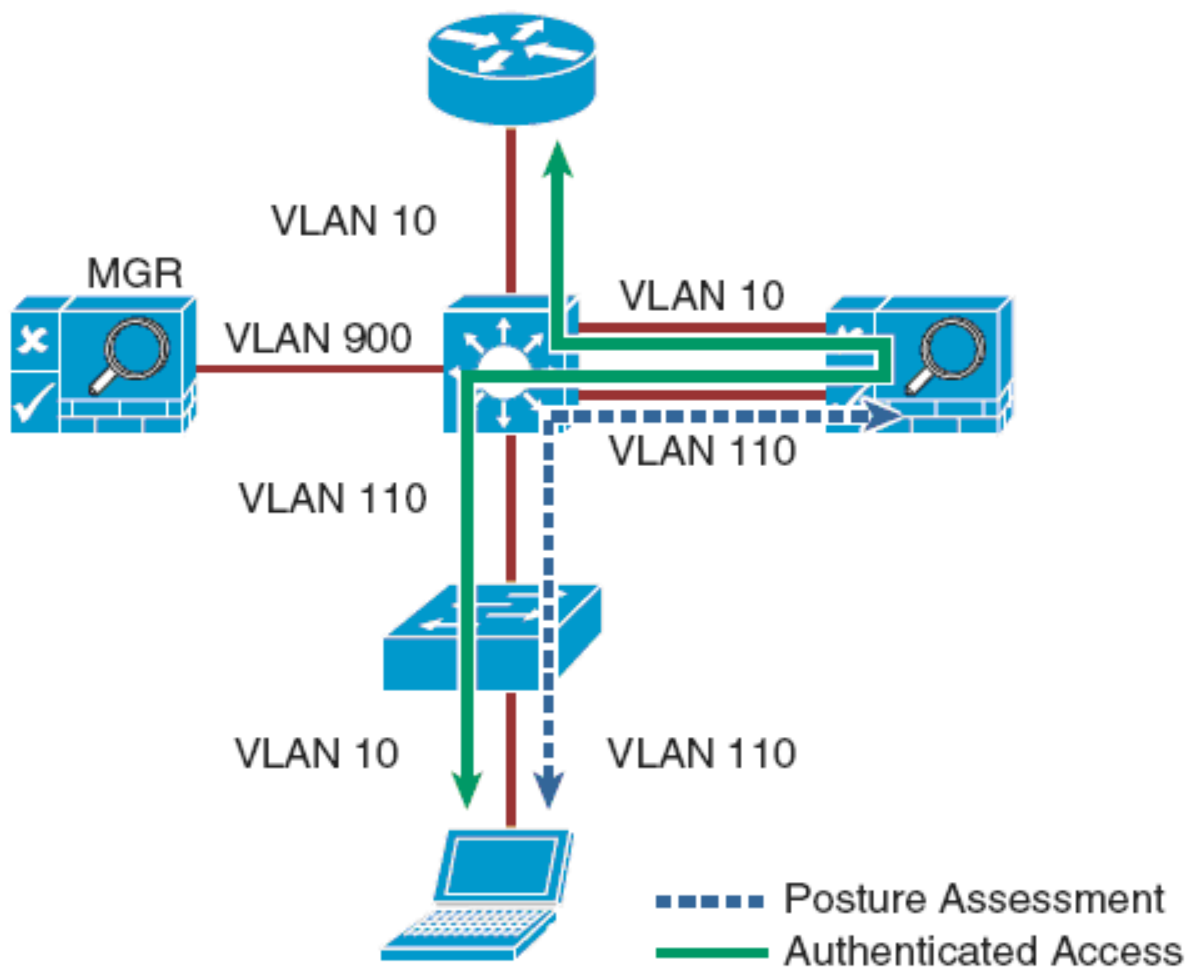
La terminología del diseño recomendado se discute:

### Modo virtual del gateway (modo del puente)

Cuando el dispositivo NAC se configura como gateway virtual, actúa como puente entre los usuarios finales y el gateway de valor por defecto (router) para la subred cliente se maneja que. Para un VLAN dado del cliente, el dispositivo NAC puentea el tráfico de su interfaz no confiable a su interfaz de confianza. Cuando actúa como puente del lado untrusted al lado de confianza del

dispositivo, se utilizan dos VLAN. Por ejemplo, el VLAN 110 del cliente se define entre el regulador LAN de la Tecnología inalámbrica (WLC) y la interfaz no confiable del dispositivo NAC. No hay interfaz encaminado ni cambió la interfaz virtual (SVI) asociada al VLAN 110 en el switch de distribución. El VLAN10 se configura entre el interfaz de confianza del dispositivo NAC y el router interface/SVI del siguiente-salto para la subred cliente. Una regla de la asignación se hace en el dispositivo NAC ese los paquetes de los forwards que llegan en el VLAN 110 hacia fuera VLAN10 cuando intercambia la información de la etiqueta del VLAN tal y como se muestra en del higo 1-1. El proceso se invierte para los paquetes que vuelven al cliente. Observe que, en este modo, BPDUs no está pasado de los VLAN del untrusted-lado a sus contrapartes de confianza-lado. La opción de la asignación del VLAN se elige generalmente cuando el dispositivo NAC se coloca lógicamente en línea entre los clientes y las redes se protegen que. Esta opción que puentea debe ser utilizada si se va el dispositivo NAC a ser desplegado en el modo virtual del gateway con un despliegue inalámbrico unificado. Porque el servidor NAC es consciente de los *protocolos de la capa superiores*, por abandono permite explícitamente los protocolos que lo requieren conectar con la red en el papel autenticado, por ejemplo, el DNS y el DHCP.

Cuadro gateway virtual de 1-1 con la asignación del VLAN



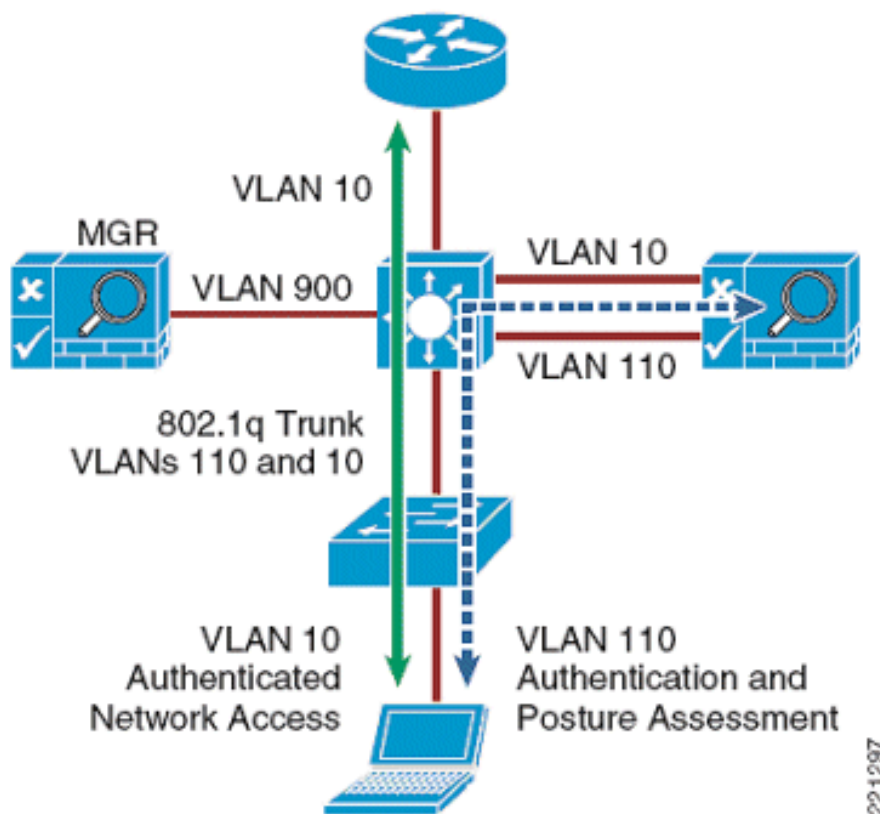
### Modo fuera de banda

Las implementaciones fuera de banda requieren el tráfico de usuarios atravesar a través del dispositivo NAC solamente dentro de la autenticación, de la evaluación de la postura, y de la corrección. Cuando autentican y pasa a un usuario todos los controles de la directiva, el tráfico se cambia normalmente a través de la red y desvía el servidor NAC. Para más información, refiera al

capítulo 4 de la [instalación de administrador y de la guía de administración Dispositivo-limpias del acceso de Cisco NAC](#).

Cuando el dispositivo NAC se configura de este modo, el WLC es un dispositivo administrado en el encargado NAC de la misma forma que eso un conmutador de Cisco es manejada por el encargado NAC. Después de que autentiquen y pase al usuario la evaluación de la postura, el encargado NAC da instrucciones el WLC para marcar el tráfico de usuarios con etiqueta del VLA N NAC para tener acceso al VLA N que ofrece los privilegios de acceso.

Cuadro dispositivo NAC de 1-2 en el modo fuera de banda con el modo virtual del gateway



## Inicio de Sesión Único

Escoja muestra-en (SSO) es una opción que no requiere la intervención del usuario y es relativamente directo ejecutar. Hace uso de la capacidad VPN SSO de la solución NAC, juntada con el software limpio del agente del acceso que se ejecuta en PC del cliente. El VPN SSO utiliza los registros de estadísticas RADIUS para notificar el dispositivo NAC sobre los usuarios de acceso remoto autenticados que conectan con la red. De la misma manera, esta característica se puede utilizar conjuntamente con el regulador de la red inalámbrica (WLAN) para informar automáticamente al servidor NAC sobre los clientes de red inalámbrica autenticados que conectan con la red.

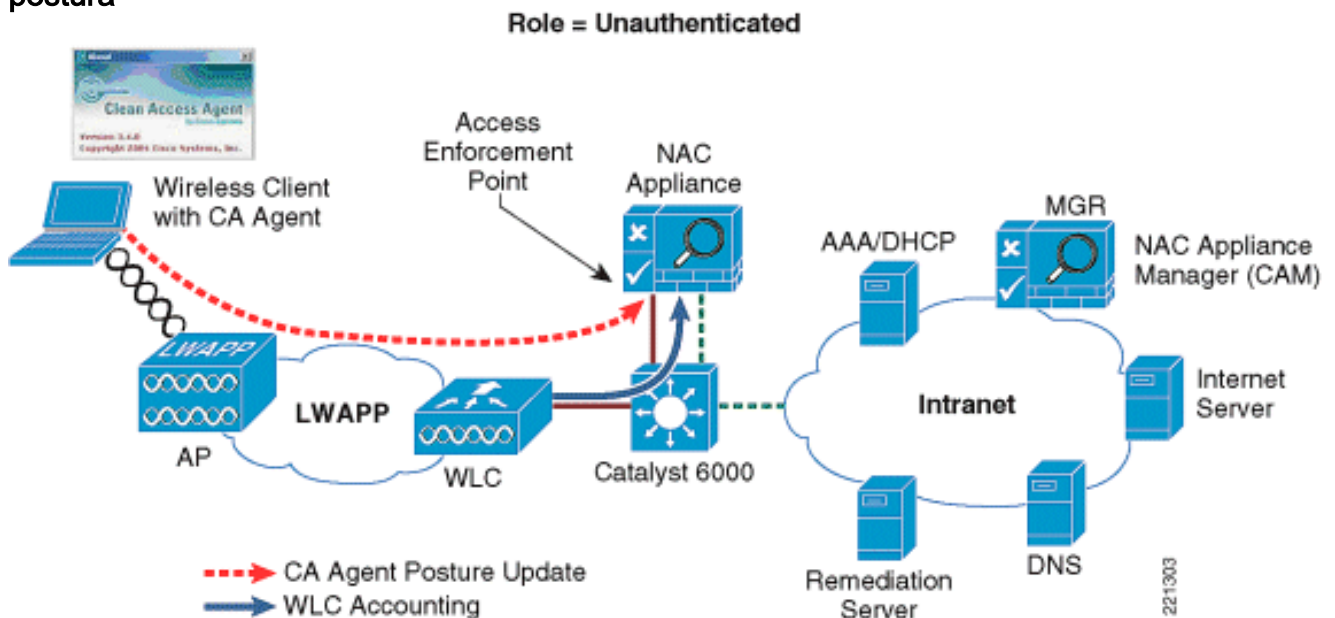
Véase los cuadros 1-3 a 1-6 por ejemplos de un cliente de red inalámbrica que realice la autenticación SSO, la evaluación de la postura, la corrección, y el acceso a la red a través del dispositivo NAC.

Esta secuencia se muestra en el cuadro 1-3:

1. El usuario de red inalámbrica realiza la autenticación 802.1x/EAP a través del regulador de

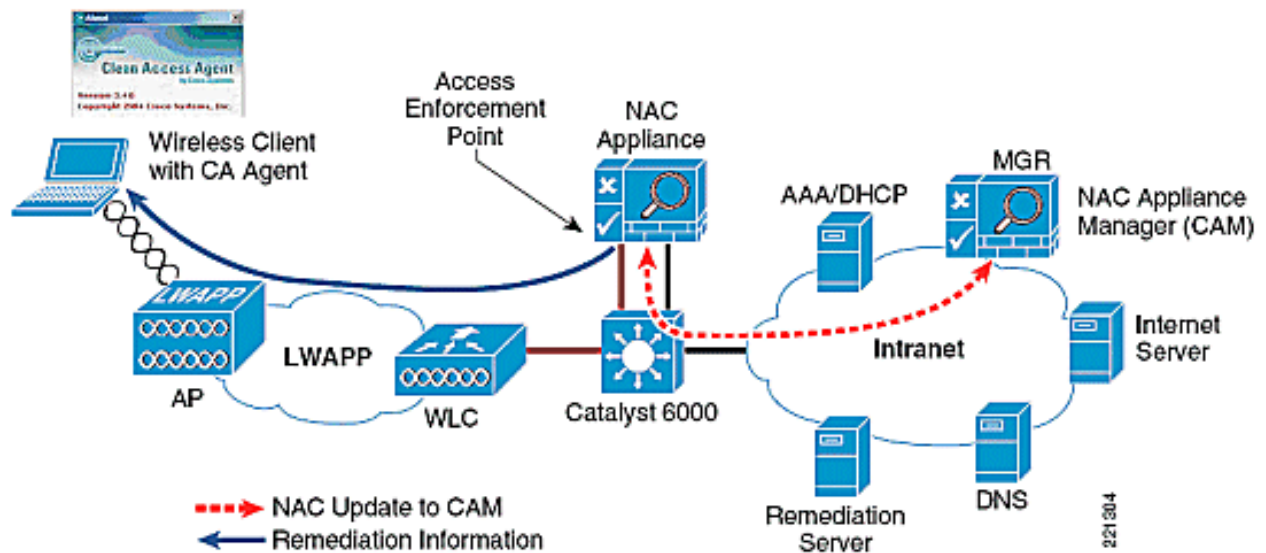
la red inalámbrica (WLAN) a un servidor por aguas arriba AAA.

2. El cliente obtiene una dirección IP del AAA o de un servidor del DHCP.
3. Después de que el cliente reciba una dirección IP, el WLC adelanta un expediente de las estadísticas RADIUS (comienzo) al dispositivo NAC, que incluye la dirección IP del cliente de red inalámbrica. **Nota:** El regulador WLC utiliza un solo registro de estadísticas RADIUS (comienzo) para la autenticación de cliente del 802.1x y la asignación de la dirección IP, mientras que el Switches del Cisco Catalyst envía dos registros de estadísticas: un comienzo de las estadísticas se envía después de la autenticación de cliente del 802.1x, y se envía una actualización interina después de que asignen el cliente una dirección IP.
4. Después de que detecte la conectividad de red, el agente NAC intenta conectar con la leva (con el protocolo SWISS). El tráfico es interceptado por el servidor NAC, que, a su vez, pregunta al encargado NAC para determinar si el usuario está en la lista de usuario en línea. Solamente los clientes se autentican que están en la lista de usuario en línea, que es el caso en el ejemplo anterior como resultado de la actualización RADIUS en el paso 3.
5. El agente NAC realiza una evaluación local de la postura de la Seguridad/del riesgo de la máquina del cliente y adelante la evaluación al servidor NAC para la determinación de la admisión de la red. **Cuadro proceso de autenticación de cliente de 1-3 y evaluación de la postura**



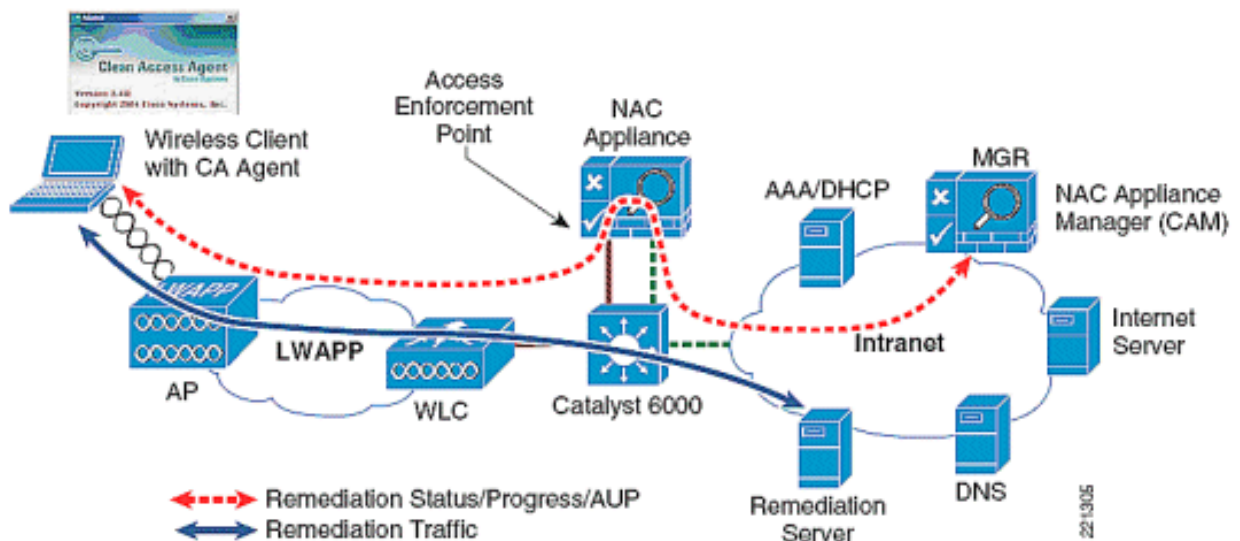
Esta secuencia ocurre en el cuadro 1-4:

1. El dispositivo NAC adelanta la evaluación del agente al encargado del dispositivo NAC (leva).
2. En este ejemplo, la leva determina que el cliente no está en la conformidad y da instrucciones el dispositivo NAC para poner al usuario en un papel de la cuarentena.
3. El dispositivo NAC entonces envía la información de la corrección al agente del cliente. **Cuadro información de la evaluación de la postura de 1-4 de CAS a la leva**



Esta secuencia ocurre en el cuadro 1-5:

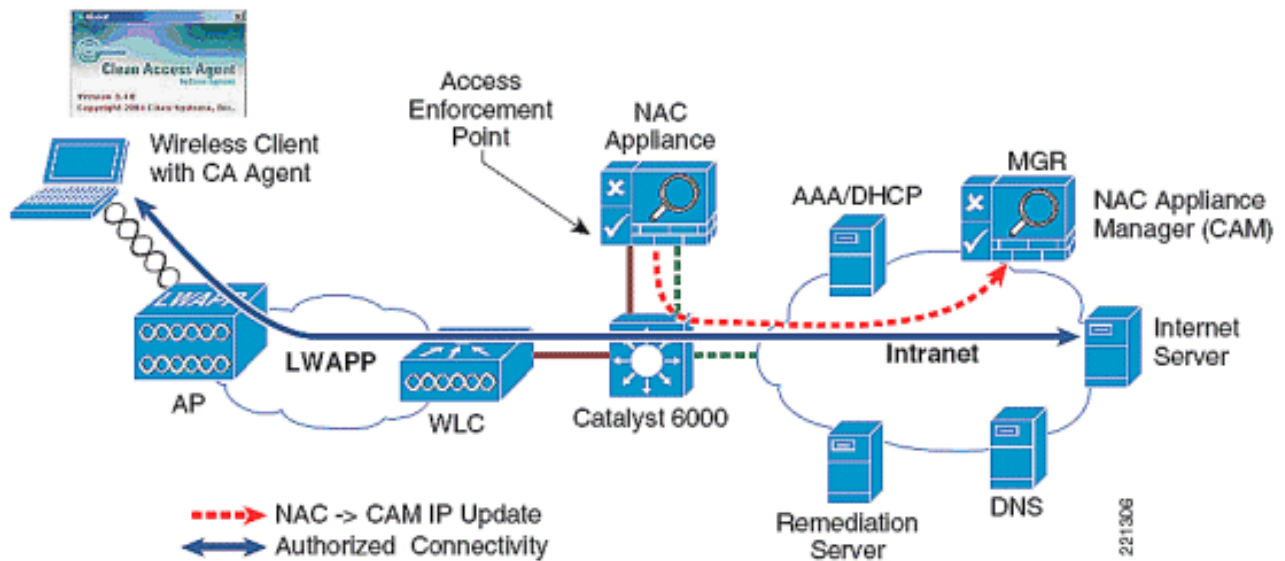
1. El agente del cliente visualiza el tiempo que sigue habiendo logrado la corrección.
  2. El agente dirige al usuario paso a paso con el proceso de la corrección; por ejemplo, en la actualización del archivo de definición del antivirus.
  3. Después de la realización de la corrección, el agente pone al día el servidor NAC.
  4. La leva visualiza una declaración del Acceptable Use Policy (AUP) al usuario.
- Cuadro proceso de la corrección del cliente de 1-5 con CAS como el dispositivo de la aplicación**



Esta secuencia ocurre en el cuadro 1-6:

1. Después de que valide el AUP, el dispositivo NAC cambia al usuario a un papel (autorizado) en línea.
2. Las funciones SSO pueblan la lista de usuario en línea con la dirección IP del cliente. Después de la corrección, una entrada para el host se agrega a la lista certificada. Ambas tablas (así como la tabla descubierta de los clientes) son mantenidas por la leva (encargado del dispositivo NAC).
3. El encargado NAC envía un SNMP escribe la notificación a WLC para cambiar el VLAN de usuario de la cuarentena para tener acceso al VLA N.
4. El tráfico de usuarios comienza a dejar el WLC con la etiqueta del VLA N del acceso. El servidor NAC está no más en la trayectoria para este tráfico del usuario determinado. El

## cuadro 1-6 certificó puente del cliente CAS cambiando para tener acceso al VLA N



El método más transparente para facilitar la autenticación de usuario de red inalámbrica es activar la autenticación VPN-SSO en el servidor NAC y configurar el WLCs para remitir el RADIUS que considera al servidor NAC. En caso que los registros de estadísticas necesiten ser remitidos a un servidor de RADIUS contra la corriente en la red, el servidor NAC se puede configurar para remitir el paquete de las estadísticas al servidor de RADIUS.

**Nota:** Si la autenticación VPN-SSO se activa sin el agente limpio del acceso instalado en PC del cliente, todavía autentican al usuario automáticamente. Sin embargo, no están conectados automáticamente a través del dispositivo NAC hasta que abran a su buscador Web y se hace un intento de conexión. En este caso, cuando el usuario abre a su buscador Web, se reorientan momentáneamente (sin un mensaje de conexión a la comunicación) dentro de la fase del “agente-menos”. Cuando el proceso SSO es completo, están conectados con su URL originalmente pedido.

## Configure la solución de red inalámbrica NAC OOB

En esta sección encontrará la información para configurar las funciones descritas en este documento.

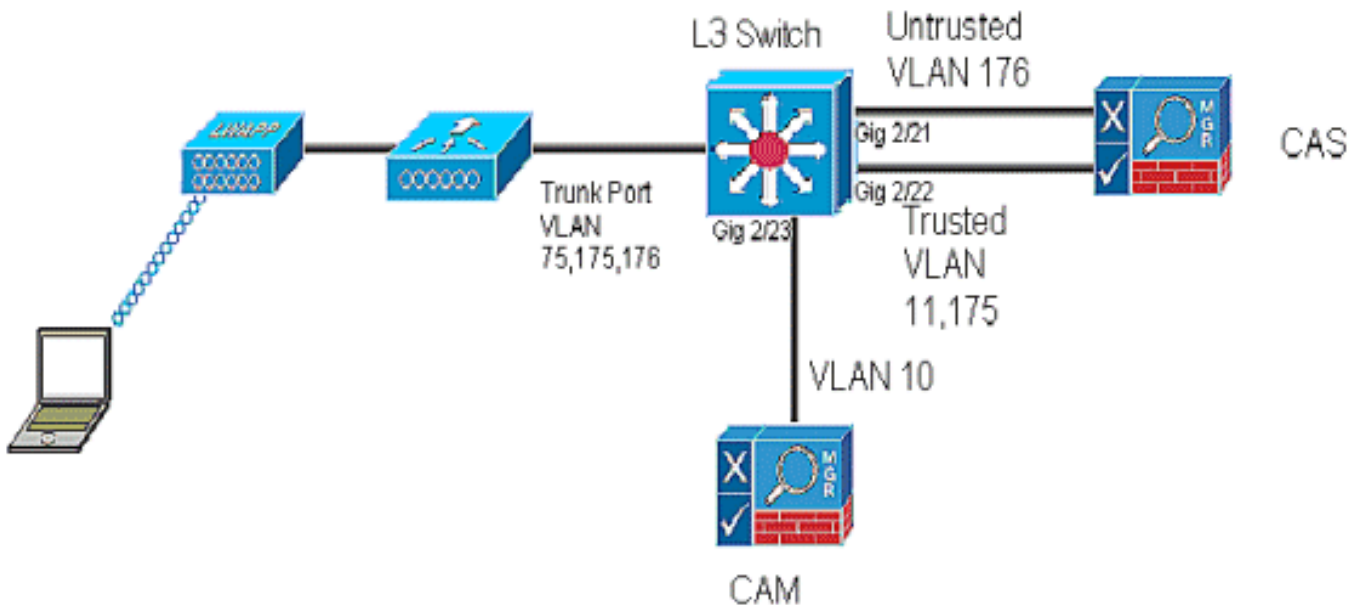
**Nota:** Utilice la [herramienta de búsqueda de comandos](#) ([clientes registrados](#) solamente) para obtener más información sobre los comandos usados en esta sección.

En la puesta en práctica actual NAC WLC integra con el dispositivo NAC de Cisco en el modo de la en-banda solamente, donde el dispositivo NAC tiene que permanecer en la trayectoria de datos incluso después certifican al usuario. Una vez que el dispositivo NAC completa su validación de la postura, el empleado/el invitado recibe el acceso de la red basada en su papel.

Con la versión NAC 4.5 y WLC 5.1, la integración de las ayudas OOB de la solución de la Tecnología inalámbrica NAC con el dispositivo NAC. Cuando el cliente asocia y completa L2Auth, se controla si el interfaz de la cuarentena está asociado al WLAN/SSID. Si sí, el tráfico inicial se envía en el interfaz de la cuarentena. Los flujos de tráfico del cliente en el VLA N de la cuarentena, que es trunked al dispositivo NAC. Una vez que se hace la validación de la postura, el encargado NAC envía un SNMP el mensaje determinado que pone al día la identificación del VLA N del acceso; el regulador se pone al día con la identificación del VLA N del acceso, y el

tráfico de datos comienza a cambiar del regulador directamente a la red sin el servidor NAC.

### Cuadro ejemplo de 2-1 de CAS independiente en el modo del puente conectado con WLC a través del conmutador



En el cuadro 2-1, el WLC está conectado con un puerto troncal que lleve el VLAN de la cuarentena y el VLAN del acceso (176 y 175). En el conmutador, el tráfico del VLAN de la cuarentena es trunked al dispositivo NAC, y el tráfico del VLAN del acceso es trunked directamente al conmutador Layer3. Tráfico que alcanza el VLAN de la cuarentena en el dispositivo NAC se asocia para tener acceso al VLAN basado en la configuración de la correlación estática. Cuando los socios del cliente completan el L2 auténtico, controla si el interfaz de la cuarentena es asociado; si sí, los datos se envían en el interfaz de la cuarentena. Los flujos de tráfico del cliente en el VLAN de la cuarentena, que es trunked al dispositivo NAC. Una vez que se hace la validación de la postura, el servidor NAC (CAS) envía un SNMP el mensaje determinado que pone al día la identificación del VLAN del acceso al regulador, y el comienzo del tráfico de datos para cambiar del WLC directamente a la red sin el servidor NAC.

### Restricciones

- Ningún perfil del puerto asociado
- Ninguna identificación del VLAN especificada en el encargo NAC: definido en WLC
- La ayuda del filtro MAC no puede utilizar la identificación del VLAN de las configuraciones del papel
- Ayuda virtual fuera de banda del modo de servidor del gateway NAC solamente
- Asociación de la capa 2 entre el servidor WLC y NAC
- El NAC ISR y WLC nanómetro no se pueden poner para hacer la Tecnología inalámbrica OOB NAC

**Nota:** Refiera a la [asignación del VLAN en la sección virtual de los modos del gateway del dispositivo NAC de Cisco - la guía de configuración del Access Server limpia, publica 4.8\(1\)](#) para más información sobre cómo configurar con seguridad los VLAN en los modos virtuales del gateway.



## Configuración del switch del catalizador

```
interface GigabitEthernet2/21
description NAC SERVER UNTRUSTED INTERFACE
switchport
switchport trunk native vlan 998
switchport trunk allowed vlan 176
switchport mode trunk
no ip address
!
interface GigabitEthernet2/22
description NAC SERVER TRUSTED INTERFACE
switchport
switchport trunk native vlan 999
switchport trunk allowed vlan 11,175
switchport mode trunk
no ip address
!
interface GigabitEthernet2/23
description NAC MANAGER INTERFACE
switchport
switchport access vlan 10
no ip address
spanning-tree portfast
!
interface GigabitEthernet2/1
description WLC
switchport
switchport trunk allowed vlan 75,175,176
switchport trunk native vlan 75
switchport mode trunk
no ip address
!
interface Vlan75
Description WLC Management VLAN
ip address 10.10.75.1 255.255.255.0
!
interface Vlan175
Description Client Subnet Access VLAN
ip address 10.10.175.1 255.255.255.0
end
```

## Pasos para configurar NAC OOB en el encargado WLC y NAC

Siga los siguientes pasos para configurar NAC OOB en el encargado WLC y NAC:

1. Active el modo SNMP v2 en el regulador.

The screenshot shows the Cisco Management interface with the 'SNMP System Summary' configuration page. The left sidebar contains a 'Management' menu with options like Summary, SNMP, HTTP, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, and Tech Support. The main content area displays the following configuration details:

Name	FRANCISCAN
Location	
Contact	
System Description	Cisco Controller
System Object ID	1.3.6.1.4.1.14179.1.1.4.3
SNMP Port Number	161
Trap Port Number	162
SNMP v1 Mode	Enable
SNMP v2c Mode	Enable
SNMP v3 Mode	Enable

An 'Apply' button is located in the top right corner of the configuration area.

2. Cree un perfil para WLC en el encargado leva. Haga clic el perfil > el dispositivo de la Administración OOB > nuevo.

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar contains a 'Cisco' logo and a menu with categories: Device Management, OOB Management, User Management, Monitoring, and Administration. The main content area is titled 'Cisco Clean Access Standard Manager' and 'OOB Management > Profiles'. It features a navigation bar with 'Group', 'Device', 'Port', 'VLAN', and 'SNMP Receiver' tabs, and a sub-menu with 'List', 'New', and 'Edit' options. The configuration form includes the following fields:

- Profile Name: wlc
- Device Model: Cisco Wireless LAN Controllers
- SNMP Port: 161
- Description: wlc profile
- SNMP Read Settings:
  - SNMP Version: SNMP V2C
  - Community String: public
- SNMP Write Settings:
  - SNMP Version: SNMP V2C
  - Community String: private

'Update' and 'Reset' buttons are located at the bottom of the form.

3. Una vez que el perfil se crea en la leva, agregue WLC en el perfil; vaya a la Administración > a los dispositivos OOB > nuevo y ingrese el IP address de la Administración de WLC.

Ahora el regulador se agrega en el encargado leva.

IP	MAC	Model	Description	Profile	Config	Ports	Delete
10.10.75.2	00:18:73:34:B2:63	WLC	wlc	wlc			

4. Agregue la leva como el receptor del SNMP trap del WLC. Utilice el nombre exacto del receptor de trampa en la leva como el receptor SNMP.

5. Configure el receptor del SNMP trap en la leva con el mismo nombre, que se especifica en el regulador; haga clic los perfiles bajo la Administración OOB > el receptor

## SNMP.

**Cisco Clean Access Standard Manager**

OOB Management > Profiles

Group Device Port VLAN **SNMP Receiver**

SNMP Trap - Advanced Settings

(Configure the SNMP daemon running on the Clean Access Manager. The device setup must match these settings to be able to send traps to the Clean Access Manager)

Trap Port on Clean Access Manager

**SNMP V1 Settings**

Community String

**SNMP V2c Settings**

Community String

**SNMP V3 Settings**

Security Method

User Name

User Auth

User Priv

En esta etapa, el WLC y la leva pueden hablar el uno al otro para las actualizaciones del estado de la validación y del acceso/de la cuarentena de la postura del cliente.

6. En el regulador, cree un interfaz dinámico con el VLA N del acceso y de la cuarentena.

**CISCO** Save Configuration Ping Logout Refresh

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Controller

General  
Inventory  
Interfaces  
Multicast  
Network Routes  
Internal DHCP Server  
▸ Mobility Management  
Ports  
NTP  
▸ CDP  
▸ Advanced

**General Information**

Interface Name nac-vlan  
MAC Address 00:18:73:34:b2:63

**Configuration**

Guest Lan   
Quarantine   
Quarantine Vlan Id

**Physical Information**

Port Number   
Backup Port   
Active Port 1  
Enable Dynamic AP Management

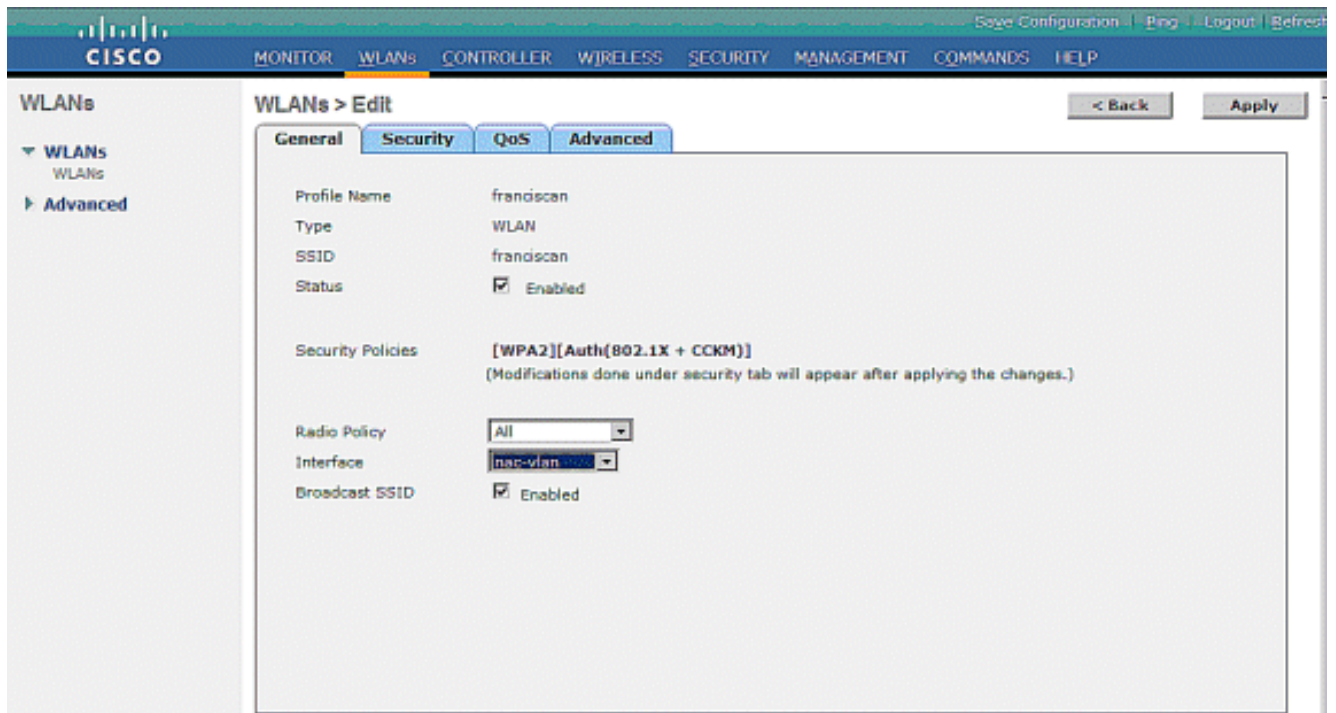
**Interface Address**

VLAN Identifier   
IP Address   
Netmask   
Gateway

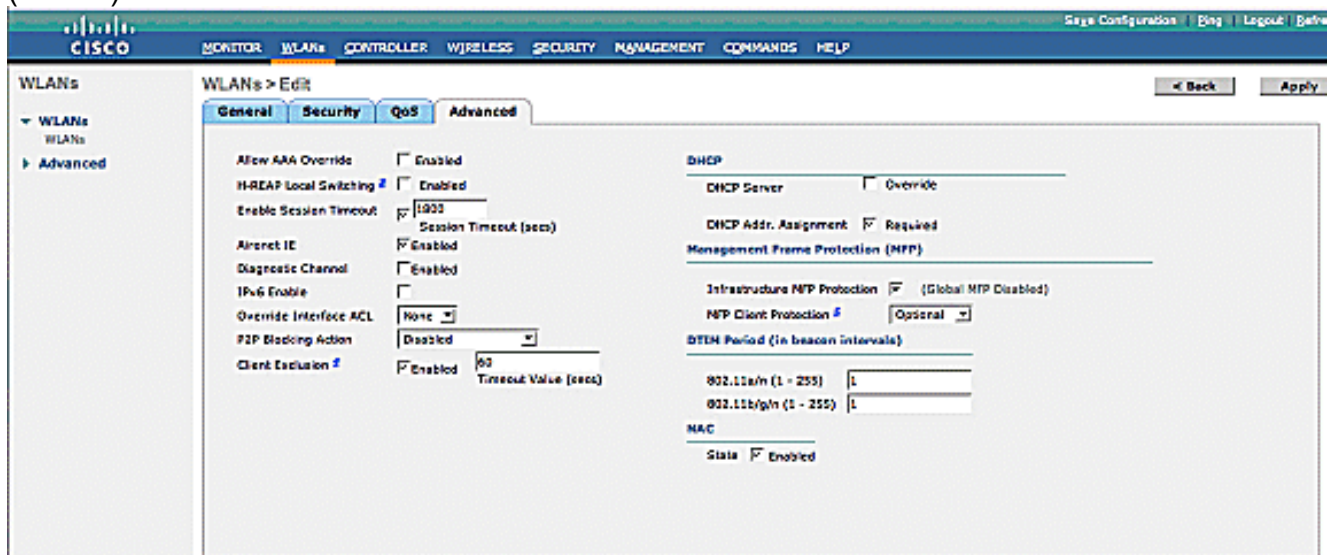
**DHCP Information**

Primary DHCP Server

7. Cree la red inalámbrica (WLAN), y asóciela al interfaz dinámico.



8. Finalmente, permiso NAC en la red inalámbrica (WLAN).



9. Agregue la subred cliente en el servidor de CAS como la subred manejada; haga clic el servidor de CAS > seleccionan su servidor de CAS > dirección IP inusitada >Advanced > manejada Manage de las subredes del >Add de la subred cliente y ponen el VLA N de la cuarentena (VLA N untrusted) para la subred manejada.

**Cisco Clean Access Standard Manager**

Device Management > Clean Access Servers > 10.10.11.19

Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy

Enable subnet-based VLAN retag

IP Address:

Subnet Mask:

VLAN ID:  (-1 for non-VLAN)

Description:

IP/Netmask	Description	VLAN	Delete
172.20.25.19 / 255.255.255.0	Main Subnet	-1	
10.10.175.10 / 255.255.255.0	Management Client Subnet IP	176	X

10. Cree las asignaciones del VLA N en CAS. Elija el **servidor de CAS > seleccionan su servidor de CAS > manejan > avanzó > asignación del VLA N**. Agregue el VLA N del acceso como VLA N confiado en y de la cuarentena como untrusted.

**Cisco Clean Access Standard Manager**

Device Management > Clean Access Servers > 10.10.11.19

Managed Subnet · **VLAN Mapping** · NAT · 1:1 NAT · Static Routes · ARP · Proxy

**VLAN Packet Handling**

Enable VLAN Pruning  
When enabled along with VLAN Mapping, disallows any VLAN Packet to pass through to other interface in either direction if VLAN mapping cannot be done for the packet. If enabled alone, discards all VLAN packets from passing through in either direction.

Enable VLAN Mapping

**VLAN Mapping Assignments**

Untrusted network VLAN ID:  (-1 for non-VLAN)

Trusted network VLAN ID:  (-1 for non-VLAN)

Description:

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
176	175	176 ---> 175	X

## [El configurar solo Muestra-en \(SSO\) con la solución de red inalámbrica OOB](#)


Éstos son los requisitos de activar la Tecnología inalámbrica SSO:

1. Autenticación del permiso VPN en el servidor NAC — WLC se define como “concentrador VPN” en el dispositivo NAC.
2. Active las estadísticas RADIUS en el WLC — el regulador que se define en el dispositivo NAC se debe configurar para enviar los registros de estadísticas RADIUS al dispositivo NAC para cada red inalámbrica (WLAN) 802.1x/EAP que sea una subred manejada en el NAC.

## [Pasos para configurar SSO en el encargado NAC](#)

Siga los siguientes pasos para configurar SSO en el encargado NAC:

1. Del menú izquierdo leva, bajo Administración de dispositivos, elija **CCA el servidor**, y después haga clic el link del **servidor NAC**.
2. De la página del estado del servidor, elija la tabulación de la **autenticación** y entonces el submenú **auténtico VPN**. Véase el cuadro 3-1. **Cuadro 3-1 activando el solo Muestra-en el servidor NAC**

Device Management > Clean Access Servers > 10.10.11.19 

---

Status	Network	Filter	Advanced	Authentication	Misc
Login Page	VPN Auth	Windows Auth	OS Detection		
General	VPN Concentrators	Accounting Servers	Accounting Mapping	Active Clients	

Single Sign-On:

Agent VPN Detection Delay:  seconds (0 means no delay)

Auto Logout:

RADIUS Accounting Port:

3. Elija los **concentradores VPN que fijan** (cuadro 3-2) para agregar una nueva entrada de WLC. Puele los campos de entrada para la dirección IP y el secreto compartido de la Administración WLC que usted quiere utilizar entre el servidor WLC y NAC. **El cuadro 3-2 agrega WLC como cliente RADIUS bajo sección del concentrador VPN**



Status	Network	Filter	Advanced	Authentication	Misc
Login Page	VPN Auth	Windows Auth	OS Detection		
General	VPN Concentrators	Accounting Servers	Accounting Mapping	Active Clients	

Name:  IP Address:

Shared Secret:  Confirm Shared Secret:

Description:

Add VPN Concentrator

VPN Concentrator	IP Address	Description	Del
WLC	10.10.75.2	WLC	X

4. Para la asignación del papel, agregue el nuevo servidor de la autenticación con el tipo sso del vpn bajo User Management (Administración de usuario) > los servidores de autenticación.

The screenshot shows the Cisco Clean Access Standard Manager interface. The breadcrumb navigation is "User Management > Auth Servers". The left sidebar shows the navigation menu with "Auth Servers" selected under "User Management". The main content area has tabs for "Auth Servers", "Lookup Servers", "Mapping Rules", "Auth Test", and "Accounting". Below the tabs, there is a field for "Authentication Cache Timeout (seconds)" set to 120, with an "Update" button. Below that is a table listing authentication providers:

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			
Cisco VPN	vpn sso				

5. Haga clic el icono de la asignación y después agregue la regla de la asignación. La asignación varía al dependiente sobre el valor del atributo de clase 25 que WLC envía en el paquete de las estadísticas. Este valor de atributo se configura en el servidor de RADIUS y varía basado sobre la autorización de usuario. En este ejemplo, el valor de atributo es ALLOWALL, y se pone en el papel AllowAll.



Auth Servers	Lookup Servers	Mapping Rules	Auth Test	Accounting																
Configure one or more conditions first using the Add/Save Condition form, then add or save the mapping rule to the selected Role using the Add/Save Mapping form. Note that if the mapping is not added or saved, conditions are not preserved.																				
Provider Name	Cisco VPN	Priority	1																	
Role Name	ALLOWALL	Description																		
Rule Expression	( 0,25 equals ALLOWALL )																			
<input type="button" value="Save Mapping"/>																				
<table border="1"> <tr> <td>Condition Type</td> <td>VLAN ID</td> <td>Operator</td> <td>equals</td> </tr> <tr> <td>Property Name</td> <td>VLANID</td> <td>Property Value</td> <td></td> </tr> <tr> <td colspan="4">VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add Condition"/></td> <td colspan="2" style="text-align: center;"><input type="button" value="Cancel"/></td> </tr> </table>					Condition Type	VLAN ID	Operator	equals	Property Name	VLANID	Property Value		VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.				<input type="button" value="Add Condition"/>		<input type="button" value="Cancel"/>	
Condition Type	VLAN ID	Operator	equals																	
Property Name	VLANID	Property Value																		
VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.																				
<input type="button" value="Add Condition"/>		<input type="button" value="Cancel"/>																		
<table border="1"> <thead> <tr> <th>#</th> <th>Type</th> <th>Left Operand</th> <th>Operator</th> <th>Right Operand</th> <th>Edit</th> <th>Del</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Attribute</td> <td>0,25</td> <td>equals</td> <td>ALLOWALL</td> <td></td> <td></td> </tr> </tbody> </table>					#	Type	Left Operand	Operator	Right Operand	Edit	Del	1	Attribute	0,25	equals	ALLOWALL				
#	Type	Left Operand	Operator	Right Operand	Edit	Del														
1	Attribute	0,25	equals	ALLOWALL																

## [Pasos para configurar SSO en el regulador LAN de la Tecnología inalámbrica](#)

Las estadísticas RADIUS necesitan ser configuradas en el WLC para alcanzar solo Muestra-en la capacidad con el servidor NAC.

The screenshot shows the Cisco WLC configuration interface for WLANs > Edit. The 'AAA Servers' tab is active, displaying the following configuration:

- Radius Servers:**
  - Authentication Servers:** Server 1: IP:10.1.1.12, Port:1812; Server 2: None; Server 3: None.
  - Accounting Servers:** Server 1: IP:10.10.11.19, Port:1813; Server 2: None; Server 3: None.
  - Enabled
- LDAP Servers:** Server 1: None; Server 2: None; Server 3: None.
- Local EAP Authentication:**  Enabled
- Authentication priority order for web-auth user:** (Empty list)

## [Verificación](#)

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos

comandos show. Utilice el OIT para ver un análisis de la salida del comando show.

## Comandos CLI de CISCO WLC para la verificación

(Cisco Controller) >show interface summary

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr	Guest
ap-manager	1	untagged	10.10.75.3	Static	Yes	No
management	1	untagged	10.10.75.2	Static	No	No
nac-vlan	1	175	10.10.175.2	Dynamic	No	No
service-port	N/A	N/A	192.168.1.1	Static	No	No
virtual	N/A	N/A	1.1.1.1	Static	No	No

(Cisco Controller) >show interface detailed management

Interface Name..... management  
MAC Address..... 00:18:73:34:b2:60  
IP Address..... 10.10.75.2  
IP Netmask..... 255.255.255.0  
IP Gateway..... 10.10.75.1  
VLAN..... untagged  
Quarantine-vlan..... 0  
Active Physical Port..... 1  
Primary Physical Port..... 1  
Backup Physical Port..... Unconfigured  
Primary DHCP Server..... 10.10.75.1  
Secondary DHCP Server..... Unconfigured  
DHCP Option 82..... Disabled  
ACL..... Unconfigured  
AP Manager..... No  
Guest Interface..... No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name..... nac-vlan  
MAC Address..... 00:18:73:34:b2:63  
IP Address..... 10.10.175.2  
IP Netmask..... 255.255.255.0  
IP Gateway..... 10.10.175.1  
**VLAN..... 175**  
**Quarantine-vlan..... 176**  
Active Physical Port..... 1  
Primary Physical Port..... 1  
Backup Physical Port..... Unconfigured  
Primary DHCP Server..... 10.10.175.1  
Secondary DHCP Server..... Unconfigured  
DHCP Option 82..... Disabled  
ACL..... Unconfigured  
AP Manager..... No  
Guest Interface..... No

## Verificación del estado del cliente del GUI WLC

La corriente está inicialmente en un estado de la cuarentena hasta que el análisis de la postura se haga en el dispositivo NAC.

Save Configuration | Bing | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

- Summary
- Access Points
- Statistics
- CDP
- Rogues
- Clients
- Multicast

Client Properties		AP Properties	
MAC Address	00:40:96:b3:be:2c	AP Address	00:18:74:fb:26:90
IP Address	10.10.175.23	AP Name	Franciscan-1
Client Type	Regular	AP Type	802.11g
User Name	test	WLAN Profile	franciscan
Port Number	1	Status	Associated
Interface	nac-vlan	Association ID	1
VLAN ID	175	802.11 Authentication	Open System
CCX Version	CCXv5	Reason Code	0
EZE Version	Not Supported	Status Code	0
Mobility Role	Local	CF Pollable	Not Implemented
Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Implemented
Mirror Mode	Disable	PBCC	Not Implemented
Management Frame Protection	Yes	Channel Agility	Not Implemented
<b>Security Information</b>		Timeout	0
Security Policy Completed	Yes	WEP State	WEP Enable
Policy Type	RSN (WPA2)		
Encryption Cipher	CCMP (AES)		
EAP Type	LEAP		
NAC State	Quarantine		

El estado NAC del cliente debe ser **acceso** después de que se complete el análisis de la postura.

Save Configuration | Bing | Logout | Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

- Summary
- Access Points
- Statistics
- CDP
- Rogues
- Clients
- Multicast

Client Properties		AP Properties	
MAC Address	00:40:96:b3:be:2c	AP Address	00:18:74:fb:26:90
IP Address	10.10.175.23	AP Name	Franciscan-1
Client Type	Regular	AP Type	802.11g
User Name	test	WLAN Profile	franciscan
Port Number	1	Status	Associated
Interface	nac-vlan	Association ID	1
VLAN ID	175	802.11 Authentication	Open System
CCX Version	CCXv5	Reason Code	0
EZE Version	Not Supported	Status Code	0
Mobility Role	Local	CF Pollable	Not Implemented
Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Implemented
Mirror Mode	Disable	PBCC	Not Implemented
Management Frame Protection	Yes	Channel Agility	Not Implemented
<b>Security Information</b>		Timeout	0
Security Policy Completed	Yes	WEP State	WEP Enable
Policy Type	RSN (WPA2)		
Encryption Cipher	CCMP (AES)		
EAP Type	LEAP		
NAC State	Access		

## Verificación de solo Muestra-en el servidor NAC con WLC

Bajo el VPN auténtico, vaya a la subdivisión del **cliente activo** a verificar si el paquete de inicio de contabilidad ha llegado del WLC. Esta entrada aparece con CCA el agente instalado en la máquina del cliente.

Usted necesita abrir a un navegador para completar el solo Muestra-en el proceso sin un agente. Cuando el usuario abre al navegador, el proceso SSO ocurre, y el usuario aparece en la lista de usuario en línea (OUL). Con las estadísticas RADIUS pare el paquete, el usuario se quita de la lista del cliente activo.

Device Management > Clean Access Servers > 10.10.11.19



Status	Network	Filter	Advanced	Authentication	Misc
Login Page	VPN Auth	Windows Auth	OS Detection		
General	VPN Concentrators	Accounting Servers	Accounting Mapping	Active Clients	

List All VPN Clients:

(For performance considerations, this page does not show all active VPN clients by default.)

Search IP Address:

Clear All Active VPN Clients

Total Active VPN Clients: 1

Active VPN Clients 1 - 1 of 1 | First | Previous | Next | Last |

Client IP	Client Name	VPN Server IP	Login Time	
10.10.175.25	004096b48bff	10.10.75.2	Wed Jul 09 16:32:04 PDT 2008	<input type="checkbox"/>

## [Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## [Comandos para resolución de problemas](#)

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la salida del comando show.

**Nota:** Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

## [Información Relacionada](#)

- [Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Pedidos los comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)