NAC Out−Of−Band (OOB) Wireless Configuration Example

Document ID: 107645

Contents

Introduction

This document provides design guidance to deploy Out of Band (OOB) Cisco Network Admission Control (NAC) appliance endpoint security in a Cisco Unified Wireless Network deployment. These best practice recommendations assume that a Cisco Unified Wireless Network has been deployed in accordance with the guidelines provided in the Enterprise Mobility Design Guide 3.0.

The recommended design is the Virtual Gateway (Bridge Mode) and central deployment OOB solution with RADIUS Single Sign−On. The Wireless Lan Controller (WLC) must be placed L2 adjacent to the NAC server. The client associates to the WLC, and WLC authenticates the user. Once the authentication is completed, the user traffic goes through the quarantine VLAN from the WLC to the NAC server. The posture assessment and remediation process take place. Once the user is certified, the user VLAN changes from quarantine to access VLAN in the WLC. The traffic bypasses the NAC server when moved to access VLAN.

Prerequisites

Requirements

This document configuration is specific to the NAC 4.5 and WLC 5.1 release

Components Used

This document is t restricted to specific software and hardware versions.

- NAC Server 3350 4.5
- NAC Manager 3350 4.5
- WLC 2106 5.1

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Cisco NAC Overview

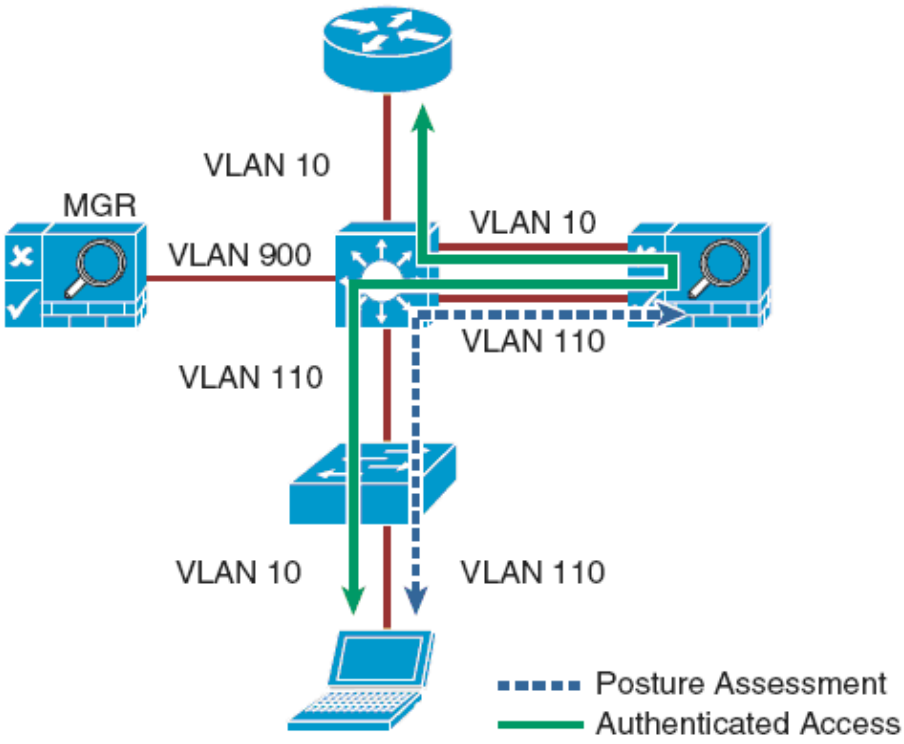
Cisco NAC uses the network infrastructure to enforce security policy compliance on all devices that seek to access network computing resources. With the Cisco NAC appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. The Cisco NAC appliance identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with network security policies, and repairs any vulnerabilities before it permits access to the network.

The terminology of the recommended design is discussed:

Virtual Gateway Mode (Bridge Mode)

When the NAC appliance is configured as a virtual gateway, it acts as a bridge between the end users and default gateway (router) for the client subnet that is managed. For a given client VLAN, the NAC appliance bridges traffic from its untrusted interface to its trusted interface. When it acts as a bridge from the untrusted side to the trusted side of the appliance, two VLANs are used. For example, Client VLAN 110 is defined between the wireless LAN controller (WLC) and the untrusted interface of the NAC appliance. There is no routed interface or switched virtual interface (SVI) associated with VLAN 110 on the distribution switch. VLAN 10 is configured between the trusted interface of the NAC appliance and the next−hop router interface/SVI for the client subnet. A mapping rule is made in the NAC appliance that forwards packets that arrive on VLAN 110 out VLAN 10 when it swaps VLAN tag information as shown in Fig 1−1. The process is reversed for packets that return to the client. Note that, in this mode, BPDUs are not passed from the untrusted−side VLANs to their trusted−side counterparts. The VLAN mapping option is usually chosen when the NAC appliance is positioned logically inline between clients and the networks that are protected. This bridging option must be used if the NAC appliance is to be deployed in the virtual gateway mode with a Unified Wireless deployment. Because the NAC server is aware of *upper layer protocols*, by default it explicitly allows protocols that require it to connect to the network in Authenticated Role, for example, DNS and DHCP.

Figure 1−1 Virtual Gateway with VLAN Mapping

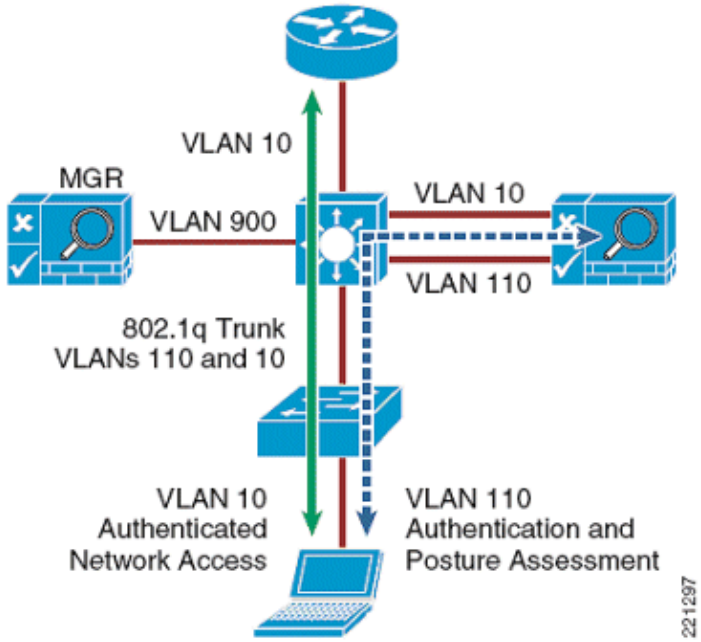


Out−of−Band Mode

Out−of−band deployments require user traffic to traverse through the NAC appliance only within authentication, posture assessment, and remediation. When a user is authenticated and passes all policy checks, the traffic is switched normally through the network and bypasses the NAC server. For further information, refer to Chapter 4 of the Cisco NAC Appliance−Clean Access Manager Installation and Administration Guide.

When the NAC appliance is configured in this manner, the WLC is a managed device in the NAC Manager, the same way that a Cisco switch is managed by the NAC Manager. After the user is authenticated and passes posture assessment, the NAC Manager instructs the WLC to tag the user traffic from the NAC VLAN to access VLAN that offers access privileges.

Figure 1−2 NAC Appliance in Out−of−Band Mode with Virtual Gateway Mode



Single Sign−On

Single sign−on (SSO) is an option that does not require user intervention and is relatively straightforward to implement. It makes use of the VPN SSO capability of the NAC solution, coupled with the Clean Access Agent software that runs on the client PC. VPN SSO uses RADIUS accounting records to notify the NAC appliance about authenticated remote access users that connect to the network. In the same way, this feature can be used in conjunction with the WLAN controller to automatically inform the NAC server about authenticated wireless clients that connect to the network.

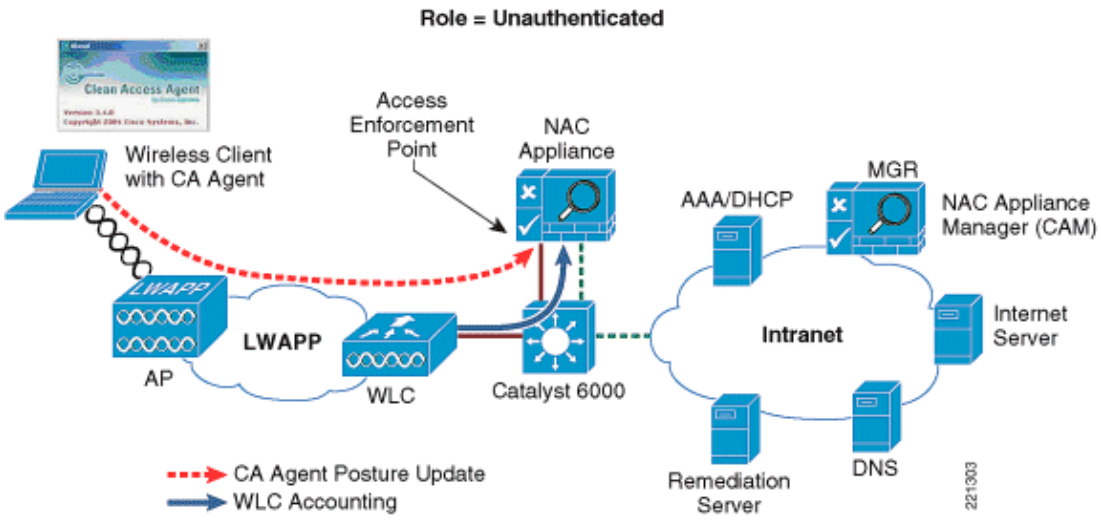
See Figures 1−3 through 1−6 for examples of a wireless client that performs SSO authentication, posture assessment, remediation, and network access through the NAC appliance.

This sequence is shown in Figure 1−3:

1. The wireless user performs 802.1x/EAP authentication through the WLAN controller to an upstream AAA server.
2. The client obtains an IP address from either AAA or a DHCP server.
3. After the client receives an IP address, the WLC forwards a RADIUS accounting (start) record to the NAC appliance, which includes the IP address of the wireless client.

   Note: The WLC controller uses a single RADIUS accounting record (start) for 802.1x client authentication and IP address assignment, while the Cisco Catalyst switches send two accounting records: an accounting start is sent after 802.1x client authentication, and an interim update is sent after the client is assigned an IP address.
4. After it detects network connectivity, the NAC Agent attempts to connect to the CAM (with the SWISS protocol). Traffic is intercepted by the NAC server, which, in turn, queries the NAC Manager to determine whether the user is in the online user list. Only clients that are authenticated are in the online user list, which is the case in the example above as a result of the RADIUS update in step 3.
5. The NAC Agent performs a local assessment of the security/risk posture of the client machine and forwards the assessment to the NAC server for network admission determination.

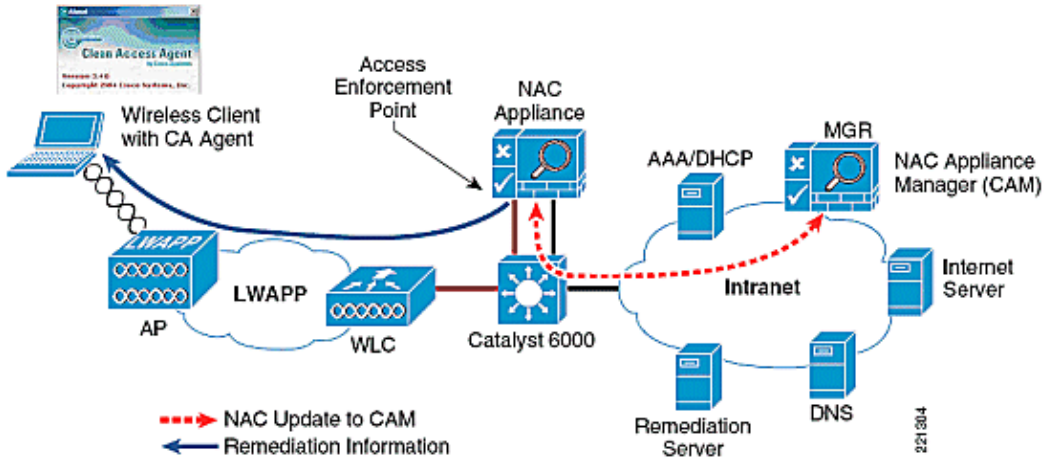
Figure 1−3 Client Authentication Process and Posture Assessment



This sequence takes place in Figure 1−4:

1. The NAC appliance forwards the agent assessment to the NAC Appliance Manager (CAM).
2. In this example, the CAM determines that the client is not in compliance and instructs the NAC appliance to put the user into a quarantine role.
3. The NAC appliance then sends remediation information to the client agent.

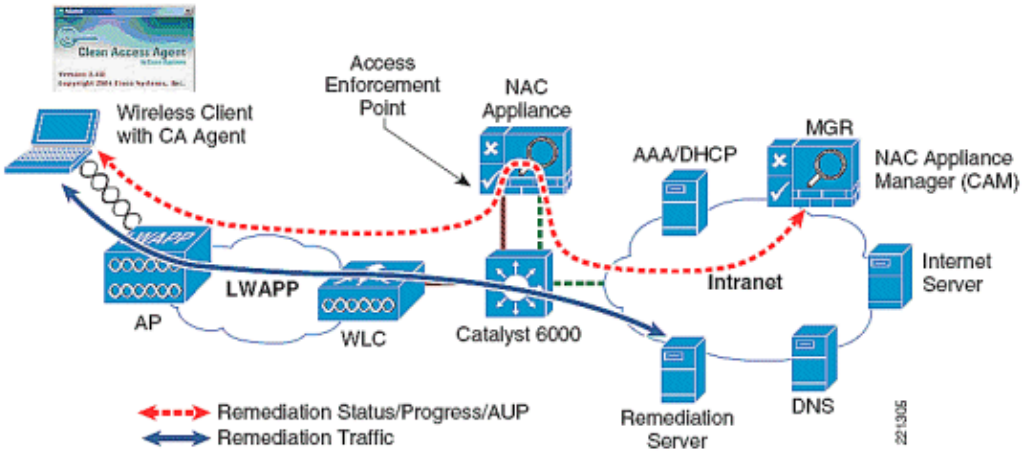
Figure 1−4 Posture Assessment Information from CAS to CAM



This sequence takes place in Figure 1−5:

1. The Client Agent displays the time that remains to accomplish remediation.
2. The Agent guides the user step−by−step through the remediation process; for example, in the update of the anti−virus definition file.
3. After remediation completion, the agent updates the NAC server.
4. The CAM displays an Acceptable Use Policy (AUP) statement to the user.

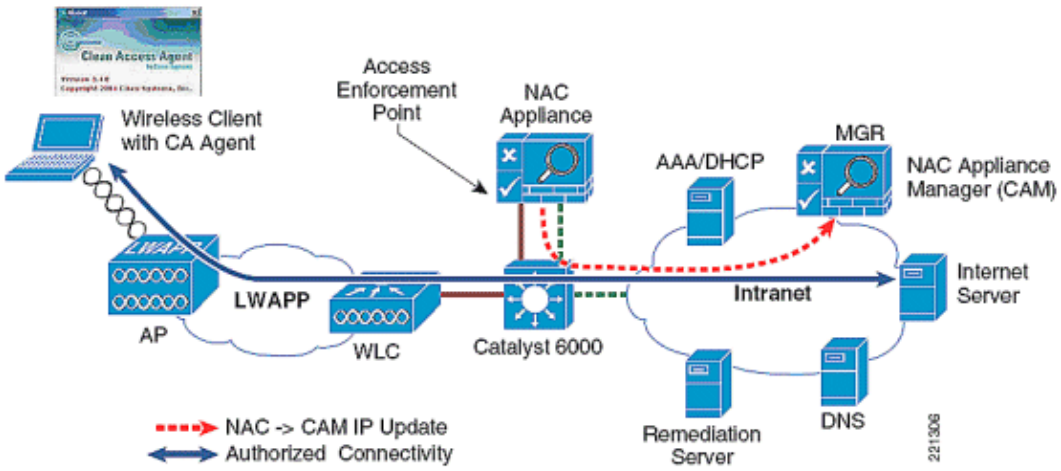
Figure 1−5 Client Remediation Process with CAS as the Enforcement Device



This sequence takes place in Figure 1−6:

1. After it accepts the AUP, the NAC appliance switches the user to an online (authorized) role.
2. The SSO functionality populates the online user list with the client IP address. After remediation, an entry for the host is added to the certified list. Both of these tables (together with the discovered clients table) are maintained by the CAM (NAC Appliance Manager).
3. The NAC Manager sends an SNMP write notification to WLC to change the user VLAN from quarantine to access VLAN.
4. The user traffic starts to leave the WLC with the access VLAN tag. The NAC server no longer is in the path for this particular user traffic.

Figure 1−6 Certified Client Bypass the CAS by Switching Over to Access VLAN



The most transparent method to facilitate wireless user authentication is to enable VPN−SSO authentication on the NAC server and configure the WLCs to forward RADIUS accounting to the NAC server. In the event that accounting records need to be forwarded to a RADIUS server upstream in the network, the NAC server can be configured to forward the accounting packet to the RADIUS server.

Note: If VPN−SSO authentication is enabled without the Clean Access agent installed on the client PC, the user is still automatically authenticated. However, they are not automatically connected through the NAC appliance until their web browser is opened and a connection attempt is made. In this case, when the user opens their web browser, they are momentarily redirected (without a logon prompt) within the agent−less phase. When SSO process is complete, they are connected to their originally requested URL.

Configure NAC OOB Wireless Solution

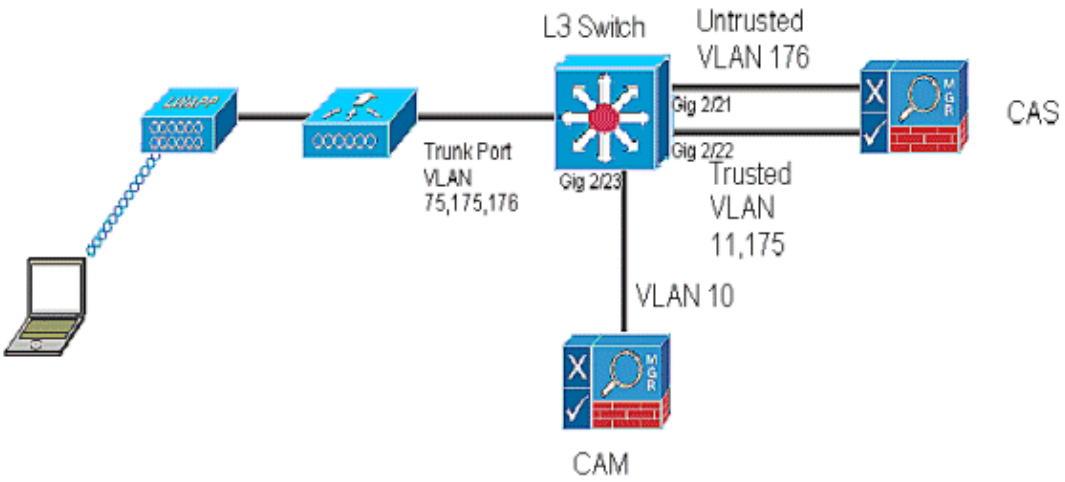
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

In the current NAC implementation WLC integrates with the Cisco NAC appliance in in−band mode only, where the NAC appliance has to remain in data path even after the user is certified. Once the NAC appliance completes its posture validation, the employee/guest receives access of the network based on their role.

With the NAC 4.5 and WLC 5.1 release, the wireless NAC solution supports OOB integration with NAC appliance. When the client associates and completes L2Auth, it is checked whether the quarantine interface is associated to the WLAN/SSID. If yes, the initial traffic is sent on the quarantine interface. The client traffic flows in quarantine VLAN, which is trunked to the NAC appliance. Once posture validation is done, the NAC Manager sends an SNMP set message that updates the access VLAN ID; the controller updates itself with the access VLAN ID, and data traffic starts switching from the controller directly to the network without the NAC server.

Figure 2−1 Example of Standalone CAS in Bridge Mode Connected to WLC Through Switch



In Figure 2−1, the WLC is connected to a trunk port that carries the quarantine VLAN and access VLAN (176 and 175). On the switch, the quarantine VLAN traffic is trunked to the NAC appliance, and the access VLAN traffic is trunked directly to the Layer3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to access the VLAN based on static mapping configuration. When client associates complete the L2 Auth, it checks if the quarantine interface is associated; if yes, the data is sent on the quarantine interface. The client traffic flows in the quarantine VLAN, which is trunked to the NAC appliance. Once posture validation is done, the NAC server (CAS) sends an SNMP set message that updates the access VLAN ID to the controller, and the data traffic starts to switch from the WLC directly to the network without the NAC server.

Restrictions

- No port profile associated
- No VLAN ID specified on the NAC Manager: defined on WLC
- MAC filter support is not able to use the VLAN ID from role settings
- Out−of−Band Virtual Gateway NAC server mode support only

- Layer 2 association between the WLC and NAC server
- NAC ISR and WLC NM cannot be set up to do Wireless OOB NAC

Note: Refer to the VLAN Mapping in Virtual Gateway Modes section of Cisco NAC Appliance − Clean Access Server Configuration Guide, Release 4.8(1) for more information on how to safely configure VLANs in virtual gateway modes.

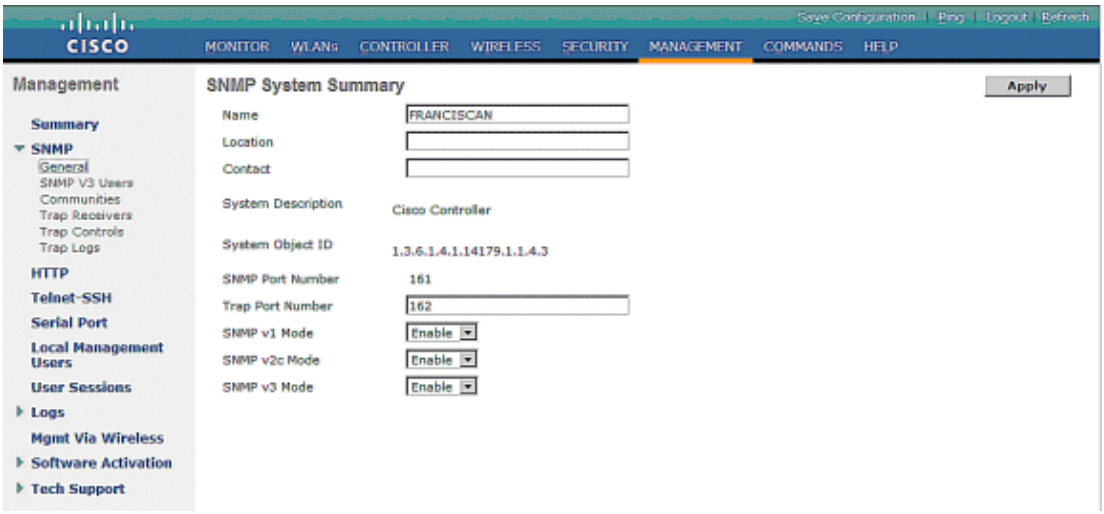
Catalyst Switch Configuration

```
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
```

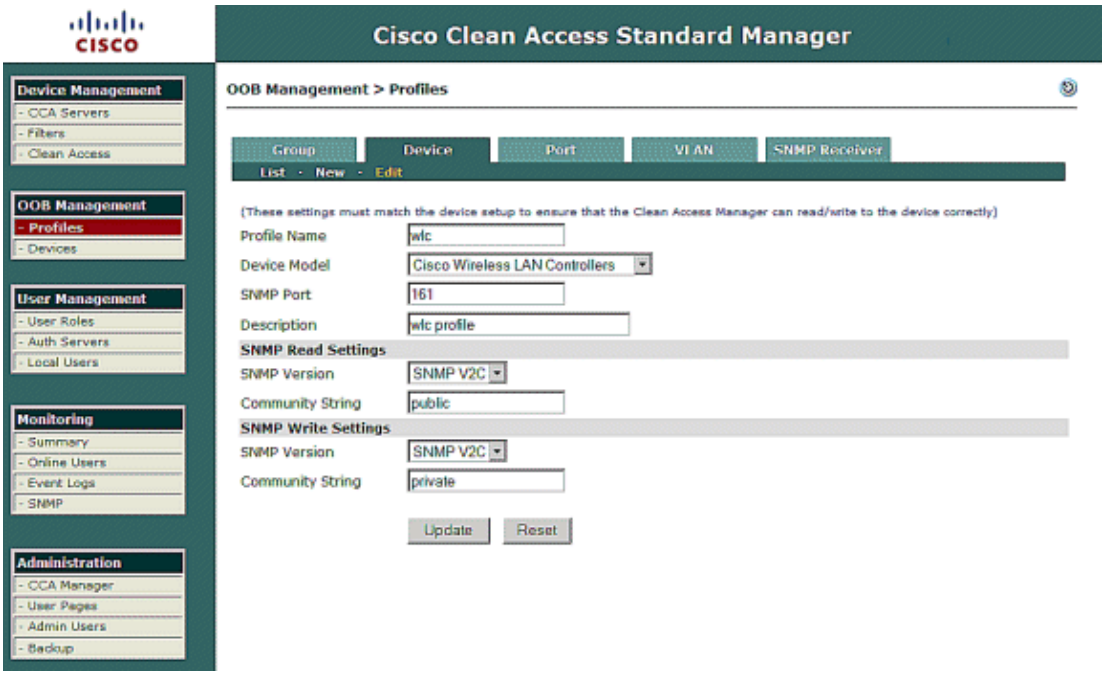
Steps to Configure NAC OOB on the WLC and NAC Manager

Follow these steps to configure NAC OOB on WLC and NAC Manager:

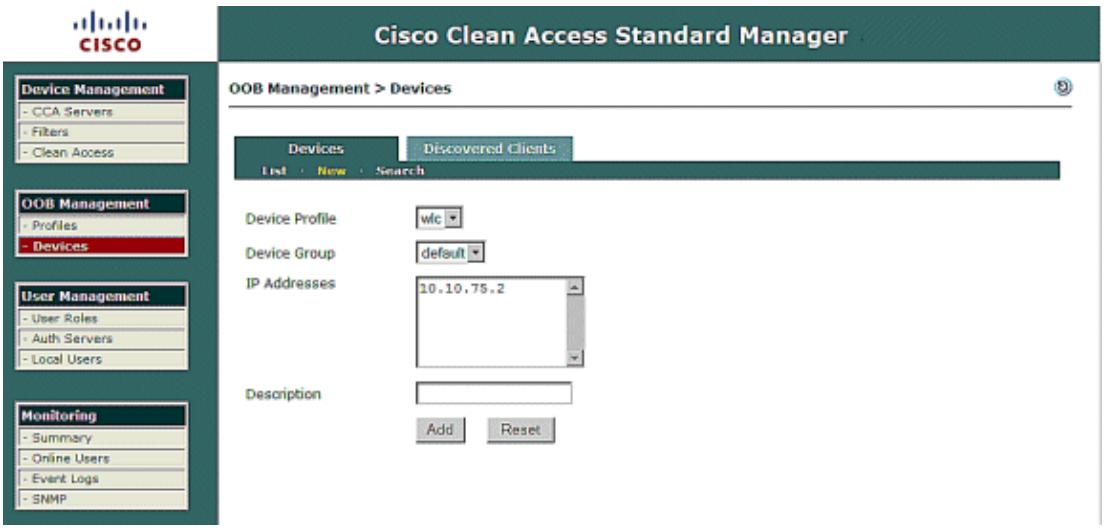
1. Enable SNMP v2 mode on the controller.



2. Create a profile for WLC on the CAM Manager. Click **OOB Management Profile > Device > New**.

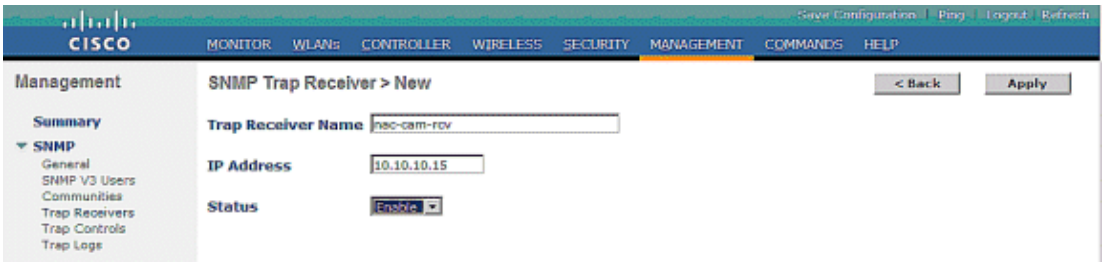


3. Once the profile is created on CAM, add WLC in the profile; go to **OOB Management > Devices > New** and enter the management IP address of WLC.

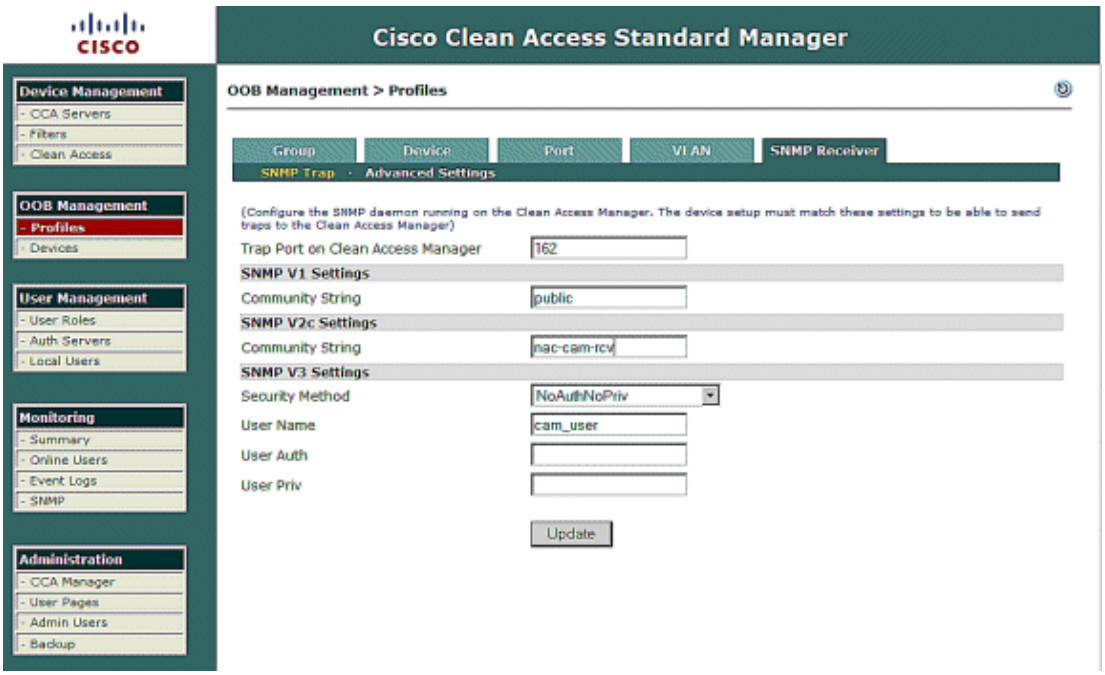


Now the controller is added in the CAM Manager.

4. Add the CAM as the SNMP trap receiver from the WLC. Use the exact name of the trap receiver in the CAM as the SNMP receiver.

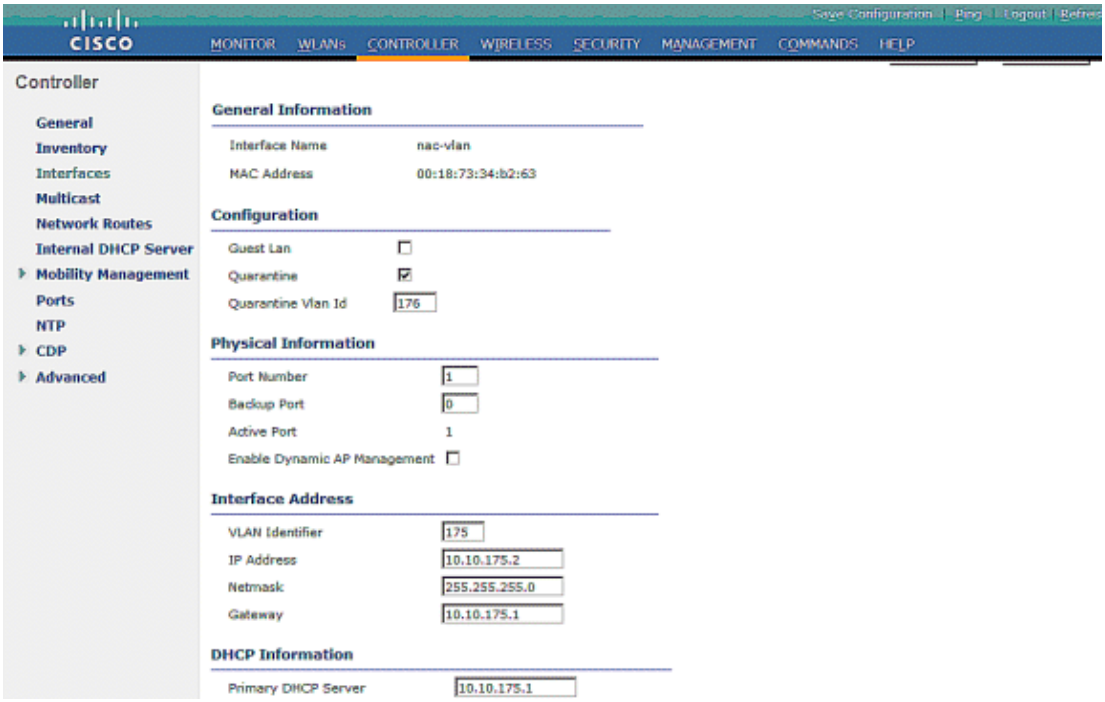


5. Configure the SNMP trap receiver in the CAM with the same name, which is specified on the controller; click Profiles under **OOB Management > SNMP Receiver**.

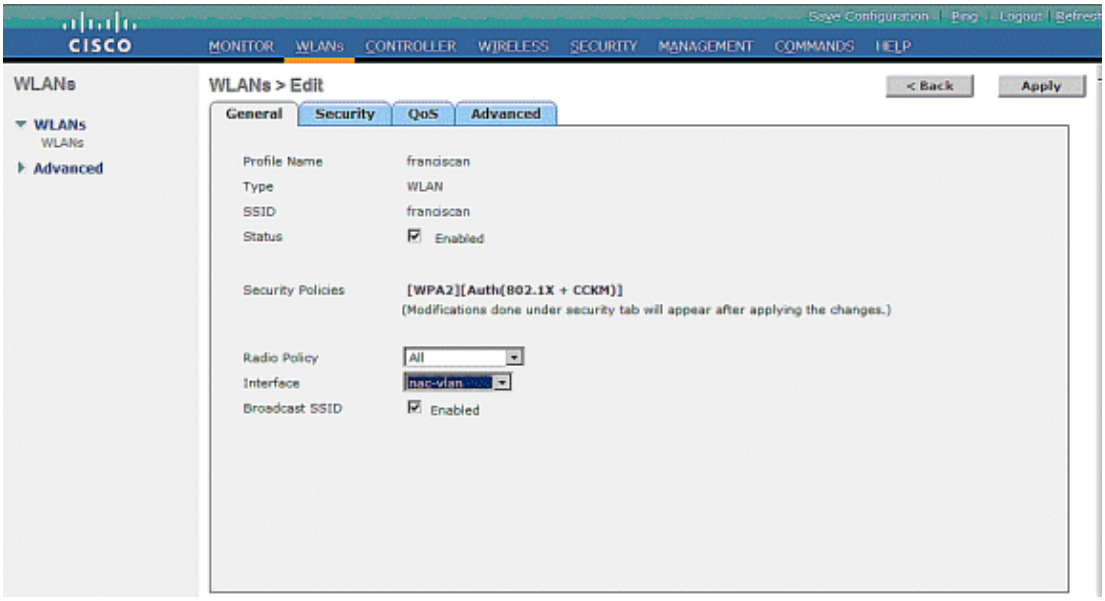


At this stage, the WLC and CAM can talk to each other for client posture validation and access/quarantine state updates.

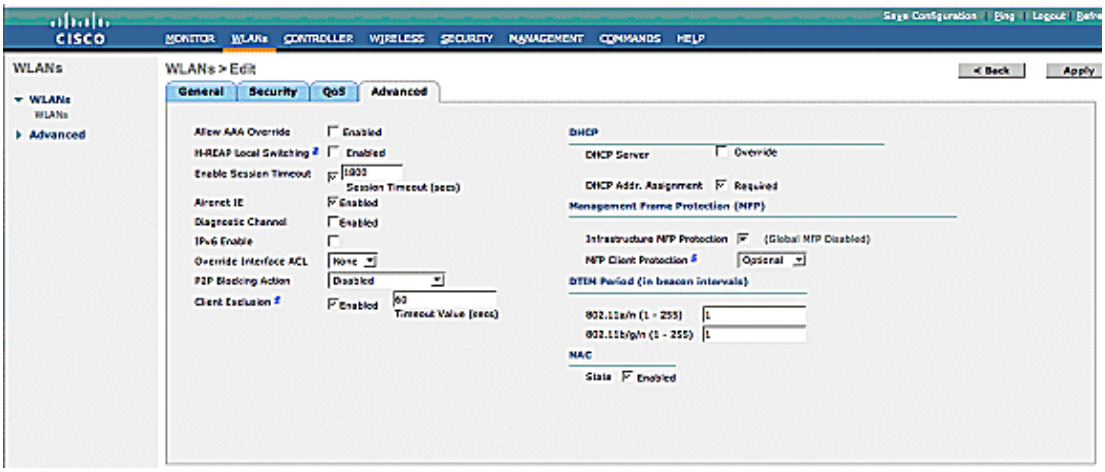
6. In the controller, create a dynamic interface with access and quarantine VLAN.



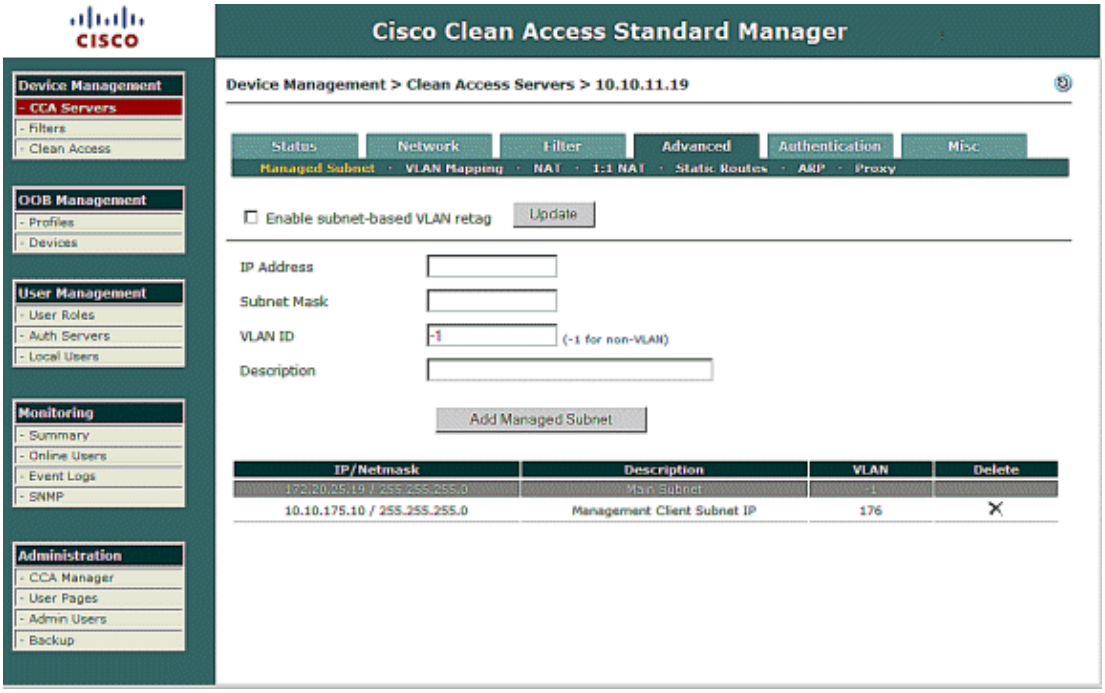
7. Create the WLAN, and associate it with the dynamic interface.



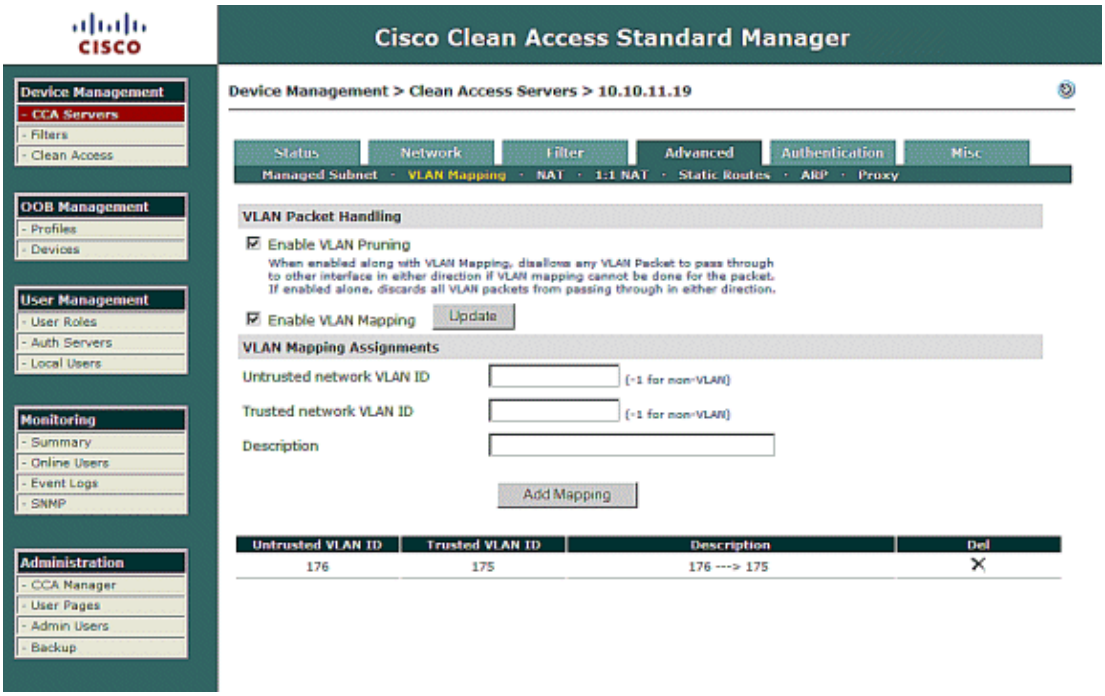
8. Finally, enable NAC in the WLAN.



9. Add the client subnet in the CAS server as the managed subnet; click the **CAS server > Select your CAS server > Manage >Advanced > Managed Subnets >Add Unused IP address from the client subnet** and put quarantine VLAN (untrusted VLAN) for the managed subnet.



10. Create VLAN mappings on CAS. Choose **CAS server > Select your CAS server > Manage > Advanced > VLAN Mapping**. Add access VLAN as trusted and quarantine VLAN as untrusted.



Configuring Single Sign−On (SSO) with the OOB Wireless Solution

These are the requirements to enable wireless SSO:

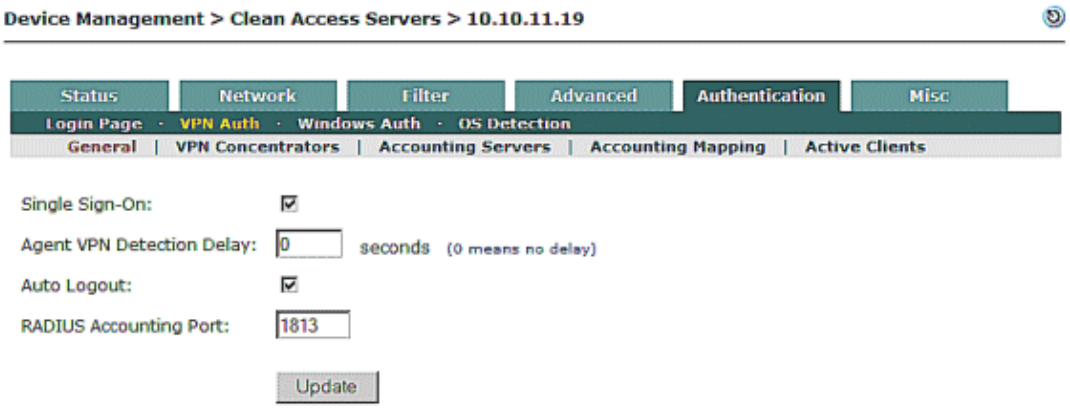
1. Enable VPN authentication on the NAC server WLC is defined as VPN concentrator in the NAC appliance.
2. Enable RADIUS accounting on the WLC the controller that is defined in the NAC appliance must be configured to send RADIUS accounting records to the NAC appliance for each 802.1x/EAP WLAN that is a managed subnet in the NAC.

Steps to Configure SSO on the NAC Manager

Follow these steps to configure SSO on the NAC Manager:

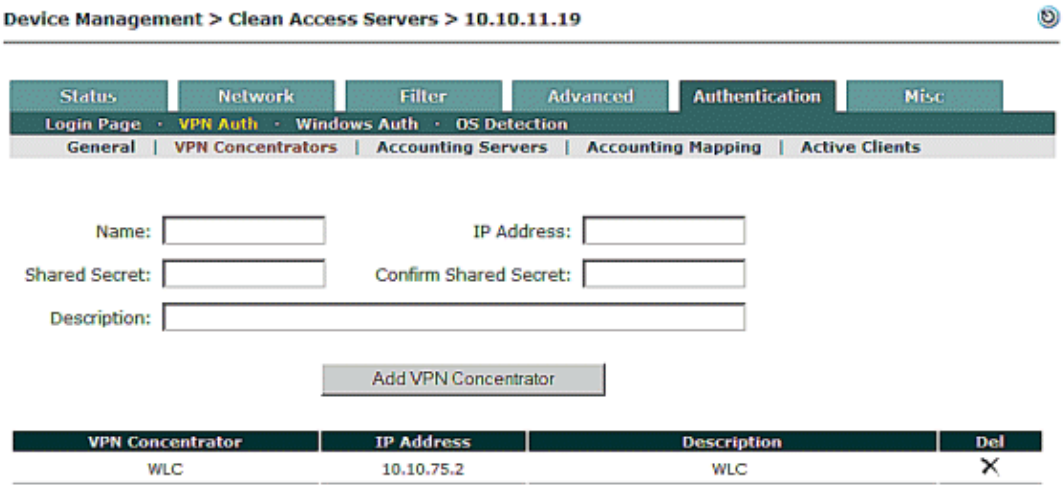
1. From the CAM left−hand menu, under Device Management, choose **CCA Server**, and then click the **NAC Server** link.
2. From the Server Status page, choose the **Authentication** tab and then the **VPN Auth** sub−menu. See Figure 3−1.

Figure 3−1 Enabling the Single Sign−On NAC Server

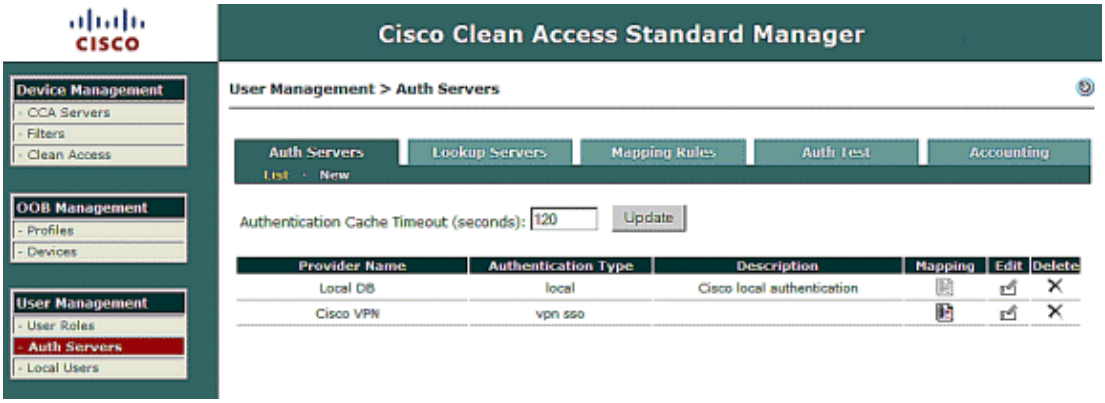


3. Choose the **VPN Concentrators Setting** (Figure 3−2) to add a new entry of WLC. Populate the entry fields for the WLC Management IP address and shared secret you want to use between the WLC and NAC server.

Figure 3−2 Add WLC as a RADIUS Client Under VPN Concentrator Section

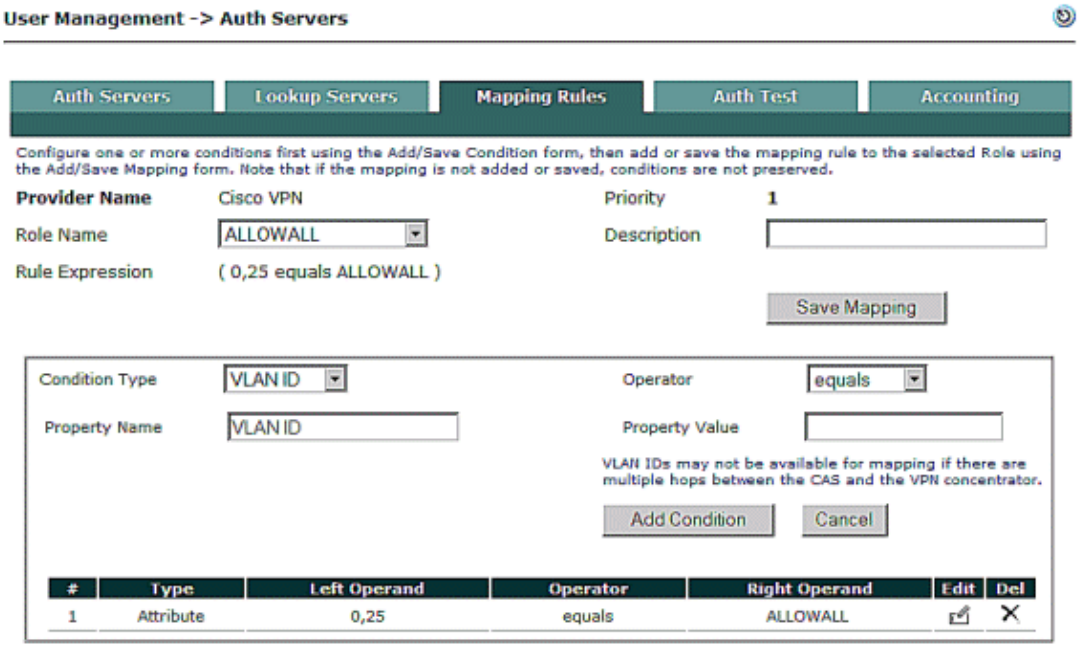


4. For Role Mapping, add the new authentication server with type **vpn sso** under **User Management** > **Auth Servers**.



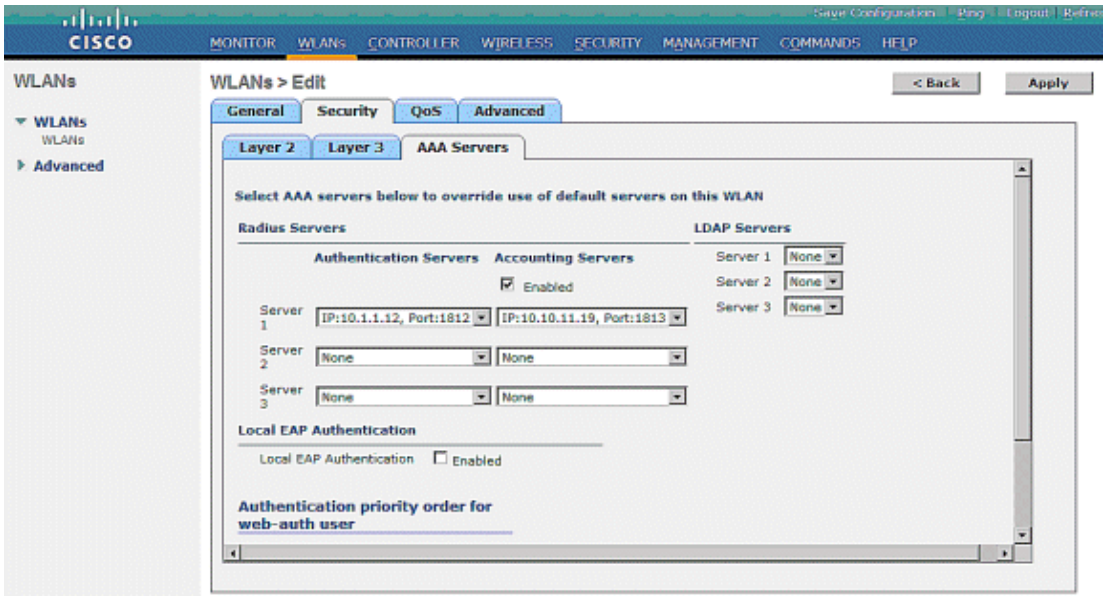
5. Click the **Mapping** icon and then add **Mapping Rule**. The mapping varies dependent upon the class attribute 25 value that WLC sends in the accounting packet. This attribute value is configured in the RADIUS Server and varies based upon the user authorization. In this example, the attribute value is

ALLOWALL, and it is placed in the role **AllowAll**.



Steps to Configure SSO on the Wireless LAN Controller

RADIUS Accounting needs to be configured on the WLC to achieve Single Sign−On capability with the NAC server.



Verify

Use this section to confirm that your configuration works properly.

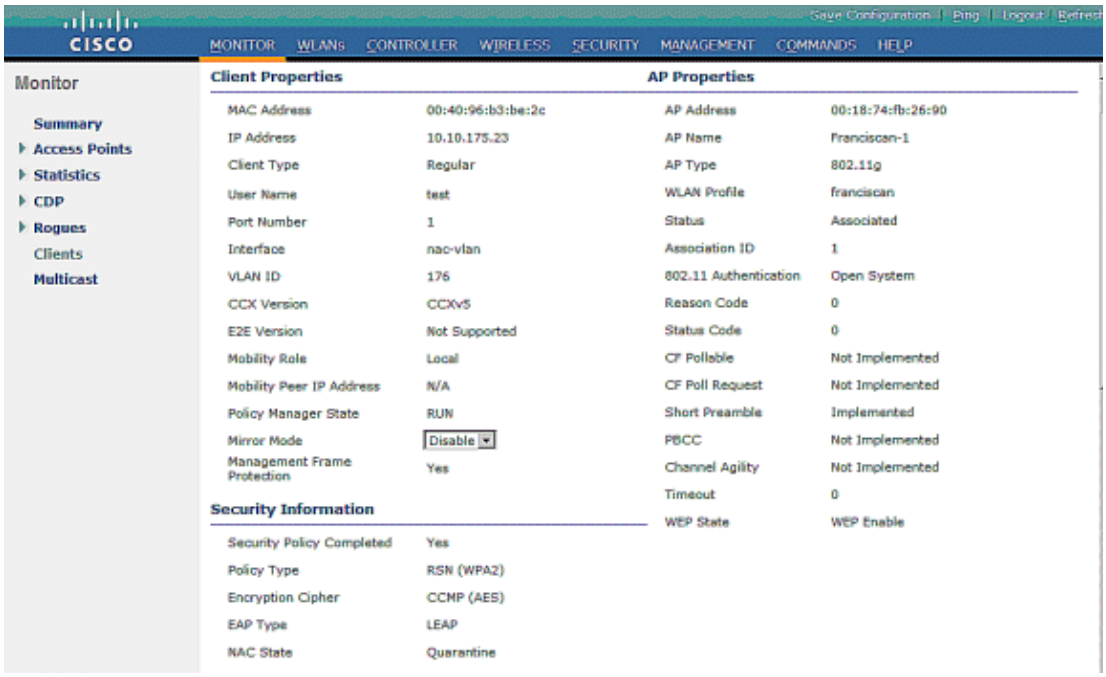
The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

CISCO WLC CLI Commands for Verification

```
(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
```

Client State Verification from WLC GUI

Initially the current is in a quarantine state until posture analysis is done in the NAC appliance.

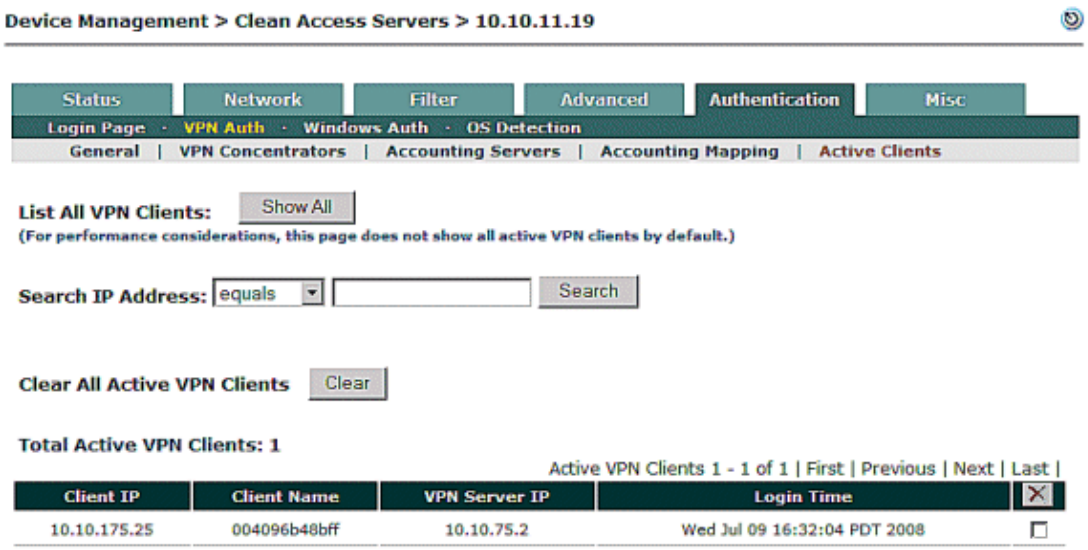


The NAC state of the client must be **Access** after the posture analysis is completed.

Verification of Single Sign−On on the NAC Server with WLC

Under VPN Auth, go to the **Active Client** subsection to verify whether the accounting start packet has arrived from the WLC. This entry shows up with the CCA agent installed on the client machine.

You need to open a browser to complete the Single Sign−On process without an agent. When the user opens the browser, the SSO process takes place, and the user shows up in the Online User List (OUL). With the RADIUS accounting stop packet, the user is removed from the Active Client list.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Related Information

- **Remote Authentication Dial−In User Service (RADIUS)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 03, 2009 Document ID: 107645