Configuring WLC

Configure the WLC for NAT

The Internet edge firewall translates the IP address of the WLC management interface in the DMZ to a publicly reachable IP address so Cisco Aironet 1815 Teleworker Access Point at teleworker locations can reach the WLC. However, in order for the Cisco Aironet 1815T(Teleworker) Access Point to communicate with the WLC, the publicly reachable address must also be configured on the WLC management interface.

To configure the WLC for NAT, perform the following steps:

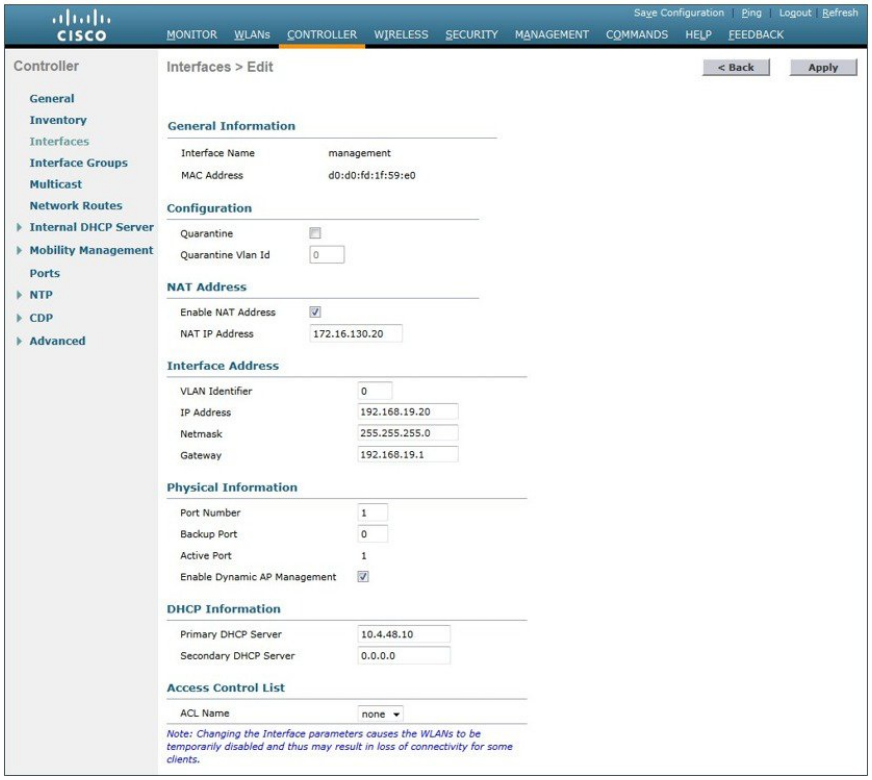
Procedure

Step 1 In **Controller** > **Interfaces**, click the management interface.

Step 2 Select Enable NAT Address.

Step 3 In the NAT IP Address box, enter the publicly reachable IP address, and then click Apply. (Example: 172.16.130.20)

Note The NAT IP Address must be the external, globally unique IP address that the Wireless LAN Controller displays on the Internet. This allows the WLC to place this IP address into the CAPWAP discovery response packet prior to encryption. The address shown here is an RFC-1918, private IP address and is used in this guide only for documentation purposes.



Configuring the Time Zone

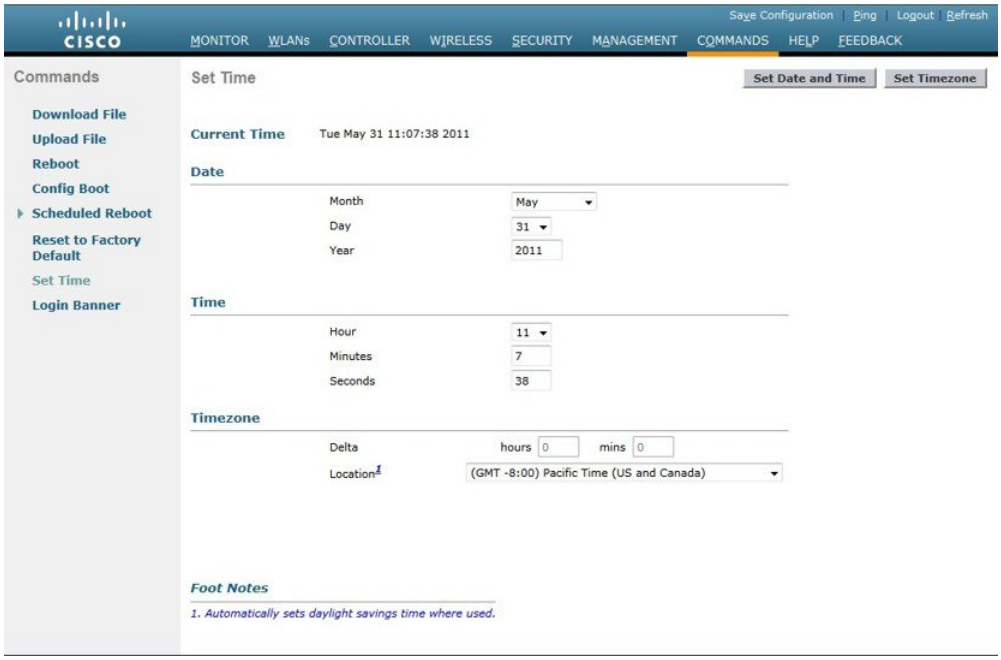
To configure the time zone, perform the following steps:

Procedure

Step 1 Navigate to **Commands** > **Set Time**.

Step 2 In the Location list, choose the time zone that corresponds to the locationof the WLC.

Step 3 Click Set Timezone.



Configuring SNMP

To configure SNMP, perform the following tasks:

Procedure

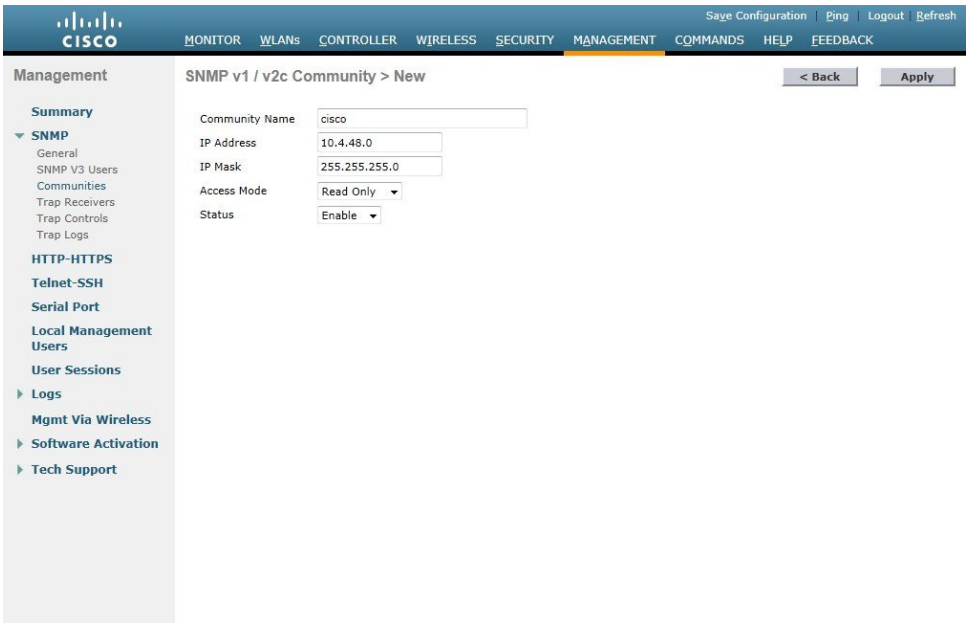
Step 1 In **Management** > **SNMP** > **Communities**, click **New**.

Step 2 Enter the **Community Name**. (Example: cisco)

Step 3 Enter the IP Address. (Example: 10.4.48.0)

Step 4 Enter the IP Mask. (Example: 255.255.255.0)

Step 5 In the **Status** list, choose **Enable**, and then click **Apply**.



Step 6 In **Management** > **SNMP** > **Communities**, click **New**.

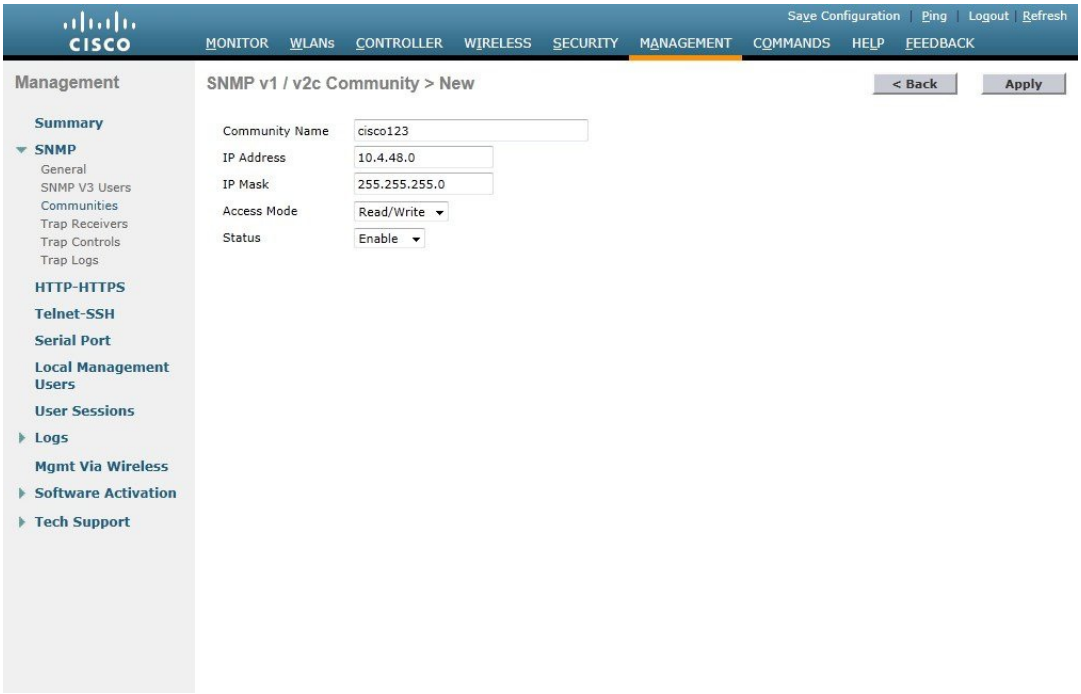
Step 7 Enter the **Community Name**. (Example: cisco123)

Step 8 Enter the **IP Address**. (Example: 10.4.48.0)

Step 9 Enter the **IP Mask**. (Example: 255.255.255.0)

Step 10 In the **Access Mode** list, choose Read/Write.

Step 11 In the **Status** list, choose **Enable**, and then click **Apply**.

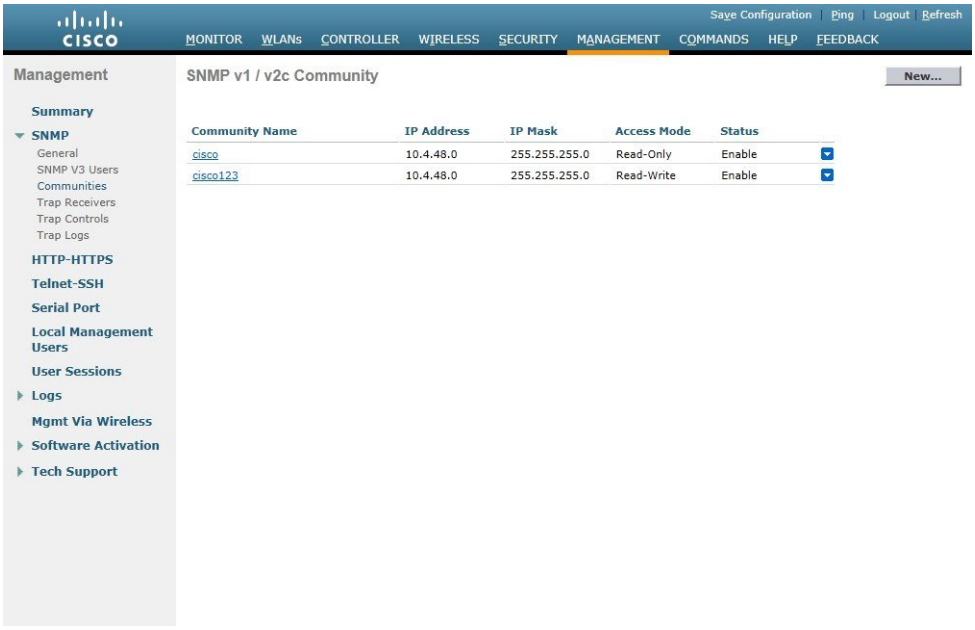


Step 12 Navigate to **Management** > **SNMP** > **Communities**.

Step 13 Point to the blue box for the public community, and then click **Remove**.

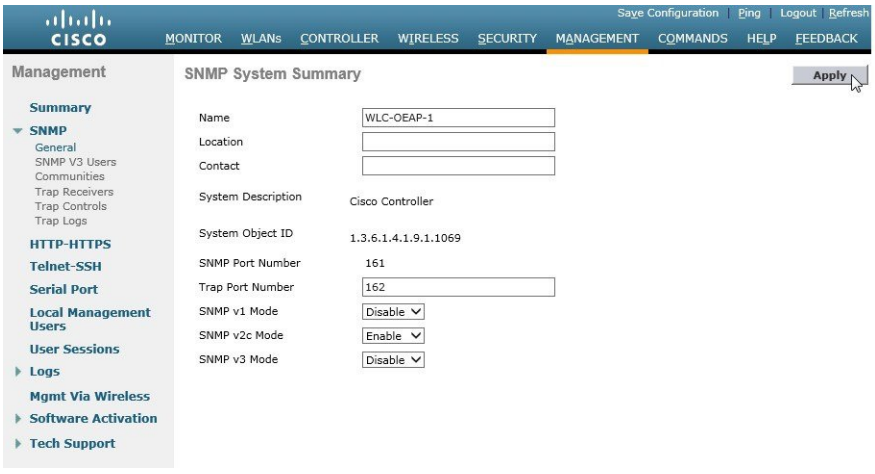
Step 14 On the "Are you sure you want to delete?" message,click **OK** .

Step 15 Repeat Step 13 and Step 14 for the private community.



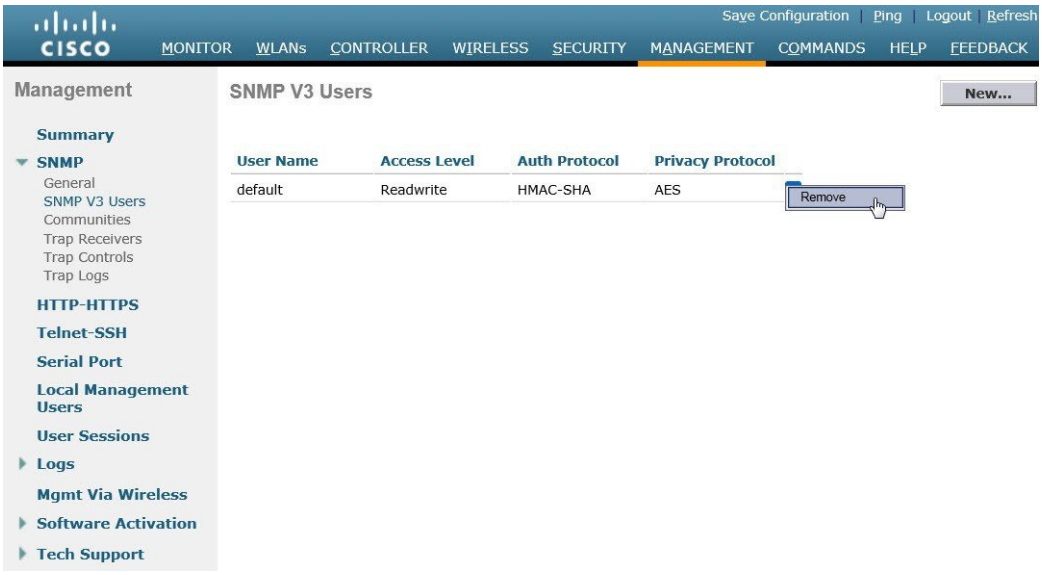
Step 16 Navigate to **Management** > **SNMP** > **General** and disable SNMP v3 Mode, and click **Apply**.

Figure 1:

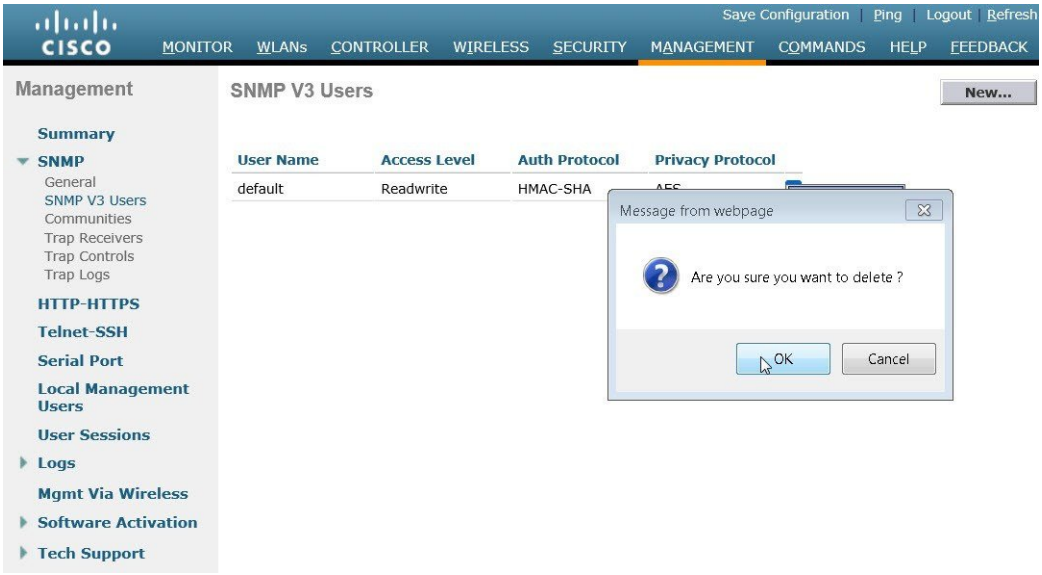


Step 17 Navigate to **Management** > **SNMP Communities** > **SNMP V3 Users**.

Step 18 On the right side of the default **User Name**, point and click the blue down arrow, and then click **Remove**.



Step 19 Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**.



Note Changes to the SNMP configuration may sometimes require that the WLC be rebooted.

Configuring Wireless User Authentication

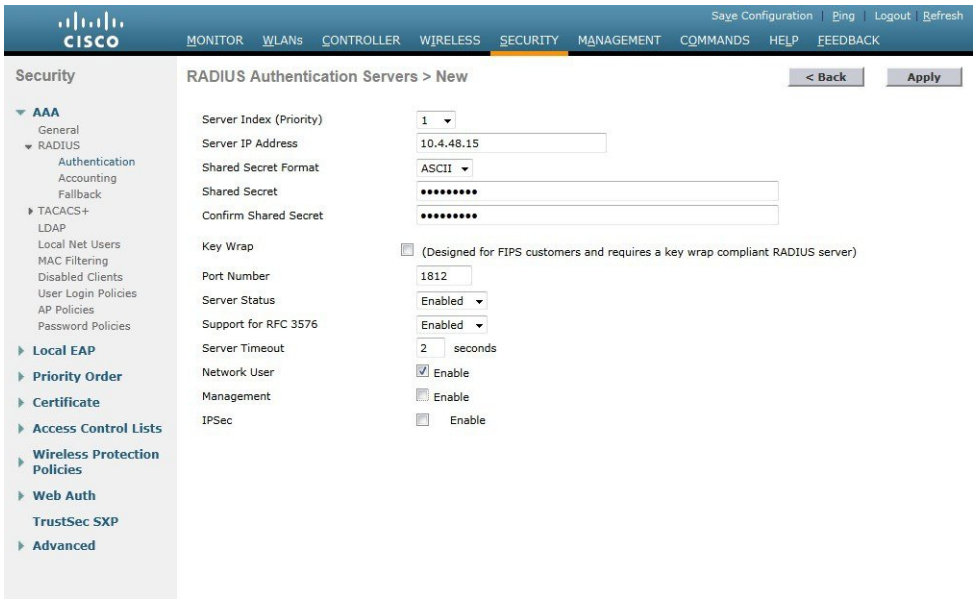
Procedure

Step 1 In **Security** > **AAA** > **Radius** > **Authentication**, click **New**.

Step 2 Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 3 Enter and confirm the **Shared Secret**. (Example: SecretKey)

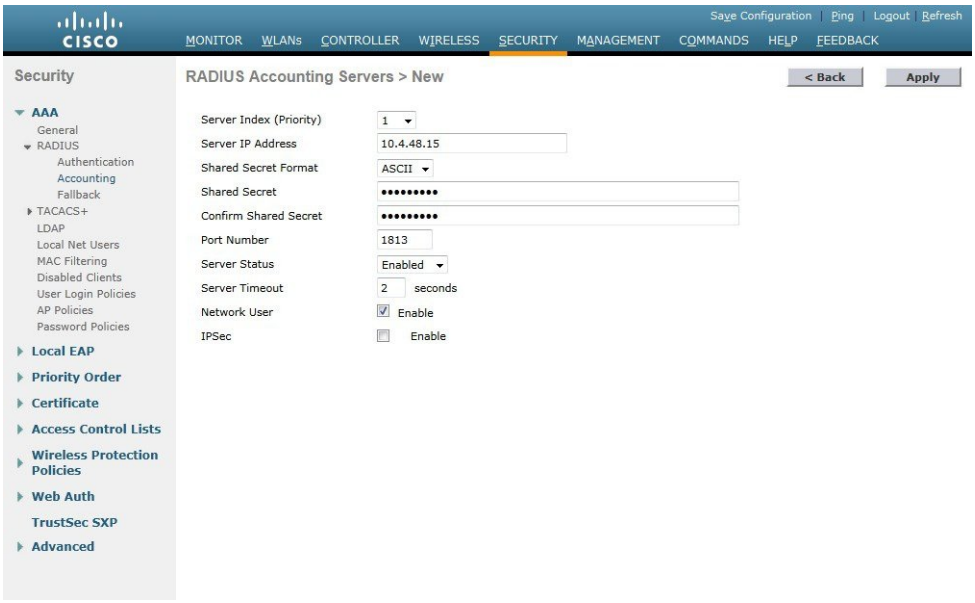
Step 4 To the right of **Management**, clear **Enable**, and then click **Apply**.



Step 5 To the right of Management, clear **Enable**, and then click **Apply**.

Step 6 Enter the **Server IP Address**. (Example: 10.4.48.15)

Step 7 Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
RADIUS Accounting Servers > New
< Back
Apply
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Advanced
Server Index (Priority) 1
Server IP Address 10.4.48.15
Shared Secret Format ASCII
Shared Secret
Confirm Shared Secret
Port Number 1813
Server Status Enabled
Server Timeout 2 seconds
Network User Enable
IPSec Enable