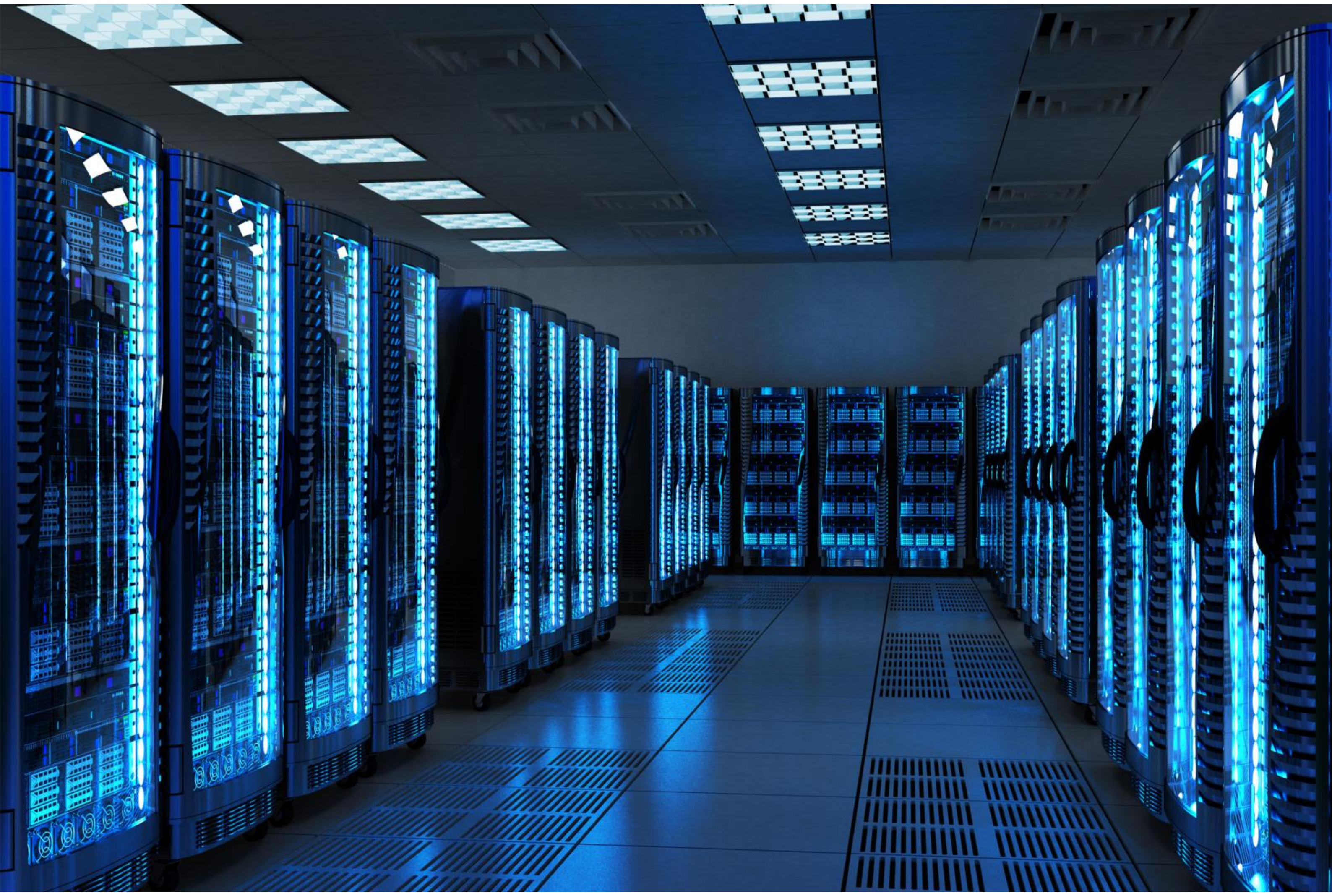


INTEGRATION GUIDE

How to Configure a Cisco Wireless Controller to Secure Your Guest Wireless Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your Cisco wireless guest environment using Portnox CLEAR to control guest user access.

Enabling CLEAR RADIUS Service

The first step is to enable the CLEAR RADIUS service.

1) Verify your organization is registered on Portnox CLEAR Cloud Services: https://clear.portnox.com/.

2) In the CLEAR portal, go to **Settings** > **Services** and expand **CLEAR RADIUS Service**. Then:

   a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.

   b. Note the RADIUS server details which you will need when configuring the Cisco WLC:

      - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Accounting port**
      - **Shared Secret** - this is the RADIUS client shared secret

Enabling CLEAR Captive Portal Service

The second step is to enable the CLEAR Captive Portal (=Guest portal).

1) In the CLEAR portal, go to **Settings** > **Services** and expand **CLEAR Captive Portal Service**. Then:

   a. If the **Enable CLEAR Captive Portal** checkbox is not checked, click **Edit** and check the **Enable CLEAR Captive Portal** checkbox.

   b. Note the following, which you will need when configuring the Cisco controller:

      - **URL**
      - **IP (for walled garden)**

Configuring the Cisco Wireless Controller

In the final step, we configure the Cisco wireless controller WLAN to control guest user access. This configuration is performed in the Cisco web interface.

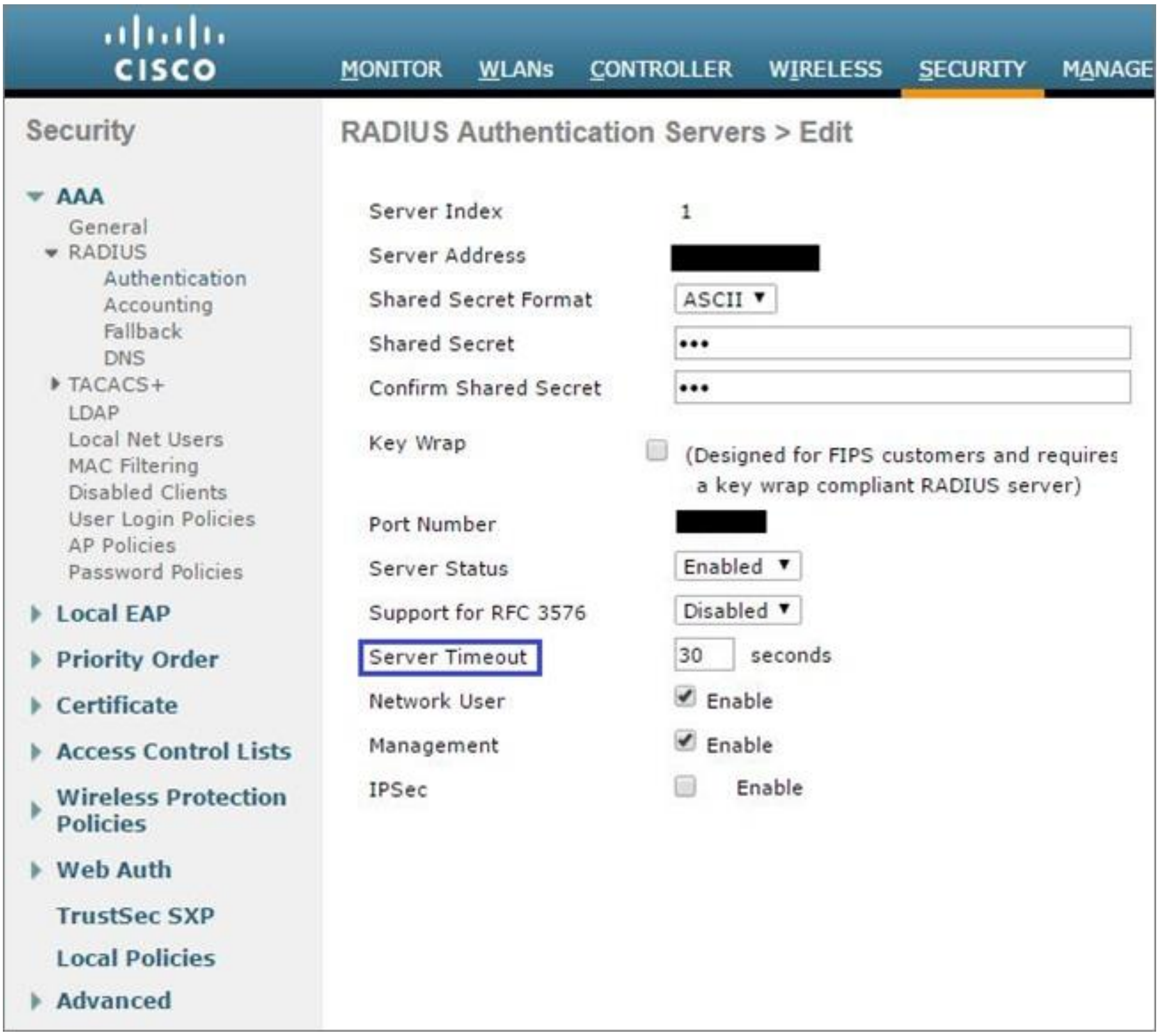
1) Navigate to **Security** > **AAA** > **RADIUS** > **Authentication** and click **New** to add a new Authentication RADIUS server.

2) In the RADIUS Authentication Servers Edit window that appears:

   a. Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step 2b:

      - In **Server Address**, enter the Cloud RADIUS IP.
      - In **Port Number**, enter the Authentication port number.
      - In **Shared Secret**, enter the Shared Secret.

   b. Set **Server Timeout** to 30 seconds



RADIUS Authentication Servers > Edit

Server Index	1
Server Address	[redacted]
Shared Secret Format	ASCII ▼
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	[redacted]
Server Status	Enabled ▼
Support for RFC 3576	Disabled ▼
Server Timeout	30 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

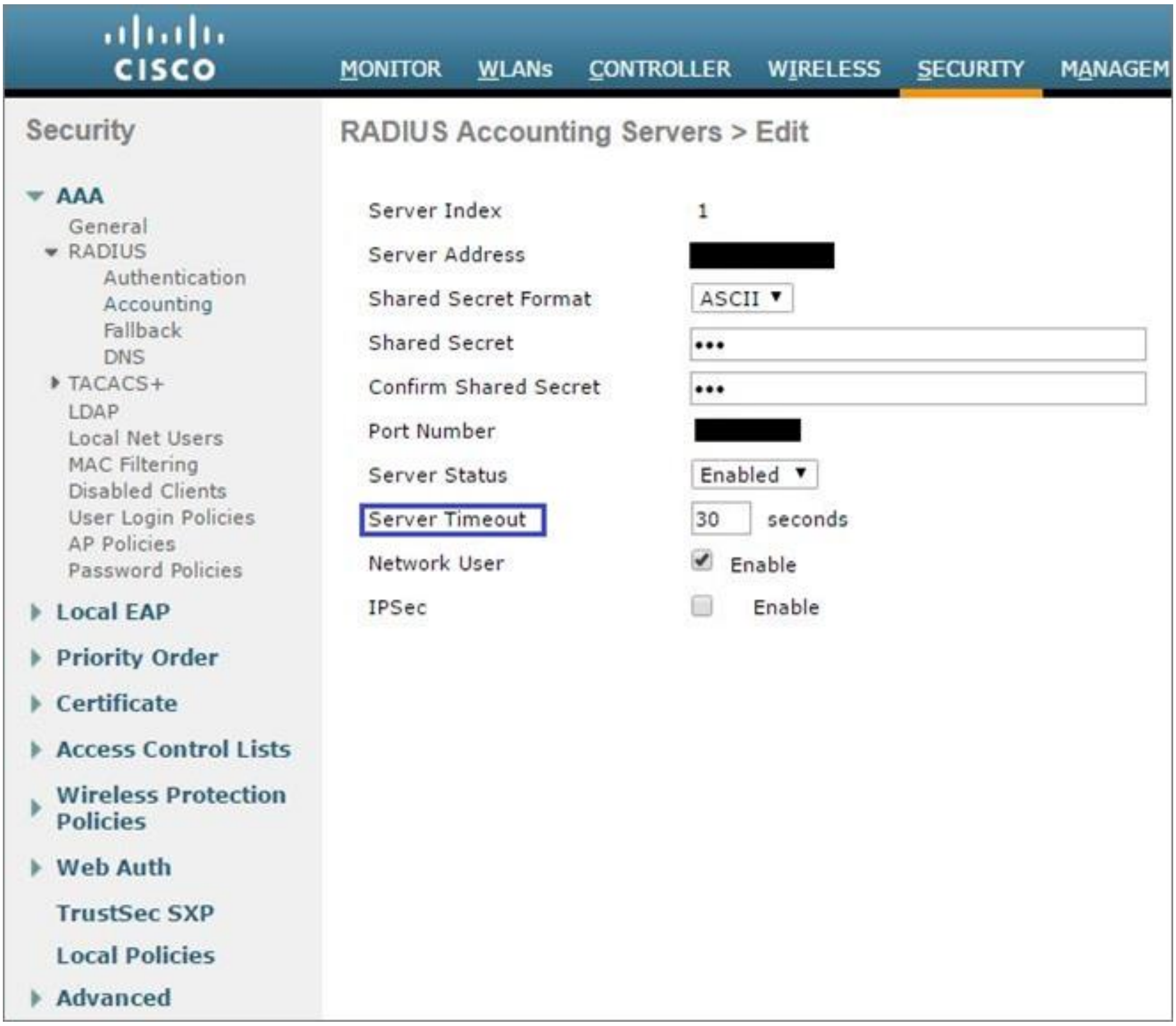
3) Navigate to **Security** > **AAA** > **RADIUS** > **Accounting** and click **New** to add a new Accounting RADIUS server.

4) In the RADIUS Accounting Servers Edit window that appears:

   a. Enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step 2b:

      - In **Server Address**, enter the Cloud RADIUS IP.
      - In **Shared Secret**, enter the Shared Secret.
      - In **Port Number**, enter the Accounting port number.

   b. Set **Server Timeout** to 30 seconds



RADIUS Accounting Servers > Edit

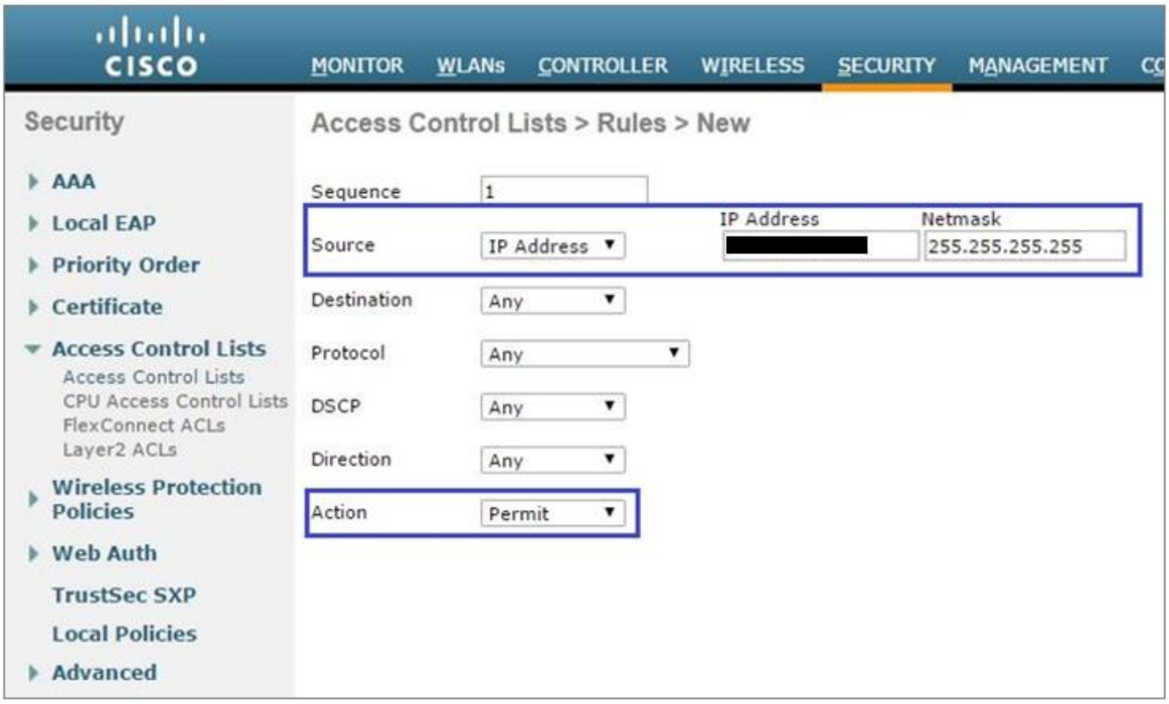
Server Index	1
Server Address	[redacted]
Shared Secret Format	ASCII ▼
Shared Secret	•••
Confirm Shared Secret	•••
Port Number	[redacted]
Server Status	Enabled ▼
Server Timeout	30 seconds
Network User	☑ Enable
IPSec	□ Enable

5) Navigate to **Security** > **Access Control Lists** and click **New** to create a new Access Control List.

6) In the Access Control List's **Rules**, click **Add New Rule** to add each of the following two rules.

   a. For the first rule:

      - In **Sequence**, enter **1**.
      - In **Source**, enter the **IP (for walled garden)** which you noted in Enabling CLEAR Captive Portal Service, step 1b.
      - In **Action**, select **Permit**.



Access Control Lists > Rules > New

Sequence: 1

Source: IP Address ▼ IP Address: [redacted] Netmask: 255.255.255.255

Destination: Any ▼

Protocol: Any ▼

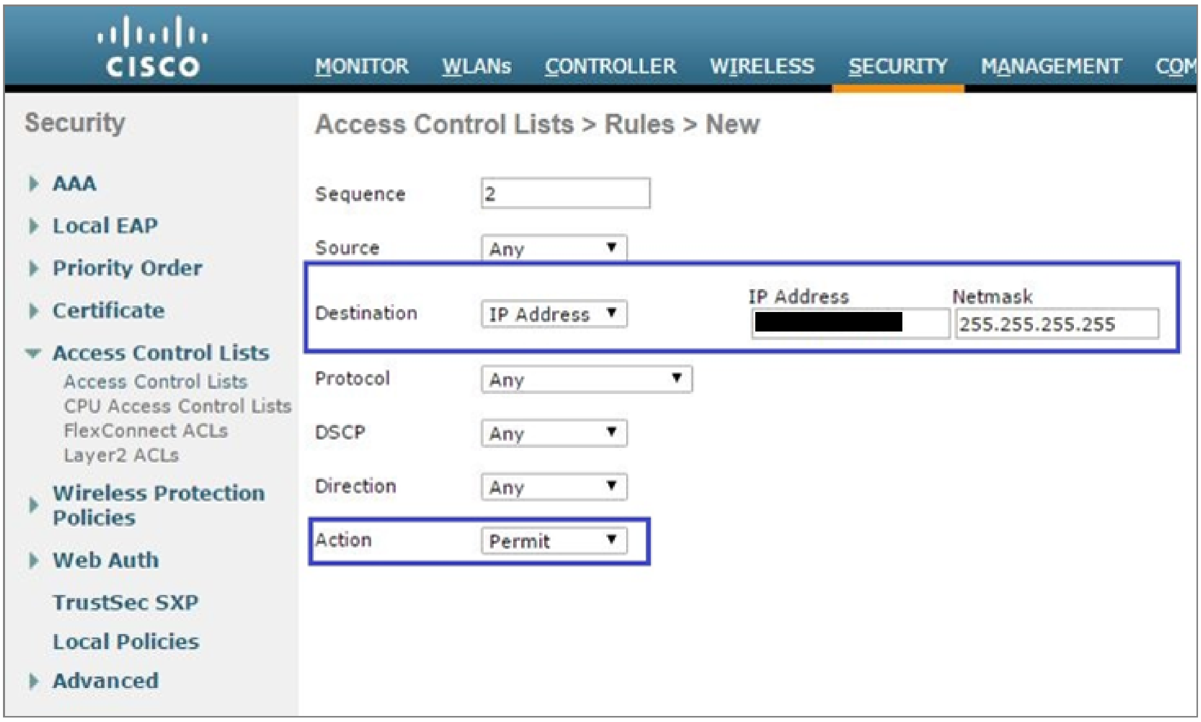
DSCP: Any ▼

Direction: Any ▼

Action: Permit ▼

b. For the second rule:

- In **Sequence**, enter **2**.
- In **Destination**, enter the **IP (for walled garden)** which you noted in Enabling CLEAR Captive Portal Service, step 1b.
- In **Action**, select **Permit**.



Access Control Lists > Rules > New

Sequence: 2

Source: Any

Destination: IP Address — IP Address: [redacted] Netmask: 255.255.255.255

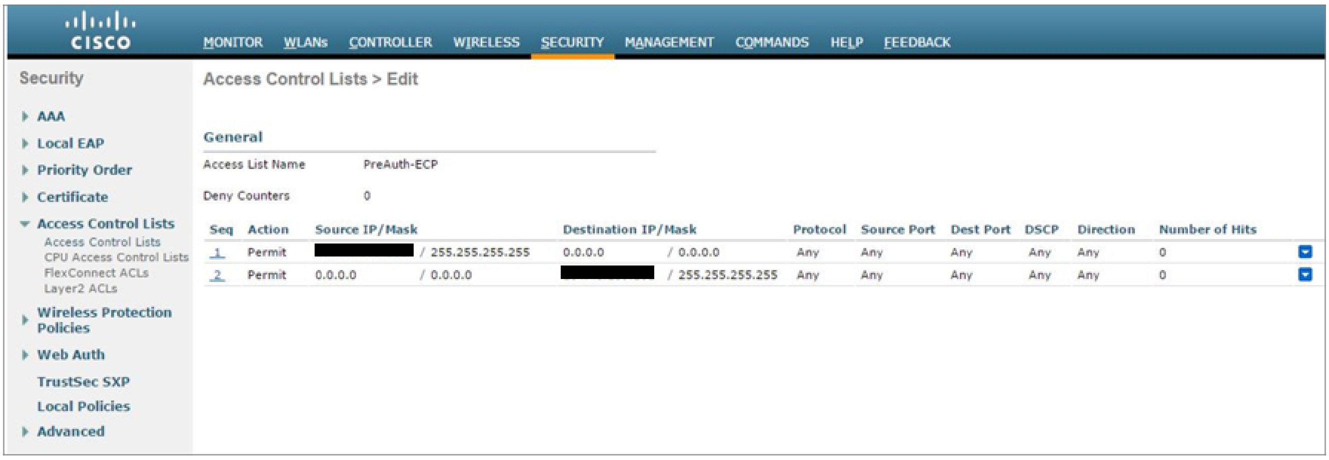
Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

c. Click **Apply**. Verify that the two rules are listed similarly to the rules shown below.



Access Control Lists > Edit

General

Access List Name: PreAuth-ECP

Deny Counters: 0

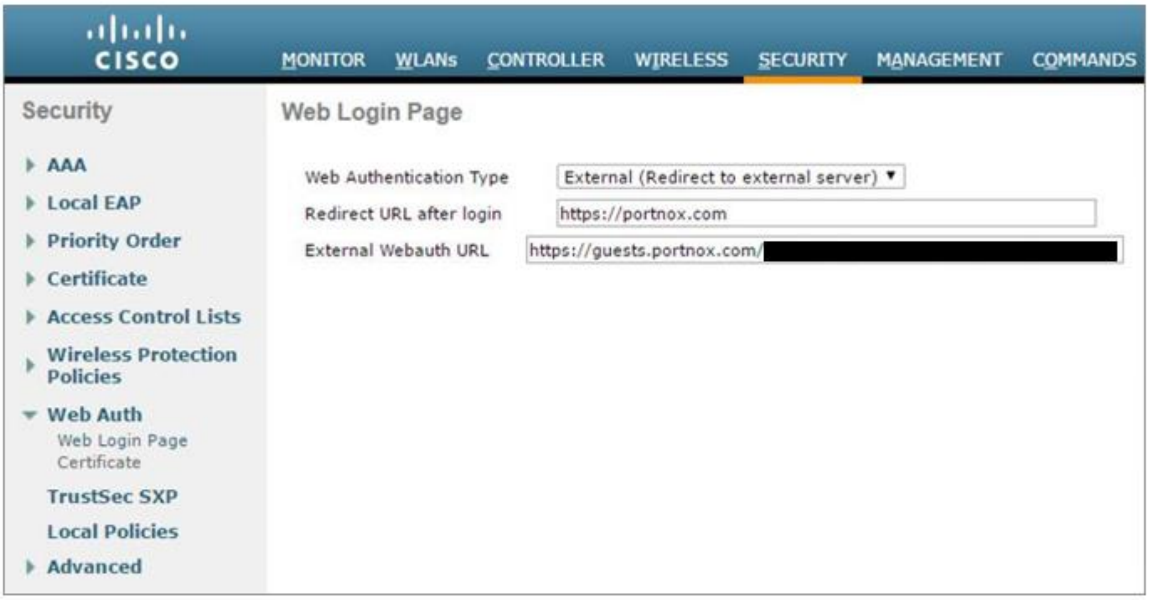
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	[redacted]	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	0
2	Permit	0.0.0.0	/ 0.0.0.0	[redacted]	/ 255.255.255.255	Any	Any	Any	Any	Any	0

7) Navigate to **Security** > **Web Auth** > **Web Login Page** and then:

   a. In **Web Authentication Type**, select **External (Redirect to external server)**.

   b. In **Redirect URL after login**, enter the URL of the page to which the user will be redirected after being successfully authenticated, or after approving the disclaimer.

   c. In **External Webauth URL**, enter the CLEAR Captive Portal Service **URL** which you noted in [Enabling CLEAR Captive Portal Service](), step 1b.



Web Login Page

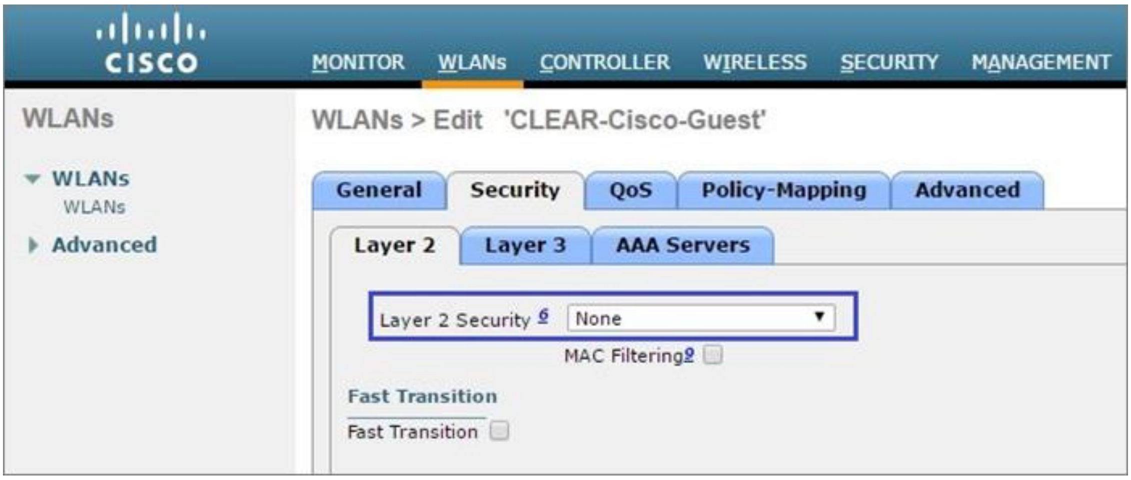
Web Authentication Type: External (Redirect to external server)

Redirect URL after login: https://portnox.com

External Webauth URL: https://guests.portnox.com/[redacted]

8) Navigate to **WLANs** and select the WLAN to be secured (or navigate to **WLANs** to create a new WLAN).

   a. Select **Security** > **Layer 2** and in **Layer 2 Security**, select **None**.



WLANs > Edit 'CLEAR-Cisco-Guest'

Layer 2 Security: None

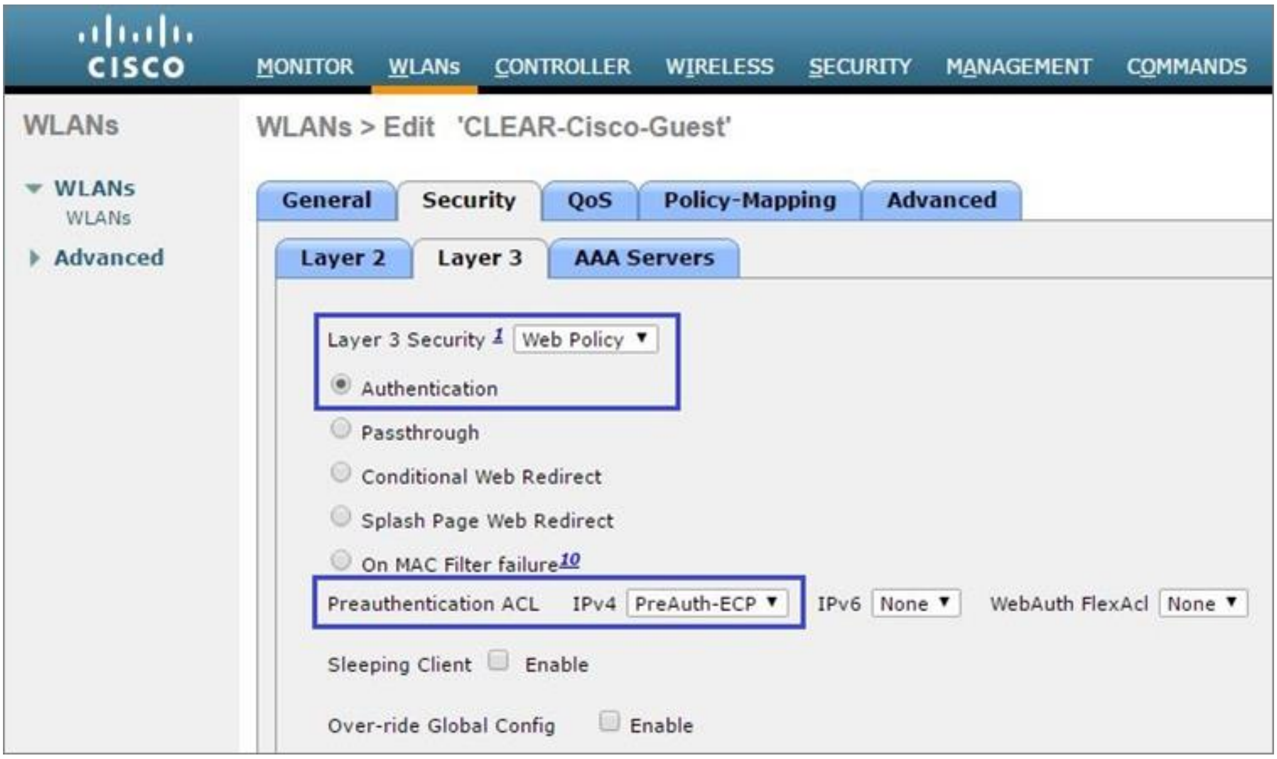
MAC Filtering □

Fast Transition □

9) Select **Security** > **Layer 3** and do the following:

   a. In **Layer 3 Security**, select **Web Policy**, and then select the **Authentication** radio button.

   b. In **Preauthentication ACL**, select the Access Control List you created in Step (5).



WLANs > Edit 'CLEAR-Cisco-Guest'

Layer 3 Security [1] Web Policy ▼

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

Preauthentication ACL IPv4 PreAuth-ECP ▼ IPv6 None ▼ WebAuth FlexAcl None ▼

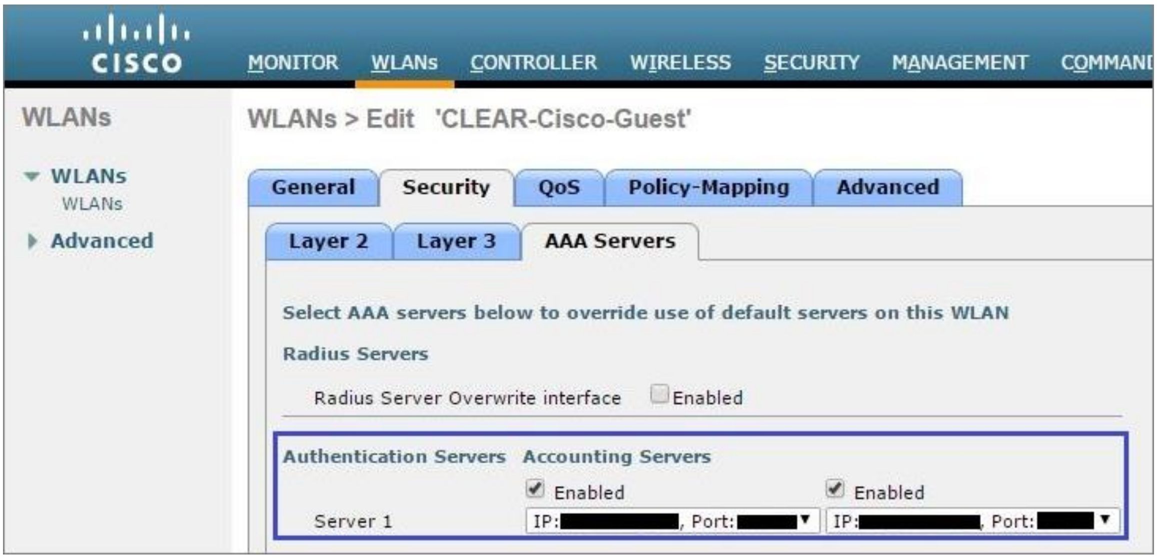
Sleeping Client □ Enable

Over-ride Global Config □ Enable

10) Select **Security** > **AAA Servers** and then:

   a. Select the RADIUS authentication server you added in Step (1).

   b. Select the RADIUS accounting server you added in Step (3).



WLANs > Edit 'CLEAR-Cisco-Guest'

Select AAA servers below to override use of default servers on this WLAN

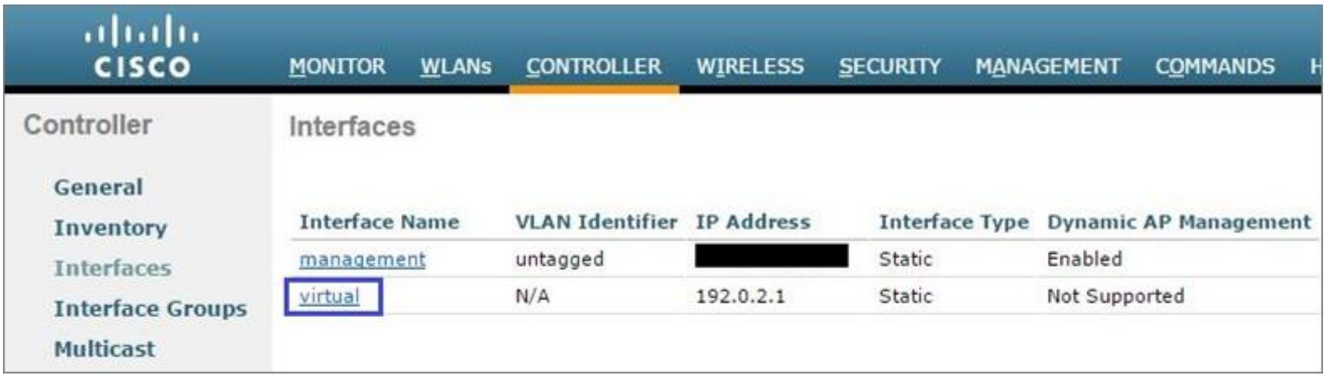
Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP: [redacted], Port: [redacted] ▼	IP: [redacted], Port: [redacted] ▼

11) Click **Apply** to apply the changes.

12) Navigate to **Controller** > **Interfaces** and select the **virtual** interface.

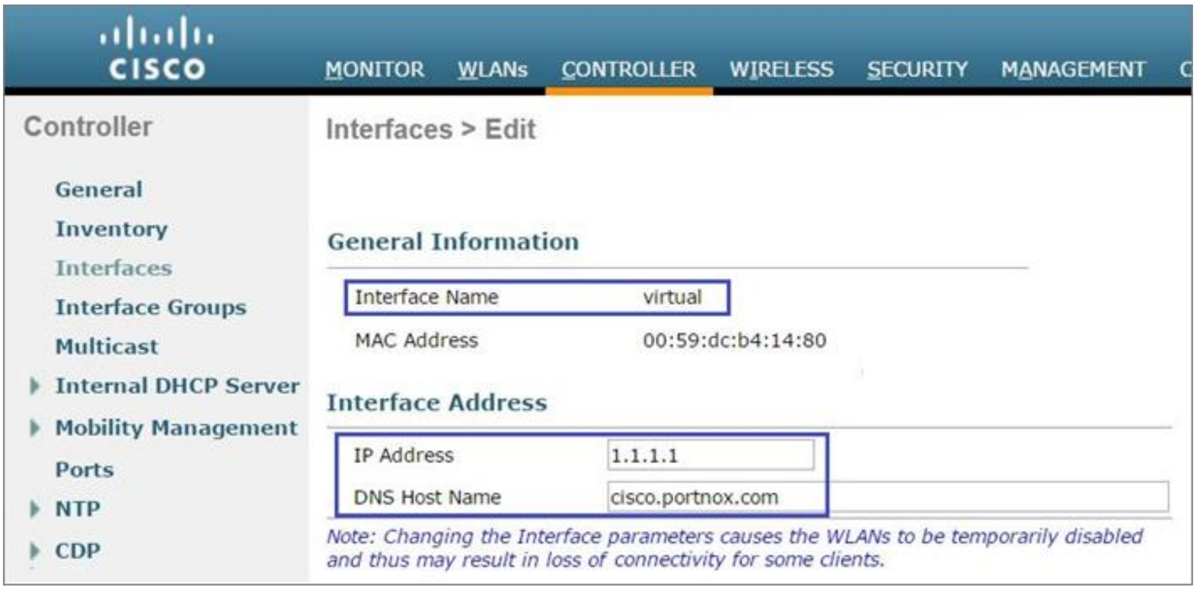


Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	[redacted]	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supported

13) Check the value in the **virtual** interface's **DNS Host Name** field:

- If a **DNS Host Name** is listed, make sure there is a DNS record for the listed Host Name, on the organizational local DNS server. (Note that this is a Cisco requirement.)
- If the **DNS Host Name** field is empty, continue to the next step.



Interfaces > Edit

General Information

Interface Name virtual

MAC Address 00:59:dc:b4:14:80

Interface Address

IP Address 1.1.1.1

DNS Host Name cisco.portnox.com

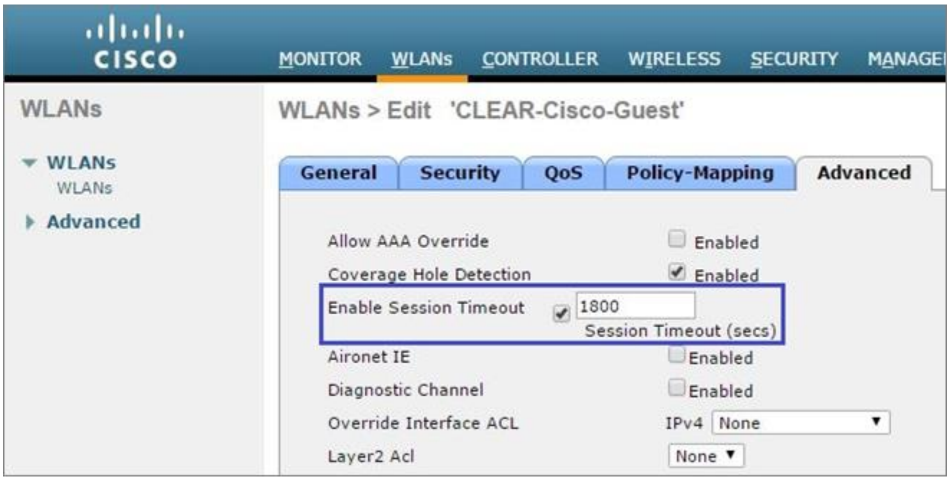
Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

14) Optionally configure the re-authentication timeout for the guest WLAN; this is the maximum time the device session remains active before requiring re-authentication.
To configure the WLAN re-authentication timeout:

a. Navigate to **WLANs**, select the relevant WLAN (= the guest wireless network to be secured), and select the **Advanced** tab.

b. In the **Advanced** tab:

- Select the **Enable Session Timeout** checkbox.
- Set the **Session Timeout** value.



WLANs > Edit 'CLEAR-Cisco-Guest'

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE □ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None ▾
Layer2 Acl None ▾