



INTEGRATION GUIDE

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

Introduction

This document guides you step by step how to configure your Meraki 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 Meraki SSID:
 - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
 - **Authentication 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 **URL**, which you will need when configuring the Meraki SSID.

Configuring the Meraki Wireless Controller

In the final step, we configure the Meraki guest wireless SSID to control guest user access.

- 1) In the Meraki portal, navigate to **Wireless > Configure > Access Control**.
- 2) In the Access Control window:
 - a. In the **SSID** drop down list, select the SSID of the wireless network to be secured (or navigate to **Wireless > Configure > SSIDs** and create a new SSID).
 - b. In **Association requirements**, select **Open (no encryption)**.

The screenshot shows the Meraki portal interface. At the top left is the Cisco Meraki logo. To the right, there is a 'Network:' dropdown menu with 'NJ' selected. On the left side, there is a navigation menu with four items: 'Network-wide', 'Switch', 'Wireless', and 'Help'. The 'Wireless' item is highlighted with a green bar. The main content area is titled 'Access control' and contains an 'SSID:' dropdown menu with 'MerakiGuest' selected. Below this, there is a section titled 'Network access' with a sub-section 'Association requirements'. This section contains four radio button options: 1) 'Open (no encryption)' with the subtext 'Any user can associate', which is selected and highlighted with a blue box. 2) 'Pre-shared key with' followed by a 'WPA2' dropdown menu, with the subtext 'Users must enter a passphrase to associate'. 3) 'MAC-based access control (no encryption)' with the subtext 'RADIUS server is queried at association time'. 4) 'WPA2-Enterprise with' followed by a 'Meraki authentication' dropdown menu, with the subtext 'User credentials are validated with 802.1X at association time' and 'Accepted EAP types cannot be inferred with this setting. They must be updated manually in any existing Systems Manager mobile settings.'

- 3) In the Access Control window, in **Splash page**, select **Sign-on with: my RADIUS server**.

Splash page

None (direct access)
Users can access the network as soon as they associate

Click-through
Users must view and acknowledge your splash page before being allowed on the network

Sign-on with my RADIUS server ▼
Users must enter a username and password before being allowed on the network

Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS. After a trial period of 25 texts, you will need to connect with your Twilio account on the [Network-wide settings](#) page.

Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier

Systems Manager Sentry enrollment ⓘ
Only devices with Systems Manager can access this network

Cisco Identity Services Engine (ISE) Authentication ⓘ
Users are redirected to the Cisco ISE web portal for device posturing and guest access

- 4) In the Access Control window, in **RADIUS for splash page**:

- a. Click **Add a server**.
- b. Enter the following CLEAR RADIUS server details, which you noted in [Enabling CLEAR RADIUS Service](#), step 2b:
 - In **Host**, enter the Cloud RADIUS IP.
 - In **Port**, enter the Authentication port.
 - In **Secret**, enter the Shared Secret.

RADIUS for splash page						
#	Host	Port	Secret	Status	Actions	
1	<input type="text" value=""/>	<input type="text" value="10000"/>	<input type="text" value="....."/>	OK	<input type="button" value="⊕"/> <input type="button" value="✕"/>	<input type="button" value="Test"/>
Add a server						

- c. Click **Save Changes**.

- 5) In the Access Control window, **Captive portal strength**, select Block all access until sign-on is complete:

Captive portal strength

- 6) Navigate to **Wireless > Splash page** and then:
- Select the relevant **SSID**.
 - In **Custom splash URL** select **Or provide a URL where users will be redirected**, and enter the CLEAR Captive Portal Service **URL** which you noted in [Enabling CLEAR Captive Portal Service](#), step 1b.

Custom splash URL	
<input checked="" type="radio"/> Or provide a URL where users will be redirected:	<input type="text" value="https://guests.portnox.com/648ab427-c00f-4d88-"/>

- 7) Click **Save Changes**.