How to Configure a Meraki Wireless Controller to Secure Your Wireless Network

LEGAL NOTICE:

Copyright © 2017 Access Layers US, Inc. (Portnox)

All rights reserved. Proprietary and confidential material.

Introduction

This document guides you step by step how to configure your Meraki wireless environment using Portnox CLEAR to ensure secure and trusted 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 switch:
      - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Accounting port** – needed for the RADIUS accounting server
      - **Shared Secret** – this is the RADIUS client shared secret

Registering the SSID in CLEAR

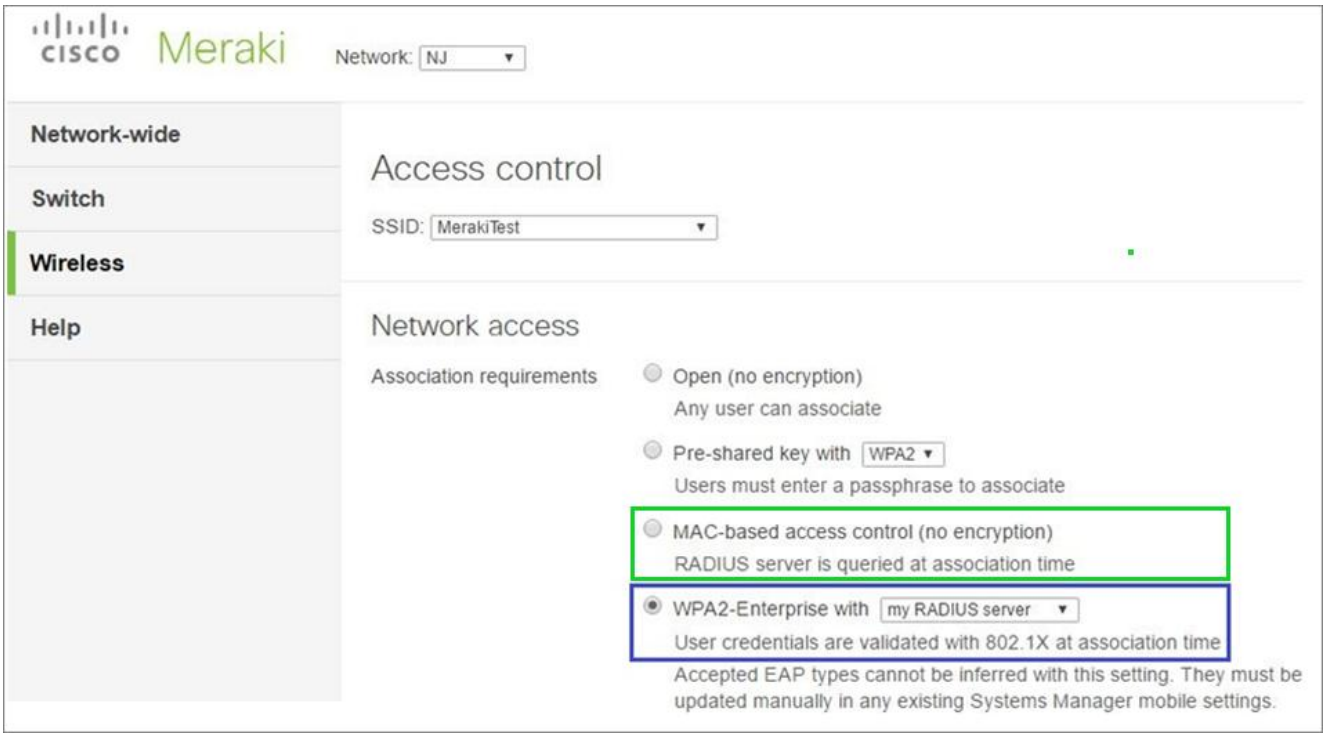
The second step is to register, in the CLEAR portal, the SSID of the wireless network you will be securing.

1) Navigate in the portal to **Settings** > **Groups**.
2) Edit the default "Unassigned" group or create a new security group.
3) Whether you are creating or editing a group, in **Group Settings** click **Add Wi-Fi network** and specify the **SSID** of the network you will be securing.

Configuring the Meraki Wireless SSID

In the following steps, we configure the Meraki wireless SSID to be secured and protected based on CLEAR RADIUS authentication.

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). Make sure this is the same SSID you entered in Registering the SSID in CLEAR, step 3.
   b. In **Association requirements**:
      - If the end-point devices support 802.1x authentication, select **WPA2-Enterprise with: my RADIUS server**.
      - If the end-point devices do not support 802.1x authentication, select **MAC-based access control (no encryption)**.

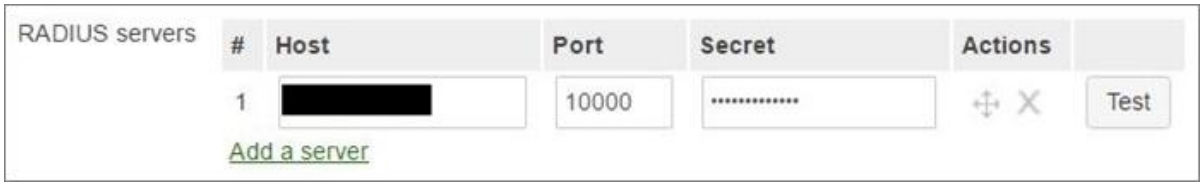


3) In the Access Control window, in **RADIUS servers**:

   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.



4) In the Access Control window, in **RADIUS accounting**:

   a. Select **RADIUS accounting is enabled**.

   b. In **RADIUS accounting servers**, click **Add a server**.

   c. 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 Accounting port.
      - In **Secret**, enter the Shared Secret.

5) In the Access Control window, click **Save Changes**.