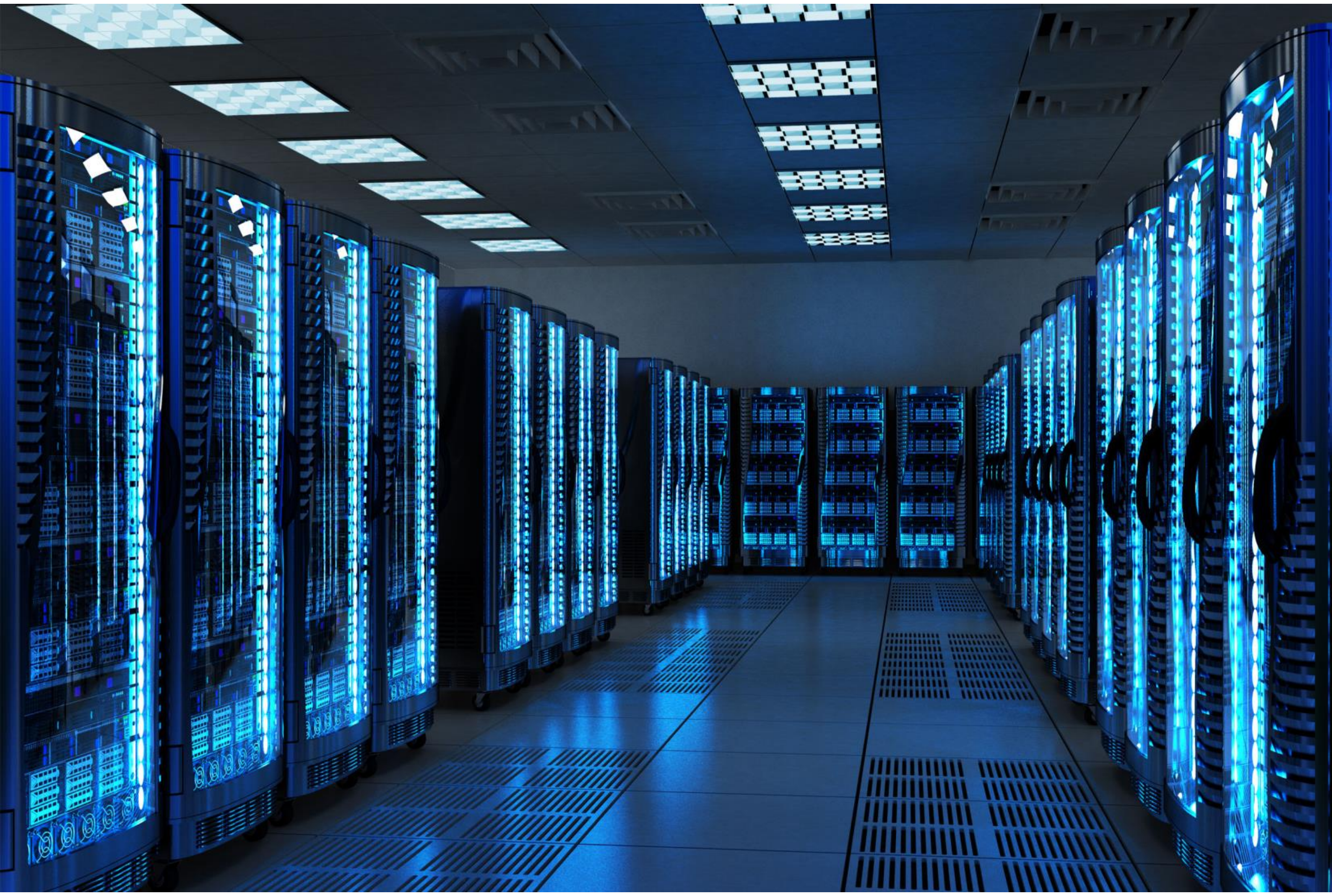


INTEGRATION GUIDE

How to Configure Meraki Z3 Teleworker to Secure your Network with Portnox CLEAR

Introduction

This document guides you step by step how to configure your Meraki Z3 Teleworker wired and 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:

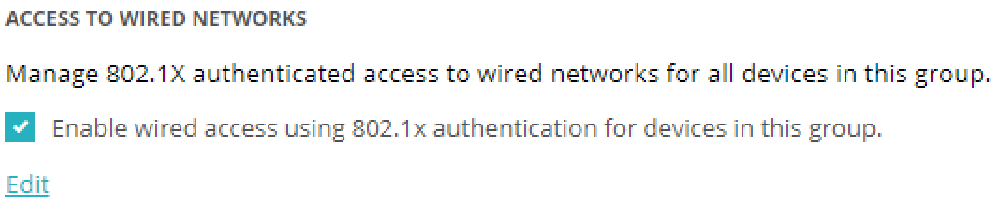
1) Verify your organization is registered on Portnox CLEAR Cloud Services: https://clear.portnox.com/.
2) In the CLEAR portal, go to **Settings** > **Services** and expand **CLEAR RADIUS Service**. Then:
   a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.
   b. Note the RADIUS server details which you will need when configuring the WatchGuard switch:
      - **Cloud RADIUS IP** - this is the IP address of the CLEAR RADIUS server
      - **Authentication port**
      - **Shared Secret** - this is the RADIUS client shared secret

Configuring the Meraki Z3 Teleworker - Wired Ports

Allow Access to Wired Networks in CLEAR

The next step is to allow, in the CLEAR portal, access to wired networks you will be securing.

1) Navigate in the portal to **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** check the **Enable wired access using 802.1x authentication for devices in this group** check box.



ACCESS TO WIRED NETWORKS

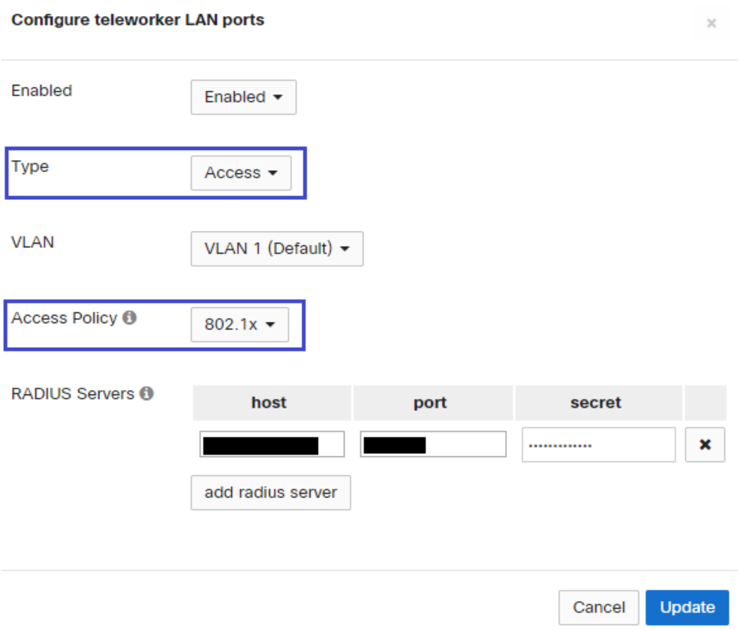
Manage 802.1X authenticated access to wired networks for all devices in this group.

☑ Enable wired access using 802.1x authentication for devices in this group.

Edit

Next, we configure the Meraki Z3 Teleworker wired ports to be secured and protected based on CLEAR RADIUS authentication:

1) In the Meraki portal, navigate to **Teleworker gateway** > **Configure** > **Addressing & VLANs**, and verify that the **VLANs** are enabled in the Routing section.
2) In the **Per-port VLAN Settings**, edit the relevant port/s:
   a. Set the **Enabled** option to Enabled.
   b. Set the **Type** to Access.
   c. Select the relevant VLAN.
   d. Select the **Access policy** type: 802.1x or MAC authentication bypass.
   e. In the Radius servers, click add radius server and enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step (2)b:
      - In **host**, enter the Cloud RADIUS IP.
      - In **port**, enter the Authentication port number.
      - In **secret**, enter the Shared Secret.



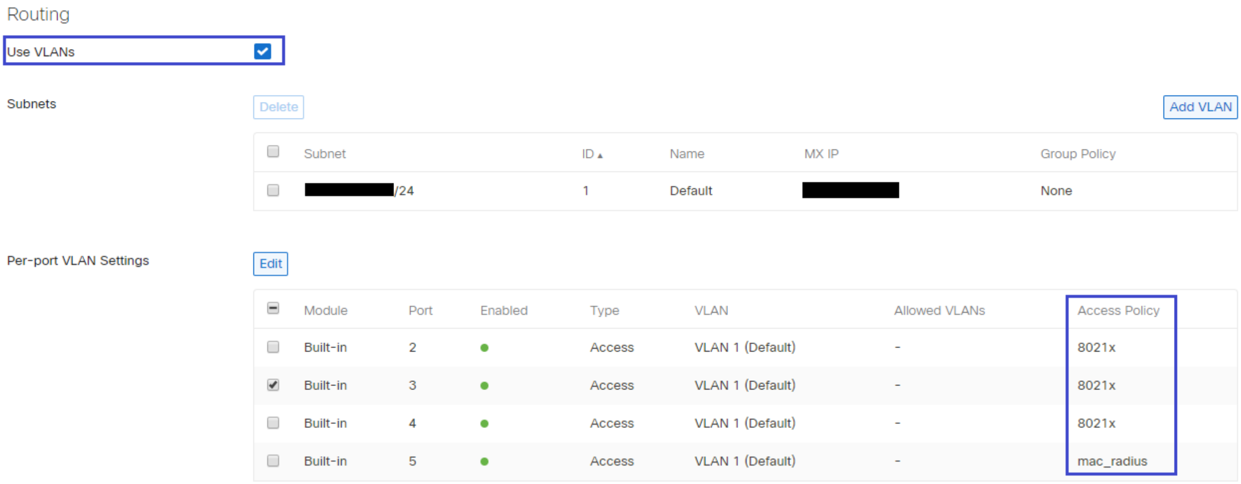
Configure teleworker LAN ports

Enabled	Enabled
Type	Access
VLAN	VLAN 1 (Default)
Access Policy	802.1x

RADIUS Servers

host	port	secret
[redacted]	[redacted]	··············

f. Click **Update**.



Routing

Use VLANs ☑

Subnets

□	Subnet	ID	Name	MX IP	Group Policy
□	[redacted]/24	1	Default	[redacted]	None

Per-port VLAN Settings

⊟	Module	Port	Enabled	Type	VLAN	Allowed VLANs	Access Policy
□	Built-in	2	●	Access	VLAN 1 (Default)	-	8021x
☑	Built-in	3	●	Access	VLAN 1 (Default)	-	8021x
□	Built-in	4	●	Access	VLAN 1 (Default)	-	8021x
□	Built-in	5	●	Access	VLAN 1 (Default)	-	mac_radius

Configuring the Meraki Z3 Teleworker - Wireless

Registering the SSID in CLEAR

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

1) Navigate in the portal to **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.

Next, we configure the Meraki Z3 Teleworker Wireless to be secured and protected based on CLEAR RADIUS authentication:

3) In the Meraki portal, navigate to **Teleworker gateway** > **Configure** > **Wireless settings**, and update the status of one of the SSIDs to **Enabled**.
4) In the **SSID settings**:

    g. Select **WPA2 Enterprise** as the **Security** type.

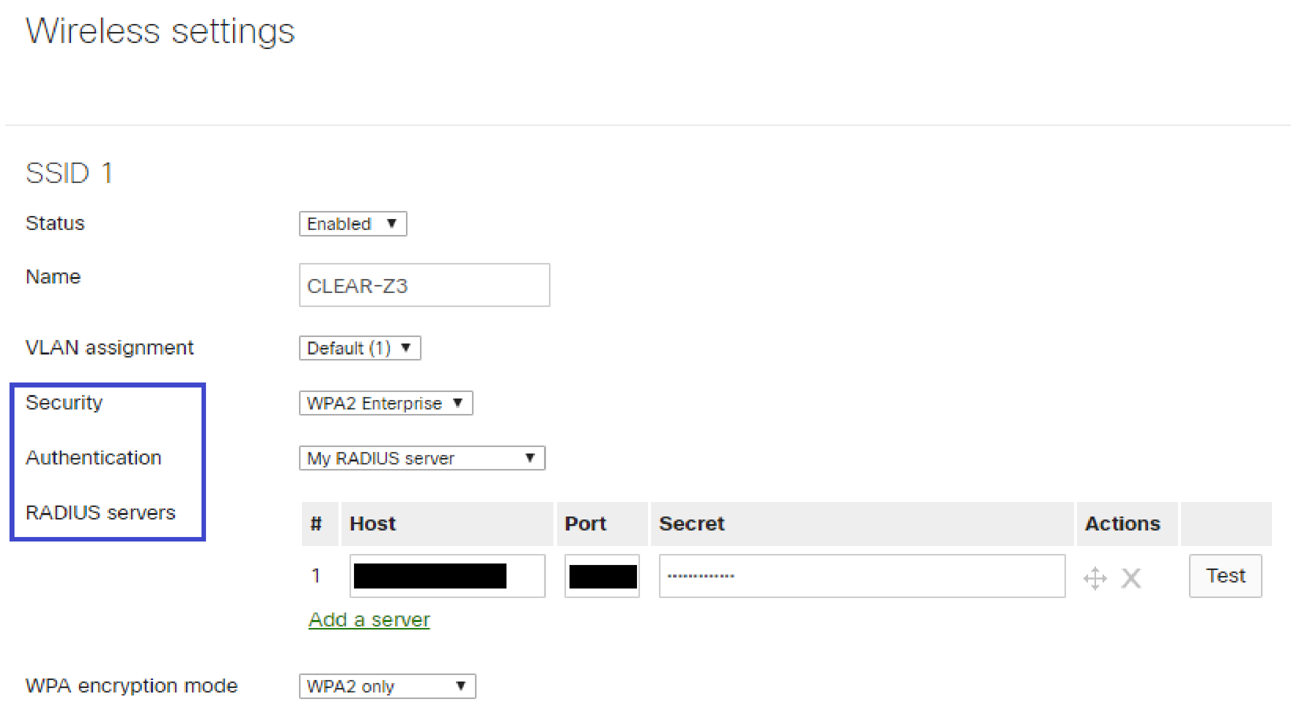
    h. Select My RADIUS server for the **Authentication**.

    i. Select the relevant VLAN.

    j. In the Radius servers, click add a server and enter the following CLEAR RADIUS server details, which you noted in Enabling CLEAR RADIUS Service, step (2)b:

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

    k. Click **Save**.



Wireless settings

SSID 1

Status: Enabled ▼

Name: CLEAR-Z3

VLAN assignment: Default (1) ▼

Security: WPA2 Enterprise ▼

Authentication: My RADIUS server ▼

RADIUS servers

#	Host	Port	Secret	Actions	
1	[redacted]	[redacted]	··············	✥ ✕	Test

Add a server

WPA encryption mode: WPA2 only ▼