Overview

MR Access points, MS Switches, and MX/Z Security Appliances (Meraki Devices) provide the ability to configure an external server for RADIUS authentication. This article outlines the general troubleshooting methodology when an issue with RADIUS troubleshooting is encountered, and provides a flow to isolate and fix the issue in a systematic manner.

For RADIUS configurations or initial setup, please look at the following articles:

- Configuring RADIUS Authentication with WPA2-Enterprise
- Configuring RADIUS Authentication with a Sign-on Splash Page
- Configuring RADIUS Authentication with Client VPN

Troubleshooting Flow for RADIUS Authentication

The following flow chart guides through the steps for isolating and troubleshooting common RADIUS authentication issues and needs to be followed from top to bottom in any given scenario. This article is outlined to solve most common RADIUS issues or to isolate the issue to a specific point in the network.
Dashboard Configuration

The first thing to verify is if the RADIUS configurations are made correctly on the dashboard. The RADIUS configurations can be accessed by navigating via the following:

**Wireless > Configure > Access Control: Select (SSID) > RADIUS Servers**

<table>
<thead>
<tr>
<th>RADIUS servers</th>
<th>#</th>
<th>Host</th>
<th>Port</th>
<th>Secret</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>192.168.128.254</td>
<td>1812</td>
<td>--------</td>
<td>Test</td>
</tr>
<tr>
<td>Add a server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Switch > Configure > Access Policies > Radius Servers**

<table>
<thead>
<tr>
<th>RADIUS servers</th>
<th>#</th>
<th>Host</th>
<th>Port</th>
<th>Secret</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>192.168.128.254</td>
<td>1812</td>
<td>--------</td>
<td>Show key Test</td>
</tr>
<tr>
<td>Add a server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Security & SD-WAN/Teleworker Gateway > Configure > Access Policies > RADIUS for Splash Page**

<table>
<thead>
<tr>
<th>RADIUS for splash page</th>
<th>#</th>
<th>Host</th>
<th>Port</th>
<th>Secret</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>192.168.128.254</td>
<td>1812</td>
<td>--------</td>
<td>Show key</td>
<td></td>
</tr>
<tr>
<td>Add a server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following parameters must be verified:

- The IP address of the RADIUS server is added correctly
- Port is configured the same on dashboard as well as the RADIUS server
- Secret is identical on the dashboard as well as the RADIUS server

**RADIUS Server Ping Test**

During a RADIUS authentication, the Meraki devices will try to reach out to the RADIUS server with RADIUS packets. In order for this to be successful, the RADIUS server should be reachable from the Meraki source. Hence, we will test the
RADIUS server reachability via the following steps:

- Navigate to the Device Status Page:
  - MR: Wireless > Access Points > Select Access Point > Tools > Ping
  - MS: Switch > Switches > Select Switch > Tools > Ping
  - MX: Security & SD-WAN > Appliance Status > Tools > Ping
  - Z-Series: Teleworker Gateway > Appliance Status > Tools > Ping

- Use the ping tool and ping the IP of the RADIUS server

- If the pings are failing, verify the routing to the RADIUS server

---

**Dashboard RADIUS Test Tool**

The dashboard configuration provides a test tool to verify the connectivity with the RADIUS Server as shown above. Clicking on “Begin test” with the RADIUS credentials can result in either “Test = Pass” or “Test = Fail”. The test tool triggers a RADIUS Access-Request/Challenge exchange using EAP-PEAP with MS-CHAPv2 between the APs and the RADIUS server. It is designed to confirm that the server is reachable from the APs and that the credentials supplied are valid only. If using an EAP type that requires a client-side certificate such as EAP-TLS, the test will fail because the AP does not have the certificate installed. It is recommended to test with a real client device. MR access points support the EAP types listed [here](#).

**Test = Pass**

If the Dashboard RADIUS test passes, the following steps can be looked into:

- When the test passes, the RADIUS server is reachable and is configured for authentication. If a client is unable to connect, check if the client device is generating an EAP session.

- Check the logs that will be generated on the RADIUS server after a failed client authentication.
Test = Fail

If the RADIUS server is ping-able but the test is failing, continue ahead with the Dashboard Packet Captures.

Dashboard Packet Captures

The Meraki Dashboard provides the ability to take packet captures directly on all RADIUS-capable Meraki devices in the network. This feature can be accessed by navigating to Network Wide > Monitor > Packet Capture.

The packet capture must be taken on the wired interface of the Meraki device through which the RADIUS server can be reached, and it is highly recommended to download the output as a .pcap file for Wireshark.

Once a packet capture is initiated, have a failed client attempt to connect to RADIUS again and let the packet capture run while this process is being completed. The packet capture can be opened in Wireshark and a filter can be applied as shown below:

Wireshark Filter for RADIUS:

Eg: ip.addr==192.168.128.254 && radius (192.168.128.254 is the IP of the RADIUS server)

A generic filtered RADIUS packet capture is shown below for reference:
The above screenshot is for a successful RADIUS authentication, as you can see bi-directional communication with Access-Requests, Access-Challenges and Access-Accept. A sample packet capture can be downloaded for reference.

RADIUS traffic flow

In case of a RADIUS authentication failure, the traffic flow would be different and one of the 3 possible outcomes shown below might be observed:

- **No RADIUS protocol traffic**
- **Unidirectional Access-Requests**
- **RADIUS server sending Access-Reject**

**No RADIUS Protocol traffic**

With the Wireshark filter mentioned above, only the RADIUS traffic will be filtered in the output and if there is no RADIUS protocol traffic being sent out to the RADIUS server from the Meraki devices, the output will be empty. If there is traffic seen, make sure to verify the username to make sure the traffic has been seen for the correct client device.

In case of no RADIUS protocol traffic seen from the Meraki device, follow the steps below:
• Verify if the client is attempting to connect to the correct SSID or port and generating an EAP session.

• Verify the configurations on the client device to make sure they match with the requirements for RADIUS authentication.

• Take a wireless or wired packet capture on the client device to check if the traffic is being sent out of the client device.

• After confirming that the client device is sending the required traffic, if the authentication fails, take another packet capture and follow the flow chart.

When a client generates an EAP session and sends traffic to a Meraki device, the Meraki device will forward an Access-Request to the RADIUS server.

**Unidirectional Access-Request(s)**

If the client device is generating EAP session traffic and we see unidirectional Access-Requests in the packet capture, the RADIUS authentication will fail as the responses were not received from the server. This can be an outcome due to multiple failure reasons as listed below:

• **SSID Tag and VLANs:**
  - Make sure the SSID is not being VLAN tagged for the native VLAN as the native VLAN is supposed to be untagged.
  - If the SSID is tagged with a specific VLAN, make sure the VLAN is allowed on the L2 network for a successful communication with the RADIUS server.

• **Routing to RADIUS server:**
  - Because the Access-Requests are being sent to the RADIUS server and no responses are noticed, the traffic might be getting dropped before reaching the RADIUS server.
  - If the pings are successful, you would need to verify where the RADIUS traffic is being dropped and fix the routing.

• **RADIUS services:**
  - If the routing is correct and the RADIUS packets are being delivered to the RADIUS server, you would need to verify if the RADIUS services are turned ON on the RADIUS server.

• **RADIUS clients:**
  - If the EAP session traffic being generated by a client is not authorized in the RADIUS server configurations, the RADIUS server will drop the packets.
  - Make sure the Meraki device is added as a RADIUS client and is authorized.
Once these settings and configurations are verified and correct, and if the authentication is still failing, take another packet capture and follow the flow chart.

**RADIUS Server Responds with Access-Reject**

Once the Access-Request is received by the RADIUS server, it can either send an Access-Accept to authenticate the client or send a Access-Reject to deny authentication.

If an Access-Reject is received from the RADIUS server, there are multiple possible reasons, some of which are listed below:

- **No certificate installed on the RADIUS Server or the certificate has expired**
  - Verify if the digital certificate installed on the RADIUS server is still valid.
  - If the certificate has expired or is missing, a renewal or an installation of the digital certificate would be needed.

- **Incorrect Username or Password**
  - If a client logs in using incorrect credentials (username or password or both), the RADIUS server will deny the authentication using an Access-Reject.

- **Incorrect Secret on the Dashboard**
  - The secret configured in dashboard should match the secret key added on the RADIUS server while configuring the RADIUS clients.

There are some factors that can cause the RADIUS server to deny an authentication and some of them are listed below:

- Network Policy is misconfigured
- Connection Request Policy is misconfigured
- Mismatch in Authentication Settings
- Root Certificate is not added to the client device(s)

In order to read about these factors, refer to the [2008 Windows NPS Server RADIUS logs](#) for reference.

**RADIUS Traffic Verification**

Once the mentioned steps are verified and the configurations are as required, another packet capture can be taken using the [Dashboard Packet Capture](#) tool, and the RADIUS traffic flow can be verified.
At this point, the client should get authenticated and we should see the server sending the client an Access-Accept message. If the server still sends an Access-Reject, it is most likely a server issue and you would need to access the RADIUS server to verify the logs that are generated.