Configuring RADIUS Authentication with a Sign-on Splash Page

The Cisco Meraki MR Access Points and MX Security Appliance allow a Splash Page to be configured, requiring users to interact with this captive portal before being granted network access. One configuration option for this Splash Page is to allow authentication with an existing RADIUS server on the network, so users must enter their domain credentials to get through the Splash Page.

This article outlines the Dashboard and RADIUS configuration steps to use a RADIUS server with a sign-on Splash Page.

Supported RADIUS Attributes

When a sign-on Splash Page is configured with RADIUS server, authentication is performed using PAP. The following attributes are present in the Access-Request messages sent from Dashboard to the RADIUS server.

- **User-Name**
- **User-Password**
- **Called-Station-ID**: Contains (1) the MAC address of the Meraki access point (all caps, octets separated by hyphens) and (2) the SSID on which the wireless device is connecting. These 2 fields are separated by a colon. Example: "AA-BB-CC-DD-EE-FF:SSID_NAME".
- **Calling-Station-ID**: Contains the MAC address of the wireless device (all caps, octets separated by hyphens). Example: "AA-BB-CC-DD-EE-FF".
- **Acct-Session-ID**
- **Framed-IP-Address**
- **NAS-Identifier**
- **NAS-IP-Address**
- **NAS-Port-Id**
- **NAS-Port-Type**
- **Service-Type**

The following attributes are honored by Cisco Meraki when received in an Access-Accept or Access-Reject message from the RADIUS server to Dashboard:

- **Session-Timeout**: This is the maximum time in seconds that the given user’s session will last. After that time, the user will need to log in (authenticate) again using their username and password. Only used in Access-Accept packets.
- **Idle-Timeout**: This is the idle timeout in seconds. If the user does not transfer any data on the network for this amount of time, the user’s session will end and they will need to log in (authenticate) again using their username and password. Only used in Access-Accept packets. This attribute is ignored if RADIUS accounting is not enabled.

Note: Please refer to RFC 2865 for details on these attributes, additional notes for certain attributes are included below.
on the network.

- **Maximum-Data-Rate-Upstream / Maximum-Data-Rate-Downstream**: These are used to impose bandwidth limits, only used in Access-Accept packets. The values are the maximum rate in bits/second. See [RFC 4679](https://rfc-editor.org): vendor-specific (set Vendor-Id 3561). If these values are not present, Dashboard will use the Bandwidth limits that the user set on the Dashboard traffic shaping page as a default. If these values are set to '0', Dashboard will set the Bandwidth limit to unlimited.

  **Note**: Maximum-Data-Rate-Upstream and Downstream must be specified in separate RADIUS vendor-specific attributes - if both values are specified in a single attribute, Dashboard will not honor them.

- **Filter-Id**: This attribute can be used to convey a group policy that should be applied to a wireless user or device. The attribute type should match that which is configured under the Configure tab > Group policies page in the Cisco Meraki Cloud Controller. The attribute value should match the name of a policy group configured on that page.

- **Reply-Message**: This is a message for the user that will be displayed inline on the splash page. It is allowed in Access-Accept and Access-Reject messages, but will only be shown to the user in the case of Access-Reject messages.

  **Note**: Matching the Filter-Id RADIUS attribute with a Group Policy for sign-on splash is currently only for the MR and is in beta - please contact support to have it enabled for your networks.

---

### Dashboard Configuration

The following instructions explain how to configure an SSID with a Splash Page using a local RADIUS server:

1. In Dashboard, navigate to **Wireless > Configure > Access Control**.
2. Select the desired SSID from the **SSID** drop-down menu.
3. Set the **Association requirement** to **Open (no encryption)**.
4. Under **Splash page**, select **Sign-on with** and choose **my RADIUS server** from the drop-down menu:

   ![Splash page options](image)

   - **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.

5. (optional) For **Captive portal strength**, choose **Block all access until sign-on is complete**.
6. (optional) For **Walled garden**, choose **Walled garden is disabled**.
7. Under **RADIUS for splash page**, click **Add a server**.
8. Enter the following information:
   - **Host** - Public IP address of the RADIUS server.
9. Read the instructions outlined in the IP addresses section and make adjustments to network firewalls if necessary. Make sure to take note of the RADIUS client IPs listed under Help > Firewall Info.

Testing RADIUS from Dashboard

Dashboard has a built-in RADIUS test utility, to ensure that all access points (at least those broadcasting the SSID using RADIUS) can contact the RADIUS server:

1. Navigate to Wireless > Configure > Access control.
2. Under RADIUS servers, click the Test button for the desired server.
3. Enter the credentials of a user account in the Username and Password fields.
4. Click Begin test.
5. The window will show progress of testing from each access point (AP) in the network, and then present a summary of the results at the end.
   - APs passed: Access points that were online and able to successfully authenticate using the credentials provided.
   - APs failed: Access points that were online but unable to authenticate using the credentials provided. Ensure the server is reachable from the APs, the APs are added as clients on the RADIUS server.
   - APs unreachable: Access points that were not online and thus could not be tested with.

RADIUS Configuration

While any RADIUS server can be used, the following configuration requirements are necessary for use with a sign-on Splash Page:

- RADIUS must be configured to allow PAP (unencrypted authentication) as the authentication method when you are using the Sign-on Splash page feature with a customer hosted RADIUS server.
• With PAP, user credentials are sent in plain text. However, in a Meraki network, user credentials are encrypted in an SSL tunnel when sent from the clients web browser to the Meraki Cloud.

• The Meraki Cloud acting as the RADIUS client sends the username and password along with other connection specific data in a RADIUS Access-request to the RADIUS server you specified in Dashboard. For security, the Meraki Cloud encrypts the password using the RADIUS shared secret and an XOR function. This ensures the users password is never transmitted in plain text.

Note: Communication between the client and Dashboard is done through the Splash Page, which is encrypted using SSL.

• Dashboard's IP addresses must be configured on the server as RADIUS clients/authenticators, with a shared secret. These IP addresses can be gathered in Dashboard from Help > Firewall Info.

Please refer to your RADIUS server vendor's documentation for configuration specifics.

Example RADIUS Server Configuration (Windows NPS + AD)
The following example configuration outlines how to configure an existing Windows 2008 server, running Network Policy Server (NPS) alongside Active Directory:

1. Add Dashboard as a RADIUS Client.
2. Configure a RADIUS Network Policy.

Adding Dashboard as a RADIUS Client in NPS
Since access request messages for a sign-on Splash Page are sourced from Dashboard, NPS must be configured to allow incoming requests from Dashboard's IP addresses:

1. From the desktop of your Windows 2008 server, click Start > Administrative Tools.
2. Click on Network Policy Server when it appears in the list.
3. In the **Network Policy Server** console, navigate to **NPS -> RADIUS clients and Servers -> RADIUS clients**.

4. Right click **RADIUS clients** and select **New RADIUS client**.
5. Fill out the fields in the **New RADIUS Client** window.

   - **Friendly name:** Unique identifier for this client.
   - **IP address:** The IP ranges used by Dashboard (gathered in step 9 of Dashboard configuration)
   - **Shared Secret:** Secret configured in the RADIUS server value in Dashboard (used in step 8 of Dashboard configuration). This needs to be the same for each RADIUS client you add.

![Meraki Cloud Controller 1 Properties](image)

6. Click **OK**.

7. Repeat these steps for each of Dashboard's IP addresses, as specified on the Access control page in Dashboard:
Configure a RADIUS Network Policy in NPS

The following instructions explain how to configure a network policy in NPS, that will allow

1. From the **Network Policy Server** console navigate to **NPS > Policies > Network Policies**.
2. Right click **Network Policies** and select **New**.
3. On the **Specify Network Policy Name and Connection Type** create a **Policy name** and verify **Unspecified** is selected in the "Type of network access server:" drop down.
4. Click **Next**.
5. On **Specify Conditions** click **Add** and append **Windows Group > Domain Users** group from the Windows Active Directory domain, then click **OK**.
6. Click **OK**, Review the conditions, then click **Next**.
7. On **Specify Access Permission** select **Access granted** and click **Next**.
8. On **Configure Authentication Methods** make sure **Unencrypted authentication (PAP,SPAP)** is the only method checked and click **Next**.
9. Click **No** when presented when the **Connection Request Policy** help pop-up appears.
10. Click **Next** on **Configure Constraints**.
11. On **Configure Settings** find the section **Network Access Protection**, select **NAP Enforcement**.

12. For **Auto Remediation** un-check the box **Enable auto remediation on client computers** and click **Next**.

13. On **Completing New Network Policy** click **Finish**.

14. Prioritize the policy by Right-clicking the policy you created and selecting **Move up**, placing the policy above any existing deny policies.

15. Review the policy values in the right side of the console:

<table>
<thead>
<tr>
<th>Conditions - If the following conditions are met:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
</tr>
<tr>
<td>Windows Groups</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings - Then the following settings are applied:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setting</strong></td>
</tr>
<tr>
<td>Extended State</td>
</tr>
<tr>
<td>Ignore User Dial-In Properties</td>
</tr>
<tr>
<td>Access Permission</td>
</tr>
<tr>
<td>Authentication Method</td>
</tr>
<tr>
<td>NAP Enforcement</td>
</tr>
<tr>
<td>Update Noncompliant Clients</td>
</tr>
<tr>
<td>Framed-Protocol</td>
</tr>
<tr>
<td>Service-Type</td>
</tr>
</tbody>
</table>

**Error: The Meraki Cloud is having difficulty connecting to your RADIUS server**

When Sign-on Splash-page is used with a RADIUS server, Dashboard must be able to communicate with the RADIUS server. Dashboard, which acts as the RADIUS client, sends authentication requests (RADIUS Access Requests) to the public IP address of the configured RADIUS server.

The source IP addresses used by Dashboard may change over time. As a precaution, Dashboard periodically tests the configured RADIUS server to verify accessibility. Specifically, Dashboard sends an Access-Request message with ‘meraki-ping’ as the username and ‘ping-test’ as the password. If the RADIUS server replies with an Access-Accept or Access-Reject, Dashboard knows the server is reachable.

In the event that Dashboard does not receive a response after 6 attempts (one every 20 seconds), it will assume the RADIUS server is unreachable and an email will be sent to the Dashboard administrator.

If you received this email, please verify the following:
1. If the RADIUS server is protected by a firewall, ensure that Dashboard is able to access the server through the firewall using the IP addresses and port number specified in the email. A current list of IP addresses and the port number can be found in Dashboard on the Help > Firewall Info page.

2. Dashboard’s IPs must be configured as RADIUS clients on the RADIUS server using the same shared secret configured in Dashboard.

3. Ensure there are no additional restrictions on the RADIUS server that would prevent it from responding to Dashboard as the test Access-Request will not contain all attributes (such as Calling-Station-ID), see below for an example message.

---

**RADIUS Accounting with a Sign-on Splash Page**

RADIUS accounting can be used with RADIUS authenticated splash pages to provide information regarding when a client was authorized through the splash page, and later had that authorization cleared/expired. These messages are sent from Dashboard to the customer's configured RADIUS server.

- **Note:** RADIUS accounting is only available by default with 802.1X authentication. To enable RADIUS accounting for splash page as well, please contact Cisco Meraki support. RADIUS accounting is not currently available on Splash Pages for Security Appliances nor Teleworker Gateways.

**Accounting Overview**

When RADIUS accounting is enabled, RADIUS ‘start’ accounting messages will be sent whenever a client is authorized through the splash page. These start messages are sent from Dashboard, typically from the same IP address as used for the authentication Access-request message. A ‘stop’ accounting message is generated when the client’s splash authorization is manually cleared or expires based on the splash frequency.

The screenshot below shows a Wireshark packet capture of an example RADIUS ‘start’ message sent by Dashboard (using an IP address of 74.50.53.101) to a RADIUS server. When the RADIUS message is expanded, there are many parameters that show the information contained within the ‘start’ message. Some data has been obfuscated for security reasons.
The screenshot below shows a wireshark packet capture of a RADIUS accounting 'stop' message sent by Dashboard because the Splash frequency time of 30 minutes was reached. This means the client has to log in again through the Splash Page to continue using the network.
The following instructions outline how to enable RADIUS accounting for a sign-on Splash Page:

1. In Dashboard, navigate to Wireless > Configure > Access Control.
2. Select the SSID currently configured to use RADIUS with a sign-on Splash Page.
3. Further down the page, set RADIUS accounting to RADIUS accounting is enabled.

4. In the RADIUS accounting servers section, click Add a server and provide the following details:
   - Host - Public IP address of the RADIUS accounting server.
   - Port - UDP port that the RADIUS server listens on for accounting messages, typically 1813.
   - Secret - RADIUS client shared secret.

Note: If this option is not available, please contact Cisco Meraki Support to have accounting enabled.
Data-Carrier Detect (DCD)

When enabling RADIUS accounting on a sing-on splash page with my RADIUS server, the option Enable data-carrier detect becomes available. If data-carrier detect is enabled, sessions will be revoked and accounted for whenever a client disassociates from a network. To allow clients to re-associate to the network without re-authorization, do not enable data-carrier detect. See also RFC 2866 Section 5.10.

Additional Resources

For more information on RADIUS and Splash Pages, please refer to the following documentation:

- Common Wireless RADIUS Configuration Issues
- Customizing the Splash Page