MS Switch Access Policies (802.1X)

Cisco Meraki MS switches offer the ability to configure access policies, which require connecting devices to authenticate against a RADIUS server before they are granted network access. These access policies are typically applied to ports on access-layer switches, to prevent unauthorized devices from connecting to the network.

This article outlines what options are available for access policies, how to configure access policies in Dashboard, and configuration requirements for RADIUS servers.

![As of MS 9.16, changes to an existing access policy will cause a port-bounce on all ports configured for that policy.]

**Host Modes**

![Support for all host modes is now available in MS 10.12.]

There are four authentication host modes to choose from:

- **Single-Host (Default)**
  With single-host authentication, a connected device will attempt authentication and if it fails to authenticate, the client will be denied access. This mode is recommended for switchports with only one client attached. If multiple devices are connected to the same switchport (for example a device connected via a hub or daisy-chained off of a VoIP phone), only one client will be allowed network access upon successful authentication. All subsequent authentication requests from other clients will be ignored and they will not be granted access as a result.

- **Multi-Domain**
  With multi-domain authentication, one device can be authenticated on each of the data and voice VLANs; if a second device is detected on one of the VLANs, the device will not be granted access. In this mode, Hybrid Authentication is used and Voice VLAN authentication is required. This mode is recommended for switchports connected to a phone with a device behind the phone. Authentication is independent on each VLAN and will not affect the forwarding state of each other.

  Cisco Meraki switches require the following attribute pairs within the Access-Accept frame to put devices on the voice VLAN:

  - Cisco-AVPair
- device-traffic-class=voice

- **Multi-Auth**
  With multi-auth, each connected device is required to authenticate. Multiple devices may be connected to each port. After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port. Only one client is supported on the voice VLAN. Guest VLANs are not supported in this mode.

- **Multi-Host**
  With multi-host, a single successful authentication will put the port into a forwarding state. All subsequent authentication attempts are ignored. This is recommended in deployments where the authenticated device acts as a point of access to the network, for example, hubs and access points.

---

**Access Policy Types**

There are three options available for an access policy in Dashboard:

- **802.1X (Default)**
  When an 802.1X access policy is enabled on a switchport, a client that connects to that switchport will be prompted to provide their domain credentials. If the RADIUS server accepts these credentials as valid, their device will be granted access to the network and get an IP configuration. If no authentication is attempted, they will be put on a "guest" VLAN, if one is defined.
  802.1X access policies are commonly used in enterprise environments, since they can authenticate against the existing domain userbase.

- **MAC Authentication Bypass (MAB)**
  When a MAB access policy is enabled on a switchport, the client's MAC address is authenticated against a RADIUS server without needing to prompt the user. If the server accepts the MAC as valid credentials for the network, the device will be allowed access.
  MAB access policies are useful for a more seamless user experience, restricting the network to specific devices without needing to prompt the user.

- **Hybrid Authentication**
  When a hybrid access policy is enabled on a switchport, the client will first be prompted to provide their domain credentials for 802.1X authentication. If 802.1X authentication fails, it will deny the client and will not move to MAB authentication. If the switch does not receive any EAP packets, 802.1X authentication will timeout in 8 seconds, and the client's MAC address will then be authenticated via MAB. If 802.1X authentication timeout and MAB fails, the device will be put on a "guest" VLAN, if one is defined.
  Hybrid authentication is helpful in environments where not every device supports 802.1X authentication since MAB exists as a failover mechanic.
Change of Authorization (CoA)

Meraki MS switches support CoA for RADIUS reauthentication and disconnection. For more information, please see the following KB article.

- **URL Redirect Walled Garden (Supported on MS210/225/250/350/410/420/425)**
  By default, URL redirect is enabled with CoA. This can be used to redirect clients to a webpage for authentication. Before authentication, the client will have access to all HTTP resources. The walled garden can be used to limit access to the web server only. This feature will only be enabled if one or more supported switches are in the network. Configurations on this feature will be ignored by unsupported switches.
Other RADIUS Features

- **RADIUS Accounting**
  RADIUS Accounting can be enabled to send start, interim-update (default interval of 20 minutes) and stop messages to a configured RADIUS accounting server for tracking connected clients. Meraki’s implementation follows the IETF’s RFC 2869 standard.
  As of MS 10.19, device sensor functionality for enhanced device profiling has been added by including CDP/LLDP information the RADIUS Accounting message.

- **RADIUS Testing**
  Meraki switches will periodically send Access-Request messages to these RADIUS servers using identity 'meraki_8021x_test' to ensure that the RADIUS servers are reachable. If unreachable, the switch will failover to the next configured server.

- **RADIUS Monitoring**
  In addition to the mechanism in RADIUS Testing, if all RADIUS servers are unreachable, clients attempting to authenticate will be put on the "guest" VLAN. When the connectivity to the server is regained, the switchport will be cycled to initiate authentication. Please contact Meraki Support to enable this feature.

  As of MS 9.13, test messages are sent every 30 minutes.

- **Dynamic VLAN Assignment**
  In lieu of CoA, MS switches can still dynamically assign a VLAN to a device by assigned the VLAN passed in the Tunnel-Pvt-Group-ID attribute. For more information, please see the following KB article.

- **Guest VLAN**
  Guest VLANs can be used to allow unauthorized devices access to limited network resources. This is not supported on the voice VLAN/domain.

Creating an Access Policy on Dashboard

1. On the Dashboard navigate to **Configure > Access Policies**.
2. Click on the link **Add Access Policy** in the main window then click the link to **Add a server**.
3. Enter the IP address of the RADIUS server, the port (default is 1812), and the secret created earlier.
4. Select the required options, as described above.
5. Click **Save changes**
Apply Access Policy to Switch Ports

1. Navigate to Configure > Switch Ports.

2. Select the port(s) you would like to apply the access policy to and press the Edit button.

3. Convert the port type from trunk to access. Note: you can only apply an Access Policy to an access port.

4. From the Access Policy drop-down box, select the Access Policy you created and press the Update ports button.
Unmanaged Switches Between MS and Client for RADIUS Authentication

When using PEAP EAP-MSCHAPv2 on an MS switchport, if an unmanaged switch is between the supplicant (user machine) and the RADIUS client (MS) the authentication will fail. The reasoning is explained below:

- The destination of the eapol (RADIUS exchange) frame is a special multicast address that 802.1D-compliant bridges do not forward.
- This destination is labeled as "nearest" in Wireshark which means that the frame should only be forwarded to the next layer 2 device.
- If the unmanaged switch is added into the topology between the client and the MS, the next layer 2 device is the unmanaged switch and because the multi-cast nearest address is not meant to traverse multiple switches, the unmanaged switch drops the packets. This prevents the client from being authorized.

There is a work-around to this but special considerations must be taking before implementing them:

- This is not due to a fault in the MS but is the way that eapol is designed.
- It is possible to circumvent this by using MAC based RADIUS authentication. If one machine authenticates via MAC based RADIUS through the MS on an unmanaged switch, the machine that has authenticated will be granted access. It is a workaround and it is less secure and requires more configuration on the NPS and DC.

Additional Resources

- Dynamic VLAN assignment via 802.1X (RADIUS) for MS Switches