Blocking and Whitelisting Clients

In some cases it is necessary to whitelist or block a specific client on a Cisco Meraki Network. This configuration is completed on a client by client basis and will effect the client immediately. Whitelisting and Blocking can be done on both the Cisco Meraki MX Security Appliances and the MR Access Points. At this time it is not possible to white-list or block a client on a Cisco Meraki Switch.

Client policies are configured on a device once it is listed in the network client list, it is possible to Pre-Configure the network policy for clients that aren't listed.

Built-in Client Policies

There are two built-in policies that can be configured for a client; whitelist and blocked. Normal is the default setting for every client subjecting the client to all of the network wide settings. If configured, group policies can also be applied to the client in the same manner as detailed below.

Whitelist

Applies the following settings to a client:

- Is exempt from all firewall rules, both Layer 3 and Layer 7 (Applies to both the MX Security Appliance and the MR Access Points)
- Bypasses AMP
- Bypasses Site to Site VPN outbound rules
- Bypasses a Click-through Splash page
- Bypasses a Billing (paid access) Splash page and access the network on an SSID without paying or authenticating
- Bypasses a Sign-on Splash page without authenticating (Applies to both the MX Security Appliance and the MR Access Points)
- Is exempt from Per-client bandwidth limit (Applies to both the MX Security Appliance and the MR Access Points)
- Is exempt from Traffic shaping rules (Applies to both the MX Security Appliance and the MR Access Points)
- Bypasses Content filtering on MX Security Appliance

- Restricted Youtube content will NOT be bypassed by whitelisted clients as it is NOT considered part of Content Filtering.
Block

Applies the following settings to a client:

- Firewall rule applied to block all communication with other devices on the Network (Only applies to traffic that traverses the Cisco Meraki Device that has the block is configured)
- **Blocked Splash Page** will be displayed when user tries to load a web page

*Note: The device will still receive an IP address and will be able to resolve DNS names.*

**Blocking or Whitelisting a Client**

There are two ways to whitelist or block a client on the Cisco Meraki Dashboard.

*Note: There is a limit of 3000 clients for whitelisting and 3000 clients for blocking. An error will appear when attempting to whitelist or block more than 3000 clients.*

**Using the Clients List**

Navigate to **Network-Wide > Clients**, then check the boxes of the clients that you want to whitelist or block. Click on the **Policy** drop down above the client list, and select **blocked** or **whitelisted**. To apply the whitelist or block on a per SSID basis or only on the MX Security Appliance, select **Different policies by connection and SSID**. To clear the setting, remove the **blocked** or **whitelisted** policy and select **normal**.

*Note: The single configuration pane to block and whitelist users on the security appliance and the SSIDs is only available when on a combined network. These settings would have to be completed on each Dashboard Network for uncombined networks.*

- **IDS/IPS under Security and SD-WAN->Threat Protection** will **NOT** be bypassed.
After this is completed it is possible to filter clients to determine which ones have a policy configured on them.

If the client has never connected to the network, or is not in the client list, it can still have a policy applied. This is done using the Add client button on the Network-wide > Monitor > Clients page. Enter a friendly name for the device, its MAC address, and then which policy you would like applied. Then click Save changes.

**Using the Client Details Page**

The current policy will be shown and can be updated at the client details page. Like above, to apply the whitelist or block on a per SSID basis or only on the MX, select the Different policies by connection and SSID. The options listed will allow you to configure blocked or whitelisted per SSID and on the MX Security Appliance. To clear the setting, remove the blocked or whitelisted policy and apply normal. Below is where the setting would be configured with a combined network:
If the Dashboard network is a wireless or a appliance network (Not **Combined**, the client details page looks a little different. The **blocked** and **whitelisted** setting is on a per Dashboard network basis and is configured on the Client Details Page in **Edit Details**:

In the Client Details configuration, the client can be blocked or whitelisted.
Details

Name: [Redacted]
MAC address: [Redacted]
IP: 171.64. [Redacted]
Hostname: [Redacted]-macbook (Bonjour)
Network access: Normal
  ○ Whitelisted
    The device can access the network without bandwidth limits or splash pages.
  ○ Blocked
    The device is prevented from accessing the network.
  ○ Apply group policy
    Apply a group policy to this device on this network.
  ○ Customize per SSID
    Apply different group policies, depending on the associated SSID

Notes:

Connection: wired, wireless
Capabilities: 802.11n, 2.4 and 5 GHz
Manufacturer: Apple
Operating system: Mac OS X 10.5