Meraki Instructions

Table of Contents

Overview

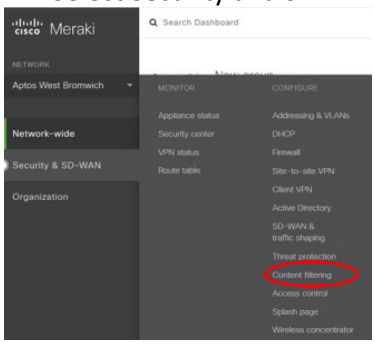
Content filtering allows the ability to block certain categories of websites based on organizational policies. It can be blocked or allow individual websites for additional customization.

- **Blocked website categories**: Select the categories that you wish to block.
- **URL category list size:** Select "Top sites only" for higher performance or "Full list" for better coverage. When 'Top sites only' is selected, the list of top sites ineach of the blocked categories will be cached locally on the appliance. In this mode, client requests for URLs that are not in the top sites list will always be permitted (if it is not on the blocklist). If "Full list" is selected, a requestfor a URL that is not in the list of top sites will cause the appliance to look the URL up in a cloud-hosted database. This may have a noticeable impact on browsing speed when visiting a site for the first time. But the result will be cached locally. Over time, the "Full list" performance should approach the speedof "Top sites" option.
- **Web search filtering:** Enable this setting to enforce safe search for Google, Yahoo!, and Bing for all users in your network. This will not affect SSL/HTTPSsearches.
- **Restricted YouTube content:** Enables restricted YouTube content functionalitywhich leverages DNS-based enforcement. Once enabled, the YouTube restrictionlevel option appears which provides a drop-down where either Moderate or Strictcan be chosen. More details about restriction levels can be found here.
- **Blocked URL patterns:** Enter specific URL patterns you wish to block, one perline. See below for details on pattern matching.
- **Allow listed URL patterns:** Enter specific URL patterns you wish to explicitlyallow, one per line. See below for details on pattern matching.

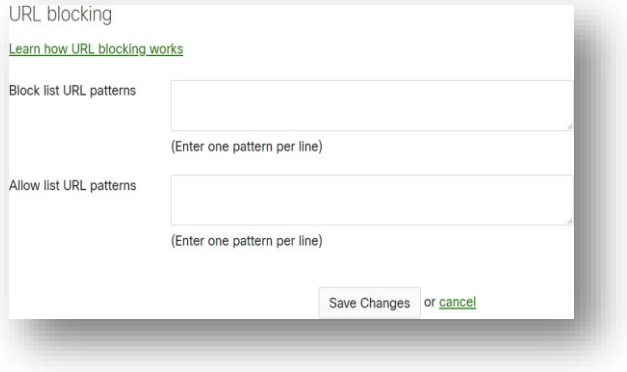
Note: IP addresses are a supported option in Block/Allow listed URL pattern fields. When you enter an IP into that field, its interpreted as a URL because as it turns out, http://192.168.1.1 is a perfectly valid URL. Note that this is not the same as an IP block - it will just block/allow list someone who types in 192.168.1.1 into their web browser. In addition, that would also mean if abc.com resolves to 192.168.1.1, contentfiltering will not block/allow list abc.com explicitly. You will need to enter abc.com as anURL in Blocked/Allow listed URL patterns as well.

Content Filtering

1. Select Security and SD WAN



2. Under configure, select **'Content Filtering.'**
3. Enter the website to block or allow.



4. Select **'Save Changes'.**

Using the Catch All Wildcard (*) in URLs

The asterisk symbol has two primary uses in URLs for content filtering.

- Standalone Catch-All Wildcard
  - The " * " (asterisk) symbol when used on its own line is an all-inclusive wildcard which represents **all** possible entries.
  - When used on its own line in allow listed URL patterns, ALL URL patternsare allowed listed.
  - When used on its own line in blocked URL patterns, ALL URL patterns are blocked, except those that are explicitly allow listed.
- In-URL Asterisk Character
  - The " * " (asterisk) symbol when used as part of a URL or in line with aURL is simply a regular asterisk symbol and is interpreted as part of theURL, NOT as a wildcard
  - Note that this is *very rarely useful*, except in URLs that actually require asterisk symbols, such as https://web.archive.org/web/*/meraki.com

Patterns for Blocking or Allowing the Listing of Specific URL's

Whenever a device on the network accesses a web page, the requested URL is checked against the configured lists to determine whether the request will be allowed or blocked.

Pattern matching follows these steps in order:

1. Try to match the full URL against either list (blocked vs allow listed patterns lists) e.g., http://www.foo.bar.com/qux/baz/lol?abc=123&true=false
2. Remove the protocol and leading "www" from the URL, and check again: e.g., foo.bar.com/qux/baz/lol?abc=123&true=false
3. Remove any "parameters" (everything following a questions mark) and check again: e.g., foo.bar.com/qux/baz/lol
4. Remove paths one by one, and check each: e.g., foo.bar.com/qux/baz, foo.bar.com/qux, foo.bar.com
5. Cut off subdomains one by one and check again: e.g., bar.com and then .com
6. Finally, check for the special catch-all wildcard, *, in either list.

Note: If any of the above steps produces a match, then the request will be blocked or allowlisted as appropriate. The allow list always takes precedence over the blocklist, so a request that matches both lists will be allowed. If there is no match, the request is subject to the category filtering settings above.

Example:

In the example above, the Whitelisted URL is allowed because it is specific to the content to allow, whereas any other access to the **foo.bar** domain will be blocked.

Blocking All Website Using Content Filtering

An MX security appliance can be used to block all web content, then be configured for a specific website only.

1. Place an asterisk (*) in the Blocked URL patterns section.

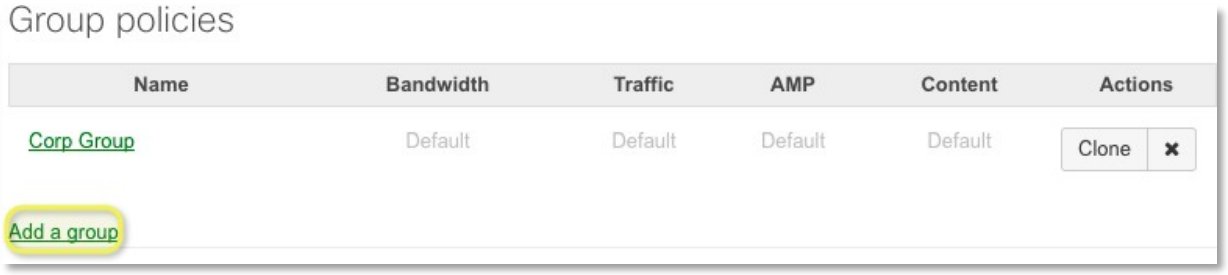
Example:

Content Filtering via Group Policies

The content filtering can be used for groups, and an active directory for specifications vs being able to block/allow the entire organization.

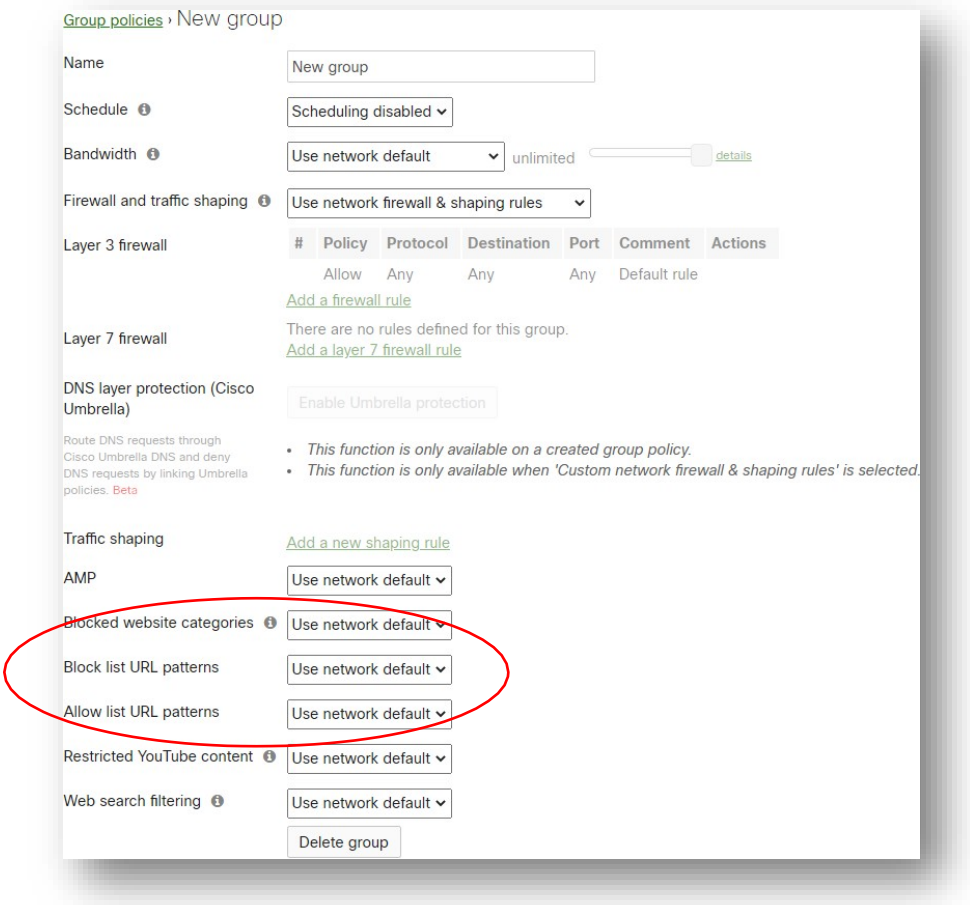
1. A group would need to be created to block/allow the content filtering.
2. Navigate to Network-wide-> Configure-> Group Policies.
3. Select Add a group to create a new policy.

Example:



4. Provide the name for the group policy. Generally, this will describe the purpose or the users it will be applied to.
5. Modify the available options desired, then **save the changes.**

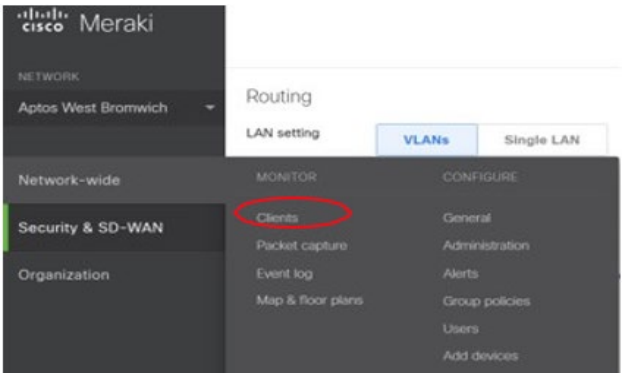
Example:



6. The group policy list will display under the Group Policies list. However, to take effect, the Group Policy needs to be applied.

Applying Group Policies

1. Navigate to Network-wide -> Monitor -> Clients.

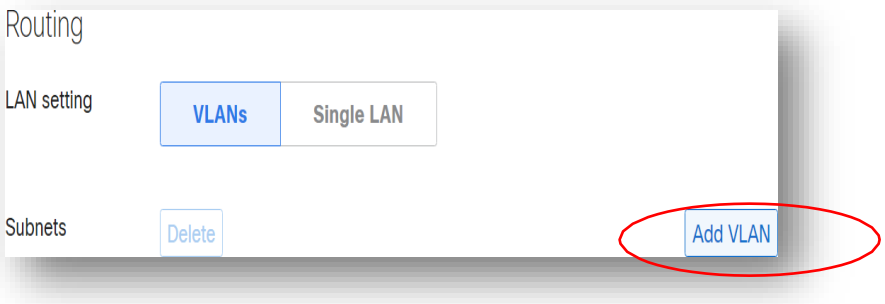


2. Check the box next to the desired Client (s) in the list.
3. Select the Policy button at the top of the list.
4. Select the Group Policy, then choose the specific policy from the drop-down menu.

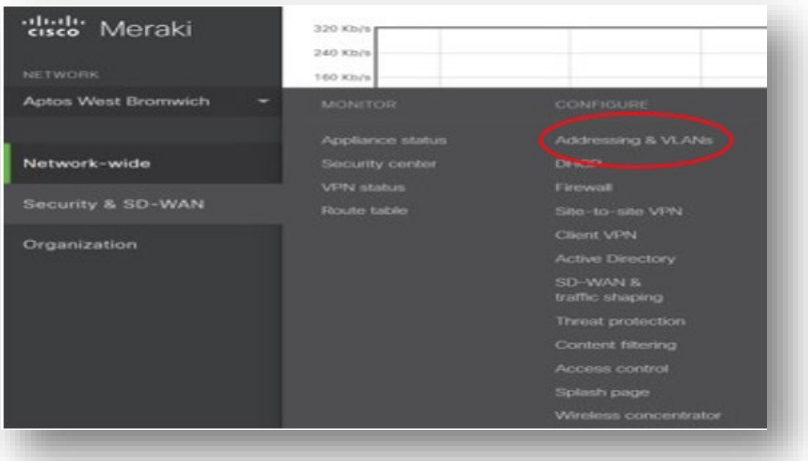
5. Click Apply Policy.

Applying Group Policies by VLAN

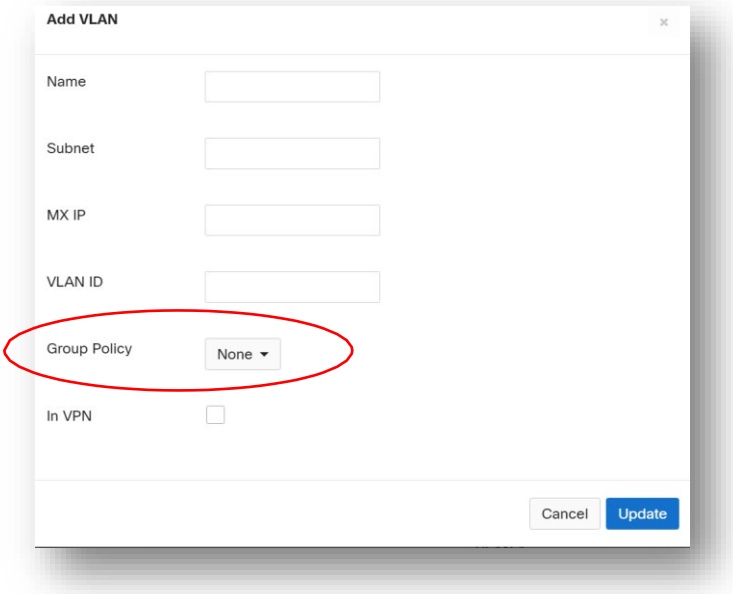
1. Navigate to security and SD-WAN -> configure -> addressing and VLANs.



2. Scroll to the routing and click **Add VLAN.**



3. Select the desired Group Policy for the VLAN.

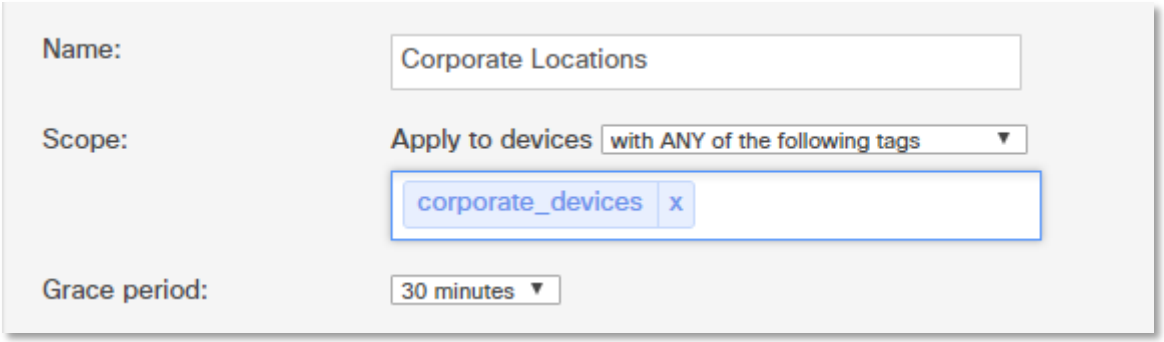


Geofencing with Managed Devices

Creating a Geofence

Multiple geofencing rules can exist, with each potentially covering multiple physical areas. This allows administrators to limit the scope of different sets of devices to different physical locations.

1. Navigate to **Systems Manager -> Configure -> Geofencing.**
2. Click **Add New** in the upper right corner.
3. Enter a **Name** for this geofence.
4. Select a **Scope** for which devices this geofence should apply to, based on tags.
5. Select a **Grace period** which determines how long a device can be outside of the defined area before an alert is generated.



6. Click **Add A New Area.**
7. Click the geocode button below **find by address.**
8. In the box that appears, search for the address or location the geofence should cover, then click **Submit.**
9. A geofence boundary indicator will appear, indicated by the semi-transparent blue circle, centered at the location provided. Click and drag the center indicator to move the boundary, while similarly using the scale indicator to control the size of the boundary, until it covers the desired area.

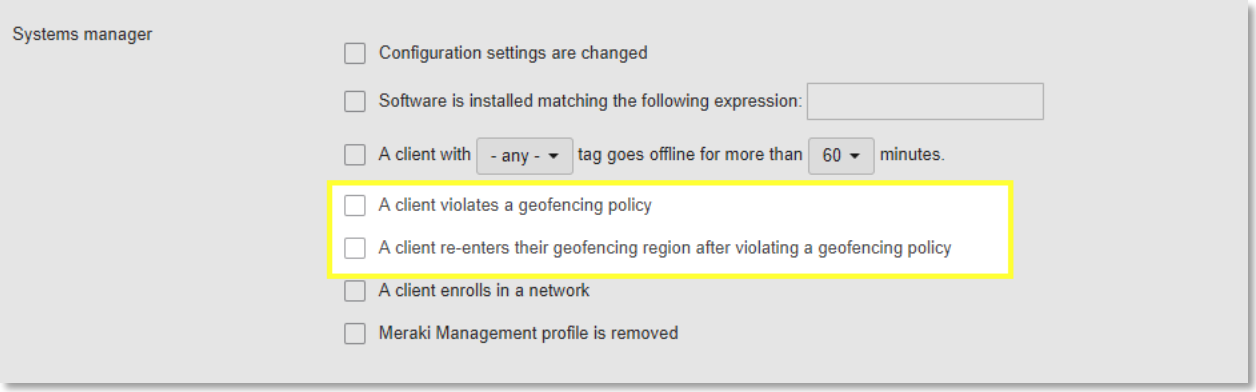
10. Update the **description** field for the row with a friendly name of the boundary, such as a building or campus name.
11. If additional geofence boundaries are desired for this scope of devices, repeat steps 6-10 as needed.
12. When done, click **Save Changes.**
13. If additional geofences need to be configured with different scopes, click **Back to List,** and repeat steps 2-12 as needed.

Enabling Geofencing Alerts

If configured, alerts can be sent to administrators whenever a device within the scope of a geofence remains outside of the designated boundary for more time than permittedby the grace period.

To configure these alerts:

1. Navigate to **Systems Manager -> Configure-> Alerts -> Geofencing alerts.**
2. Click the checkbox for any options that are desired.



3. Click **Save Changes.**

If an alert must be generated, based on the geofences defined and the selection made above, it will be sent to the address (es) indicated in the delivery settings section of the page.

Linking Geofencing to a Profile

Once a geofence has been created and applied to devices, those will automatically receive one of two tags, dependent on whether they are within the geofence or not. These tags can be used to control the scope of profiles. The feature is only available with Systems Manager Enterprise.

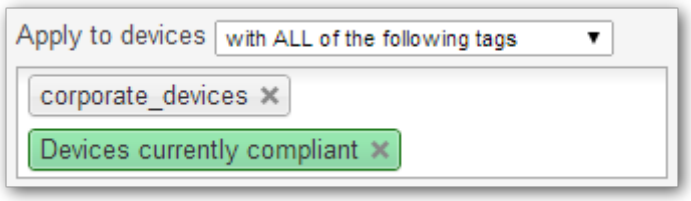
Devices currently compliant: Device is currently inside a geofence that it is within the scope of, or it has not yet exceeded the grace period.

Devices currently violating: Device is not within any of its geofence and is beyond the grace period.

To make a profile dependent on device compliance:

1. Navigate to **Systems Manager -> Manage -> Settings.**
2. Select a profile.
3. Under **Scope**, choose an appropriate option that allows for use of tags.
4. Click in the tags box, and under Geofencing, select one of the following options explained above, in addition to any other desired tags.

In the screenshot below, only devices with the “corporate devices” tag will receive this profile and only when they are within a geofence boundary. Once they leave the geofence and exceed the grace period, the profile will be removed from the device the next time it is unlocked and checks in. If the device is within the scope of multiple geofences, compliance takes priority, and the device will be considered compliant as long as it is within at least one geofence boundary.

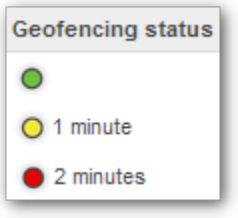


Note: The geofencing auto tags cannot be used with apps, due to how app association with accounts is handled.

Checking the Status of Geofenced Devices

It is also possible to manually check on devices to determine if they are currently withinthe geofence boundary or not. To do this:

1. Navigate to **Systems Manager > Monitor > Devices.**
2. Add the "Geofencing status" column, if it does not already exist, by clicking onthe + to the right of the other column headers, then checking the box for **Location > Geofencing status.**
3. Click the + button again to close the dropdown window.
4. The **Geofencing status** column will indicate if the device is within the geofence.
    i. **Green** - Device is within geofence.
    ii. **Red** - Device is outside of geofence and beyond grace period (time outside of geofence will be indicated)
    iii. **Yellow** - Device is outside of geofence but within grace period (time outside of geofence will be indicated).



To check the status of a specific client, as well as see which auto tag is currently applied:

Note: Auto tags based on geofence compliance are only available with Systems Manager Enterprise.

1. Navigate to **Systems Manager > Monitor > Devices.**
2. Click on the client in question.
3. Under Auto tags the device should be listed as violating or compliant.