Creating and Applying Group Policies

Group policies define a list of rules, restrictions, and other settings, that can be applied to devices in order to change how they are treated by the network. Group policies can be used on wireless and security appliance networks, and can be applied through several manual and automated methods. This article will describe the options available, how to create policies, and how those policies are applied to clients.

**Note:** There is a limit of **3000 clients** that can have any group policy applied (combined).

Creating Group Policies

Available Options

The following table describes what rules, restrictions, and other settings can be controlled via group policy on each platform. Only features that are available for the network will be displayed when configuring a group policy.

<table>
<thead>
<tr>
<th></th>
<th>MR Access Points</th>
<th>MX or Z1 with Enterprise License</th>
<th>MX with Advanced Security License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduling</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Per-client bandwidth limit</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Hostname visibility</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>VLAN tag</strong></td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Splash page authorization</strong></td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Layer 3 firewall rules</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Layer 7 firewall rules</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Traffic shaping rules</strong></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### Creating a Group Policy

1. Navigate to **Network-wide > Configure > Group policies**
2. Click **Add a group** to create a new policy.

#### Group policies

<table>
<thead>
<tr>
<th>Name</th>
<th>Bandwidth</th>
<th>Traffic</th>
<th>AMP</th>
<th>Content</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corp Group</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td></td>
</tr>
</tbody>
</table>

#### Add a group

3. Provide a **Name** for the group policy. Generally, this will describe its purpose, or the users it will be applied to. Ex. "Guests", "Throttled users", "Executives", etc.
4. Modify the available options as desired. Unless changed, all options will use the existing network settings.
5. When done, click **Save Changes**.

The group policy listed will now be displayed on the **Group policies** page and made available for use. Remember that a group policy has no effect until it is applied.

---

### Example Group Policies

The following examples outline two common use cases, and how group policies can be used to provide a custom network experience:
The following example is meant to demonstrate how a group policy could be configured on a Security Appliance network to limit the access and speed of guest clients. This policy would accomplish the following:

- Limit client bandwidth to 2Mbps up/down.
- Deny access to the internal network (which uses the 10.0.0.0/8 address space).
- Block all peer-to-peer sharing applications.
- All other settings would be inherited from network defaults (such as security and content filtering settings).
Executive Users on Wireless

This example demonstrates how a group policy could be used on a wireless network to provide executive users with more freedom and special treatment over other users. This policy would accomplish the following:

- Remove any bandwidth restrictions.
- Disable hostname visibility.
- Remove any layer 3/7 firewall rules.
- Provide QoS tagging for Voice and Video conferencing traffic.
- Remove the splash page requirement.
- All other settings would be inherited from network defaults.

Bandwidth limit cannot be set lower than 20 kbps.
Applying Group Policies

Group policies can be applied to client devices in a variety of ways, dependent on the platform being used. The table below illustrates what options are available for each platform. The rest of this section explains how to use each method.
**Note:** Only one policy can be active on a client at a time.

<table>
<thead>
<tr>
<th>MR Access Points</th>
<th>MX or Z1 with Enterprise License</th>
<th>MX with Advanced Security License</th>
</tr>
</thead>
<tbody>
<tr>
<td>By client</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>By device type</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>By VLAN</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>By Sentry Policy</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>By Active Directory Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By RADIUS Attribute</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

**By Client**

Group policies can be manually applied to clients from the **Network-wide > Monitor > Clients** page.

1. Check the box next to the desired client(s) in the list.
2. Click the Policy button at the top of the list.
3. Select *Group policy* and then choose the specific policy in the dropdown.
4. Click *Apply policy*.

Alternatively, on wireless and combined networks different group policies can be applied dependent on the SSID the client is associated to. This is applied from the same page as the previous steps.

1. Check the box next to the desired client(s) in the list.
2. Click the Policy button at the top of the list.
3. Select *Different policies by [connection or] SSID*.
4. For each SSID, select the desired group policy, built-in policy, or leave as Normal.
5. Click *Apply policy*.

Policies can also be applied to individual clients by clicking on the client in the clients list, and then choosing a *Device policy* under the Policy section.
By Device Type

In wireless networks, group policies can be automatically applied to devices by type when they first connect to an SSID and make an HTTP request.

1. Navigate to **Wireless > Configure > Access control**.
2. Select the desired **SSID**.
3. Set **Assign group policies by device type** to 'Enabled'.
4. Click **Add group policy for a device type**.
5. Select the desired **Device type** and the **Group policy** that should be applied to it.
6. Repeat steps 4-5 as needed to assign policies to all desired devices.
7. Click **Save changes**.

Keep in mind that this only occurs when a device first connects to the SSID and persists until it is manually overridden. Thus, some previously connected clients may need to have policies manually assigned. It is also possible for a client to be mis-classified based on the initial HTTP request, dependent on how it is generated by the device. If this occurs, manually assign the desired policy.

For more info on applying group policies by device type, please refer to our [documentation](#).

By VLAN

On security appliance networks, group policies can be automatically applied to all devices that connect to a particular VLAN. From the **Security appliance > Configure > Addressing & VLANs** page:

1. Ensure that **VLANs** is 'Enabled'.

---

By Device Type

In wireless networks, group policies can be automatically applied to devices by type when they first connect to an SSID and make an HTTP request.

1. Navigate to **Wireless > Configure > Access control**.
2. Select the desired **SSID**.
3. Set **Assign group policies by device type** to 'Enabled'.
4. Click **Add group policy for a device type**.
5. Select the desired **Device type** and the **Group policy** that should be applied to it.
6. Repeat steps 4-5 as needed to assign policies to all desired devices.
7. Click **Save changes**.

Keep in mind that this only occurs when a device first connects to the SSID and persists until it is manually overridden. Thus, some previously connected clients may need to have policies manually assigned. It is also possible for a client to be mis-classified based on the initial HTTP request, dependent on how it is generated by the device. If this occurs, manually assign the desired policy.

For more info on applying group policies by device type, please refer to our [documentation](#).

By VLAN

On security appliance networks, group policies can be automatically applied to all devices that connect to a particular VLAN. From the **Security appliance > Configure > Addressing & VLANs** page:

1. Ensure that **VLANs** is 'Enabled'.
2. Click on the desired Local VLAN.
3. Select the desired **Group policy**.

![Local VLAN Configuration](image)

4. Click **Update**.
5. Click **Save Changes**.

Any clients that are placed in this VLAN will now be given the desired **Group policy**.

**Routing**

<table>
<thead>
<tr>
<th>VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routers</strong></td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
</tr>
<tr>
<td>192.168.128.0/24</td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

Add a Static Route, Add a Local VLAN

![Routing Table](image)

When a group policy is applied to a VLAN, that policy becomes the new "network default" for any other group policies applied to clients in that VLAN.

For example, a group policy named "Guest Network" with more restrictive Layer 3 firewall rules than the network-wide configuration is applied to the Guest VLAN, and a second group policy "Low Bandwidth" has a
By Active Directory Group

Security appliance networks with Advanced Security licensing can use Active Directory groups to assign policies to clients. Refer to the article on Configuring AD-based Group Policy for more information.

By RADIUS Attribute

Wireless networks that are using RADIUS to authenticate clients can be configured to assign group policies via RADIUS attributes. Refer to the article on Configuring Group Policies with RADIUS Attributes for more information.

Scheduling

Group policies can be scheduled, using the Schedule option. This allows the policy to only be active during the times specified. In the example below, a policy has been scheduled to only be active from 8am-5pm on weekdays:

![Schedule](image)

When enabled, elements of the policy that are subject to scheduling will be indicated with a small clock icon, as shown below. Options without this icon will always be in effect, regardless of time.