Best Practices for Merging Networks and Organizations

Overview

On occasion, situations may arise where separate Cisco Meraki dashboard networks or organizations need to be merged or consolidated into one. While this can typically be avoided with proper planning, circumstances such as a company merger, redesign of an outdated network, or oversight in initial planning, may present a need to merge networks/organizations.

Therefore, as all configuration and usage information is held within the Meraki dashboard, it is critical to understand which configuration options can or cannot be transferred between networks and organizations in order to minimize downtime and/or the need for reconfiguration. This article aims to explain how to navigate these situations should they arise and touches on best practices to help avoid these situations in the first place.

Understanding the Different Levels of Configuration

**Organization**: Configuration options set at the organizational level to impact all networks within the organization. Examples include SNMP settings, MDM settings, or dashboard administrators.

**Network**: Configuration options specific to the network they are configured within. These configuration settings will be applied to any device that is added to the particular network. Examples include SSID settings, firewall rules, or traffic-shaping rules.

**Device**: Configuration options specific to one device in a network, such as the management IP address, switchport configuration, or transmit power settings.
Merging/Combining Networks within the Same Organization

Dashboard networks allow for grouping the same type of devices (such as access points or switches) into logical containers for organization, administration, and configuration. Moreover, networks are typically used to define a specific site or location within an organization. As many deployments are not part of a single, encompassing project, but instead the efforts of many smaller projects, there may be a need to consolidate multiple dashboards networks into one. To accomplish this, the steps outlined below will need to be followed:

1. Determine the Destination Dashboard Network

Depending on the destination dashboard network, slightly different steps will need to be taken. If moving to an existing network, this step can be skipped. When moving to a new network, the steps outlined below will need to be completed to ensure the destination network is preconfigured for the move. There are two

**Note**: Moving devices between either dashboard networks or organizations should be done during a planned maintenance window, as there may be a brief window of downtime while the devices check in and download their configuration following the move.

**Note**: Moving devices between networks will cause back-end configuration options to be removed, depending on if they're applied. For assistance or questions on this, please contact Meraki support.
ways to create another dashboard network:

- **New Network**

  This will create a network with the default configuration. A new dashboard network can be created under Organization > Configure > Create Network. For more information on creating a new network, refer to the Creating and Deleting Dashboard Networks article.

- **Cloned Network**:

  A cloned network will copy most network and configuration settings between networks of the same type. To create a dashboard network that is a clone of another, begin following the same steps outlined above, however, instead of selecting *Use default* at the Network Configuration step, select *Clone from existing* and then select the original network that should have its configuration copied over to the new network that is being created.

---

**Create network**

---

**Setup network**

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization.

**Network name**

- Scranton Branch Office

**Network type**

- Combined hardware

**Network configuration**

- Default Meraki configuration
- Bind to template
- Clone from existing network

*Note:* The network settings will remain on the original network (unless it is deleted) even if there are no devices claimed in it. However, while it will not necessarily be lost, the original configuration will not be transferred over to the destination network.
2. Move the Meraki Devices from the Original Dashboard Network to the Destination Network

Once the destination network is created, the devices can be moved between them. This step will vary depending on the type of Meraki devices that need to be moved. Detailed information on how to move each particular device type between networks can be found in the Moving Devices between Networks article.

Note: When moving a device to another dashboard network, it is important to remember that most device-level configuration will be lost upon the move. Please reference the “reconfigure necessary settings” section for more information.

Note: The Meraki devices will immediately begin to download and upgrade their firmware if moved to a network that is set to a different firmware version that what they were previously running.

3. Reconfigure Necessary Settings

When moving devices between dashboard networks, the devices will assume the network-level configuration of the network where it is claimed. Therefore, under most circumstances, the majority of the network-level configuration can be staged ahead of time by either cloning the original network or reconfiguring the destination dashboard network through dashboard or via the API.

Most device-level configuration will be lost upon the move between networks. Please see the outline below for the configuration that is device-level and would be lost when moving these devices.

- **MX**

  The MX appliances and Z-Series gateways are unique from other devices as a network can only contain one MX (or two identical devices in a warm spare configuration). Therefore, there is rarely a need to move an MX between networks, but if it does need to be moved, all configuration will be lost.

- **MS**

  When moving an MS switch to a new network, all settings in the current network will be lost. The following device settings will be moved to the new network:

  - Name
  - Geolocation address
  - Management address
  - Notes
  - Tags

  All other switch and port settings will be lost upon moving to the new network.
• MR

When moving an MR access point to a new network, all settings in the current network will be lost. The following device settings will be moved to the new network:

• Name
• Geolocation address
• Management address
• Radio settings (manual channel and power)
• Notes
• Tags

Are you sure?

Existing switch and port settings will be lost.

Yes, move 1 switch  Cancel

Move to network:

Testing Network – wireless

Move

Are you sure?

The static IP uplink configurations of the following access point may be lost:

Device Name (-redacted)

Yes, move 1 access point  Cancel
• **MV**

When moving an MV to a new network, you can choose to either delete the historical video or retain it. The default option is to delete the video.

Though the video is retained, the following settings and functionality will be affected:

- The recording schedule from the initial network is not retained so the destination camera will need the schedule to be reapplied; if the camera was using motion-based retention, it will continue to do so after the move
- Motion alerts will need to be reenabled
- While historical video exists after the move, the video from the earlier network will not be motion searchable; the video after the move will continue to be motion searchable

All other camera settings are retained upon moving to the new network.

• **MG**

When moving an MG to a new network, the following settings are retained:
- SIM PIN
- Static APN username and password

**SM**

Devices that are enrolled in SM (EMM) networks can be moved by navigating to **Systems Manager > Monitor > Devices > Select the checkbox next to the device that should be moved > Move > Select the destination network**

**Note:** When moving enrolled devices between networks, previously installed **tags**, **profiles**, and **owners** will remain installed once moved. Therefore, if you do not wish to move these settings along with the device, it is recommended that the device is untagged and the owners are removed as necessary before being moved between networks.

**Merging Networks with Configuration Templates**

Through the use of configuration templates, multiple networks can be configured and managed by a single base configuration. Therefore, networks should only be bound to a configuration template if they are similar deployments, such as a storefront location with all the sites being nearly the same. This section aims to assist with navigating the process of binding preexisting networks to configuration templates and vice versa. For more information on configuring templates and how they should be used, refer to the **Managing Multiple Networks with Configuration Templates** document.

**Binding a Network to a Template for the First Time**

Networks that are bound to the configuration templates will assume the configuration set at the template level. Since configuration templates should only be used in the event that template-level configuration is required, there should not be any risk of losing the network-level configuration if templates are used properly.

When using configuration templates, there are local overrides and configuration options that can still be configured normally on the network level.

Networks can be bound to a template under **Organization > Configuration templates > Bind additional networks**. Review the linked article for more information on **binding networks to a template**.

**Note:** The network will revert back to its original state from before it was bound to the configuration template if it is unbound from the template.

**Moving Networks between Configuration Templates**

When networks are bound to configuration templates, they will assume the configuration of the template itself. Therefore, when networks need to be moved between configuration templates, they will need to be unbound from one template before being bound to another, as they cannot be moved directly between templates. However, since the network configuration is held on the template, there should not be any risk of losing the network-level configuration if templates...
are used properly.

**Merging Organizations**

An organization acts as the upper-level container for an individual brand, business unit, or geographical location. While multiple organizations can be linked together by using the same username and password, this is allowed for ease of manageability. An organization is designed to be a boundary of configuration, meaning there is no dedicated tool to move devices or networks between them.

However, deployments may not always go as planned, and certain situations may arise where it is necessary to combine multiple organizations into one. This section explains what to expect when working through the process and how to ensure a smooth transition.

**Transferring Ownership by Adding and Removing Organization Administrators**

In the event that an existing dashboard organization is obtained, and they should remain separate organizations (such as separate business units or different geographical regions). It is highly recommended to transfer ownership of the organization by adding/removing administrators as opposed to moving the devices and recreating the networks. This will result in a much smoother transition and will not require any network reconfiguration or downtime.

The steps to complete this process are below:

1. Have an existing organization administrator add a new email address that belongs to the destination organization administrator to the new organization. More information on how to add/remove organization administrators can be found in the Managing Dashboard Administrators and Permissions document.

2. Log in with the account for the destination administrator and remove any original organization administrators that should no longer have access.

3. Add additional administrators as necessary. It is highly recommended to have at least two administrators in the event that one is locked out or another is lost. Refer to the Managing Dashboard Administrators and Permissions document for more information on organization management best practices.

**Note:** A dashboard organization should be treated as any other asset to the company. In the event that access is lost to the organization by mistake, Meraki cannot assist in reestablishing access. Such events should be settled with the other party involved. For more information, refer to the Supplemental End User License Agreement.

**Merging Two Existing Dashboard Organizations**

1. Define the destination organization that will become the master and will have the devices and networks from the other organization added to it.

2. Ensure that the networks and devices that are going to be moved can afford the downtime during the removal and reconfiguration on the new organization.

3. Navigate to the network that will be moved and remove the devices from the network.

4. Unclaim the devices from the organization. View the Moving Devices between Organizations article for more information.

**Note:** To move Systems Manager devices, they will to be unenrolled from the original organization and then reenrolled in the destination organization. Refer to the Uninstalling Systems Manager and Removing Managed Devices document for information on unenrolling and the Enrolling Devices for guidance on enrolling devices.

5. Claim the devices into the destination (master) organization.
6. Create the new networks if they do not already exist.
7. Add the devices to the networks.
8. Reprovision the networks to the desired settings.

**Note:** When moving a device between organizations, all configuration will be lost.

### Avoiding the Need to Merge Networks and Organizations

Ultimately, the best practice surrounding merging networks and organizations comes down to designing a deployment thoroughly beforehand to avoid the scenarios outlined above.

Before rolling out any type of deployment, it is important to understand what exactly needs to be accomplished. Once this vision of success is defined, steps towards achieving that goal can begin to be taken. The logic is also true for a Meraki deployment. Understanding specifically what you are seeking to accomplish with the Meraki deployment can ensure that the proper steps are taken during the planning/design phase. For example, are we deploying a teleworker solution to seamlessly connect remote workers to a corporate network, upgrading the existing switches with cloud-managed switches to provide ease of client tracking and analytics, or rolling out retail sites across the globe that are all mirror-images of one another? Each of these situations requires special consideration before deploying.

To ensure that future roadblocks or limitations are not encountered further down the line, it is critical to follow best-practice design and allow proper forethought before implementation begins. The following section aims to touch on the key aspects of a successful deployment that help to negate any unexpected situations.

### Understanding Meraki Cloud Structure

The relationship between Meraki User Account, Organizations, and Networks is a fundamental part of the Meraki platform. The layout of these aspects are the foundation for the future scalability and flexibility of the deployment. To learn more about the Meraki platform and the breakdown of these terms, refer to the Meraki cloud architecture article.

- Devices can easily be moved and their configurations can be cloned between different dashboard networks in the same organization, but when needing to move between organizations, things are less malleable.
Planning Organization Architecture

An organization should act as the upper-level container for an individual brand/business unit or geographical location. As mentioned in the Meraki Cloud Architecture article, customers with globally dispersed networks should create separate organizations for each data storage region. With this in mind, the organization should be thought of as the boundary for merging configuration or easily transferring devices.

- Plan for size and scalability; refer to the Building a Scalable Meraki Solution article for more information

- It is equally as important to keep in mind specific features that may behave differently depending on how the deployment is planned. Some examples include:
  - Auto VPN topology
    - The Auto VPN feature operates within the boundaries of a single dashboard organization and cannot be extended to another organization
  - Summary and analytics information
    - Gathering information such as the summary report and security

- Licensing model is set at the organization level
  - Co-termination vs. per-device licensing (PDL)
  - Co-termination requires support intervention to move between
  - PDL allows for customer to move licenses between devices

- Firmware upgrades
  - With firmware upgrades, an important consideration is how they interact with configuration templates vs. stand-alone networks. With configuration templates, the entire template for like device types must use the same firmware version. Firmware upgrades can be managed at the organization level under Organization > Configure > Firmware Upgrades. More information can be found in the Managing Firmware Upgrades article as well as the Cisco Meraki Firmware FAQ article.

- Planning network design
  - Determine if a combined network vs. a stand-alone network should be used; view the linked article for more information on the benefits of using a combined dashboard network

Performing Organization Splits Sparingly

Organization splits can be utilized in a situation where specific networks need to be moved into a different organization. This can create further complications if organizations are moved unnecessarily, as this process cannot be reverted. The steps outlined previously in this document will need to be taken to merge them once again.

For more information on this process, reference the Organization Split Overview and FAQ document.

Client-Tracking Forethought

The Meraki MX appliances and Z-Series teleworker gateways have three different ways to track clients. This will define how clients are seen in dashboard, impacting how the corresponding reports will be viewed.

Depending on the network design and integration on non-Meraki equipment downstream, different client-tracking options should be used. More information can be found in the Client-Tracking Options article.

Note: When an MX appliance or Z-Series gateway is not being used, the clients will be tracked by MAC address.
Using Configuration Templates

Configuration templates are useful in situations where a large number of sites exist that share a common network design, such as a retail deployment with multiple stores or a teleworker solution with many home users connecting to the corporate network over Auto VPN.

Through the use of configuration templates, multiple networks can be provisioned at the same time from a single template. When using templates, much of the configuration cannot be provisioned on an individual network level, as the majority of configuration must be completed at the template level. Some options can still be configured normally on a network level, but this only applies to a small subset that typically will vary between sites, such as DHCP exceptions on the MX, switch ports on the MS, and radio settings on the MR. For more information on configuration templates and local overrides, please visit the Managing Multiple Networks with Configuration Templates document.

In a situation where granular control over the configuration is needed on a site-to-site basis, it is best to steer towards using stand-alone networks and using the dashboard API to make bulk changes where necessary.

Using the Dashboard API

The dashboard API allows for bulk changes to be made while still allowing for granular control on a network level, resulting in a flexible and scalable solution. Reference the Cisco Meraki Dashboard API for more information, and refer to the developer hub for more information on getting started.

The API can also be used to automate configuration changes within the dashboard based on other factors, such as performance of a VPN tunnel. As an example, check out the Tag-Based IPsec VPN Failover article, as this provides a breakdown of how the dashboard API can be used in combination with a python script to automatically reconfigure the availability tags for third-party VPN tunnels when performance suffers.

FAQ

Can I back up/export my dashboard configuration?

The dashboard configuration cannot be backed up or exported to a local copy. All configurations are stored as a container in the Meraki back end. Please review the Meraki Cloud Architecture document for more information.

Can I move networks between organizations?

It is not possible to move dashboard networks between existing organizations. An organization is designed to be a container of networks and their configuration, so there is no dedicated tool to move devices or networks between them.