Managing Dashboard Administrators and Permissions

This article will cover the different permission levels within Dashboard and how to manage administrative users. These are the users that have access to log in to dashboard and view/administer Cisco Meraki networks/devices. For information on how to manage users with access to join a client VPN or wireless network, please review the article on Managing user accounts using Meraki authentication.

Summary

There are two basic types of Dashboard administrators: Organization and Network.

- Organization administrators have complete access to their organization and all its networks. This type of account is equivalent to a root or domain admin, so it is important to carefully maintain who has this level of control. Please see below for best practices regarding these accounts.

- Network administrators have access to individual networks and their devices. These users can have complete or limited control over their network configuration, but do not have access to organization-level information (licensing, device inventory, etc).

Most Dashboard administrators will fall into one of the two above categories, the remainder of this article goes in-depth about the options and limitations associated with different admin types.

Organization Permission Types

**Read-only**: User able to access most aspects of network and organization-wide settings, but unable to make any changes.

**Full**: User has full administrative access to all networks and organization-wide settings. This is the highest level of access available.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email address</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org - Full admin</td>
<td></td>
<td>Organization</td>
</tr>
<tr>
<td>Org - Read-only admin</td>
<td></td>
<td>Organization (Read)</td>
</tr>
</tbody>
</table>

**Note**: Dashboard organizations should always have at least two organization admins. This is best practice in case one account is locked out or if email access to that account's email address is lost.

Network Permission Types

**Guest ambassador**: User only able to see the list of Meraki authentication users, add users, update existing users, and authorize/deauthorize users on an SSID or Client VPN. Ambassadors can also remove wireless users, if they are an ambassador on all networks. The existence of network templates anywhere in a dashboard organization prevents guest ambassadors from deleting wireless users.

Presented with user management portal only.
Monitor-only: User only able to view a subset of the Monitor section in Dashboard and no changes can be made. Please note - monitor-only admins can view summary reports but not schedule reports via email in the dashboard.

Read-only: User able to access most aspects of a network, including the Configure section, but no changes can be made.

Full: User has access to view all aspects of a network and make any changes to it.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email address</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network - Full admin</td>
<td>[Redacted]</td>
<td>Wireless</td>
</tr>
<tr>
<td>Network - Guest ambassador</td>
<td>[Redacted]</td>
<td>Wireless (Guest Ambassador)</td>
</tr>
<tr>
<td>Network - Monitor-only admin</td>
<td>[Redacted]</td>
<td>Wireless (Monitor-only)</td>
</tr>
<tr>
<td>Network - Read-only admin</td>
<td>[Redacted]</td>
<td>Wireless (Read-only)</td>
</tr>
</tbody>
</table>

Managing Organization Permissions

All permissions for a Dashboard organization can be managed under Organization > Administrators, however, this page is only visible to users with Full or Read-only organization access. Changes on this page can only be made by users with Full organization access.

Adding an Organization Admin

Under Organization > Administrators

1. Click Add admin along the right side of the page.

2. Enter the admin's Name and Email they will use to login.
3. Choose a level of Organization Access, as defined in the Organization Permission Types section.
4. Click Create admin.
5. An e-mail will be sent to the e-mail address entered with a temporary password and instructing the user how to log in.

6. Click **Save changes**.

**Modifying/Removing Organization-wide Access**

Under **Organization > Administrators**

1. Click the row for the admin.

2. Change their **Organization Access** to "None", or the desired privilege level.

3. Click **Update admin**
4. Click **Save changes**.

*Note: If an admin has no other network-specific access and is given "None" for Organization Access, they will be deleted from the list of administrators.*

---

### Deleting an Organization Admin

**Under Organization > Administrators**

1. Click the checkbox next to the name of the admin.

   ![Checkbox](image1)

   - Example admin

2. Click **Delete**.

   ![Delete Button](image2)

3. Click **Save changes**.

---

### Policy and Best Practices for Organization Management

By policy, Cisco Meraki’s support team does not make Dashboard configuration changes on behalf of the customer. Dashboard administrators must make their own configuration and account changes on the Meraki Dashboard. Just as Cisco Meraki will not make any configuration changes, they can not make any adjustments to organization or network permissions; all changes to dashboard administration must be made by an existing org admin on that dashboard account. Please refer to section 1.3.1 of our [End Customer Agreement](#) for details.

This policy is designed to protect the owners of the network from malicious intent. As such, it is strongly recommended to follow these best practices when determining org administration, to ensure the security of your dashboard network:

- Dashboard organizations should always have **at least two organization admins**
  - This is best practice in case one account is locked out or if email access to that account’s email address is lost.
- Be cautious in selecting an appropriate org admins, as the org admin has the highest level of control in the dashboard organization.
  - The active owner of the Cisco Meraki hardware and licenses should be org admins on the account.
- Ensure that the username/email address of the org admin is associated with a domain under your control.
  - Aids when separating relationships with previous org admins, for account recovery purposes.
  - Allows control of the email alias of the org admin.
- Use two-factor authentication and store backup authentication keys in a safe place.
  - For example, [Google Authenticator](#) can be used as a two-factor auth solution with dashboard.
- Any consultants should be granted limited access as needed.
Most likely, for technical configuration changes, offering temporary access as a network admin is the best option.

If the consultant requires org admin permissions, be sure to revoke all org admin permissions once the necessary changes have been implemented. Ideally, the hardware/license owner should be the only org admin.

- If the current org admin is leaving the company, it is strongly recommended to revoke and/or reassign their account permissions early in the off-boarding process.
- Treat a Dashboard Organization Administrator like a Domain Admin for Active Directory, or the primary contact for domain name registration; only the person in this role has the ability to promote other users to this role.

Managing Network Permissions

Privileges granted at the organization level will apply to all networks in an organization, and can only be managed from the Organization > Administrators page. Permissions for specific networks can be managed in two locations. Under Organization > Administrators, or under Configure > Alerts & administration/Network-wide settings.

Adding a Network Admin

Under Organization > Administrators

1. Click Add admin.

2. Enter the admin's Name and Email they will use to login.

3. (Optional) Choose a level of Organization Access, as defined in the Organization Permission Types section.

4. Click Add access privileges.
5. Select the network to grant access to in the **Target** field.

6. Select the level of privilege to provide under the **Access** field, as defined in the Network Permission Types section.

7. Click **Create admin**.

8. Click **Save changes**.

9. An e-mail will be sent to the e-mail address entered with a temporary password and instructing the user how to log in.

Under **Configure > Alerts & administration/Network-wide settings**

1. Select a user in **Add an existing user...** or click **Create new user**.

2. If using Create new user, Enter the admin’s **Name** and **Email** they will use to login.

3. Click **Create user**.
4. If a message indicates the user already exists, use the **Add an existing user...** field to search for the e-mail address.

5. Under **Privileges** for the new user, choose the level of network access to provide, as defined in the [Network Permission Types](#) section.

6. Click **Save changes**.

### Modifying Network Access

**Under Organization > Administrators**

1. Click the row for the admin.

2. In the row for the **Target** network, change the **Access** to the desired level.
3. Click **Update admin**.

4. Click **Save changes**.

Under **Configure > Alerts & administration/Network-wide settings**

1. Update the **Privilege** dropdown for the admin user to the desired level.

<table>
<thead>
<tr>
<th>User</th>
<th>Account status</th>
<th>Privileges</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example admin</td>
<td>Active</td>
<td>Full</td>
<td>Log out</td>
</tr>
</tbody>
</table>

2. Click **Save changes**.

**Removing Network Access**

Under **Organization > Administrators**

1. Click the row for the admin.

2. Click the **X** in the row for the **Target** network.

3. Click **Update admin**.
4. Click **Save changes**.

Under **Configure > Alerts & administration/Network-wide settings**

1. Click the X in the row for the admin user.

![User table](image)

2. Click **Save changes**.

*Note: At present, current and past administrative users will continue to appear in the Configure > Users list when using Meraki authentication, even if no permissions are granted. Unless the user has been authorized for the SSID/VPN or given dashboard permissions, they will have no access as a result of appearing in this list.*

---

**Troubleshooting Network Permissions**

**Error - This email is already in use**

When attempting to add a network admin (from **Configure > Network-wide settings** or **Configure > Alerts and administration**) by using the **Create new user** button, an error may appear indicating that 'This email is already in use'. Even when the user doesn't appear in the list above. This is because an account had been previously created for this e-mail address, either on this page or elsewhere in the organization. To add the user, click in the **Add an existing user** box and begin entering the e-mail address of the user. It should appear in the dropdown and can be selected. Then choose the **Privileges** desired and click **Save changes**.

For additional information on adding network or organization admins, visit [Managing Organization/Network Administrators and Guest Ambassador Accounts](#).

---

**Permissions by Network Tag**

To simplify the assignment of network-level permissions in an organization with many networks, permissions can be granted to users for a given network tag. Those permissions will then be applied to all networks in an organization with that tag. These changes can only be made by users with Full organization access.

![Network tag table](image)

Start by tagging any appropriate networks:

1. Navigate to **Organization > Overview**.
2. Click the checkboxes next to the desired networks.

3. Click **Tag**.

4. In the **Add** field, select or enter any desired tags.
   a. To add a new tag, type the name of the new tag as a single world, with no spaces. (ex. "newtag" or "new_tag")
   b. Then click **Add option** next to the name of the tag desired.

5. Once the tag appears as a bubble in the **Add** field, click the **Add** button.
Then grant permissions to those networks based on the tag:

1. Navigate to Organization > Administrators.
2. Click the row for the admin.

3. Click Add access privileges.

4. Under Target select the entry that begins with Tag and includes the name of the tag applied earlier.

5. Under Access indicate the level of access this admin should have to the networks with this tag.

6. Click Update admin.

7. Click Save Changes.

Switch Port Management Privileges

Permissions can also be assigned at the switch port level, to allow for lower tier technicians or external contractors to make basic changes to the network. This is done by tagging individual switch ports, creating a port management privilege for the tag(s), and then granting that privilege to an administrator.
Adding Port Tags

1. Navigate to **Configure > Switch ports**.

![Switch Configuration Image]

2. Click the checkbox next to any switch ports that should be tagged.

   ![Checkbox List]

3. Click **Tag**.

   ![Tag Button]

4. In the **Add** box, select an existing tag....

   ![Add Box]

   ...or create a new tag by entering the name, and clicking **Add option**.

   *Note: Tags cannot contain spaces.*
5. Once any desired tags appear in the box as bubbles, click **Add**.

**Add:**

- `new_tag`

No results match "new_tag"

*Add option: "new_tag"

6. The selected ports will now be tagged as desired.

*Note: The "Tags" column may need to be added to the table using the + button on the right side of the header column.*

---

### Removing Port Tags

1. Navigate to **Configure > Switch ports**.

2. Click the checkbox next to any switch ports that should be tagged.
3. Click **Tag**.

4. In the **Remove** box, select any existing tags that should be removed.

5. Once any desired tags appear in the box as bubbles, click **Remove**.

---

**Creating Port Management Privileges**

1. For a **combined network**, navigate to **Network-wide > Administration**.

2. For a non-combined network, navigate to **Network-wide > General**.
3. Under **Port management privileges** click **Add a port management privilege**.

These privileges allow read-only access to the entire network and configuration of switch ports that have any of the selected tags. Packet capture settings apply to the entire network.

4. Enter a **Privilege name** that describes the purpose of the privilege.

```
Privilege name
Port_admin
```

5. Select any **Port tags** that the privilege provides access to.

```
Port tags
example_tag
```

6. Select whether **Packet capture** is allowed or not on these ports.

```
Packet capture
Not allowed
```
Removing Port Management Privileges

1. Navigate to Configure > Alerts & administration.

   ![Configure > Alerts & administration](image)

2. Under Port management privileges, click the X in the Actions column for the privilege to be removed.

   ![Port management privileges](image)

3. Click Save changes.

Assigning a Port Management Privilege

Port management privileges are assigned to network administrators the same way as other privileges described in the Managing Network Permissions section above. Just select the privilege created earlier from the Privilege drop-down for the desired administrator.

![Privileges](image)
Unlocking an Administrator Account

It is possible to configure a lockout policy for accounts in a Dashboard organization, under Organization > Configure > Settings > Security, by enabling the Account lockout option.

In the event an administrator's account has been locked as a result of too many failed authentication attempts, it can be unlocked by another user with Full network permissions (for network admins) or Full organization permissions. The user unlocking the account must have equivalent or greater permissions (i.e. a network-only admin cannot unlock the account for an organization-only admin).

For admin users with Organization permissions:

1. Navigate to Organization > Administrators.
2. Click the checkbox next to the admin with the locked account.
3. Click Unlock.

For admin users with Network permissions:

1. Navigate to Configure > Alerts & administration/Network-wide settings.
2. Click the Unlock button next to the admin with the locked account.

Resetting an Admin User's Password

In order to reset an admin user's password:

1. Log out of Dashboard by clicking sign out in the upper right corner
2. Go to https://account.meraki.com/login/reset_password
3. Enter the e-mail address of the admin account that needs to be reset
4. Click Submit

An e-mail will be sent to the e-mail address with details on how to reset their password.

---

**Privilege Precedence**

Privileges in Dashboard are additive, and a user will be granted rights on a page based on their highest level of applicable assigned permissions. Thus an admin with Read-only rights at the organization level, but Full permissions for a particular network will effectively have Full permissions to that network.

This is similarly applied with tags. If a user has Read-only and Full access to a network based on different tags, the user will be given Full access.