Managing Firmware Upgrades

Overview

Firmware upgrades allow network administrators to utilize the latest features and security enhancements on their Meraki devices. The Cisco Meraki Dashboard allows admins to easily schedule and reschedule firmware upgrades on their networks, opt-in to beta firmware releases, view firmware changelog notes, and to set maintenance windows. This article outlines the functions of the firmware upgrades tool in Dashboard, as well as additional considerations for using and managing firmware.

Managing Firmware as an Organization Admin

The Firmware Upgrades tool in Dashboard allows organization admins to quickly and easily manage firmware versions on a per-network and per-device type basis. Additionally, the Firmware Upgrades tool can be used to schedule, reschedule, and cancel bulk upgrades of networks, view firmware changelog notes, view firmware version numbers, and to rollback the firmware on a recently upgraded network.

Scheduling Firmware Upgrades

Keeping up-to-date on firmware allows administrators to utilize the latest features and ensures that the latest security enhancements are running on their hardware. Admins can upgrade to the latest stable or latest beta firmware. Follow the steps below to schedule a firmware upgrade.

1. Navigate to Organization > Monitor > Firmware upgrades.
2. Click the All networks tab in the upper-left.
3. Select the devices or networks to be upgraded by clicking the checkboxes beside the network names. Admins can specify upgrades on a per-network or per-device type basis by using the Device type, Current version, and/or Firmware status dropdown selectors.
4. Click the Schedule upgrades button.
5. Select the firmware version that should be upgraded to using the Target firmware version selector.
6. Select either Perform the upgrade now or Schedule the upgrade for, specifying a specific date and time for the upgrade.
7. Review the Change Summary and select Schedule change for network.

Note: When downgrading from a beta firmware to a stable firmware, a feedback request page will be presented. Please select any options that reflect the downgrade reason before selecting Schedule change for network.

Rescheduling or Canceling a Firmware Upgrade

Rescheduling or canceling a firmware upgrade can be performed after a firmware upgrade has been scheduled. Follow the steps below to reschedule or cancel a firmware upgrade.

1. Navigate to Organization > Monitor > Firmware upgrades.
2. From the **Overview** tab, view the **Scheduled changes** section, and find the applicable scheduled upgrade.

3. Scheduled upgrades will be grouped by their respective products and scheduled upgrade time.

4. For any given scheduled product upgrade, Click either the **Reschedule** or **Cancel** button. If selecting **Reschedule**, choose either **Perform the upgrade now** or **Schedule upgrade for**, specifying a date and time for the upgrade to take place.

5. By selecting **Cancel** for a given scheduled upgrade, the upgrade will be canceled for all networks listed for that upgrade.

**Note:** Firmware upgrades can be scheduled up to one month in advance and as such, can only be deferred/rescheduled for one month at a time. Cancelling scheduled firmware upgrades does not exclude a given network from future scheduled upgrades.

---

### Rolling Back a Recent Firmware Upgrade

Firmware upgrades can be rolled back to their previous version up to 14 days after an upgrade takes place. Follow the steps below to roll back a firmware upgrade.

1. Navigate to **Organization > Monitor > Firmware upgrades**.
2. From the **Overview** tab, view the **Most recent upgrades** section, and find the applicable upgrade entry.
3. Click on the applicable upgrade entry where it lists the number of networks and devices that were upgraded.
4. Click the **Rollback** button.
5. Select a reason for the rollback and enter a brief description.
6. Select **Perform the upgrade now** or **Schedule the upgrade for**, specifying a date and time for the rollback.
7. Click **Submit** to schedule the rollback.

---

### Viewing Firmware Changelog Notes

Changelog notes are maintained on a per-firmware version basis and include information about new features, bug fixes, and known issues that are associated with a particular firmware version. Follow the steps below to view the firmware changelog notes.

1. Navigate to **Organization > Monitor > Firmware upgrades**.
2. From the **Overview** tab, refer to where it lists **Current stable firmware versions**.
3. Select **Release notes**. This will display the current stable firmware changelog notes.
4. To view older or newer changelog notes, select **Previous version** or **Next version** from the changelog notes window.

**Note:** The firmware changelog can also be view from the **All networks** tab, and clicking on the firmware version links listed in the "Current firmware version" column.

---

### Managing Firmware as a Network Admin

Firmware upgrades can be scheduled on a per-device type basis for each Dashboard network. Follow the steps below to schedule a firmware upgrade.

1. Navigate to **Network-wide > Monitor > General**.
2. Scroll down to where it lists **Firmware upgrades**.

3. If there is a new firmware available, select either **Reschedule the firmware upgrade**, **Perform the upgrade now**, or **Upgrade as scheduled**.

4. Navigate to the bottom of the page and select **Save**.

To elect to run beta firmware, select **Try beta firmware** and select **Yes**.

---

**Viewing Firmware Changelog Notes as a Network Admin**

Changelog notes are maintained on a per-firmware version basis and include information about new features, bug fixes, and known issues that are associated with a particular firmware version. Follow the steps below to view the firmware changelog notes.

1. Navigate to **Network-wide > Configure > General**.
2. Scroll down to where it lists **Firmware upgrades**.
3. If there is a new firmware available, select the **What’s new** button beside the corresponding firmware. This page lists the firmware changelog notes.

---

**Firmware Upgrade Barriers**

Firmware Upgrade Barriers is a feature built in to prevent certain upgrade paths on devices running older firmware versions and trying to upgrade to a build that would otherwise cause compatibility issues. Having devices use intermediary builds defined by Meraki will ensure a safe transition when upgrading your devices.

Here is an example of when firmware upgrade barriers come into effect. You might find yourself in a situation where you are unable to upgrade a device for an extended period of time due to uptime or business requirements. There is a switch in the network that is running MS 9.27 and would like to update to the latest stable version (which at the time of writing, is) 11.30. Attempting to upgrade from 9.27 to 11.30 will not be a selectable option in the dashboard and administrators will have to upgrade to 10.35 first.

---

### Cisco Meraki MS Switch Firmware

<table>
<thead>
<tr>
<th>Current</th>
<th>Intermediary</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.27 X</td>
<td>10.35</td>
<td>11.30</td>
</tr>
</tbody>
</table>

In order to complete the upgrade from the current version to the target version, two manual upgrades will be required. The first from your current to the intermediary version, and another from the intermediary to your target version.
1. Select the **Organization > Monitor > Firmware upgrades > All networks**. From here you can select an individual or many networks within your organization.

2. Select the **Target firmware version** you are trying to upgrade to from the dropdown menu. In this case, because we are upgrading from MS 9.27 we must upgrade to MS 10.35 first. Note that the latest stable is not a selectable option and won't be until you upgrade to the required intermediary firmware version. This is a prime example of a firmware barrier.

3. Select a scheduled time you want to perform the upgrade. You can cancel the upgrade from the **Firmware upgrades** page and select **Reschedule**.
4. After the first upgrade has completed, repeat steps 1 - 3 to perform the second half of the upgrade from your intermediary version to your target version

**Firmware Version Status**

Cisco Meraki is committed to delivering powerful yet easy to manage firmware updates for all Meraki products via Firmware upgrades tool in the Dashboard. In order to further simplify and streamline the firmware update process, we are introducing Firmware Status for Meraki firmware. It’s always recommended to run at least the latest Stable version for each respective product in order to ensure the best performance, stability, and protection from security vulnerabilities.

Each firmware version now has an additional Status column as follows:

1. **Good** (Green) status indicates that your Network is set to the latest firmware release. Minor updates may be available, but no immediate action is required.

2. **Warning** (Yellow) status means that a newer stable major firmware or newer minor beta firmware is available that may contain security fixes, new features, and performance improvements. We recommend that you upgrade to the latest stable or latest beta firmware version.

3. **Critical** (Red) status indicates that the firmware for your Network is out of date and may have security vulnerabilities and/or experience suboptimal performance. We highly recommend that you upgrade to the latest stable and latest beta firmware release.
The number of Networks with firmware matching "Warning" and "Critical" status will appear on the Overview tab of the Firmware upgrades page.

FAQ:

Q: What does the date beside "Warning" and "Critical" mean?

A: This date is an End of Support date for that particular firmware version. 6 months prior to this date firmware will go into the "Warning" status. Once the End of Support date has passed the firmware will go into the "Critical" status. We highly recommend updating the firmware before it reaches the "Critical status.

Q: What are the implications of running firmware marked with "Warning" and "Critical" status?

A: You might experience performance degradation, stability issues, and be exposed to the security vulnerabilities addressed in the latest Stable or latest Beta firmware.