Operations

The **Operations** menu is used by administrators to perform operational tasks on the Secure Malware Analytics Appliance. This chapter describes these tasks, including activating configuration changes, reloading the Admin UI, managing jobs and power settings, and updating the appliance.

Activate

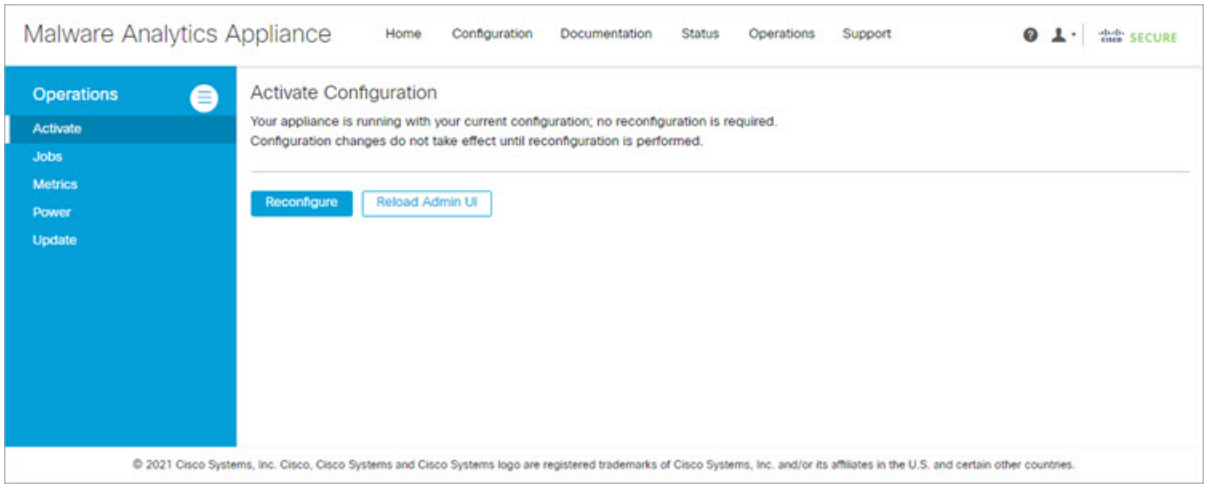
Changes to the Admin UI configuration settings must be saved, and several changes also require that you finalize the changes with a reconfiguration. Configuration changes do not take effect until reconfiguration is completed.

If a reconfiguration is required, a light orange alert message appears in a banner in the upper portion of the page. When you click the **Reconfigure** button on this banner, it takes you to **Activate Configuration** page in the **Operations** menu. From this page, you can apply the configuration changes and also reload the Admin UI.

Step 1 Click **Reconfigure** on the alert message to launch the reconfiguration process.

Step 2 On the **Activate Configuration** page, click **Reconfigure** to run the reconfiguration job.

Figure 1: Activate Configuration



Step 3 On the confirmation dialog, click **Reconfigure** to start the reconfiguration job.

Configuration is activated, and messages on its progress are displayed in the jobs window. Details are kept in the Jobs page if you need to review error messages or other information.

When completed, a confirmation message is displayed indicating the reconfiguration was successful.

Step 4 Click **Continue**.

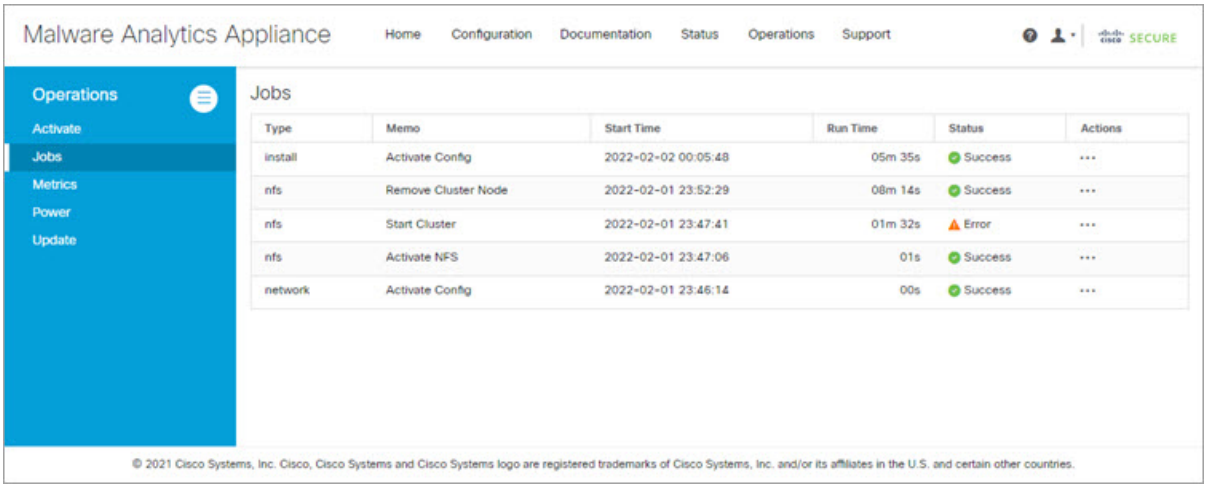
Step 5 If you want to refresh the Admin UI, click **Reload Admin UI**.

Jobs

You can view the jobs that have been run on the Secure Malware Analytics Appliance using the **Jobs** page in the Admin UI. You can use this page to view error messages or other information about a specific job.

Step 1 Click the **Operations** tab and choose **Jobs**.

Figure 2: Jobs



The job type, start time, run time, and status is displayed for each job.

Step 2 Click the **Details** button in the **Actions** column to view information about the job.

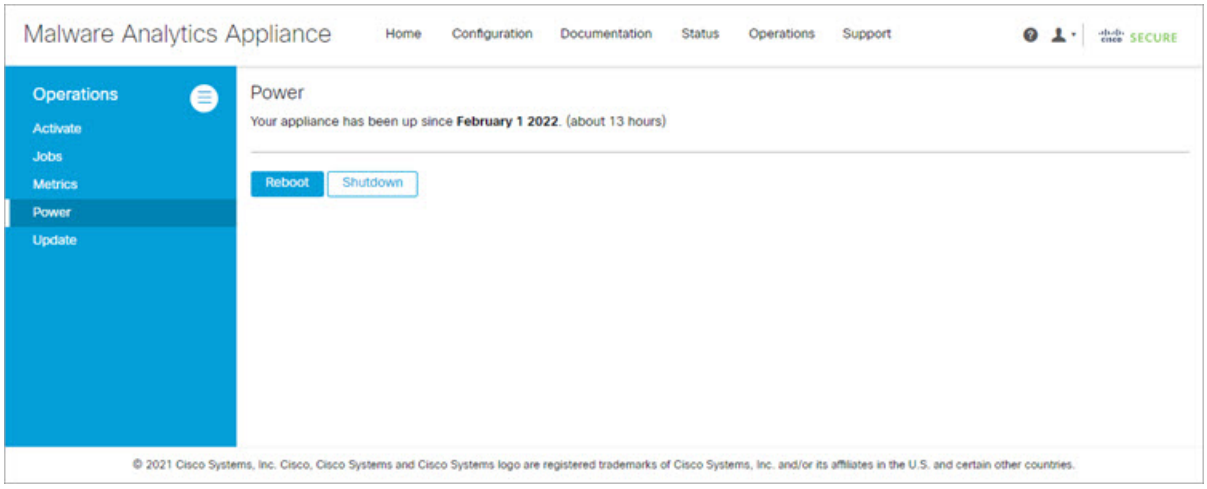
Power

You can reboot or shut down the Secure Malware Analytics Appliance from the **Power** page in the Admin UI.

Note The GNU GRUB bootloader is completely removed from the Secure Malware Analytics Appliance software stack. Whereas our prior configuration did not allow unsigned configuration files to be loaded (and thus was not vulnerable to CVE-2020-10713), the new boot mechanism removes GRUB entirely.

Step 1 Click the **Operations** tab and choose **Power**.

Figure 3: Power



The date from which your appliance has been powered up is displayed.

Step 2 Click **Reboot** to restart the appliance, or **Shutdown** to completely shut the appliance off.

Update

Before you can update the Secure Malware Analytics Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the *Cisco Secure Malware Analytics Appliance Getting Started Guide*.

Note If you have a new Secure Malware Analytics Appliance that shipped with an older version of software and want to install updates, you must first complete the initial configuration. Updates will not download unless the license is installed, and may not apply correctly if the Secure Malware Analytics Appliance has not been fully configured, including the database.

You can check for new updates (**Operations** > **Update**) and apply them.

Configuration now happens as part of the regular boot process. With each reboot, the appliance is reset to a completely pristine software loadout (with code signatures checked at runtime). Configuration operations that previously happened only during a reconfiguration cycle with multiple reboots now occur as part of every boot cycle. This means that:

- The reconfigure with reinstall operation is made redundant.
- Installing upgrades is now faster, and only requires one reboot.

The following considerations should be observed when installing updates:

- Secure Malware Analytics Appliance updates are applied through the Admin UI.

- If the update server sends an update, the client moves all the way forward to that version. It's not always possible to skip interim releases; when not possible, the update server will require the appliance to install the release before it can download the next update.
- If the server allows you to download a version, you are eligible to move to that version directly; that is, with no intervening reboots beyond those needed for a single upgrade.
- Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.
- For offline (airgapped) update process, see Update Secure Malware Analytics Appliance.

Version Lookup Table

To identify the correct build number and corresponding release version, see the *Cisco Secure Malware Analytics Appliance Version Lookup Table*.

Updates Port

The Secure Malware Analytics Appliance downloads release updates over SSH, port 22.

- Release updates can also be applied from the textual (curses) interface, not just from the web-based administrative interface (Admin UI).
- Systems using DHCP need to explicitly specify DNS. An upgrade of a system without a DNS server explicitly specified will fail.

Database Schema Updates

Historically, on standalone appliances, database migrations associated with updates occurred while the system was offline in single-user mode, except in a cluster, where the updates occurred after the first upgraded node came back online. (The exception to this was for unusually long updates that could be run in the background, which were handled on a case-by-case basis.)

Secure Malware Analytics Appliance (v2.5.0 and later) updates the database schema after the system finishes reboot, which may cause the boot process to take slightly longer. (Very long reboots continue to be handled on a case-by-case basis.)

In prior releases, non-clustered systems with backup support enabled would make a best-effort attempt to operate correctly when their NFS server was down. Due to changes in ElasticSearch functionality, we can no longer guarantee this behavior.

Background Elasticsearch index migration to ES6-native indexes is enabled in v2.7.2 and later. This migration must successfully complete before any version of the Secure Malware Analytics Appliance which requires Elasticsearch 7.0 or newer is installed.

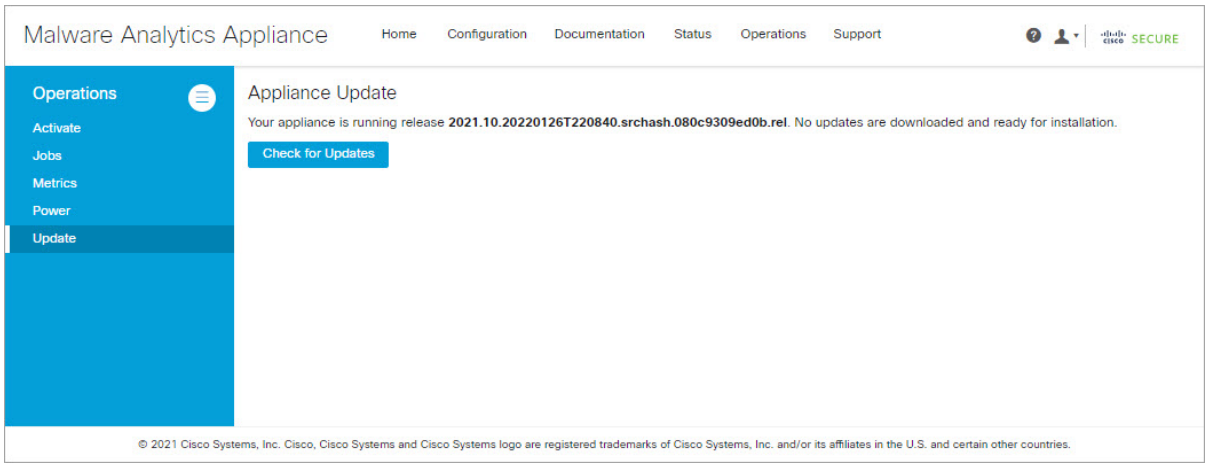
Note Elasticsearch index migration may cause substantial delays in the NFS backup process, causing related warnings. These warnings should be disregarded, as service notices indicate that index migration is actively ongoing. You should only raise a ticket with Support if the index migration process fails to make progress over an extended period.

Installing Updates

Perform the following steps to check for updates and to update the Secure Malware Analytics Appliance.

Step 1 Click the **Operations** tab and choose **Update** to open the**Appliance Updates** page.

Figure 4: Appliance Updates Page



The current release version is displayed in the upper portion of the page. It also informs you if there is an update available to install. For information about the release versions, see the *Cisco Secure Malware Analytics Appliance Version Lookup Table*.

Step 2 Click **Check for Updates**.

A check is run to see if there is a more recent update/version of the Secure Malware Analytics Appliance software, and if so, downloads it. This may take some time.

Step 3 Once the update has been downloaded, click **Apply Update** to install it.

Troubleshooting Updates

This section includes issues that may occur while updating the appliance and how to resolve them.

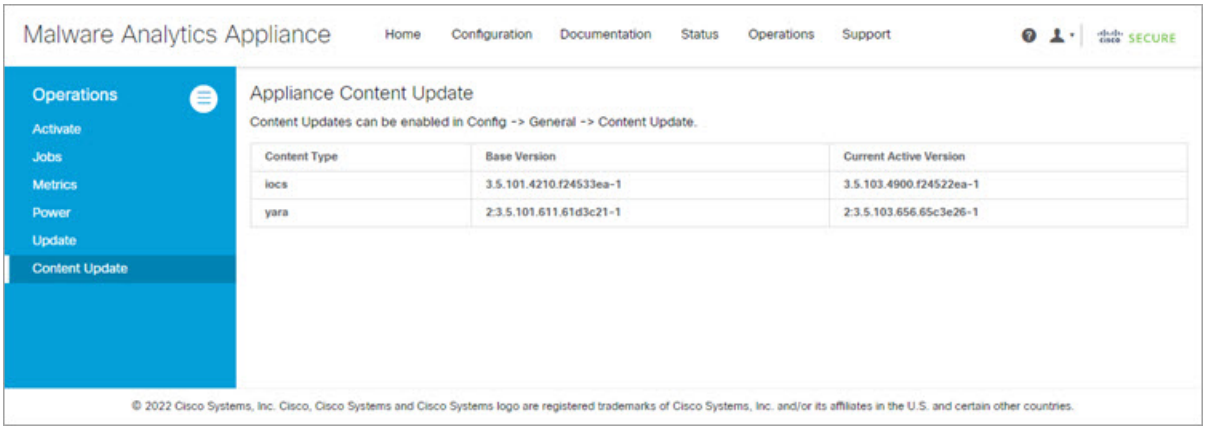
Database Upgrade Not Successful Message

A *database upgrade not successful* message may be displayed if a new Secure Malware Analytics Appliance is running an older version of PostgreSQL and the automated database migration process failed. It is critical that this be fixed prior to any upgrade to v2.0. See *Cisco Threat Grid Appliance Release Notes v2.0.1* for more information.

Appliance Content Update

The Appliance Content Update page provides the base and the current version of the behavioral indicators or iocs (Indicators of Compromise) and yara.

Figure 5: Appliance Content Update



Note Update your appliance to the latest *iocs* and *yara* while you update the appliance. For more information on updating the appliance, see Update, on page 4.