Administration

This chapter provides general information that is useful for Administrators. It includes the following topics:

Login Names and Passwords (Default)

The default login names and passwords are listed in the following table:

User	Login/Password
Web UI Administrator	Login: **admin** Password: **changeme**
OpAdmin and Shell User	Use the initial Threat Grid/TGSH Dialog randomly generated password, and then the new password entered during the first step of the OpAdmin configuration workflow. If you lose the password, follow the **Lost Password** instructions located in the **Support** section of the Cisco Threat Grid Appliance Administrator Guide.
CIMC	Login: **admin** Password: **password**

Reset Administrator Password

The default administrator password is only visible in the TGSH Dialog during the initial appliance setup and configuration. Once the initial configuration is completed, the password is no longer displayed in visible text.

Note LDAP authentication is available for TGSH Dialog and OpAdmin login when you have multiple administrators. If the appliance is configured for LDAP authentication only, resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.

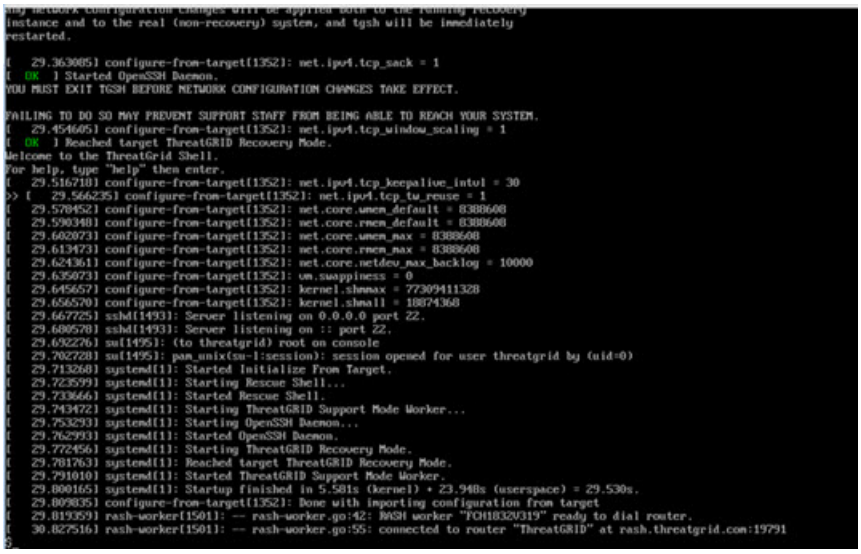
If you lose the administrator password and are unable to login to OpAdmin, complete the following steps to reset the password.

Step 1 Reboot the Threat Grid Appliance and immediately select **Recovery Mode** from the Recovery Options.

Figure 1: Boot Menu - Recovery Mode

The Threat Grid Shell opens.

Figure 2: Threat Grid Shell in Recovery Mode



Step 2 Run `passwd` to change the password.

Figure 3: Enter New Password

Note The command prompt is not always visible in this mode and logging output may be displayed at any point on top of your input. This does not affect input; you can keep typing *blindly*. Ignore the two lines of logging output.

Step 3 Enter (blindly) the password and press **Enter**.

Step 4 Re-type the password and press **Enter**.

Note The password will not be displayed.

Step 5 Type **exit** from the command line to save.

Important You must exit before rebooting to save the new password. If you do not exit, although everything appears to be OK, the password change will be quietly discarded.

Step 6 Type **reboot** and press **Enter** to start the appliance in normal mode.

Install Updates

Before you can update the Threat Grid Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the Cisco Threat Grid Appliance Setup and Configuration Guide.

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

The following considerations should be observed when installing updates:

- Threat Grid Appliance updates are applied through the OpAdmin Portal.
- 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 instructions on installing updates, see the Install Updates section in the Cisco Threat Grid Appliance Setup and Configuration Guide.

Version Lookup Table

To identify the correct build number and corresponding release version, see the Cisco Threat Grid Appliance Version Lookup Table.

Updates Port

The Threat Grid Appliance downloads release updates over SSH, port 22.

- Release updates can also be applied from the textual (curses) interface (Threat Grid Appliance v1.1 and later), not just from the web-based administrative interface (OpAdmin).
- Systems using DHCP need to explicitly specify DNS (v1.3 and later). An upgrade of a system without a DNS server explicitly specified to 1.3 will fail.

Troubleshoot Updates

A *database upgrade not successful* message means that a new Threat Grid 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 Threat Grid Appliance Release Notes v2.0.1 for more information.

Database Schema Updates

Historically, on standalone appliances, database migrations associated with updates would occur while the system was offline in single-user mode, except in a cluster, where the updates would occur 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 we handled on a case-by-case basis.)

Threat Grid Appliance (v2.5.0 and later) now updates the database schema after the system finishes reboot. This may potentially cause the boot process to take slightly longer. (Very long ones will continue to be handled case-by-case.)

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 Threat Grid 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.