

Introduction

Welcome to the *Cisco Threat Grid Appliance Administration Guide*. This chapter provides a brief description of the appliance, the intended audience and how to access relevant product documentation.

- About the Cisco Threat Grid Appliance, on page 1
- What's New In This Release, on page 2
- Audience, on page 2
- About This Guide, on page 3
- User Documentation, on page 4
- Login Names and Passwords (Default), on page 6
- Resetting the Administrator Password, on page 7

About the Cisco Threat Grid Appliance

The Cisco Threat Grid appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Threat Grid Appliance provides the complete Threat Grid malware analysis platform, installed on a Cisco Threat Grid M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

Note Cisco UCS C220-M3 (TG5000) and Cisco UCS C220 M4 (TG5400) servers are still supported for Threat Grid Appliance but the servers are end of life.

Many organizations that handle sensitive data, such as banks and health services, must follow various regulatory rules and guidelines that do not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Threat Grid Appliance on-premises, organizations are able to send suspicious documents and files to it to be analyzed without leaving the network.

With a Threat Grid Appliance, security teams can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. The appliance correlates the analysis results with hundreds of millions of previously analyzed malware artifacts, to provide a global view of malware attacks and campaigns, and their distributions. A single sample of observed activity and characteristics can quickly be correlated against millions of other samples to fully understand its behaviors within an historical and global context. This ability helps security teams to effectively defend the organization against threats and attacks from advanced malware.

What's New In This Release

The following changes have been implemented in this guide in Version 2.12:

Table 1: Changes in Version 2.12

Feature or Update	Section
Updated screenshots and instructions. (The GNU Bootloader is no longer used.)	Resetting the Administrator Password Power.
NTP server can now be made available from the Clean interface.	NTP Server Access Firewall Rules - Clean Interface Outbound (Optional)
Operations not supported in tgsh have been removed.	Threat Grid Shell (tgsh)
Added NTP to the Clean interface table.	Network Interfaces
Updated the diagram for NTP being available on the Clean interface for users to need to use an internal NTP server.	Network Interface Setup Diagram
Wipe is no longer activated from the boot loader menu, but from a command invocation within tgsh in recovery mode.	Wipe Appliance Operation Removing All Data with the Wipe Appliance Operation
Added new topic about Customer Data to the Planning chapter.	Customer Data
Updated the SSL Keys page screenshot.	SSL Keys Page
Added info on downloading a .cert file.	Regenerating SSL Certificates
New topic for restored download functionality.	Downloading SSL Certificates
Updated to reflect download functionality and the new ellipses (**...**) **Actions** menu.	Uploading SSL Certificates
New topic for Backup Details.	Backup Details
New update process.	Update
Updated Live Support Session section to include new heading for Support Servers.	Live Support Session

Audience

This guide is intended to be used by the Threat Grid Appliance administrator after the appliance has been set up and configured, and an initial test malware sample has been successfully submitted and analyzed. It describes

how to manage organizations and users for the Threat Grid malware analysis tool, appliance updates, backups, and other server administration tasks.

This guide also provides information for administrators who are integrating the Threat Grid Appliance with other Cisco products and services, such as Cisco Email Security Appliance, Cisco Web Security Appliance, and AMP for Endpoints Private Cloud devices.



Note For information about Threat Grid Appliance setup and configuration, see the *Cisco Threat Grid Appliance Getting Started Guide*.

About This Guide

This guide provides planning information, configuration tasks, and general administrative tasks, and is organized as follows:

Chapter	Description
Introduction	Provides brief description of the appliance, the intended audience, how to access relevant product documentation, log in names and passwords, how to reset the administrator password, and contacting Support.
Planning	Describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration.
Network Configuration Using the TGSH Dialog	Provides information about using the TGSH Dialog to make changes to your initial network configuration, reconnecting to the TGSH Dialog, and configuring the network in recovery mode.
Configuration Using the Admin UI	Provides information about using the Admin UI to make configuration changes to your appliance. See About the Admin UI for a complete list of tasks that can be performed.
Status	Provides information about viewing system information in the Admin UI, such as installed system packages and their version, detailed logs, and available storage.
Operations	Provides information about activating configuration changes, reloading the Admin UI, managing jobs and power settings, and installing updates.
Support	Provides instructions for starting a live support session and taking support snapshots to aid in resolving issues with the appliance.
Organizations and Users	Provides instructions for creating organizations, managing users, and activating a new device user account.
Inbound and Outbound Connections	Provides information about connecting other Cisco appliances (ESA and WSA), and AMP for Endpoints Private Cloud to the Threat Grid Appliance.
Removing All Data with the Wipe Appliance Boot Option	Describes how to use the Wipe Appliance boot option to remove all data from the Threat Grid Appliance, including clusters.

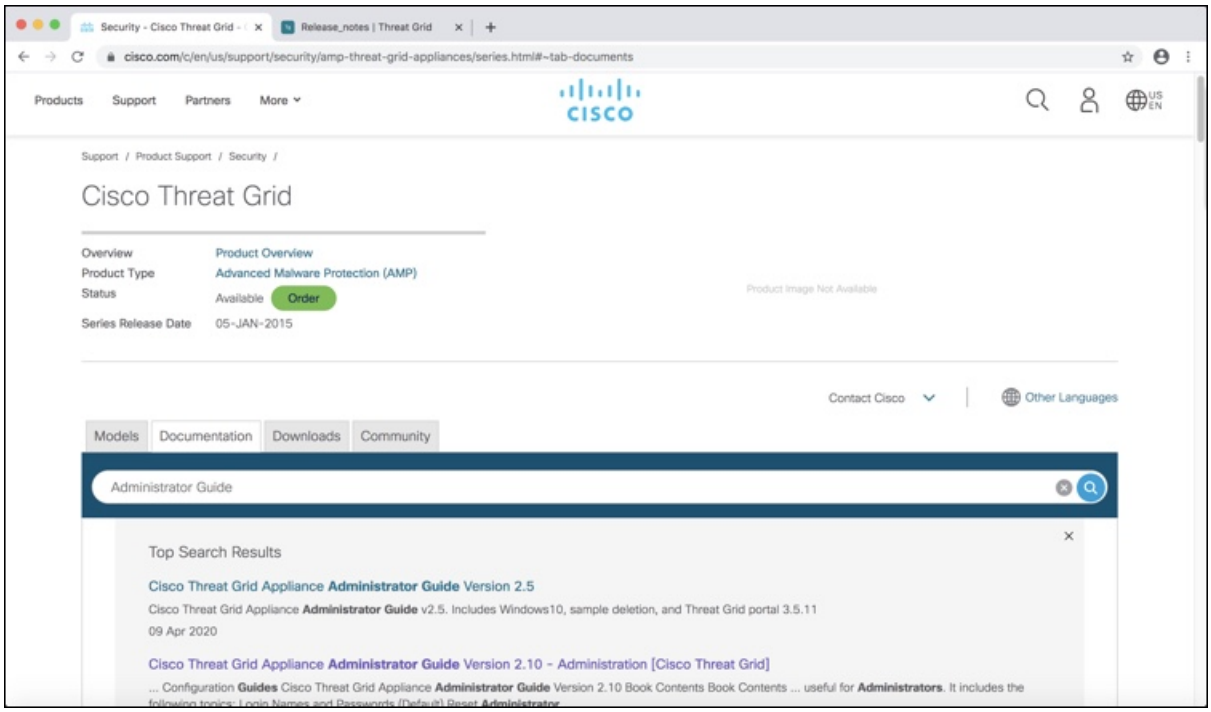
Chapter	Description
CIMC Configuration	Provides information about using the CIMC utility to set up remote server management.

User Documentation

Threat Grid Appliance User Guides

The latest versions of Cisco Threat Grid Appliance product documentation can be found on Cisco.com.

Figure 1: User Guides on Cisco.com



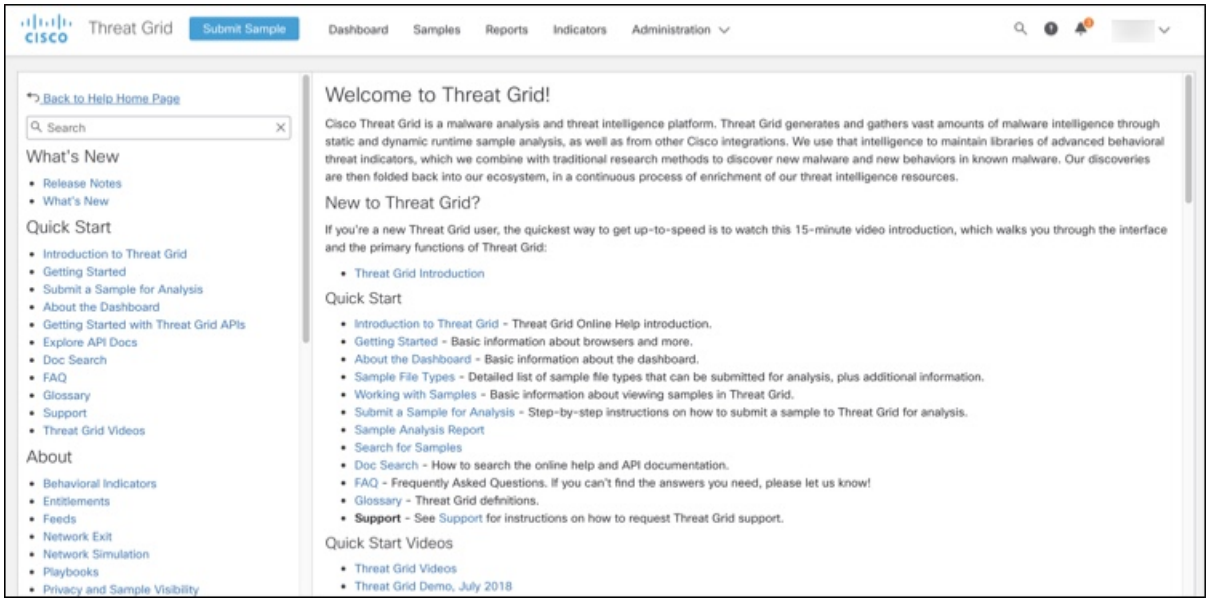
- *Cisco Threat Grid Appliance Release Notes*
- *Cisco Threat Grid Appliance Getting Started Guide*
- *Cisco Threat Grid Version Lookup Table*
- *Cisco Threat Grid M5 Hardware Installation Guide*

Note The Cisco Threat Grid M5 Appliance is supported in Threat Grid Version 3.5.27 and later, and appliance version 2.7.2 and later.

Threat Grid Portal UI Online Help

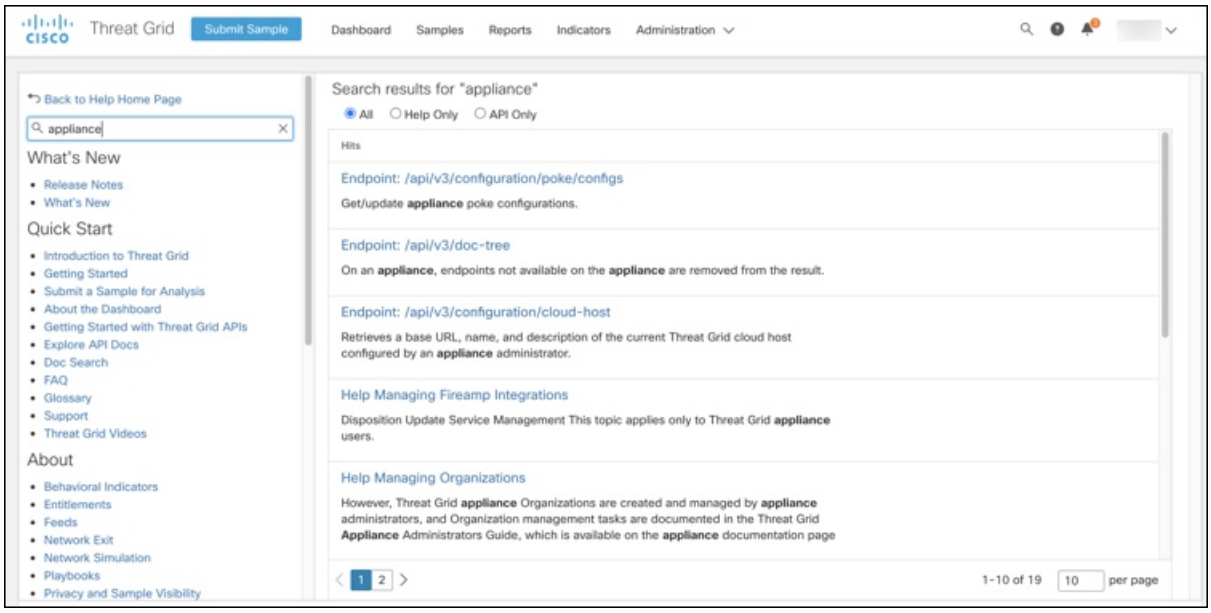
Threat Grid Portal user documentation, including Release Notes, Using Threat Grid Online Help, API documentation, and other information is available from the **?** (**Help**) icon located in the navigation bar in the upper right corner of the Threat Grid user interface.

Figure 2: Threat Grid Portal Online Help



Use the online help Search feature located at the top of the left column to find appliance-specific information.

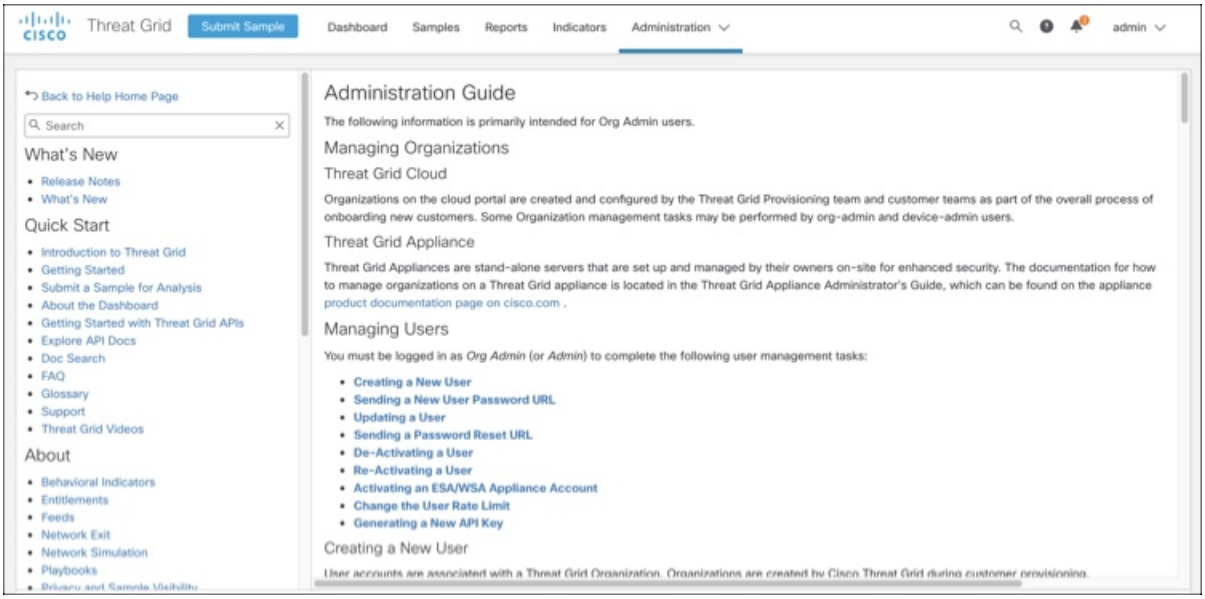
Figure 3: Online Help Search Feature



Threat Grid Portal UI Administration Guide

A portal online help topic is available for administrators, with instructions on how to manage users and other information. Click the **Administration** tab and choose **Administration Guide**.

Figure 4: Administration Guide for the Threat Grid Portal UI



Email Security Appliance and Web Security Appliance Documentation

For information on connecting an Email Security Appliance (ESA) or Web Security Appliance (WSA), see Integrations.

See the instructions for Enabling and Configuring File Reputation and Analysis Services in the online help or user guide for your ESA/WSA:

- *Cisco Secure Email Gateway User Guide*
- *Cisco Secure Web Appliance User Guide*

Login Names and Passwords (Default)

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

User	Login/Password
Admin UI 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 Admin UI configuration workflow. If you lose the password, follow the instructions in Resetting the Administrator Password.

User	Login/Password
Threat Grid Web portal UI Administrator	Login: **admin** Password: Initialize with the first Admin UI password, and then it becomes independent.
CIMC	Login: **admin** Password: **password**

Password Criteria

Passwords must include the following:

- Minimum of 8 characters
- At least one number
- At least one special character
- Uppercase and lowercase characters

Resetting the 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 Admin UI 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 log in to the Admin UI, complete the following steps to reset the password.

Procedure

Step 1 Reboot the Threat Grid Appliance: click the **Operations** tab and choose **Power**, and then click the **Reboot** button. The appliance reboots, and opens the BIOS window.

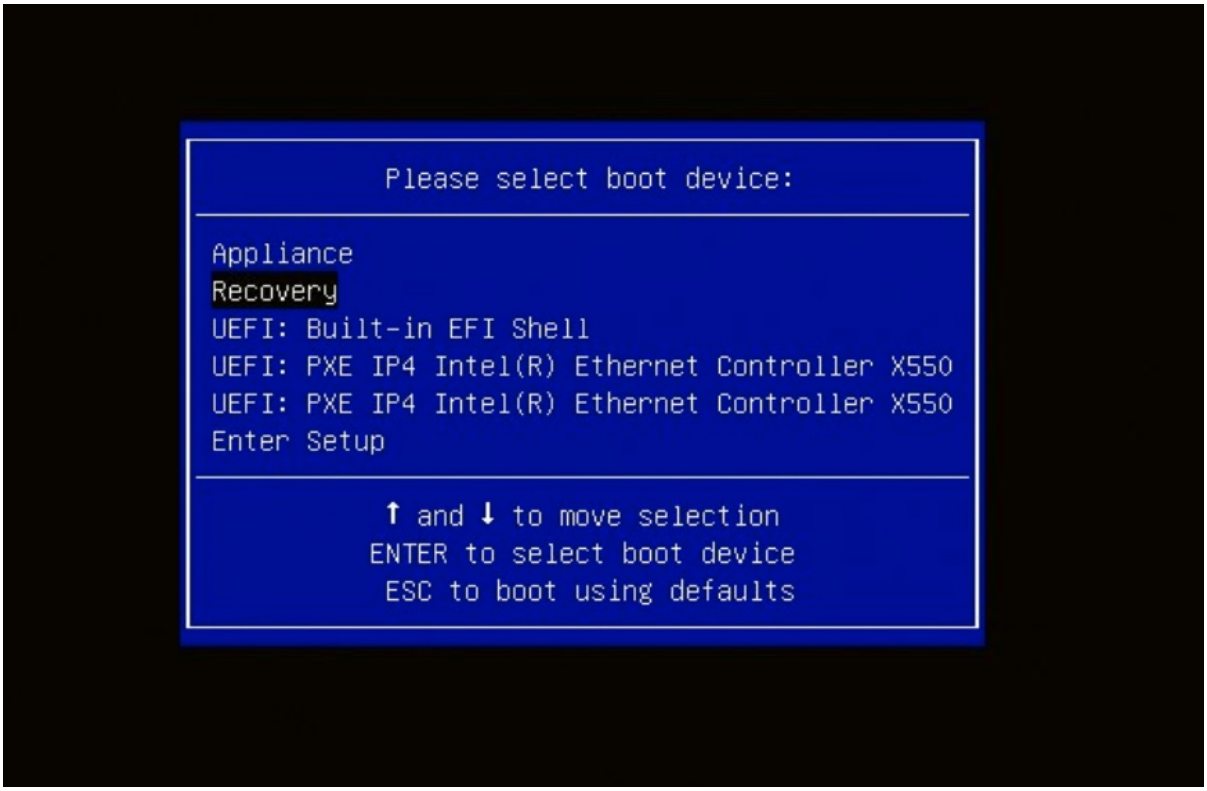
Figure 5: BIOS Window - Choose Boot Menu <F6> for Recovery Mode



Step 2 In the BIOS window, press **F6** to open the **Boot** menu.

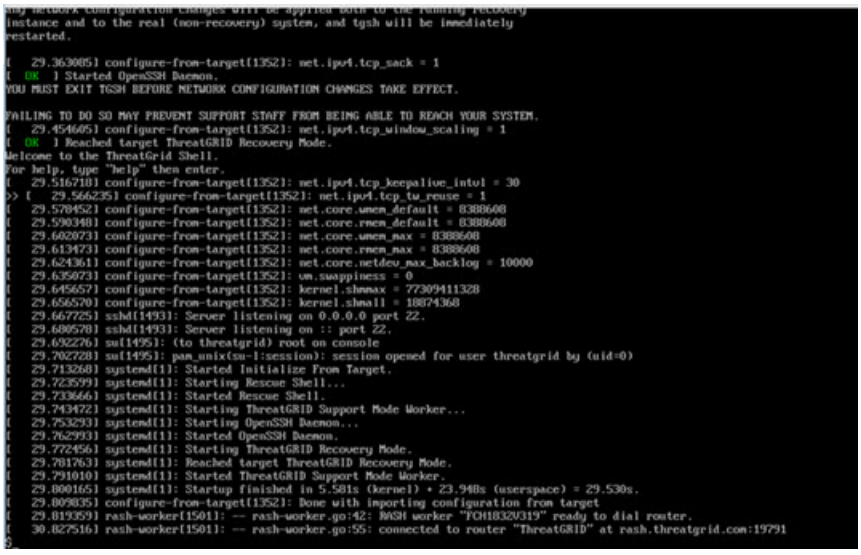
Step 3 Choose **Recovery** and press **Enter**.

Figure 6: Boot Menu



The Threat Grid Shell opens in Recovery Mode.

Figure 7: Threat Grid Shell (tgsh) in Recovery Mode



Step 4 Run `passwd` to change the password.

Figure 8: 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 5 Enter (blindly) the password and press **Enter**.

Step 6 Re-type the password and press **Enter**.

Note
The password will not be displayed.

Step 7 Type **reboot** and press **Enter** to start the appliance in normal mode.

Note
The exit command is no longer required before rebooting for a password reset to take effect (for v2.10 and later).