

Cisco Threat Grid Appliance Administrator Guide Version 2.12

First Published: 2020-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Introduction 1

About the Cisco Threat Grid Appliance 1

What's New In This Release 2

Audience 2

About This Guide 3

User Documentation 4

Login Names and Passwords (Default) 6

Password Criteria 7

Resetting the Administrator Password 7

CHAPTER 2

Planning 11

Supported Browsers 11

Environmental Requirements 12

Hardware Requirements 12

Network Requirements 12

DNS Server Access 13

NTP Server Access 14

Integrations 14

DHCP Requirements 14

License 15

Rate Limits 15

Organizations and Users 15

Updates 15

User Interfaces 16

TGSH Dialog 16
Threat Grid Shell (tgsh) 16
Admin UI 17
Threat Grid Portal 17
Network Interfaces 17
Network Interface Setup Diagram 19
Firewall Rules 20
Privacy and Sample Visibility 22
Samples Submitted by Integrations 23
Wipe Appliance Operation 24
Customer Data 24

CHAPTER 3 **Network Configuration Using the TGSH Dialog** 25
Modifying Network Configuration 25
Reconnecting to TGSH Dialog 26
Configuring Network in Recovery Mode 26

CHAPTER 4 **Configuration Using the Admin UI** 29
About the Admin UI 29
Applying Configuration Changes 31
Authentication 33
LDAP Authentication 33
RADIUS Authentication 35
CA Certificates 36
Change Password 37
Clustering 37
Building a Threat Grid Appliance Cluster 40
Cluster Configuration 41
Start Building Cluster from Existing Standalone Appliance 43
Start Building Cluster with New Appliance 46
Joining Threat Grid Appliances to a Cluster 47
Joining Existing Appliances to a Cluster 48
Joining New Appliances to a Cluster 48
Designating the Tiebreaker Node 49

Removing a Cluster Node 50
Resizing a Cluster 50
Failure Tolerances 50
Failure Recovery 51
API/Usage Characteristics 51
Operational/Administrative Characteristics 51
Sample Deletion 52
Date and Time 52
Email 54
Integrations 54
License 55
Network 57
Configuring DNS 60
Network Exit 60
NFS 63
Appliance Backup 67
Reset Appliance as Backup Restore Target 68
Restore Backup Content 70
Notifications 71
SSH 71
SSL 73
Configuring SSL Certificates 74
Replacing SSL Certificates 75
Regenerating SSL Certificates 76
Downloading SSL Certificate 76
Uploading SSL Certificates 76
Generating SSL Certificates Using OpenSSL 76
Syslog 78

CHAPTER 5 **Status** 81
About 81
Backup Details 82
Logs 83
Storage 83

CHAPTER 6 **Operations** 85
Activate 85
Jobs 86
Power 87
Update 88
Installing Updates 90
Troubleshooting Updates 91

CHAPTER 7 **Support** 93
Opening a Support Case 93
Live Support Session 95
Support Servers 96
Starting a Live Support Session 96
Support Snapshots 97
Use Snapshots to Verify Backups 98

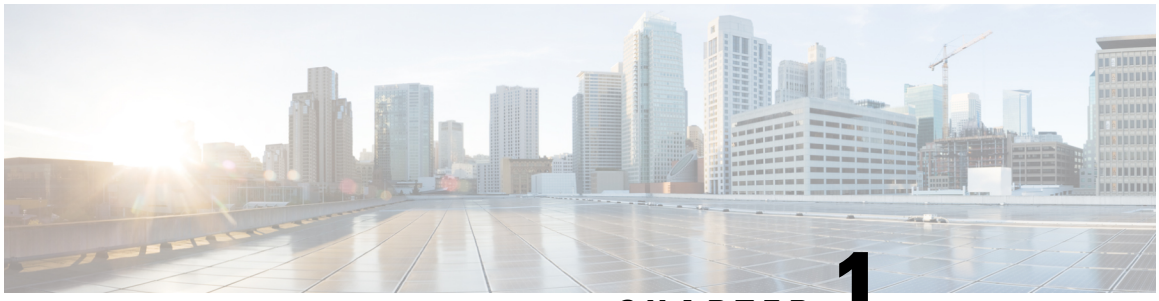
CHAPTER 8 **Organizations and Users** 99
Creating a New Organization 99
Managing Users 100
Removing Organizations and Users 101
Activating a New Device User Account 101

APPENDIX A **Inbound and Outbound Connections** 103
Connecting ESA or WSA to Threat Grid Appliance 103
Configuring Inbound Connection 104
Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance 105
Managing Disposition Update Syndication Services 106

APPENDIX B **Removing All Data with the Wipe Appliance Operation** 109
About Wipe Appliance 109
Wipe Appliance Procedure 109
Wipe Appliance and Clusters 110

APPENDIX C **CIMC Configuration** 111

Using CIMC Configuration Utility 111



CHAPTER 1

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.	Configuring SSL Certificates
Added info on downloading a .cert file.	Regenerating SSL Certificates
New topic for restored download functionality.	Downloading SSL Certificate
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 Operation	Describes how to use the Wipe Appliance boot option to remove all data from the Threat Grid Appliance, including clusters.

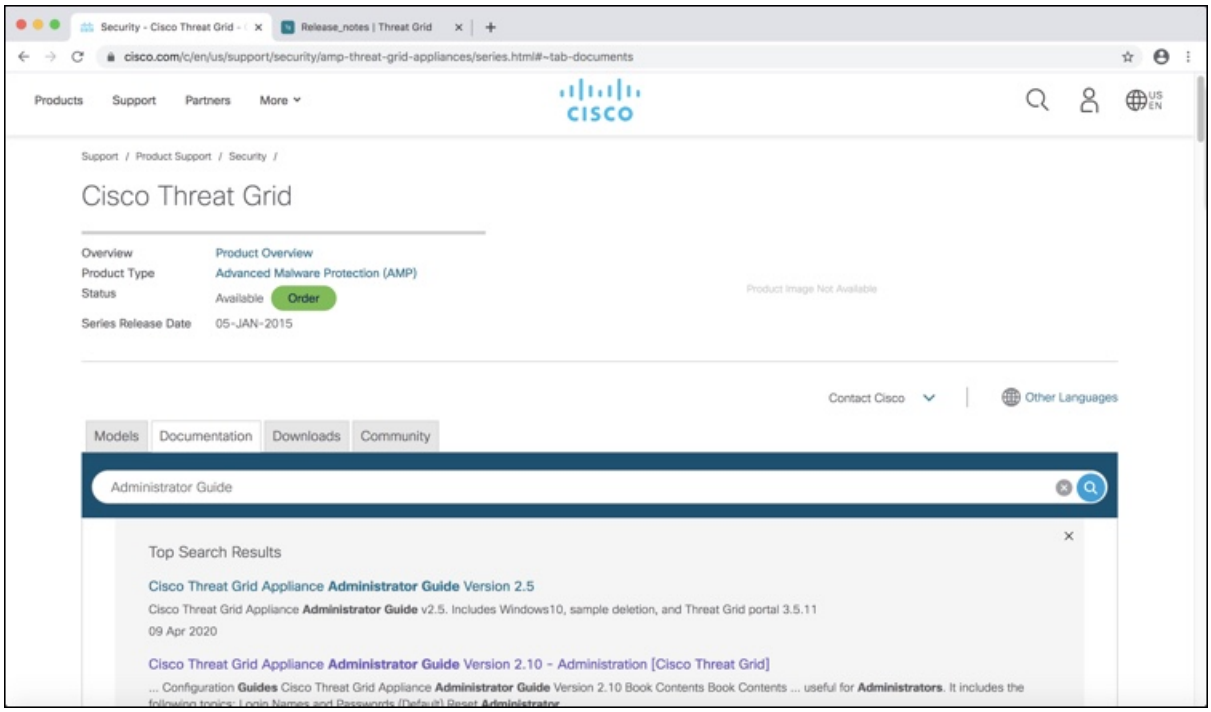
Chapter	Description
CIMC Configuration	Provides information about using the CIMC utility to set up remote server management.

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



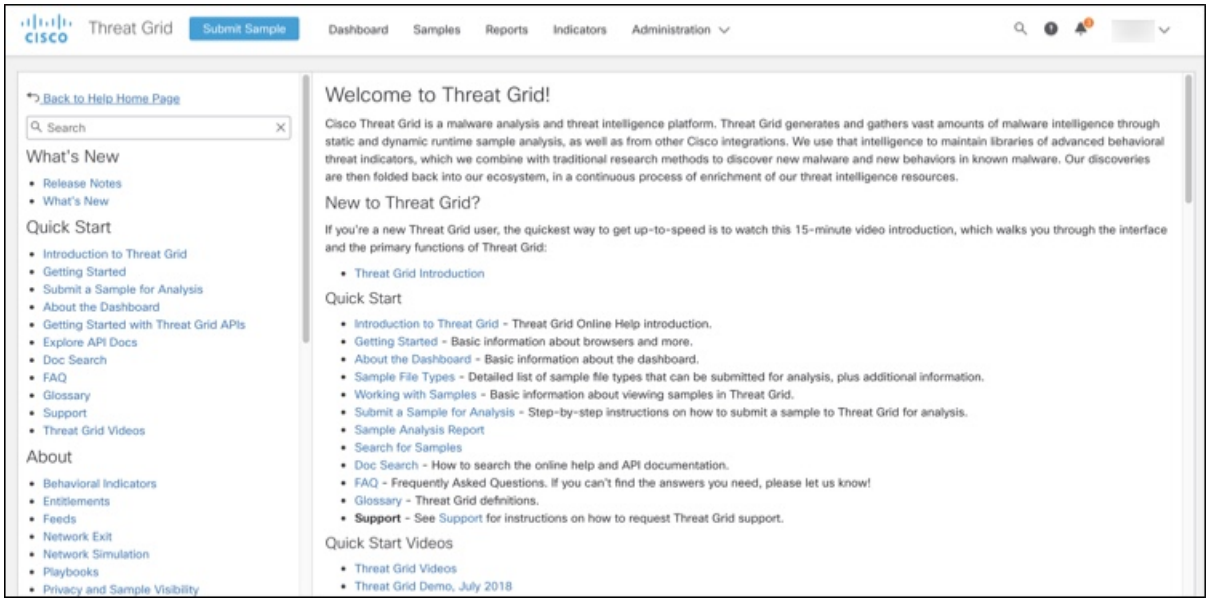
- *Cisco Threat Grid Appliance Release Notes*
- *Cisco Threat Grid Appliance Getting Started Guide*
- *Cisco Threat Grid Version Lookup Table*
- *Cisco Threat Grid M5 Hardware Installation Guide*

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

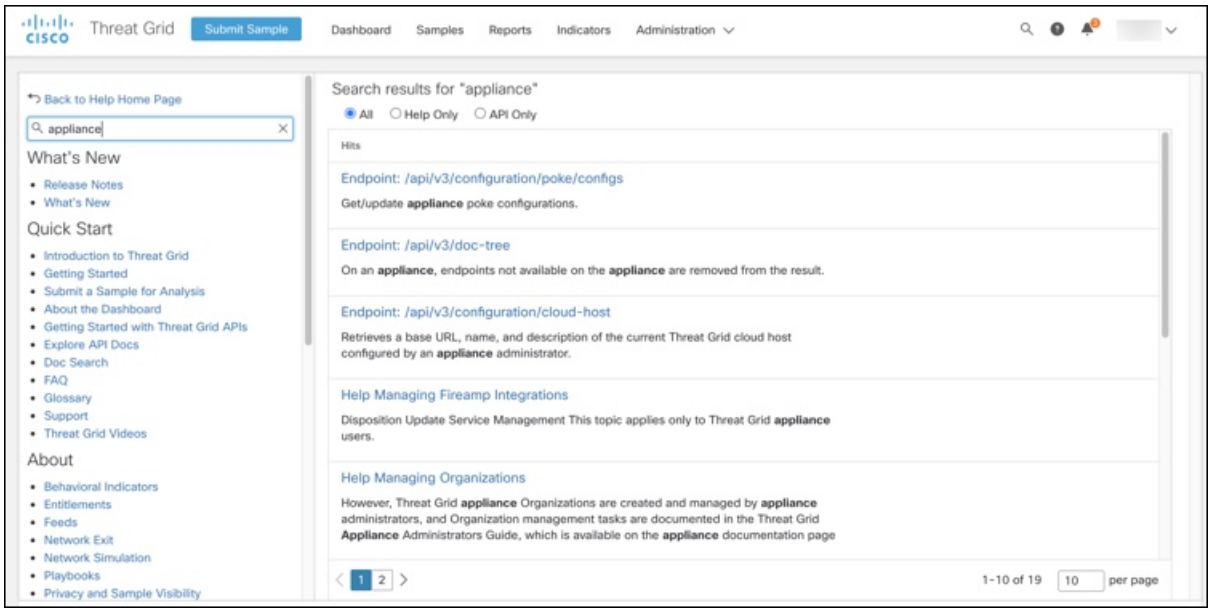
Threat Grid Portal user documentation, including Release Notes, Using Threat Grid Online Help, API documentation, and other information is available from the **?** (**Help**) icon located in the navigation bar in the upper right corner of the Threat Grid user interface.

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.

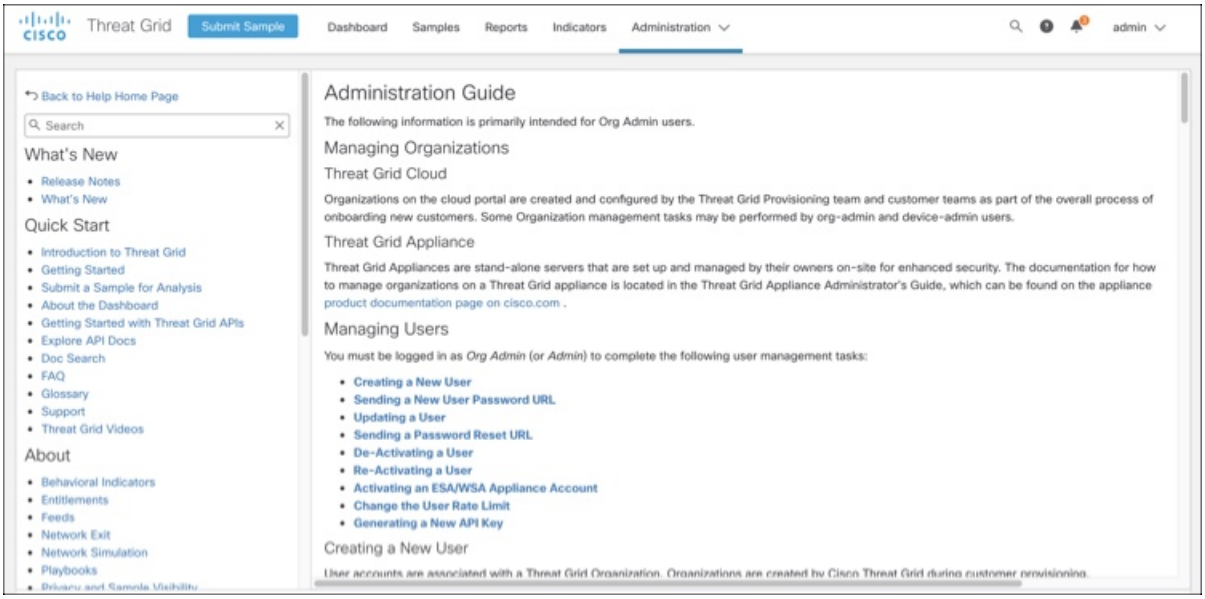
Figure 3: Online Help Search Feature



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 Inbound and Outbound Connections.

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.

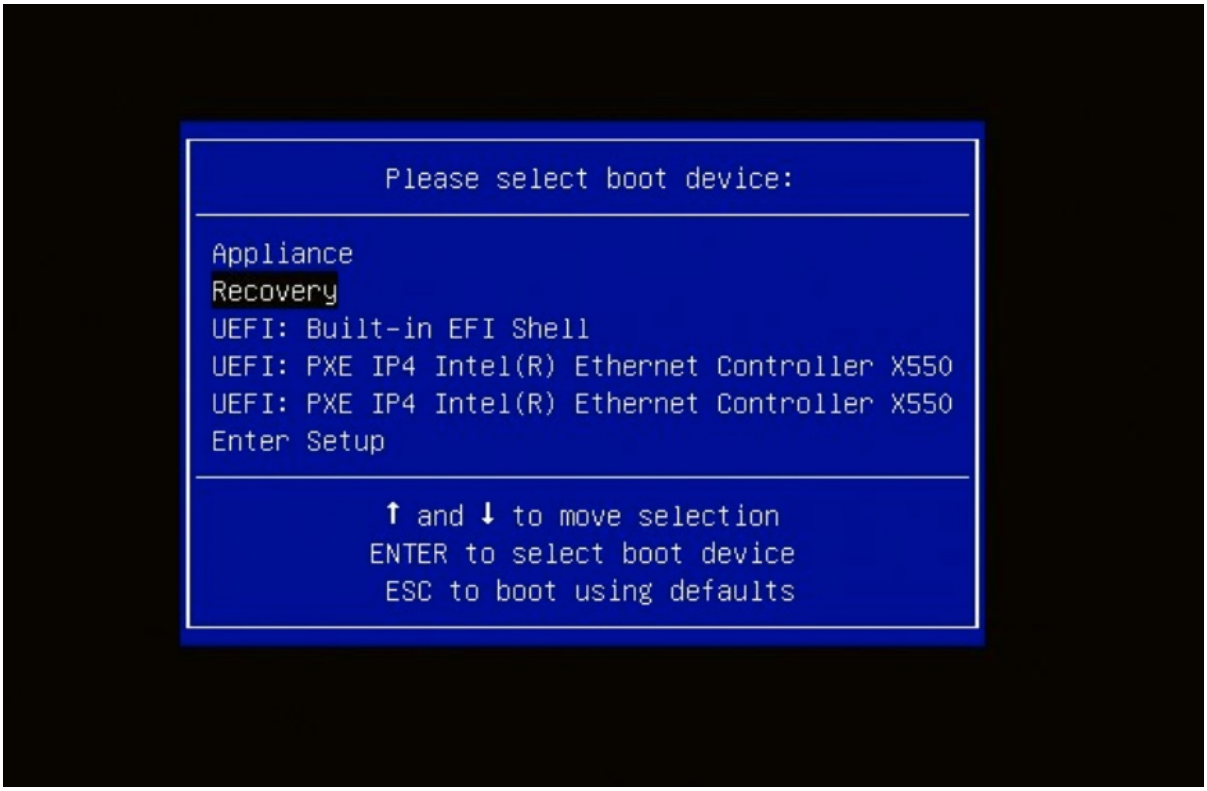
Figure 5: BIOS Window - Choose Boot Menu <F6> for Recovery Mode



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

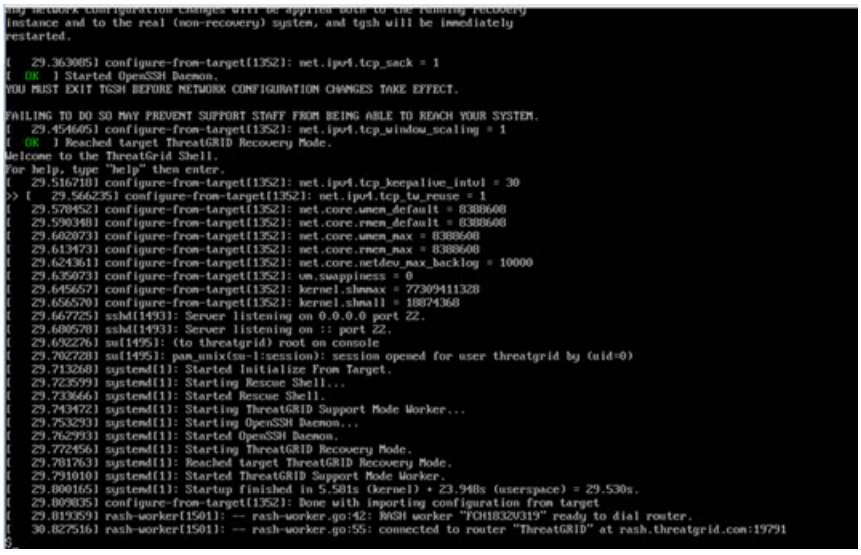
Step 3 Choose **Recovery** and press **Enter**.

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.

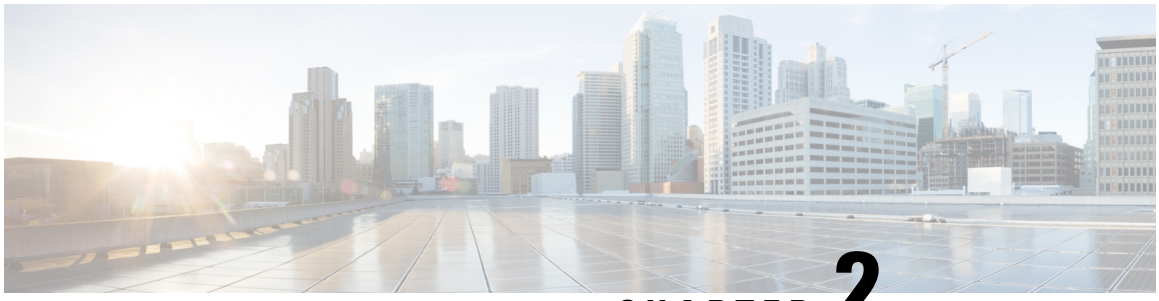
Step 5 Enter (blindly) the password and press **Enter**.

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).



CHAPTER 2

Planning

The Cisco Threat Grid Appliance is a Linux server with Threat Grid software installed by Cisco Manufacturing prior to shipment. Once a new Threat Grid Appliance is received, it must be set up and configured for your on-premises network environment.

This chapter describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration:

- Supported Browsers, on page 11
- Environmental Requirements, on page 12
- Hardware Requirements, on page 12
- Network Requirements, on page 12
- DNS Server Access, on page 13
- NTP Server Access, on page 14
- Integrations, on page 14
- DHCP Requirements, on page 14
- License, on page 15
- Rate Limits, on page 15
- Organizations and Users, on page 15
- Updates, on page 15
- User Interfaces, on page 16
- Network Interfaces, on page 17
- Firewall Rules, on page 20
- Privacy and Sample Visibility, on page 22
- Wipe Appliance Operation, on page 24
- Customer Data, on page 24

Supported Browsers

Threat Grid supports the following browsers:

- Google Chrome™
- Mozilla Firefox®
- Apple Safari®

Note Microsoft® Internet Explorer® is **not** supported.

Environmental Requirements

Threat Grid Appliance (v2.7.2 and later) is deployed on the Threat Grid M5 Appliance server. Before you set up and configure the Threat Grid Appliance, make sure the necessary environmental requirements for power, rack space, cooling, and other issues are met, according to the specifications in the *Cisco Threat Grid M5 Hardware Installation Guide*.

Hardware Requirements

The SFP+ form factor is used for the Admin interface. If you are clustering Threat Grid Appliances, each one will require an additional SFP+ module on the Clust interface.

Note The SFP+ modules must be connected *before* the Threat Grid Appliance is powered on for the session in which the configuration wizard is going to be run.

If there are no SFP+ ports available on the switch, or SFP+ is not desirable, then a transceiver for 1000Base-T can be used (for example, Cisco Compatible Gigabit RJ 45 Copper SFP Transceiver Module Mini -GBIC - 10/100/1000 Base-T Copper SFP Module).

Figure 9: Cisco 1000BASE-T Copper SFP (GLC-T)



You can attach a monitor to the server, or, if Cisco Integrated Management Controller (CIMC) is configured, you can use a remote KVM (on UCS C220-M3 and C220-M4 servers).

Note CIMC is not supported on the Threat Grid M5 Appliance server.

The Cisco UCS Power Calculator is available to get a power estimate.

Network Requirements

The Threat Grid Appliance requires three networks:

- **ADMIN** - The Administrative network must be configured to perform the Threat Grid Appliance setup.

- Admin UI Management Traffic (HTTPS)
- SSH
- NFSv4 (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.)

- **CLEAN** - The Clean network is used for inbound, trusted traffic to the Threat Grid Appliance (requests), and integrated appliances such as the Cisco Email Security Appliance and Web Security Appliance; integrated appliances connect to the IP address of the Clean interface.



Note The URL for the Clean network interface will not work until the Admin UI configuration is complete.

The following specific, restricted types of network traffic can be outbound from the Clean network:

- Remote syslog connections
- Email messages sent by the Threat Grid Appliance
- Disposition Update Service connections to AMP for Endpoints Private Cloud devices
- DNS requests (related to any of the above)
- LDAP

- **DIRTY** - The Dirty network is used for outbound traffic from the Threat Grid Appliance (including malware traffic).



Note To protect your internal network assets, we recommend using a dedicated external IP address (for example, the Dirty interface) that is different from your corporate IP.

For network interface setup information, see Network Interfaces.

DNS Server Access

The DNS server needs to be accessible via the Dirty network when used for purposes other than Disposition Update Service lookups, resolving remote syslog connections, and resolving the mail server used for notifications from the Threat Grid software.

By default, DNS uses the Dirty interface. The Clean interface is used for AMP for Endpoints Private Cloud integrations. If the AMP for Endpoints Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI.

NTP Server Access

The NTP server needs to be accessible via the Dirty network.

Starting with the 2.12 release, an appliance can be optionally configured to connect to an NTP server from the clean interface rather than the dirty interface (default). This makes it possible to use an internal NTP server.

Integrations

Additional planning may be required if the Threat Grid Appliance is going to be used with other Cisco products, such as the Email Security Appliance, Web Security Appliance, or AMP for Endpoints Private Cloud. See Connecting ESA or WSA to Threat Grid Appliance for more information.

DHCP Requirements

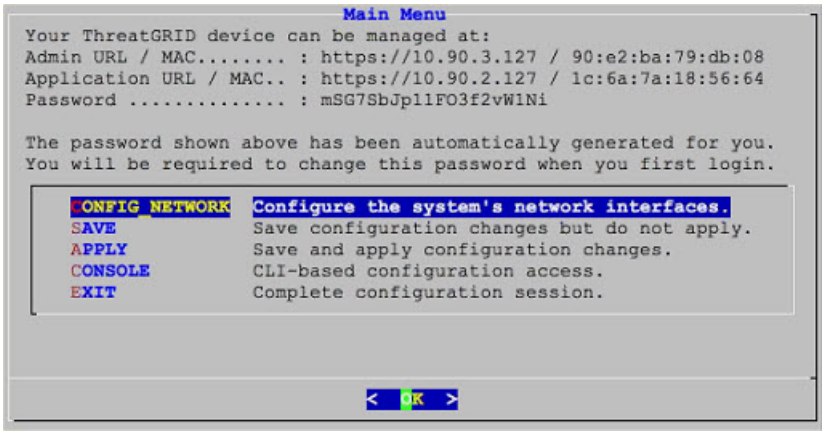
If you are connected to a network configured to use DHCP, it is important that you understand the requirements. Threat Grid Appliances that use DHCP need to explicitly specify DNS.

Warning An upgrade of a system without a DNS server explicitly specified will fail.

Note The TGSH Dialog displays the information you will need to access and configure the Admin UI. It may take some time for the IP addresses for DHCP to display after your appliance boots.

Open the TGSH Dialog and note the following information:

Figure 10: TGSH Dialog (Connected to a Network Configured to Use DHCP)



- **Admin URL** - The Admin network. You will need this address in order to continue the remaining configuration tasks in the Admin UI.

- **Application URL** - The Clean network. This is the address to use after completing the configuration in the Admin UI.

  The Dirty network is not shown.

- **Password** - The initial Admin password that is randomly generated during the Threat Grid Appliance installation. You will need to change this password later as the first step the Admin UI configuration process.

If you need to change your initial IP assignments from DHCP to static IP addresses, see Network.

License

When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration > License** page is enabled. However, if that doesn't work or if there's a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

For additional questions about licenses, contact Opening a Support Case.

Rate Limits

The API sample submission rate limit is global for the Threat Grid Appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

Rate limits are based on a window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying. See the portal online Help for more information.

Organizations and Users

Once you have completed the Threat Grid Appliance setup and network configuration, you must create the initial Threat Grid organizations and add user account(s), so that people can login and begin submitting malware samples for analysis. This task may require planning and coordination among multiple organizations and users, depending on your requirements.

See Creating a New Organization and the Threat Grid portal Help (click **Administration > Administrator's Guide** to open the Administration Guide topic) for additional information.

Updates

The initial Threat Grid Appliance setup and configuration steps **must be completed** before installing any Threat Grid Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Threat Grid Appliance updates cannot be downloaded until the license is installed, and the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.

User Interfaces

After the server has been correctly attached to the network and powered up, there are several user interfaces available for configuring the Threat Grid Appliance.

Note LDAP authentication is available for TGSH Dialog and the Admin UI. RADIUS authentication is available for the Threat Grid Application UI (v2.10 and later).

TGSH Dialog

The **TGSH Dialog** interface is used to configure the network interfaces. The TGSH Dialog is displayed when the Threat Grid Appliance successfully boots up.

Reconnecting to the TGSH Dialog

The TGSH Dialog remains open on the console and can be accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

Note CIMC is not supported on the Threat Grid M5 Appliance server.

To reconnect to the TGSH Dialog, ssh into the Admin IP address as the user **threatgrid**.

The required password is either the initial, randomly generated password, which is visible initially in the TGSH Dialog, or the new Admin password you create during the first step of the Admin UI Configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Threat Grid Shell (tgsh)

The Threat Grid Shell (tgsh) is an administrator's interface that is used to execute commands (including destroy-data and forced backup), and for expert, low-level debugging. To access tgsh, choose **CONSOLE** in the TGSH Dialog.

Note The Admin UI uses the same credentials as the Threat Grid user, so any password changes/updates made via tgsh will also impact the Admin UI.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Threat Grid support; the Admin UI or TGSH Dialog should be used instead. Options to modify admin email, glovebox URL, SMTP configuration, etc. have been removed with the 2.12 release. The Wipe Appliance operation is now activated within recovery mode tgsh rather than the bootloader menu.

Admin UI

This is the primary Threat Grid user interface used for configuration. Much of the Threat Grid Appliance configuration can ONLY be done via the Admin UI, including licenses, email host, and SSL certificates.

Threat Grid Portal

The Threat Grid user interface application is available as a cloud service, and is also installed on Threat Grid Appliances. There is no communication between Threat Grid Cloud service and the Threat Grid Portal that is included with a Threat Grid Appliance.

The Threat Grid Appliance v2.11 release updates the Threat Grid application to release 3.5.50.

Network Interfaces

The available network interfaces are described in the following table:

Interface	Description
Admin	• Connect to the Admin network. **Only inbound** from Admin network. • Admin UI traffic • SSH (inbound) for TGSH Dialog • NFSv4 for backups and clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster notes. • The Admin port can be disabled (from the tgsh shell); from the Admin UI with v2.11. When disabled, non-clustered Threat Grid Appliances can operate correctly with only the clean and dirty ports connected, and the admin UI will be presented on port 8443 of the clean interface (an also port 18443 with the v2.11 release). If the port is not disabled, unplugging the admin port results in a non-functional (or at best, a partially functional) Threat Grid Appliance. **Note** The form factor for the Admin interface is SFP+. See Hardware Requirements.
Clust	The non-Admin SFP+ port is used for clustering. • Clust interface required for clustering (optional) • Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.

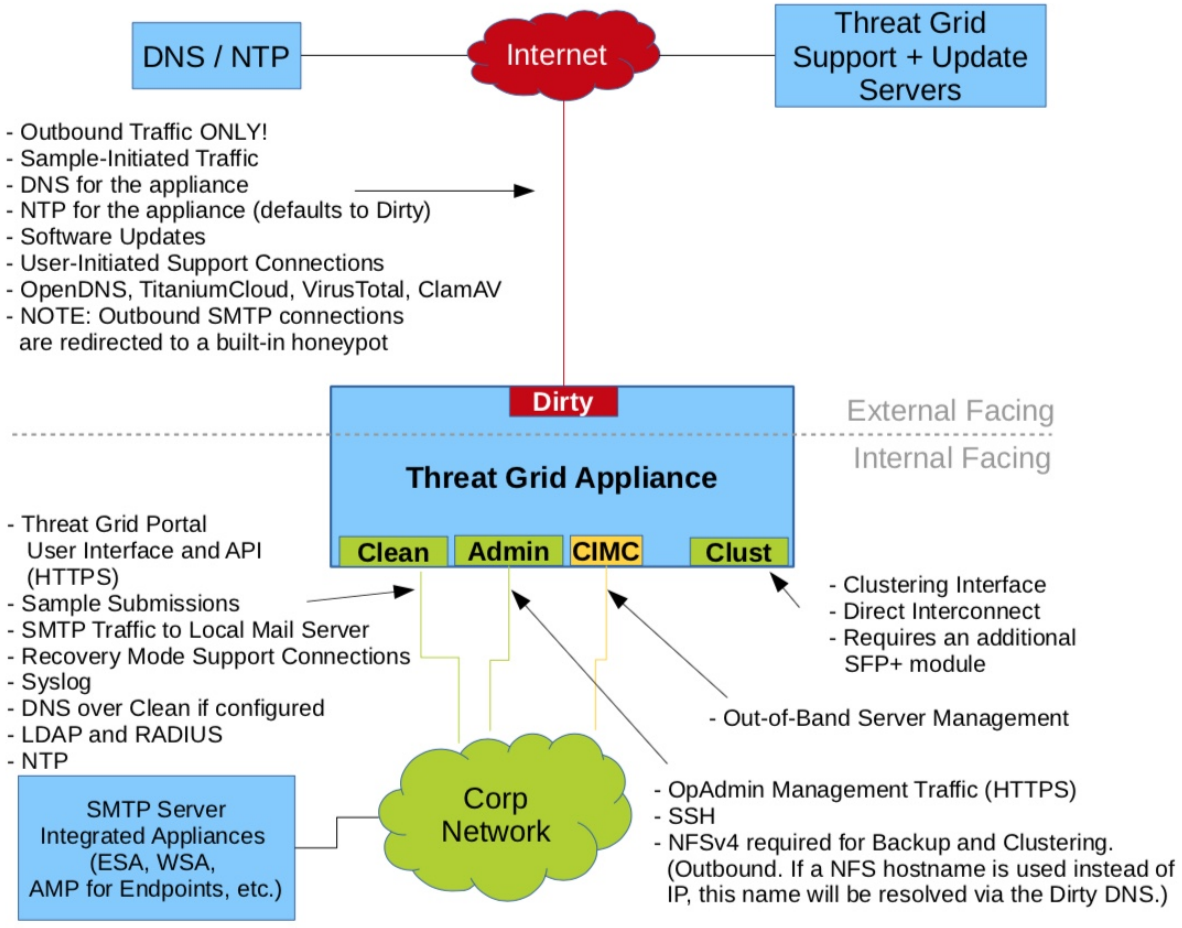
Interface	Description
Clean	• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. • UI and API traffic (inbound) • Sample submissions • SMTP (outbound connection to the configured mail server) • SSH (inbound for TGSH Dialog) • Syslog (outbound to configured syslog server) • ESA/WSA and CSA Integrations • AMP for Endpoints Private Cloud Integration • DNS optional • LDAP (outbound) • RADIUS (outbound) • NTP (for using an internal NTP server)
Dirty	Connect to the Dirty network; requires Internet access. Outbound Only. You should not use your own DNS (private IP) for the Dirty Interface because traffic sent to a private IP is dropped at the Network Exit Localization firewall. • DNS **Note** If you are setting up an integration with a AMP for Endpoints Private Cloud, and the AMP for Endpoints appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI. • NTP (defaults to Dirty) • Updates • Support session in Normal operations mode • Support snapshots • Malware sample-initiated traffic • Recovery mode support session (outbound) • OpenDNS, TitaniumCloud, VirusTotal, ClamAV • SMTP outbound connections are redirected to a built-in honeypot **Note** Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Interface	Description
CIMC Interface	If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. See CIMC Configuration. **Note** CIMC is not supported on the Threat Grid M5 Appliance server.

Network Interface Setup Diagram

This section describes the most logical and recommended setup for a Threat Grid Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may decide to connect the Dirty interface to the inside, or the Clean interface to the outside with appropriate network security measures in place.

Figure 11: Network Interfaces Setup Diagram



Note In Threat Grid Appliance (v2.7.2 and later), the **enable_clean_interface** option is available but is disabled by default. This option (after applying configuration and rebooting) enables access to the administrative interface on port 8443 of the assigned clean IP.

Firewall Rules

This section provides suggested firewall rules.

Note Implementing a restrictive outgoing policy on the Dirty interface for ports 22 and 19791 requires tracking updates over time and spending more time maintaining the firewall.

Note Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples. (To get accurate results it is required that malware be allowed to contact its command and control server using whatever port and protocol it is designed to use.)

Dirty Interface Inbound

Source	Destination	Protocol	Port	Action	Note
ANY	Dirty Internet	ANY	ANY	Deny	Deny all incoming connections.

Clean Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Clean Interface	SMTP Servers	TCP	25	Allow	The appliance uses the clean interface to initiate SMTP connections to the configured mail server.

Clean Interface Outbound (Optional)

Source	Destination	Protocol	Port	Action	Note
Clean Interface	Corporate DNS Server	TCP/UDP	53	Allow	Optional, only required if Clean DNS is configured.
Clean Interface	AMP Private Cloud	TCP	443	Allow	Optional, only required if AMP for Endpoints Private Cloud integration is used.
Clean Interface	Syslog Servers	UDP	514	Allow	Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications.
Clean Interface	LDAP Servers	TCP/UDP	389	Allow	Optional, only required if LDAP is configured.
Clean Interface	LDAP Servers	TCP	636	Allow	Optional, only required if LDAP is configured.
Clean Interface	RADIUS Servers	DTLS	2083	Allow	Allow login to Threat Grid application UI (Face). Optional, only required if RADIUS is configured.
Clean Interface	Internet	UDP	123	Allow	Optional, use this off-by-default functionality to use an internal NTP server.

Clean Interface Inbound

Source	Destination	Protocol	Port	Action	Note
User Subnet	Clean Interface	TCP	22	Allow	Allow SSH connectivity to the TGSH Dialog.
User Subnet	Clean Interface	TCP	80	Allow	Appliance API and Threat Grid user interface. This will redirect to HTTPS TCP/443.
User Subnet	Clean Interface	TCP	443	Allow	Appliance API and Threat Grid user interface.
User Subnet	Clean Interface	TCP	9443	Allow	Allow connectivity to the Threat Grid UI Glovebox.

Admin Interface Outbound (Optional)

The following depends on what services are configured.

Source	Destination	Protocol	Port	Action	Note
Admin Interface	NFSv4 Server	TCP	2049	Allow	Optional, only required if Threat Grid Appliance is configured to send backups to an NFSv4 share.

Admin Interface Inbound

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	22	Allow	Allow SSH connectivity to the TGSH Dialog.
Admin Subnet	Admin Interface	TCP	80	Allow	Allow access to the Admin UI. This will redirect to HTTPS TCP/443.
Admin Subnet	Admin Interface	TCP	443	Allow	Allow access to the Admin UI.

Dirty Interface for Non Cisco-Validated/Recommended Deployment

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.
Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.
Dirty Interface	Internet	TCP	19791	Allow	Allow connectivity to Threat Grid support.
Dirty Interface	Cisco Umbrella	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	VirusTotal	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	TitaniumCloud	TCP	443	Allow	Connect with third-party detection and enrichment services.

Privacy and Sample Visibility

When submitting samples to a Threat Grid Appliance for analysis, an important consideration is the privacy of the content. Privacy is a particularly important consideration if sensitive documents or archive types are

submitted for analysis, because locating sensitive material could be relatively easy for those with access to the Threat Grid Appliance, especially with the search API.

The privacy and sample visibility model for sample submissions to Threat Grid is as follows:

- Unless samples are designated as Private, they are visible to users who are outside the submitter's organization.
- Private samples can only be seen by Threat Grid users within the same organization as the user who submitted the sample.

Samples Submitted by Integrations

The privacy and sample visibility model is modified on Threat Grid Appliances for samples that are submitted by integrations. Integrations are Cisco products such as Email Security Appliance (ESA), Web Security Appliance (WSA), and other devices or third-party services (you may see the term CSA Integrations, which refers to ESA/WSA and other Cisco appliances, devices, and services that are integrated; for example, registered, with Threat Grid Appliance via the Cisco Sandbox API.)

All sample submissions on Threat Grid Appliances are Public by default, and can be viewed by any other appliance user, including integrations, regardless of the organization to which they belong. All appliance users can see all details of samples submitted by all other users.

Threat Grid users may also submit Private samples to the Threat Grid Appliance, which are only visible to other Threat Grid Appliance users, including integrations, from the same organization as the sample submitter.

Privacy and sample visibility model on Threat Grid Appliances are illustrated in the table.

Figure 12: Privacy and Visibility on a Threat Grid Appliance

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **Full Access** - The green check mark indicates that users have full access to the sample and the analysis results.
- **Scrubbed Reports** - The grey check mark indicates that the Private submission results are scrubbed. Users have partial access to the sample and analysis results, but all potentially sensitive information

about the sample is removed. There are no filenames, process names, screenshots, or even specifics about its activity in the glovebox.

We omit details from the Metadata section, such as the sample submitter's login information. If you encounter a hash from a private sample in the course of doing business, this will let alert you to known threats, and if you need more details, submit your own copy of the sample for full analysis.

Private samples may not be downloaded. Scrubbed reports include Artifacts (with filename removed), Behavioral Indicators, Domains, and IPs.

- **No Access** - The red X indicates that users have no access to the sample or the analysis results.

The same basic privacy rules apply to Threat Grid Appliance integrations with AMP for Endpoints Private Cloud.

Wipe Appliance Operation

The Wipe Appliance operation enables you to wipe the disks on a Threat Grid Appliance to remove all data prior to decommissioning or returning it to the Cisco Demo Loan Program.



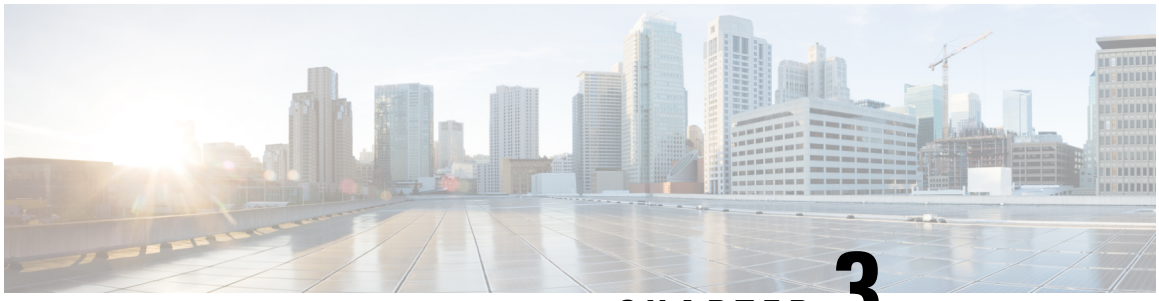
Important After performing the wipe appliance procedure, the Threat Grid Appliance will no longer operate without being returned to Cisco for reimaging.

For more information, see Removing All Data with the Wipe Appliance Operation.

Customer Data

Logs, active configuration, and other customer-owned data is now stored almost exclusively on the RAID 5 data array, rather than being distributed between data and OS drives. The remaining appliance-specific content stored on OS drives is limited to information required for correct operation of recovery mode should the data drives not be mountable, and has limited privacy impact if disclosed.

Because less content is stored on the OS array with the 2.12 release, early appliances (with smaller OS drives) are less likely to need to delete VM images other than the mandatory default image during a data reset (and thus need to download updates online before those deleted VM images become available again).



CHAPTER 3

Network Configuration Using the TGSH Dialog

The initial Threat Grid Appliance network configuration is completed during the appliance setup using the TGSH Dialog, as documented in the *Cisco Threat Grid Appliance Getting Started Guide*. This chapter provides additional information about using the TGSH Dialog to make changes to your initial network configuration:

- Modifying Network Configuration, on page 25
- Reconnecting to TGSH Dialog, on page 26
- Configuring Network in Recovery Mode, on page 26

Modifying Network Configuration

The initial network configuration is completed using the TGSH Dialog. If you want to make changes to your initial network configuration, perform the following steps.

Note If you are using DHCP to obtain IPs, see the Network section.

Procedure

Step 1 Login to TGSH Dialog.

Note
If you are configured for **LDAP Only** authentication, you can only log into TGSH Dialog using LDAP. If authentication mode is set to **System Password or LDAP**, the TGSH Dialog login only allows the **System** login.

Step 2 In the TGSH Dialog interface, choose **CONFIG_NETWORK**.

The **Network Configuration** console opens and displays the current network settings.

Step 3 Make any necessary changes (you need to backspace over the old entry before you can enter the new one).

Step 4 Leave the Dirty network **DNS Name** blank.

Step 5 After you finish updating the network settings, tab down and choose **Validate** to verify your entries.

If errors occur, fix the invalid values and choose **Validate** again.

After validation, the **Network Configuration Confirmation** page displays the entered values

Step 6 Choose **Apply** to apply your configuration settings.

Detailed information about the configuration changes that have been made are displayed.

Step 7 Choose **OK**.

The **Network Configuration** console refreshes again and displays the IP addresses. Network configuration is now complete.

Reconnecting to TGSH Dialog

TGSH Dialog remains open on the console and can be accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

To reconnect to the TGSH Dialog, SSH into the Admin IP address as the user **threatgrid**. The required password is either the initial randomly generated password, which is visible initially in the TGSH Dialog, or the new Admin password you created during the first step of the Admin UI configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*.

Configuring Network in Recovery Mode

Network configuration in recovery mode mirrors the full system (v2.7 and later):

- All interfaces are brought up.
- Firewall rules and policy routing restricts which processes can communicate on which interfaces.

Note Support mode traffic on port 19791 is allow-listed across all three interfaces.

Perform the following steps to set up networking in recovery mode.

Procedure

Step 1 Reboot the Threat Grid Appliance (**Operations > Power > Reboot**) and then choose **Recovery Mode** in the boot menu.

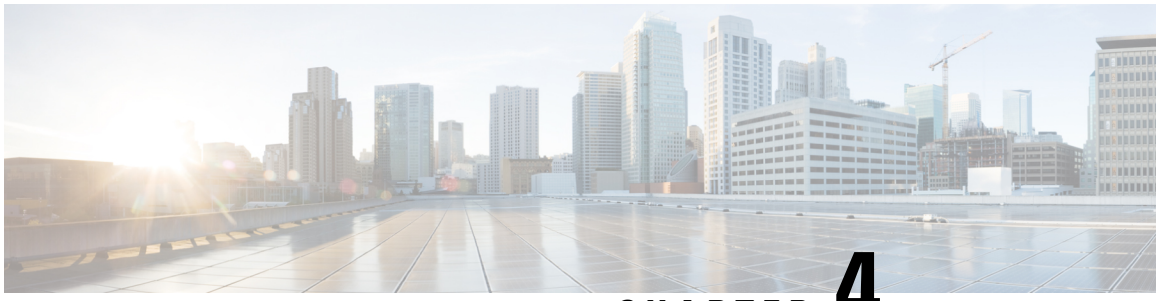
Step 2 Once the system is up, press **Enter** several times to get a clean command prompt.

Step 3 Enter **netctl clean** and provide the following information:

- **Configuration type** - static
- **IP Address** - <Clean IP Address>/<Netmask>
- **Gateway Address** - <Clean network gateway>
- **Routes** - <leave blank>
- **Final Question** - Enter **y**

Step 4 Enter **Exit** to apply the configuration.

The appliance will attempt to open an outbound support connection on the Clean interface on port 19791/tcp.



CHAPTER 4

Configuration Using the Admin UI

The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide. New Threat Grid Appliances may require the administrator to complete additional configuration, and Admin UI settings may require updates over time. This chapter provides information about using the Admin UI to make configuration changes to your appliance.

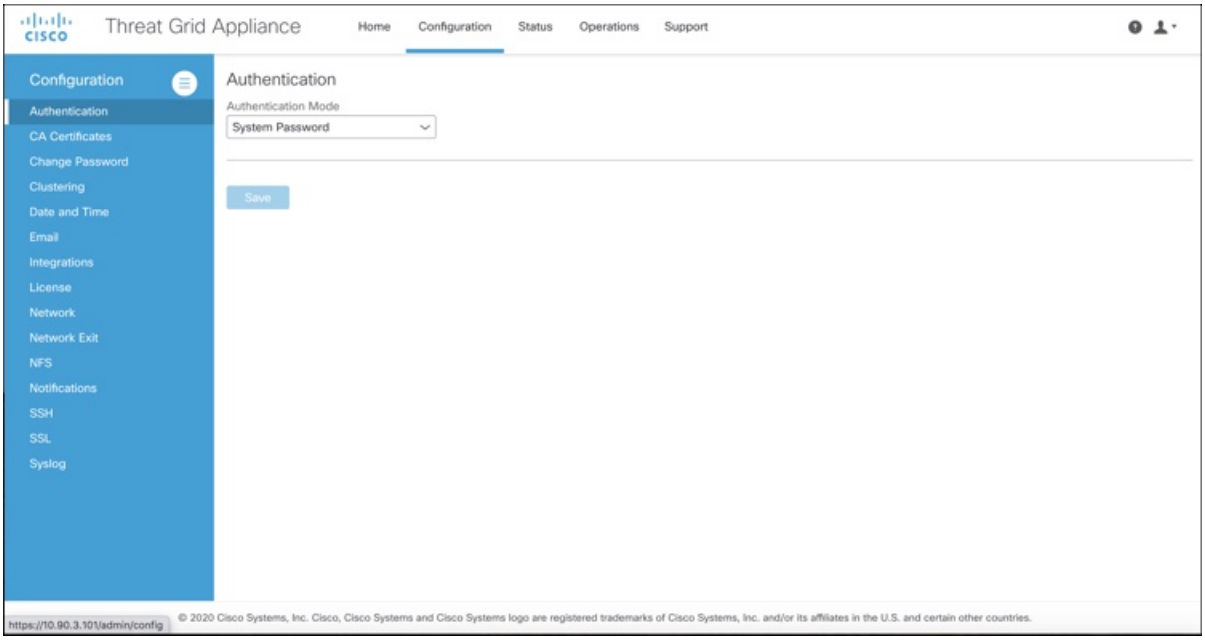
- About the Admin UI, on page 29
- Applying Configuration Changes, on page 31
- Authentication, on page 33
- CA Certificates, on page 36
- Change Password, on page 37
- Clustering, on page 37
- Date and Time, on page 52
- Email, on page 54
- Integrations, on page 54
- License, on page 55
- Network, on page 57
- Network Exit, on page 60
- NFS, on page 63
- Notifications, on page 71
- SSH, on page 71
- SSL, on page 73
- Syslog, on page 78

About the Admin UI

The Admin UI is the Threat Grid Appliance administrator's main configuration interface. It is a Web portal that can be used once an IP address has been configured on the Threat Grid Appliance Admin interface.

Note The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide.

Figure 13: Configuration



The **Configuration** menu in the Admin UI is used to configure and manage various Threat Grid Appliance configuration settings, including:

Section	Description
Authentication	Describes how to configure LDAP and RADIUS authentication for logging into the Threat Grid Appliance Admin UI.
CA Certificates	Describes how to add CA certificate for outbound SSL connections for the appliance to trust the Cisco AMP for Endpoints Private Cloud.
Change Password	Describes how to change your Admin UI password.
Clustering	Describes features, limitations, and requirements of clustering Threat Grid Appliances; network and NFS storage requirements; how to build a cluster, join appliances to the cluster, remove cluster nodes, and designate a tie-breaker node; failure tolerances and failure recovery; API and operational usage and characteristics for clusters, and sample deletion.
Date and Time	Describes how to add Network Time Protocol (NTP) server to configure date and time.
Email	Describes how to configure your email settings (SMTP) for system notifications.
Integrations	Describes how to configure third-party detection and enrichment services (OpenDNS, TitaniumCloud, VirusTotal); enable or disable ClamAV automatic updates.
License	Describes how to upload your Threat Grid Appliance license or retrieve it from the server.

Section	Description
Network	Describes how to adjust the IP assignment from DHCP to your permanent static IP addresses, and how to configure DNS.
Network Exit	Describes how to configure the network exit options that are available in the Threat Grid portal when submitting samples for analysis.
NFS	Describes appliance backup, including NFS requirements, backup storage requirements, backup expectations, and configuring the strict retention period limits; how to perform a backup.
Notifications	Describes how to manage notification recipients.
SSH	Describes how to set up SSH keys to provide access to the TGSH Dialog via SSH.
SSL	Describes how to configure SSL certificates to support Threat Grid Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), AMP for Endpoints Private Cloud, and other integrations; replacing SSL certificates.
Syslog	Describes how to configure a system log server to receive syslog messages and notifications.



Note

- Configuration updates in the Admin UI should be completed in one session to reduce the chance of an interruption to the IP address during configuration.
- The Admin UI does not validate the gateway entries. If you enter the wrong gateway and save it, the Admin UI will not be accessible. You will need to use the console to fix the networking configuration if that was done on the Admin interface. If Admin is still valid, you can fix it in the Admin UI and reboot.
- Threat Grid Appliances (v2.7 or later) use the serial number as the hostname to improve interoperability with some NFS v4 servers.



Important The Admin UI uses HTTPS and you must enter this in the browser address bar; pointing to only the Admin IP is not sufficient. Enter the following address in your browser:

https://adminIP/

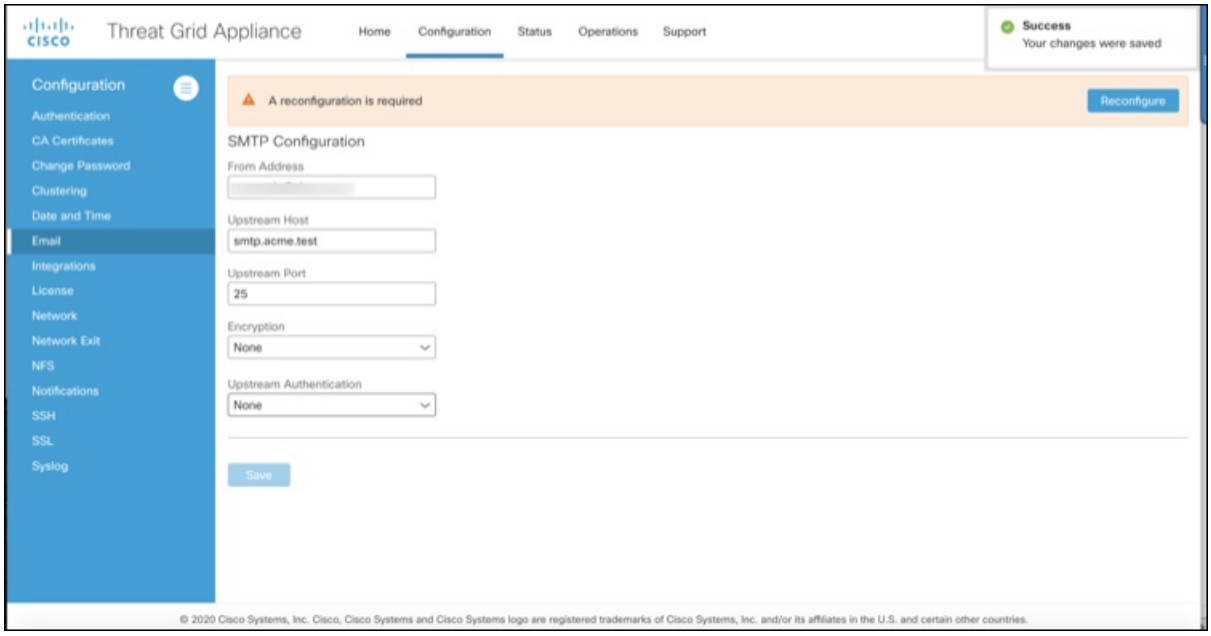
OR

https://adminHostname/

Applying Configuration Changes

Any time changes are made to configuration settings, a light orange alert message appears in a banner in the upper portion of the **Configuration** page.

Figure 14: Reconfigure Required Alert Message



Changes to the Admin UI configuration settings must be saved, and several also include a step to activate the change. However, you must also finalize the changes with a reconfiguration in a separate step. Configuration changes do not take effect until reconfiguration is completed.

Note Reconfiguration may affect other users logged in to Threat Grid portal and the Admin UI.

Procedure

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.

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**.

Authentication

The Threat Grid Appliance supports LDAP authentication and authorization for logging into the Admin UI and the TGSH Dialog. It also supports RADIUS authentication, which allows for single sign-on to the Admin UI in v2.10 and later.

LDAP Authentication

The Threat Grid Appliance supports LDAP authentication and authorization for Admin UI and TGSH Dialog login. You can authenticate multiple appliance administrators with different credentials that are managed on the domain controller or the LDAP server. Authentication modes include: System Password Only, System Password or LDAP, and LDAP Only.

There are three LDAP Protocol options: LDAP, LDAPS, and LDAP with STARTLS.

The following considerations should be observed:

- The dual authentication mode (**System Password or LDAP**) is required to avoid accidentally locking yourself out of the Threat Grid Appliance when setting up LDAP.

  Choosing **LDAP Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of the Admin UI after the initial configuration, and then log back in using LDAP credentials to toggle to **LDAP Only**.

- You can only log into the TGSH Dialog using LDAP if you are configured for **LDAP Only** authentication. If authentication mode is set to **System Password or LDAP**, the TGSH Dialog login only allows the System login.
- If the Threat Grid Appliance is configured for LDAP authentication only (**LDAP Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.
- Make sure that the authentication filter is set up to restrict membership.
- The TGSH Dialog and the Admin UI require LDAP credentials only in **LDAP Only** mode/ if **LDAP only** is configured, the TGSH Dialog only prompts for the LDAP user/password; not the system password.
- If authentication is configured for **System Password or LDAP**, the TGSH Dialog prompts for for only the system password; not both.
- To troubleshoot LDAP issues, disable it by resetting the password in Recovery Mode.
- To access the TGSH Dialog via SSH, a system password or a configured SSH key is required in addition to LDAP credentials when in **LDAP Only** mode.
- LDAP is outbound from the Clean interface.

Perform the following steps to configure LDAP authentication in the Admin UI.

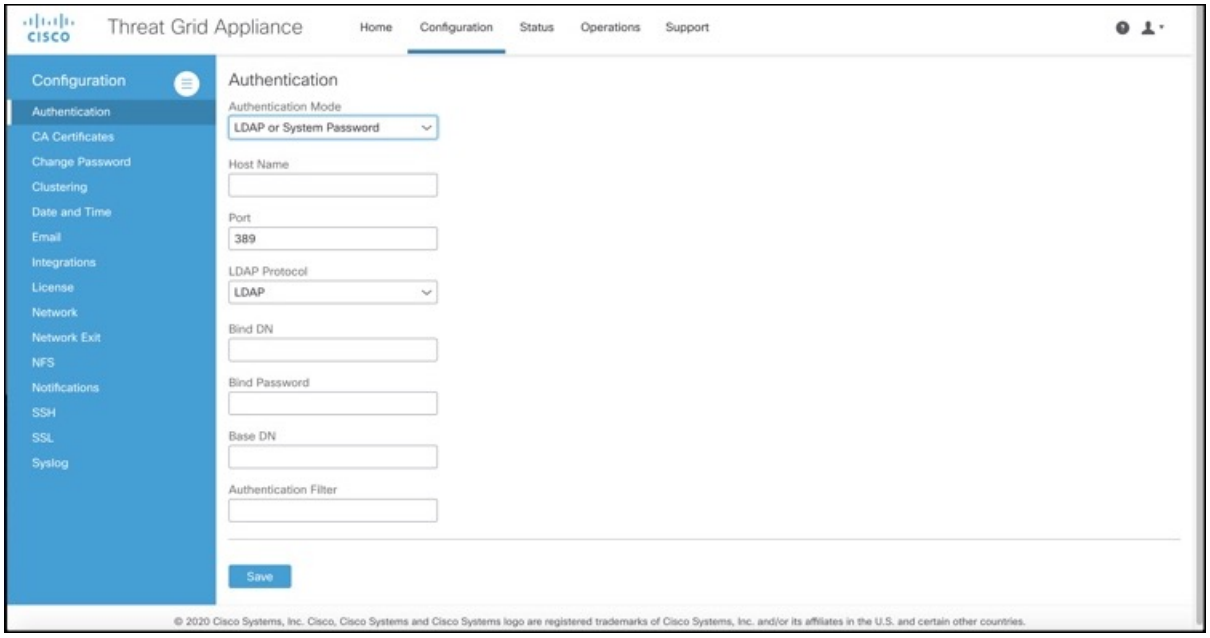
Procedure

Step 1 Click the **Configuration** and choose **Authentication**.

Step 2 From the **Authentication Mode** drop-down, choose **LDAP or System Password** to open the LDAP configuration page.

Note
The first time you configure LDAP authentication, you must choose **LDAP or System Password**, log out of the Admin UI, and then log back in using your LDAP credentials. You can then change the setting to **LDAP**.

Figure 15: LDAP Authentication Configuration Page



Step 3 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via LDAP.
- **Port** - The port number to connect to via LDAP (default 389).
- **Authentication Mode** - The authentication mode to be used upon login.
- **LDAP Protocol** - The LDAP protocol in use.
- **Bind Password** - The password to use for binding via LDAP.
- **Bind DN** -The Distinguished Name to bind to via LDAP; for example: cn=admin,dc=foo,dc=com.
- **Base** - The base to bind to via LDAP; for example: ou=users,dc=foo,dc=com (LDAP only).
- **Authentication Filter** - The filter to be applied for authentication upon login; for example: (&(cn=%LOGIN%) (memberOf=cn=admingroup, ou=groups,dc=foo,dc=com)).

Step 4 Click **Save**.

When users log in to the Admin UI or TGSH Dialog, they will now be prompted for their LDAP authentication.

RADIUS Authentication

Threat Grid Appliance (v2.10 and later) supports RADIUS authentication, which uses Cisco Identity Services Engine with DTLS enabled. If RADIUS authentication is enabled, users can log in to the main Threat Grid application UI with the appropriate single sign-on password.

Perform the following steps in the Admin UI to configure RADIUS authentication:

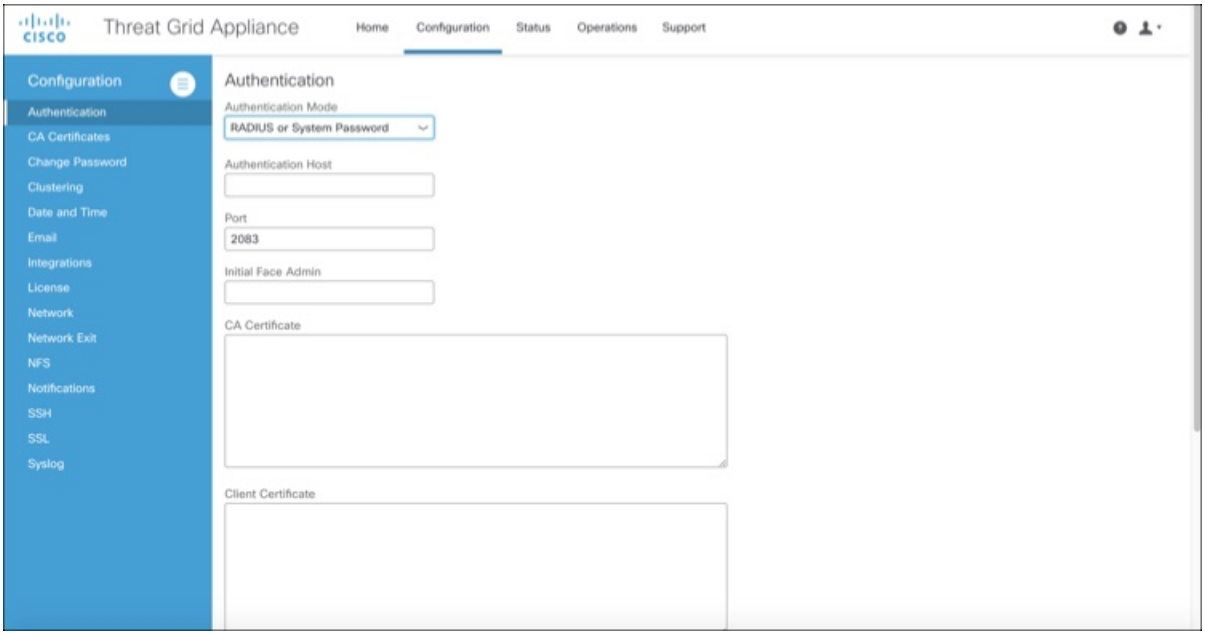
Procedure

Step 1 Click the **Configuration** tab and choose **Authentication**.

Step 2 From the **Authentication Mode** drop-down, choose **RADIUS or System Password** to open the RADIUS configuration page.

Note
The first time you configure RADIUS authentication, you must choose **RADIUS or System Password**, log out of the Admin UI, and then log back in using your RADIUS credentials. You can then change the setting to **RADIUS**.

Figure 16: RADIUS Authentication Configuration Page



Step 3 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via RADIUS.
- **Port** - The DTLS port number to connect to via RADIUS (default 2083). Unlike conventional RADIUS, DTLS uses a single port for both authentication and accounting. Only DTLS-based RADIUS authentication is supported.
- **Initial Face Admin** - The RADIUS user to whom the initial/default administration user in the primary Threat Grid UI shall be mapped. This account should be the party responsible for creating other user accounts in Threat Grid and configuring their permissions.

- **CA Certificate** - A PEM-format CA certificate to be used to authenticate the RADIUS server used for authentication. Will change to <VALID> when successfully saved. Clear this to empty the field.
- **Client Certificate** - A PEM-format client certificate to be used to authenticate this host to the RADIUS server used for authentication. This value will change to <VALID> when successfully saved; you can clear it to empty the field.
- **Client Private Key** - A PEM-format key to be used to authenticate this host to the RADIUS server used for authentication. The value must correspond with the client certificate given above. The value will change to <VALID> when successfully saved; you can clear it to empty the field. Private keys in PEM-encoded PKCS#8 format are supported by the new Admin UI.

Step 4 Click **Save**.

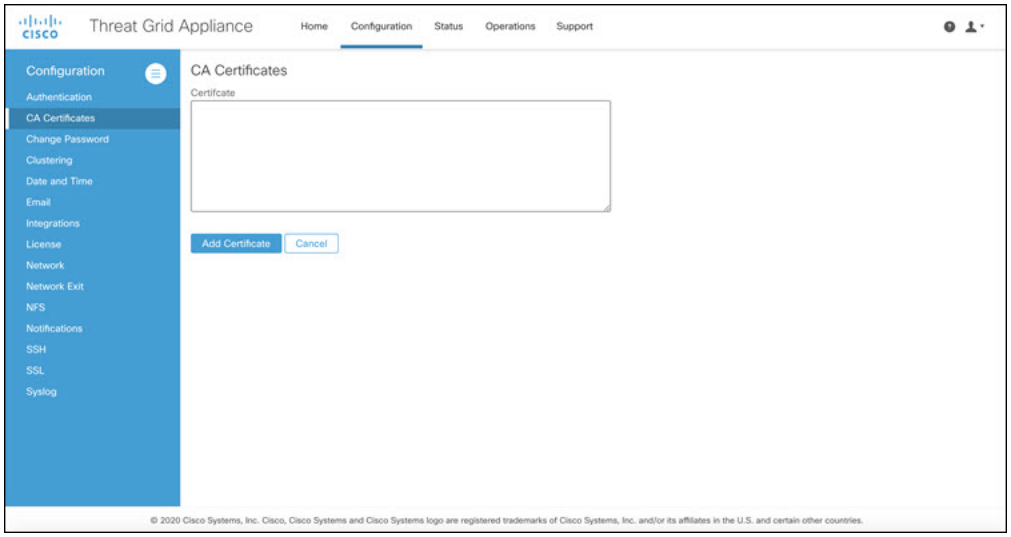
CA Certificates

The **CA Certificates** page in the Admin UI is used to manage the Certificate Authority (CA) certificate trust store for outbound SSL connections so that the Threat Grid Appliance can trust the Cisco AMP for Endpoints Private Cloud to notify it about analyzed samples that are considered malicious.

Procedure

Step 1 Click the **Configuration** tab and choose **CA Certificates** to open the **CA Certificates** page.

Figure 17: CA Certificates Page



Step 2 Create a **.pem** file that contains the outbound SSL connections (CA certificates) for the AMP for Endpoints Private Cloud, copy the contents, and paste it into the **Certificate** field.

Step 3 Click **Add Certificate** and confirm. Changing a CA certificate does ot require reconfiguration.

Change Password

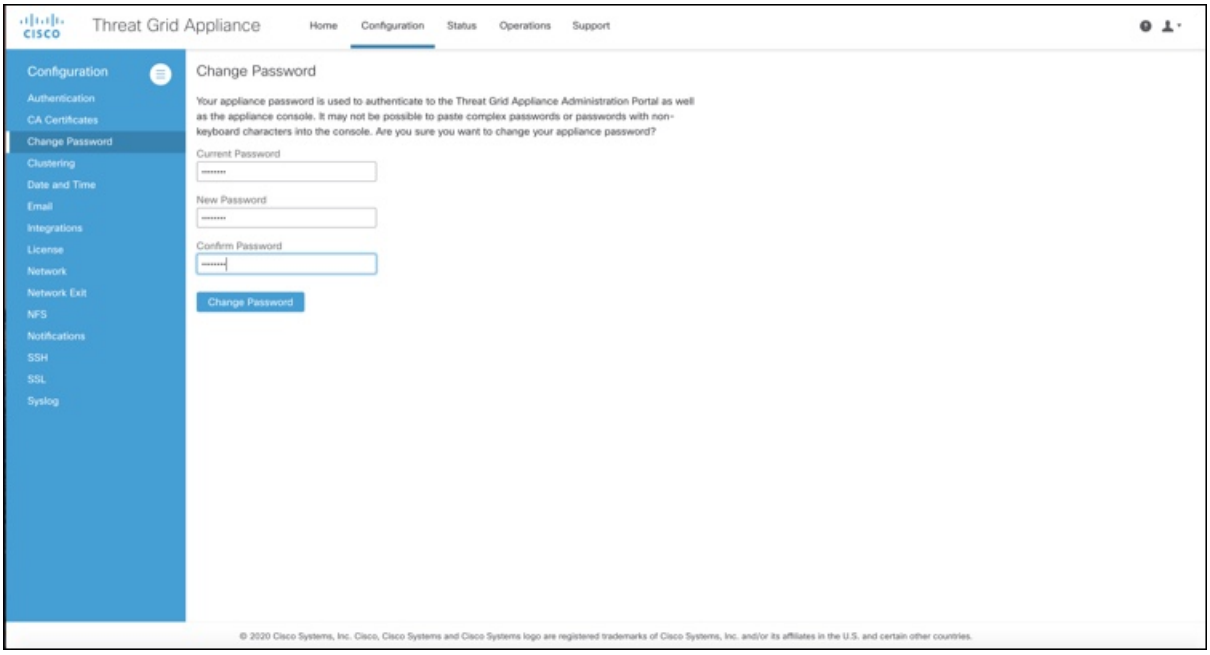
Your appliance password is used to authenticate to the Threat Grid Appliance Admin UI as well as the appliance console. You can change your password from the Admin UI using the **Change Password** page.

Note It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console so be careful when you change your password.

Procedure

Step 1 Click the **Configuration** tab and choose **Change Password**.

Figure 18: Change Password



Step 2 Enter your **Current Password**, and then enter the **New Password** and **Confirm Password**.

Step 3 Click **Change Password** and confirm the change. Changing a password does not require reconfiguration.

Clustering

The ability to cluster multiple Threat Grid Appliances is available in v2.4.2 and later. Each Threat Grid Appliance in a cluster saves data in the shared file system, and has the same data as the other nodes in the cluster.

The main goal of clustering is to increase the capacity of a single system by joining several Threat Grid Appliances together into a cluster (consisting of 2 to 7 nodes). Clustering also helps support recovery from failure of one or more appliances in the cluster, depending on the cluster size.

For more information about clustering, see the *Threat Grid Appliance Clustering FAQ*.



Important If you have questions about installing or reconfiguring clusters, contact Cisco Support for assistance to avoid possible destruction of data.

Features

Clustering Threat Grid Appliances offers the following features:

- **Shared Data** - Every Threat Grid Appliance in a cluster can be used as if it a standalone; each one is accessing and presenting the same data.
- **Sample Submissions Processing** - Submitted samples are processed on any one of the cluster members, with any other member able to see the analysis results.
- **Rate Limits** - The submission rate limits of each member are added up to become the cluster's limit.
- **Cluster Size** - The preferred cluster sizes are 3, 5, or 7 members; 2-, 4- and 6-node clusters are supported, but with availability characteristics similar to a degraded cluster (a cluster in which one or more nodes are not operational) of the next size up.
- **Tiebreaker** - When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a second vote in the event of an election to decide which node has the primary database.

  Each node in a cluster contains a database, but only the database on the primary node is actually used; the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

  Odd-numbered clusters won't have a tied vote. In an odd-numbered cluster, the tiebreaker role only becomes relevant if a node (not the tiebreaker) is dropped from the cluster; it then becomes even-numbered.



Note This feature is fully tested only for clusters with two nodes.

Limitations

Clustering Threat Grid Appliances has the following limitations:

- When building a cluster of existing standalone Threat Grid Appliances, only the first node (the initial node) can retain its data. The other nodes must be manually reset because merging existing data into a cluster is not allowed.

  Remove existing data with the destroy-data command, as documented in Reset Appliance as Backup Restore Target

Important Do not use the Wipe Appliance feature as it will render the appliance inoperable until it's returned to Cisco for reimaging.

- Adding or removing nodes can result in brief outages, depending on cluster size and the role of the member nodes.
- Clustering on the M3 server is not supported. Contact Opening a Support Case if you have any questions.

Requirements



Important **Clustering in Airgapped Deployments Strongly Discouraged** - Due to the increased complexity of debugging, appliance clustering is **strongly discouraged** in airgapped deployments or other scenarios where a customer is unable or unwilling to provide L3 support access to debug.

The following requirements must be met when clustering Threat Grid Appliances:

- **Version** - All Threat Grid Appliances must be running the same version to set up a cluster in a supported configuration; it should always be the latest available version.
- **Clust Interface** - Each Threat Grid Appliance requires a direct interconnect to the other Threat Grid Appliances in the cluster; a SFP+ must be installed in the Clust interface slot on each Threat Grid Appliance in the cluster (not relevant in a standalone configuration).

  Direct interconnect means that all Threat Grid Appliances must be on the same layer-two network segment, with no routing required to reach other nodes and no significant latency or jitter. Network topologies where the nodes are not on a single physical network segment are not supported.
- **Data** - A Threat Grid Appliance can only be joined to a cluster when it does not contain data (only the initial node can contain data). Moving an existing Threat Grid Appliance into a data-free state requires the use of the database reset process (available in v2.2.4 or later).



Important Do not use the destructive Wipe Appliance process, which removes all data and renders the application inoperable until it's returned to Cisco for reimaging.

- **SSL Certificates** - If you are installing SSL certificates signed by a custom CA on one cluster node, then the certificates for all of the other nodes should be signed by the same CA.

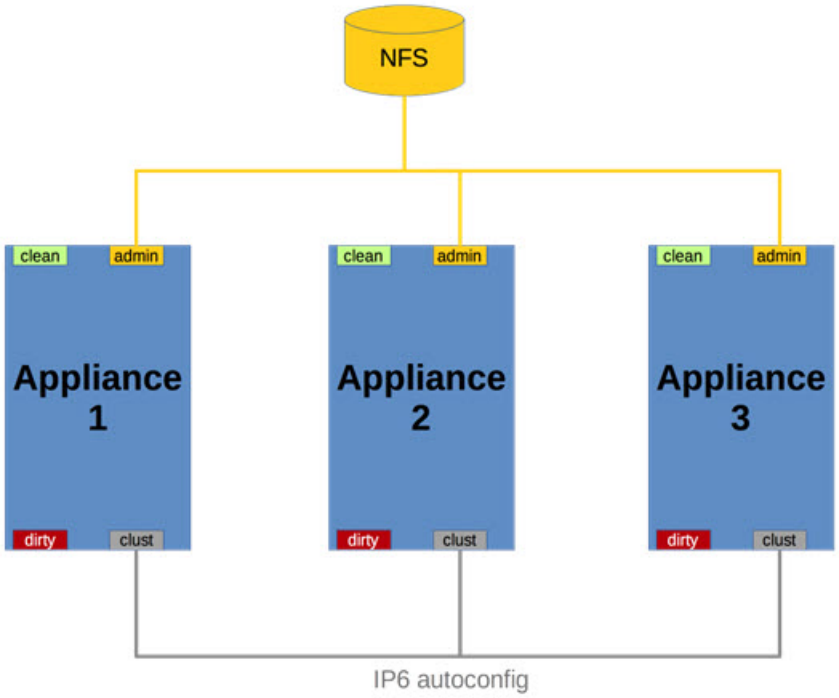
Networking and NFS Storage

Clustering Threat Grid Appliances requires the following networking and NFS storage considerations:

- Threat Grid Appliance clusters require a NFS store to be enabled and configured. It must be available via the Admin interface and accessible from all cluster nodes.
- Each cluster must be backed by a single NFS store with a single key. While that NFS store may be initialized with data from a pre-existing Threat Grid Appliance, it must not be accessed by any system that is not a member of the cluster while the cluster is in operation.

- The NFS store is a single point of failure, and the use of redundant, highly reliable equipment for that role is essential.
- The NFS store used for clustering must keep its latency consistently low.

Figure 19: Clustering Network Diagram



Building a Threat Grid Appliance Cluster

Building a Threat Grid Appliance cluster in a supported manner requires that all members be on the same version, which should always be the latest available version. This may mean that all of the members have to be built standalone first to get fully updated.

If the Threat Grid Appliance has been in use as a standalone appliance prior to clustering, only the data of the first member can be preserved. The others need to be reset as part of the build.

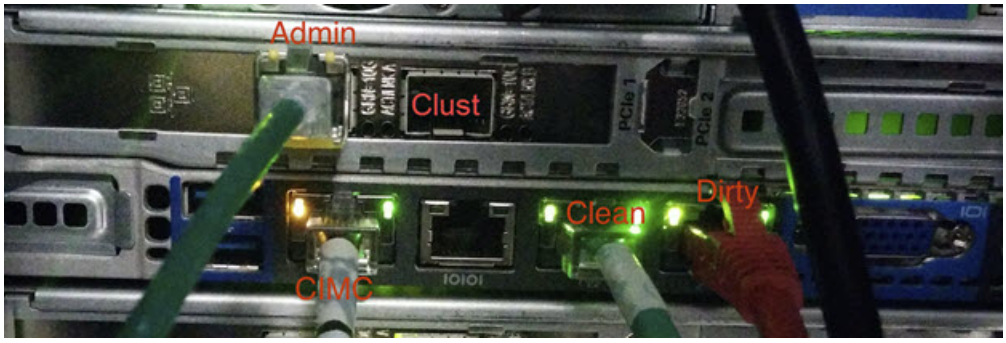
Start a new cluster with an initial node, and then join other Threat Grid Appliances to it. There are two distinct paths that are available for building a new cluster:

- Start Building Cluster from Existing Standalone Appliance
- Start Building Cluster with New Appliance

Clust Interface Setup

Each appliance in the cluster requires an additional SFP+ for the Clust interface. Install a SFP+ module in the fourth (non-Admin) SFP port. On the M5, this is the second SPF interface from the left (see the Cisco Threat Grid M5 Hardware Installation Guide for more information).

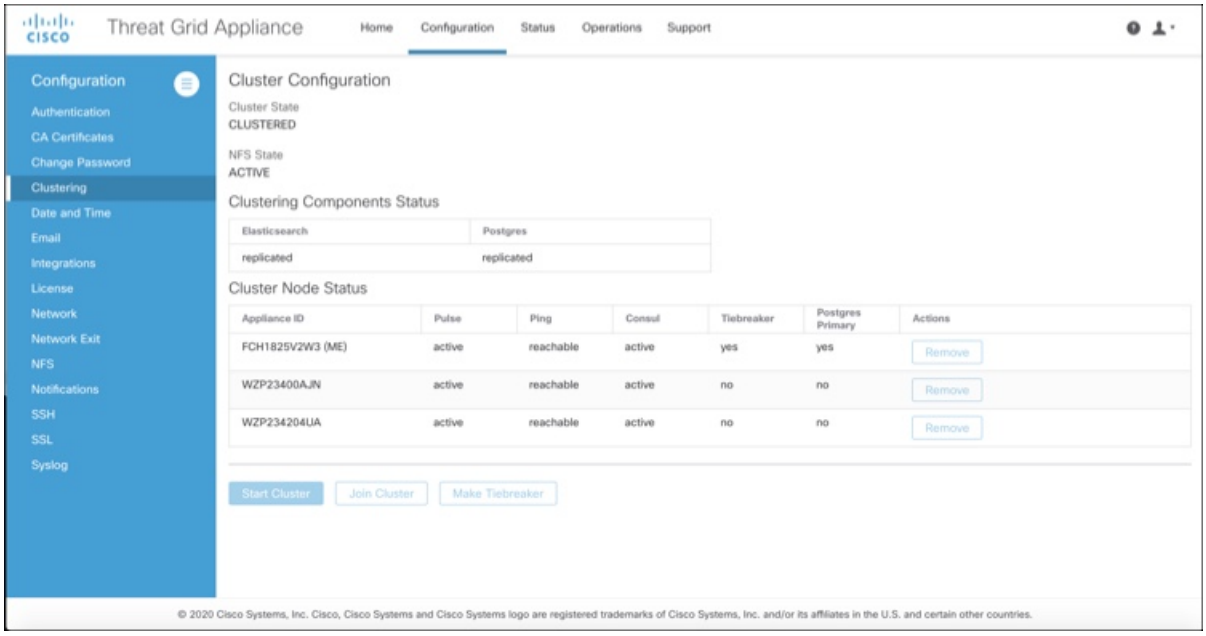
Figure 20: Clust Interface Setup for Cisco UCS M4 C220



Cluster Configuration

Clusters are configured and managed in the Admin UI on the **Cluster Configuration** page **(Configuration > Clustering)**. This section describes the fields on this page to gain an understanding of an active and healthy cluster (the screenshot shows a cluster with three nodes).

Figure 21: Cluster Configuration for Active Cluster



Cluster Prerequisites

- The appliance must be fully set up and configured.
- The NFS State must be **Active**.

Cluster State

- **Unconfigured** - Not yet configured as explicitly part of a cluster or as a standalone Threat Grid Appliance; you make this choice in the initial setup wizard if the prerequisites for clustering have been met.

- **Pending_NFS_Enable** - Cluster is pending NFS enablement.
- **Pending_NFS_Key** - Cluster is pending NFS key.
- **Standalone** - Appliance is configured as a standalone node; cannot be configured as part of a cluster without a reset.
- **Clustered** - Is clustered with one or more other Threat Grid Appliances.
- **Unknown** - Status cannot be determined.

Clustering Components Status

- **Elasticsearch**- The service used for queries that require search functionality.
- **PostgreSQL** - The service used for queries that require up-to-date, definitive data (such as account lookups).

Both services are described with one of the following status values:

- **Replicated** - Everything is working properly. Additionally, everything required to take over on failure is also in place. The appliance is able to tolerate failure and continue working. Being in a replicated state does not mean that a failure will have zero downtime. Rather, a failure should entail zero data loss and constrained downtime (less than a minute in normal circumstances, with the exception of any active analysis on the specific cluster node that fails).

  Maintenance operations that bring down nodes should only be performed when the cluster is in the replicated state.

  For a fully replicated cluster, recovery should be automatic and require less than a minute to complete in any normal scenario.
- **Available** - Everything is working properly and the referenced service is available for use (that is, it can service API and user requests), but it is not replicated.
- **Unavailable** - The service is known to be non-functional.

For more information, see the *Threat Grid Appliance Clustering FAQ* on Cisco.com.

Cluster Nodes Status

- **Pulse** - Indicates whether the node is actively connected to and using the NFS store (not during initial setup, but while running services).
- **Ping** - Describes whether the cluster node can be seen over the Clust interface.
- **Consul** - Indicates whether the node is participating in the consensus store. This requires both a network connection over Clust and a compatible encryption key.
- **Tiebreaker** - Designates the node as the tiebreaker, which will cast the deciding vote in an election to decide the cluster's primary node. See Designating the Tiebreaker Node.
- **Postgres Primary** - Indicates whether the node is the PostgreSQL primary node.

Start Building Cluster from Existing Standalone Appliance

When you start building a cluster of Threat Grid Appliances, you must start the cluster with the first node being either an existing standalone Threat Grid Appliance or a new appliance. This section describes how to build a cluster from an existing standalone Threat Grid Appliance, which allows you to preserve existing data from one appliance and use it to start a new cluster.



Note

- An existing backup must be available on NFS from which the cluster is started.
- All other nodes to be joined to the cluster must have data removed before joining; the data from additional nodes cannot be merged into the cluster.
- In releases prior to v2.4.3, standalone Threat Grid Appliances with data backed up to NFS no longer require a database reset and restore-from-backup to become the initial node of a new cluster. If you have a Threat Grid Appliance with an earlier version, we suggest that you upgrade to v2.4.3 or later and then perform a reset operation prior to initializing a new cluster.

Perform the following steps to start building the first node in a cluster from an existing standalone appliance:

Procedure

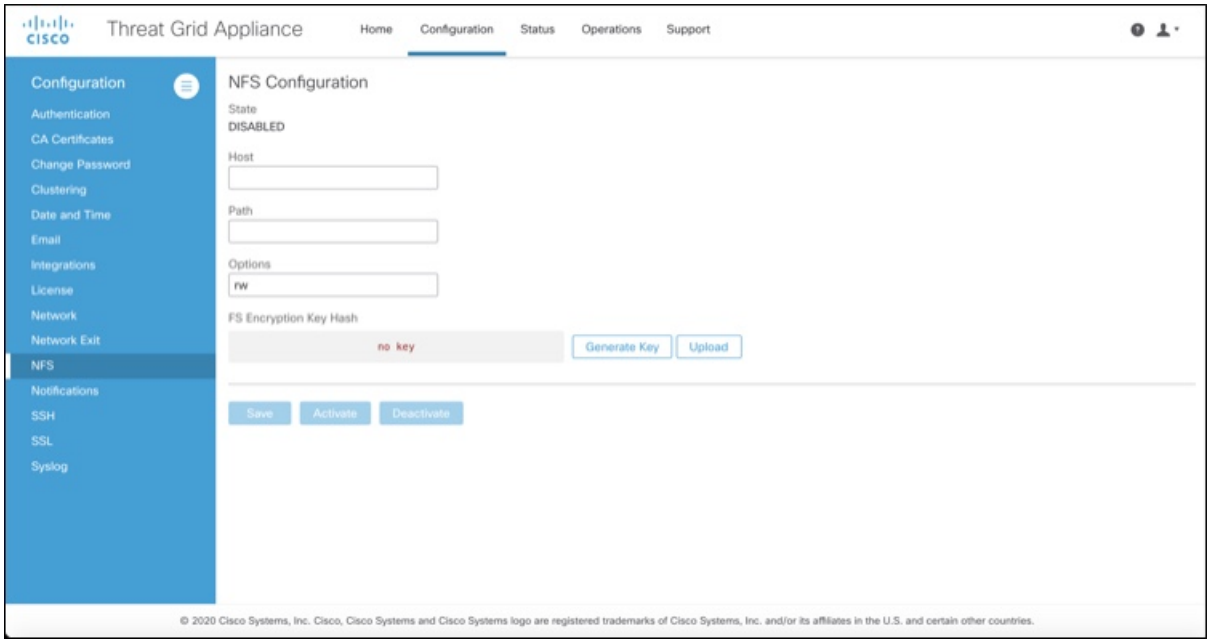
Step 1 Fully update the Threat Grid Appliance to the latest version. Depending on which version is currently running, this may require more than one update cycle to reach the latest version.

Step 2 If not already completed, configure NFS for backup of the appliance:

Note
This step describes the default Linux NFS server implementation; it may be different for your server setup.

a) Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Figure 22: NFS Configuration



b) Complete the following fields:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server where files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

c) Click **Save**.

The page refreshes and the **Generate Key** button becomes available.

The first time you configure this page, the **Remove** and **Download** buttons are available for removing and downloading the encryption key.

The **Upload** button is available if you have NFS enabled but no key created. Once you create a key, the **Upload** button changes to **Download**. If you delete the key, the **Download** button becomes **Upload** again.

Note
If the key correctly matches the one used to create a backup, the **KeyID** displayed in the Admin UI after upload should match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

d) Click **Generate Key** to generate a new NFS encryption key.

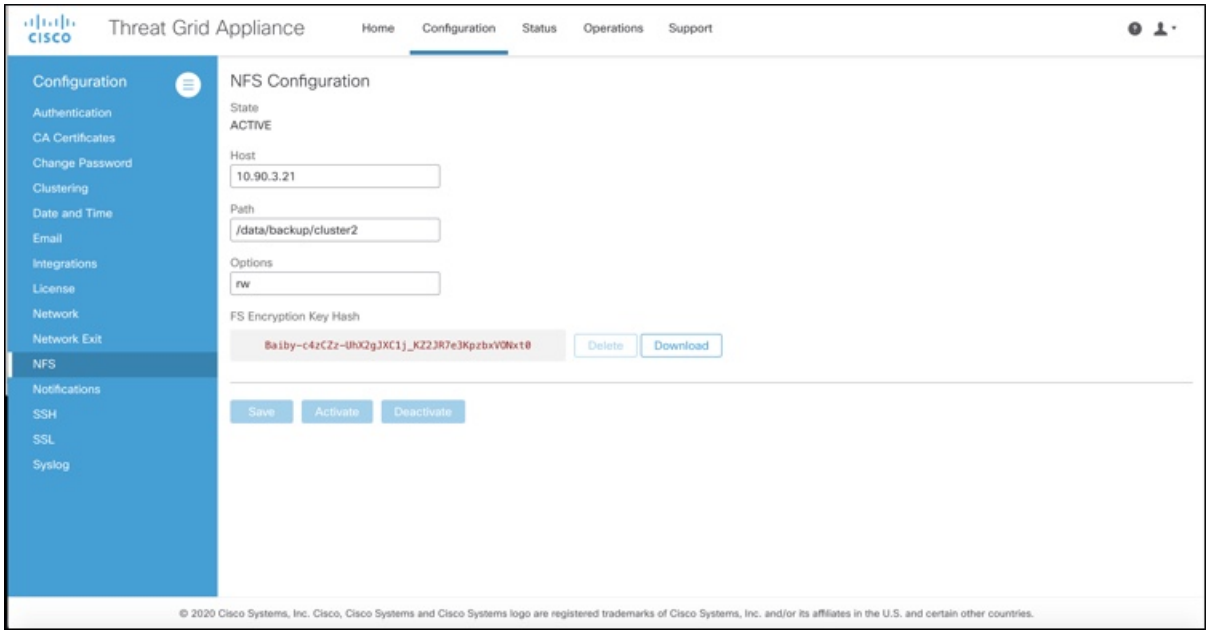
e) Click **Save**.

The page refreshes and the **Key ID** is displayed; the **Activate** and **Download** buttons become available.

f) Click **Activate**.

After a few seconds, the **State** becomes **Active**.

Figure 23: NFS Active



g) Click **Download** to download the backup encryption key. Save the generated file in a secure location. You will need the key for joining additional nodes to the cluster.

Important
If this step is missed, all data will be lost in the following steps.

Step 3 Complete the configuration, as needed, and reboot the Threat Grid Appliance to apply the NFS backup configuration.

Step 4 Perform a backup.

Note
If you do the backup at least 48 hours in advance, as recommended, and there are no service notices indicating problems with the backup, then the following manual steps are unnecessary.

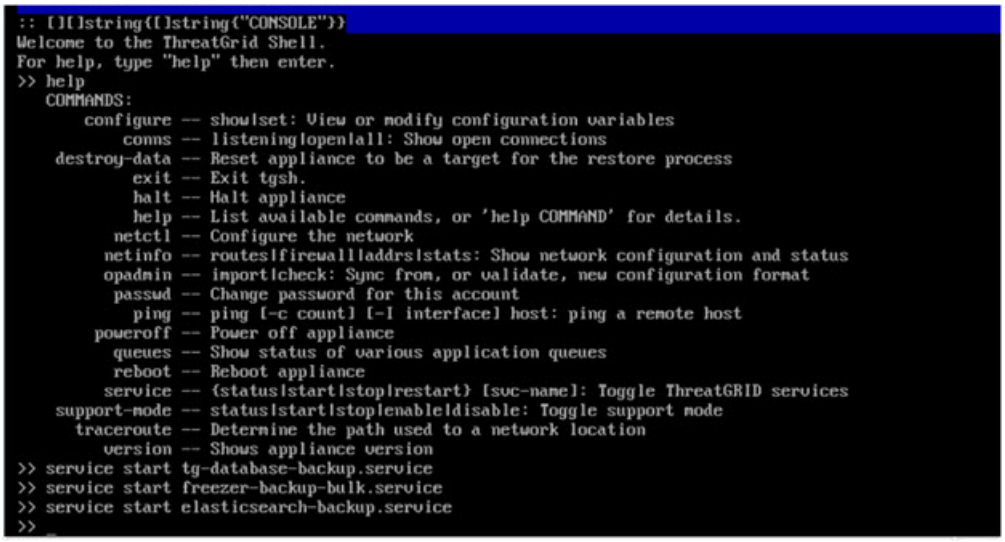
Backup and other service notices are available in the Threat Grid portal UI from the icon in the upper-right corner. If a service notice **There is no PostgreSQL backup yet** is displayed, DO NOT PROCEED.

If you do the backup immediately after reboot, you will need to manually initiate a backup of all data to NFS to ensure it's complete. Performing the manual backup is only necessary if you are setting up backup immediately before rebuilding the standalone appliance in a cluster.

a) Open **tgsh** and enter the following commands:

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

Figure 24: Initiating a Backup of All Data to NFS



b) Wait about 5 minutes after the last command returns.

Step 5 In the Threat Grid portal UI, check for service notices. If any notices indicate a backup process failure, such as a warning that there is no PostgreSQL backup yet, then DO NOT PROCEED.

Important
Do not continue unless these processes have completed successfully.

Step 6 Click the **Configuration** tab and choose **Clustering** to open the **Clustering Configuration** page.

Step 7 Click **Start Cluster**.

Step 8 On the confirmation dialog, click **OK**.

The **Clustering Status** changes to **Clustered**.

Step 9 Finish the installation. This initiates a restore of the data in cluster mode.

What to do next

Now you can begin joining other Threat Grid Appliances to the new cluster, as described in Joining Threat Grid Appliances to a Cluster.

Start Building Cluster with New Appliance

When you start building a cluster of Threat Grid Appliances, you can start the cluster with the first node being new Threat Grid Appliance. This method of building a cluster can be used for new appliances that are shipped with cluster-capable versions of the software, or for existing appliances that have had their data reset.

Note Remove existing data with the `destroy-data` command, as documented in Reset Appliance as Backup Restore Target. Do not use the Wipe Appliance feature.

Procedure

Step 1 Set up and begin the Admin UI configuration as normal.

Step 2 Configure the Network and License.

Step 3 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Note
See the figures in Start Building Cluster from Existing Standalone Appliance.

Step 4 Complete the following fields:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server where the files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

Step 5 Click **Save**.

The page refreshes, and the **Generate Key** and **Activate** buttons become available.

Step 6 Click **Generate Key** to generate a new NFS encryption key.

Step 7 Click **Activate**.

The **State** changes to **Active**.

Step 8 Click **Download** to download a copy of the encryption key for safekeeping. You will need the key for joining additional nodes to the cluster.

Step 9 On the **Cluster Configuration** page, click **Start Cluster**, and then click **OK** on the confirmation dialog.

The **Clustering State** changes to **Clustered**.

Step 10 Complete the remaining steps in the wizard and click **Start Installation**. This initiates a restore of the data in cluster mode.

Step 11 Open the **Cluster Configuration** page and check the health of the new cluster.

What to do next

Proceed to Joining Threat Grid Appliances to a Cluster.

Joining Threat Grid Appliances to a Cluster

This section describes how to join new and existing Threat Grid Appliances to a cluster.

Note A Threat Grid Appliance can be joined to an existing cluster only when it contains no data; unlike the initial appliance, which may contain data.

Also, it is critically important that the Threat Grid Appliance that is joining a cluster has the latest software version installed (all nodes in a cluster must be running the same version). This may require setting up the Threat Grid Appliance and update it, then reset the date and join it to the cluster.

Add one node at a time, and wait for Elasticsearch and PostGreSQL to reach the state of **Replicated** before adding the next node. The **Replicated** status is expected in clusters of two or more nodes.

Note The wait for the state change for Elasticsearch and PostGreSQL to reach **Replicated** does not apply to the single-node case. If you are initializing a single-node cluster from a backup, you should wait for the restore to be completed and the application to be visible in the UI before adding the second node.

When joining a Threat Grid Appliance to a cluster, the NFS and clustering must be configured during the initial setup.

Joining Existing Appliances to a Cluster

Perform the following steps to join an existing Threat Grid Appliance to a cluster:

Procedure

Step 1 Update the Threat Grid Appliance to the latest version. This may require several update cycles depending on the current version that is installed. All nodes in a cluster must be the same version.

Step 2 Run the `destroy-data` command in **tgsh** to remove all data; when joining an existing Threat Grid Appliance to a cluster, all data must be removed prior to being merged into the cluster. See Reset Appliance as Backup Restore Target.

After running the `destroy-data` command on an existing Threat Grid Appliance, it basically becomes a new node, and joining it to a cluster follows the same steps as Joining New Appliances to a Cluster.

Joining New Appliances to a Cluster

Perform the following steps to join a new Threat Grid Appliance to a cluster:

Procedure

Step 1 Begin the new Admin UI configuration as described in the Cisco Threat Grid Appliance Getting Started Guide.

Step 2 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Step 3 Specify the **Host** and **Path** to match what was set in the first node in the cluster.

The **Status** is **Enabled_Pending Key**.

Step 4 Click **Save**. The page refreshes and the **Upload** button becomes available.

Note
If the key correctly matches the one used to create a backup, the **Key ID** displayed in the Admin UI after upload should match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

Step 5 Click **Upload** and choose the NFS encryption key you downloaded from the first node when you started the new cluster.

Step 6 Click **Save**.

The page refreshes; the **Key ID** is displayed and the **Activate** button is enabled.

Step 7 Click **Activate**.

The **Status** changes to **Active** after a few seconds (lower left corner).

Step 8 In the **Configuration** menu, choose **Clustering** to open the **Cluster Configuration** page.

Step 9 Click **Join Cluster** and then click **OK** on the confirmation dialog.

The **Cluster State** changes to **Clustered**.

Step 10 Finish the installation. This will initiate a restore of the data in cluster mode.

Step 11 Repeat the Step 1 through Step 10 for each node you want to join to the cluster.

Designating the Tiebreaker Node

When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a second vote in the event of an election to decide which node has the primary database.

Each node in a cluster contains a database, but only the database on the primary node is actually used; the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

We recommend that clusters contain three, five, or seven nodes. Having tiebreaker support is part of an ongoing effort to mitigate the loss of reliability in moving from a standalone Threat Grid Appliance to a two-node cluster.

When a cluster is completely healthy and the *current node* is not the tiebreaker, the **Make Tiebreaker** button is active on the **Cluster Configuration** page.

To designate a node as the tiebreaker, click **Make Tiebreaker**. There will be a brief service disruption, after which the current node will be the one which is not allowed to fail, and the other node can be shut down without breaking the cluster.

In the event of a permanent failure of the tiebreaker node where you are unable to modify the designation ahead of time, either reset the surviving node and restore from backup, or contact Opening a Support Case for assistance.

Removing a Cluster Node

To remove a node from a cluster, navigate to the **Cluster Configuration** page (**Configuration > Clustering**) and click **Remove** in the **Action** column for the node to be removed.

- Removing a node from the cluster indicates that it should no longer be considered part of the cluster, rather than a node that is temporarily down. You should remove a Threat Grid Appliance when it is being decommissioned; either being replaced with different hardware or will be rejoined to a cluster only after its data has been reset.
- Removing a node indicates to the system that you are not going to re-add a node, or if you do re-add it, it has been reset.
- A node is not marked as having been permanently removed from a cluster if it has pulse (is actively writing to NFS), or is active on consul (part of the consensus store).

To replace a still-live node (in a cluster with less than seven nodes), add the new node, wait for the cluster to go green, then remove the old one offline using the **Remove** button. This alerts the system that it's not coming back.

When you first take the node offline, the cluster status changes to yellow. After you click **Remove**, the status reverts back to green (since the cluster will resize such that it no longer expects the now-removed node to be present).

Resizing a Cluster

When a node is removed from a cluster using the **Remove** button, the cluster resizes; this may affect the number of failures it is expected to tolerate. If a cluster is resized in such a way as to change the number of expected failure tolerances (as defined in Failure Tolerances), it will force an Elasticsearch restart, which will cause a brief service interruption.

Exception: This does not include a system other than the PostgreSQL master being rebooted or having a transient failure. Disruption should be minimal in that case except for clients actively using that node, or if samples are running on it.

If you add a Threat Grid Appliance that was not already part of the cluster, or if you click **Remove**, and this changes the cluster size such that the number of tolerated failures is changed, then there will be a brief interruption as the rest of the cluster reconfigures.

Failure Tolerances

In the event of a failure, clustered Threat Grid Appliances will not lose any data, with the exception of any analysis being actively run by the failed node, and will recover service with a minimal (less than one minute) service disruption period and no user involvement.

Most failures will recover in less than a minute if the number of available nodes is not smaller than the number shown in the **Nodes Required** column in the **Failure Tolerances** table; or will recover after the number of available nodes increases to meet that count. This is true if the cluster was in a healthy state prior to failures (as indicated by services listed as **Replicated** on the **Clustering** page).

The number of failures a cluster of a given size is expected to tolerate is shown in the following table.

Table 2: Failure Tolerances

Cluster Size	Failures Tolerated	Nodes Required
1	0	1
2	1*	1*
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

These figures represent best-case scenarios. If the cluster is not showing green across the board when all nodes are up, then it may not be able to tolerate the full failure count indicated.

For example, if you have a 5-node cluster size with 2 failures tolerated, 3 nodes required, and all 5 appliances are actively processing data, the cluster will be able to reconfigure itself and continue operation without human administrative action if up to 2 failures take place.

Another consideration, in a 5-, 6-, or 7-node cluster, the +1 in the number of failures tolerated means that the percentage of nodes that can fail is higher, which is particularly important because the number of nodes acts as a multiplier to the failure rate. (If you have two nodes, and each has a hardware fault once every 10 years, then you just change your hardware fault rate to once every 5 years.)

Failure Recovery

Most failures recover automatically. If not, you should contact Opening a Support Case, or restore the data from backups. See Restore Backup Content for more information.

API/Usage Characteristics

Status of samples submitted to any node in a cluster may be queried from any other node in the cluster; there is no need to track to which individual node a submission took place.

Processing of sample submissions made to one node will be split across all nodes in the cluster; there is no need to actively load-balance from the client side.

Operational/Administrative Characteristics

In a cluster with two nodes, one of the nodes is the tiebreaker and acts as a single-point-of-failure. However, the other node may be removed from the cluster without ill effect (beyond transient failures during cutover). When a 2-node cluster is healthy (both nodes are fully operational), the tiebreaker designation may be modified by the user, to alter which of the nodes is a single point of failure.

Service may be temporarily disrupted during a failover event; samples which were actively running during a failover will not be automatically rerun.

In the context of clustering, capacity refers to throughput, not storage. A cluster with three nodes prunes data to the same maximum storage levels as a single Threat Grid Appliance. Consequently, a cluster of three

5000-sample appliances, with a total 15,000-samples/day rate limit, will (when used at full capacity), have retention minimums of 33 percent shorter than the 10,000-sample/day estimates provided in the *Threat Grid Appliance Data Retention Notes* on Cisco.com.

Sample Deletion

Support for deleting samples is available on Threat Grid Appliances (v2.5.0 or later):

- The **Delete** option is available in the **Actions** menu in the samples list.
- The **Delete** button is available in the upper-right corner of the sample analysis report.



Note It may take up to 24 hours for backup copies of deleted samples to be removed from all nodes.

Deleted samples are removed from the shared NFS store immediately; removed from the node processing the deletion request immediately, but the other nodes will lag until the nightly cron job is run. In clustered mode, the NFS store is considered the primary source for samples, so even if the sample is not physically removed from other nodes, it should no longer be retrievable from any of them.

In Threat Grid Appliance v2.7 and later, sample deletion is extended to include artifacts, which matches the behavior of the cloud product.

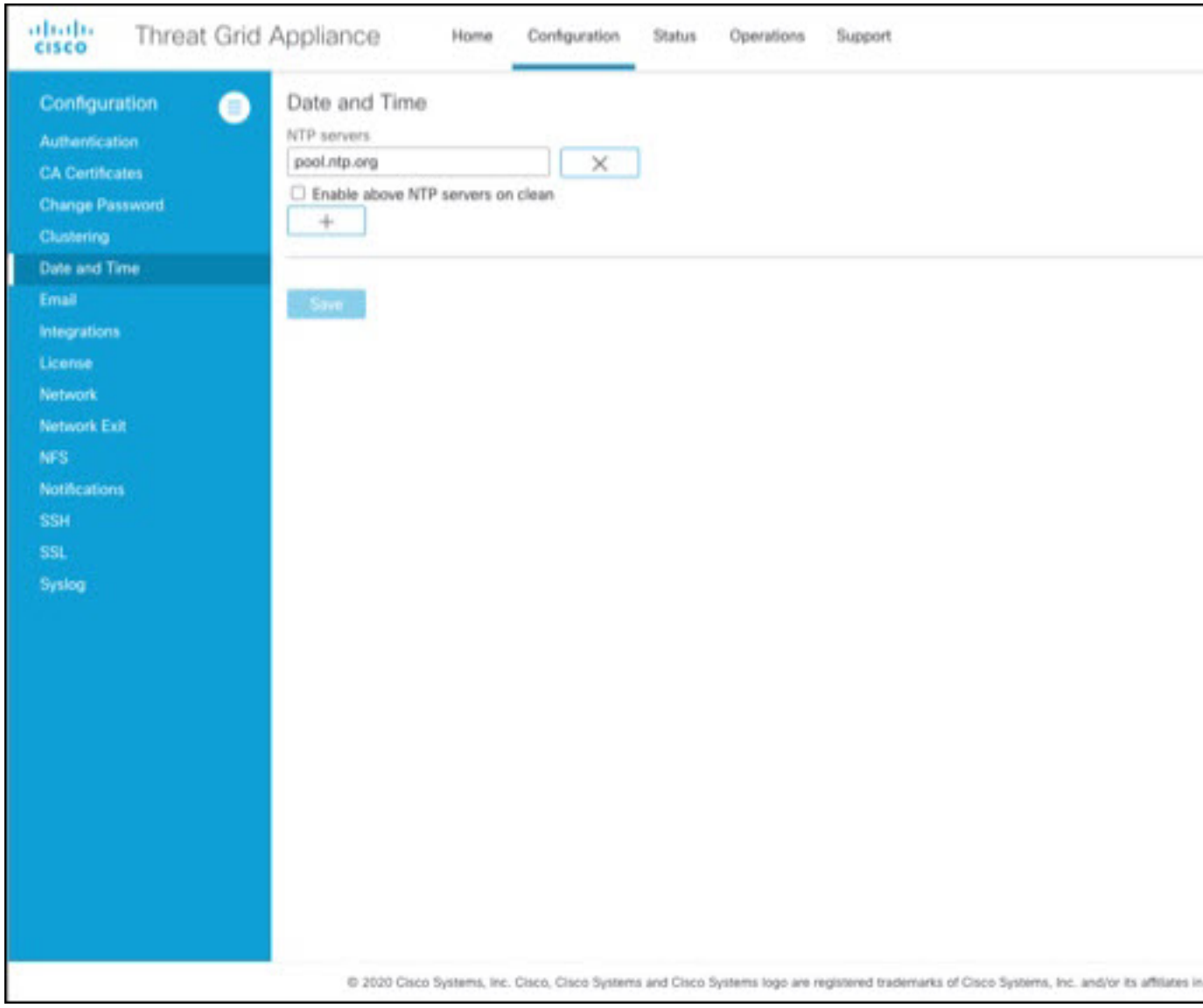
Date and Time

When you initially set up the Threat Grid Appliance, you specify the Network Time Protocol (NTP) servers to configure the date and time. You can add or delete NTP servers using the **Date and Time** page.

Procedure

Step 1 Click the **Configuration** tab and choose **Date and Time** to open the **Date and Time** page.

Figure 25: Date and Time



Step 2 Add or remove NTP Server(s):

- Click the + icon to add another field and enter the NTP server name or IP address; repeat as needed.
- Click the **x** icon to remove a server.

Step 3 Click **Save**.

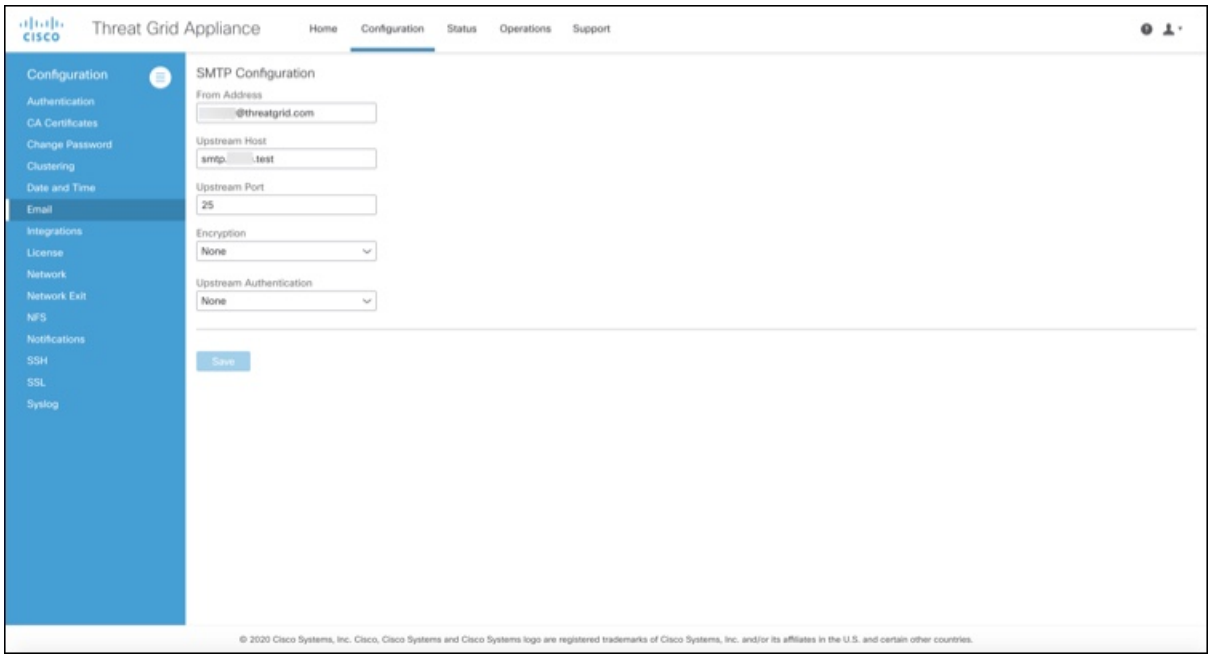
Email

When you initially set up the Threat Grid Appliance, you configure your email settings. You can modify these settings on the **Email** page.

Procedure

Step 1 Click the **Configuration** tab and choose **Email** to open the **SMTP Configuration** page.

Figure 26: SMTP Configuration



Step 2 Make your modifications and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Integrations

Integrations with several third-party detection and enrichment services, including OpenDNS, TitaniumCloud, and VirusTotal, can be configured on the appliance using the **Integrations** page (v2.2 and later).

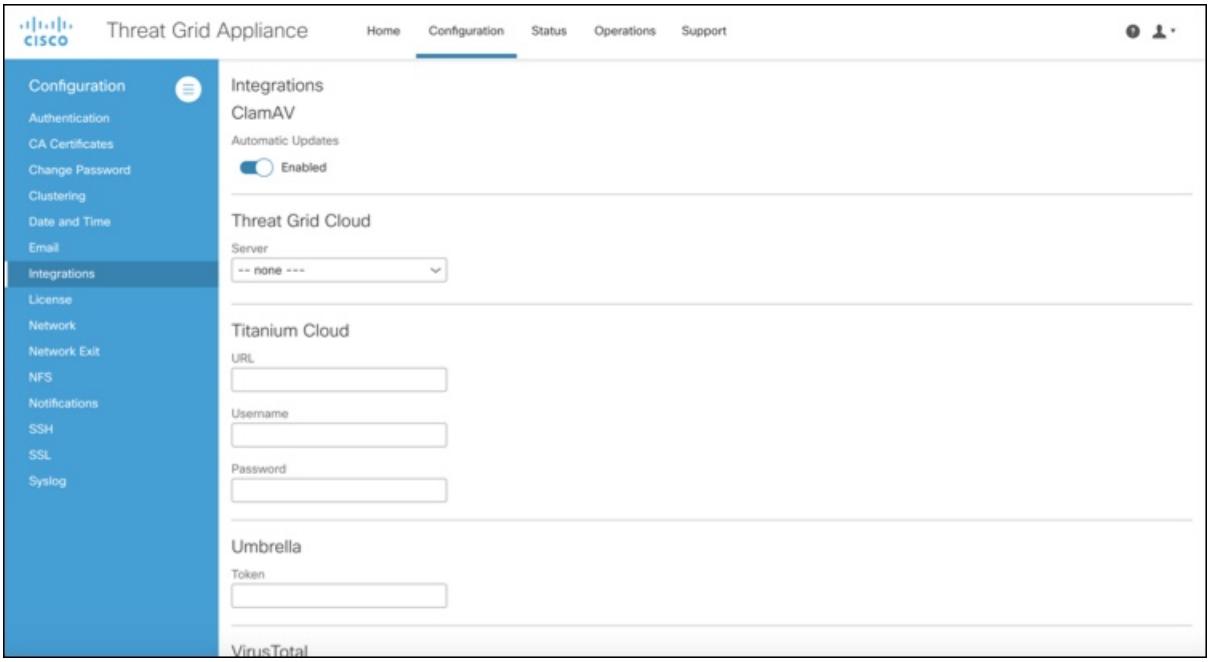
The Cloud Search Federation feature (available in v2.8 and later), provides users with an option in the Threat Grid portal UI to rerun a search query against the Threat Grid cloud instance, if a cloud endpoint is configured as described below.

Note If OpenDNS is not configured, the **whois** information on the Domains entity page in the analysis report (in the Mask version of the UI) will not be rendered.

Procedure

Step 1 Click the **Configuration** tab and choose **Integrations** to open the **Integrations** configuration page.

Figure 27: Integrations Configuration Page



Step 2 Enter the authentication or other values required for each integration.

Note
ClamAV signatures can be automatically updated on a daily basis, and is enabled by default. You can disable the **Automatic Updates** setting in the **ClaimAV** section.

Step 3 Click **Save**.

License

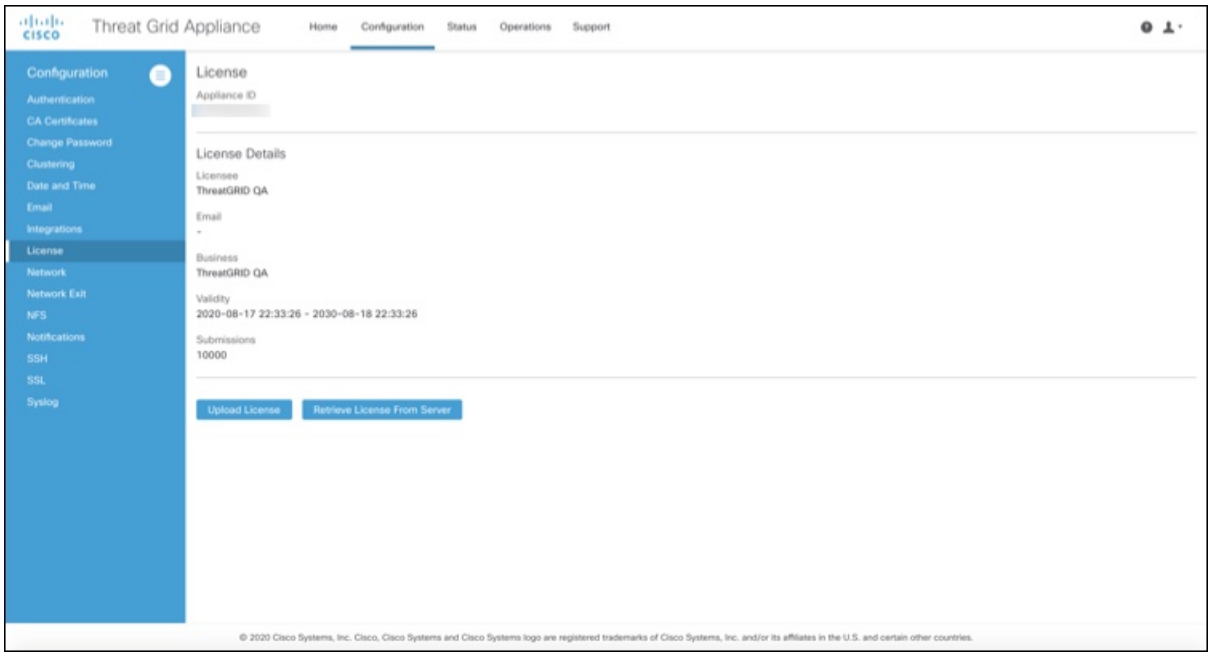
When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration > License** page is enabled. However, if that doesn't work or if there's a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

You can view or update your license information using the **License** page.

Procedure

Step 1 Click the **Configuration** tab and choose **License** to open the **License** page.

Figure 28: License Page

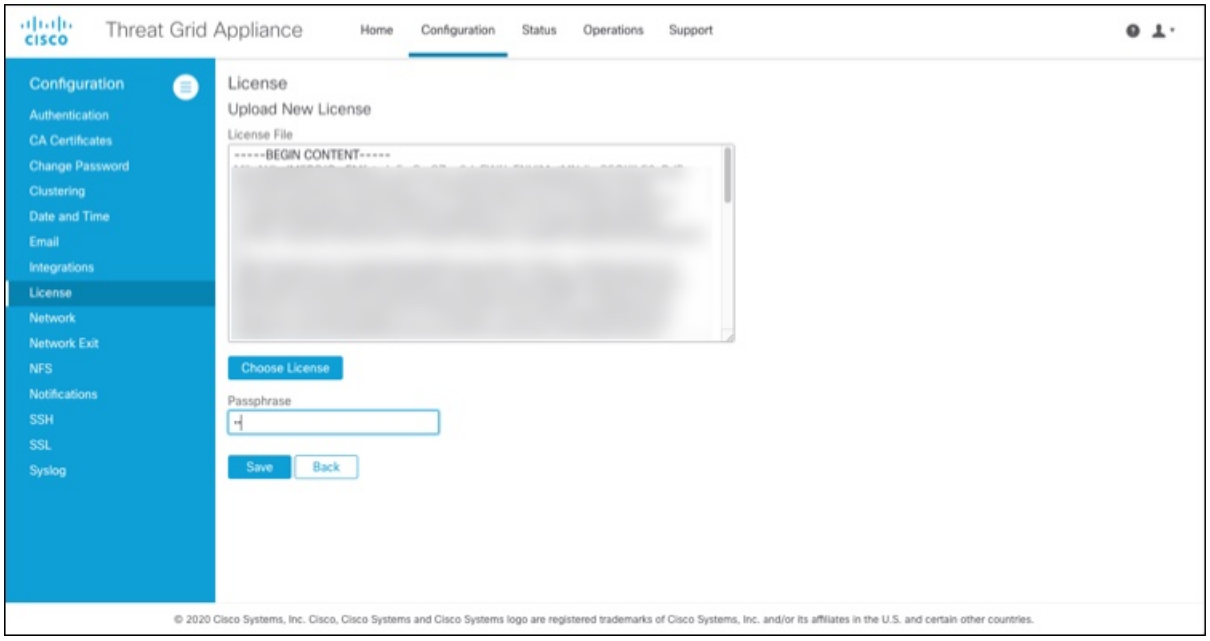


Step 2 Upload the license or retrieve it from the server. Typically, you must upload the license for air-gapped appliances.

To Upload License:

a) Click **Upload License** to open the **Upload New License** page.

Figure 29: Upload License



b) Click **Choose License** to open the **File Manager**, choose the license file you received from Threat Grid (the file has .lic extension), and click **Open**.

The contents of the license are added to the **License File** field.

c) Enter the password that Threat Grid provided (with the .lic file) in the **Passphrase** field and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

To Retrieve License from Server:

a) Click **Retrieve License From Server** to retrieve and add the license.
b) Click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Network

If you used DHCP for the initial configuration, and you need to adjust the IP assignment from DHCP to your permanent static IP addresses for all three networks, perform the following steps.

Note The Admin UI does not validate the gateway entries. If you enter the wrong gateway and save it, the Admin UI will not be accessible. You will need to use the console to fix the networking configuration if that was done on the admin interface. If Admin is still valid, you can fix it in the Admin UI and reboot.

Procedure

Step 1 Click the **Configuration** tab and choose **Network** to open the **Network Configuration** page.

Figure 30: Network Configuration

Step 2 Complete the following fields:

Note
The Admin network settings were configured using the TGSH Dialog during the initial Threat Grid Appliance setup and configuration.

- **IP Assignment** - Choose **Static** from the drop-down lists for all three interfaces (Clean, Dirty, and Admin).
- **IP Address** - Enter a static IP address for the Clean or Dirty network interface.
- **Subnet Mask and Gateway** - Complete as appropriate for the type of network interface.
- **Host Name** - Enter the host name for server.
- **Primary DNS Server** - Enter the primary DNS server address.
- **Secondary DNS Server** - Enter the secondary DNS server information.

Step 3 Click **Save** to save your network configuration settings, and then click **Activate**.

A message is displayed indicating that reconfiguration is required (see Applying Configuration Changes).

Configuring DNS

By default, DNS uses the Dirty interface. If the hostname of an integrating appliance or service, such as AMP for Endpoints Private Cloud, cannot be resolved over the Dirty interface because the Clean interface is used for the integration, a separate DNS server that uses the Clean interface can be configured in the Admin UI.

Procedure

Step 1 Click the **Configuration** tab and choose **Network** to open the **Network Configuration** page.

Step 2 Complete the **DNS** fields for the Dirty and Clean networks.

Step 3 Click **Save**.

Network Exit

Geographic location is often an important issue for malware analysis. Some types of malware behave differently depending on geographic location, while other types may target a specific area. Similar in concept to VPN, the **Network Exits** mode (available in v2.4.3 and later) makes any outgoing network that is generated during sample analysis appear to exit from that location. Configuration files are automatically distributed and there is no need for support staff to manually install or update them.

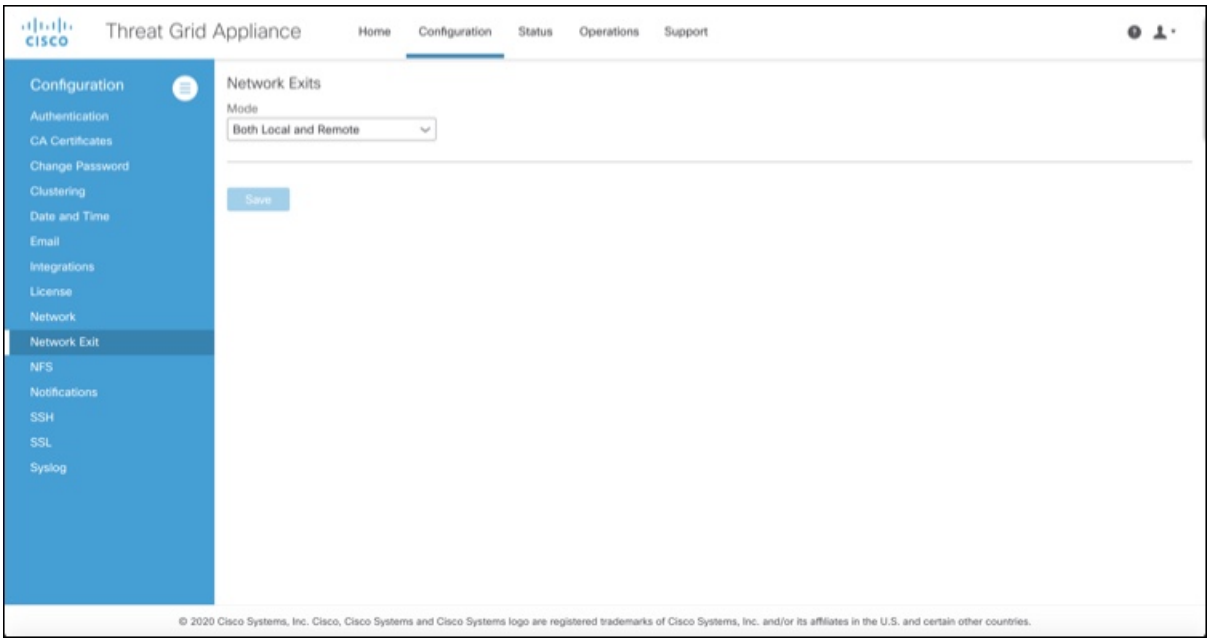
Note **tg-tunnel and v2.4.3:** If you were previously using tg-tunnel, you must allow outbound traffic to specific IP addresses and ports required for Network Exit before installing v2.4.3; otherwise, that traffic only needs to be permitted before enabling remote exit use. The required IP addresses and ports change occasionally. See Required IP and Ports for Threat Grid for the most recent list.

Procedure

Step 1 Click the **Configuration** tab and choose **Network Exit** to open the **Network Exits** configuration page.

The setting on this page determines the **Network Exit** options that will be available in the Threat Grid portal when submitting samples for analysis.

Figure 31: Network Exits Configuration



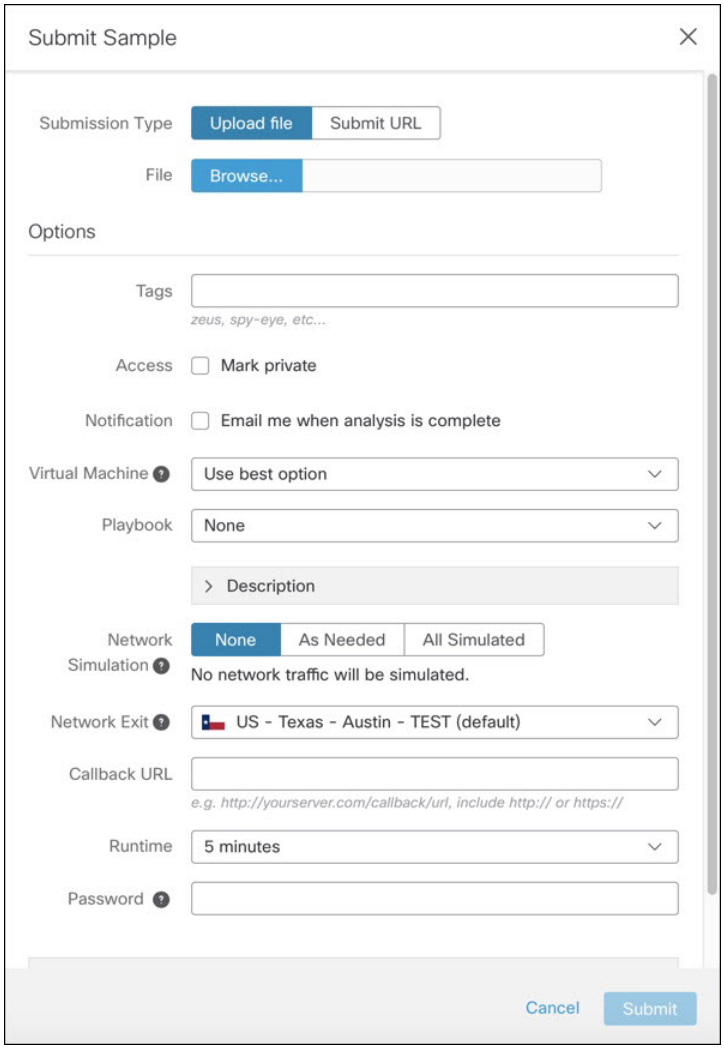
Step 2 From the Mode drop-down list, choose **Local Only**, **Remote Only**, **Both Local and Remote**, or **Simulation Only**.

If you choose **Local Only** or **Remote Only**, the application makes only those options available to users; if you choose **Both Local and Remote**, both options will be available to users.

If you choose **Simulation Only**, the API and UI users cannot choose any option to send network traffic from virtual machines to destinations outside of the local Threat Grid Appliance.

Accessing private networks, even for DNS lookup, is not allowed even for Network Exit. All malware traffic comes out of the Dirty interface, using the Dirty DNS server configured.

Figure 32: Submit Sample



Note
Sometimes it may be necessary to simulate network connections during analysis. Network simulation provides analysts with a way to present network resources to malware samples that may otherwise be unavailable, and for other reasons. For example, you may want to choose a network simulation option to simulate network connections when the upstream servers are not accessible; when they have been taken down; when their DNS records are gone; or if other restrictions on outbound connectivity apply in order to improve sample execution and convictions.

In addition, network simulation can provide at least some connectivity to air-gapped appliances and improve sample execution on them.

The **Network Simulation** option for sample analysis is available on Threat Grid Appliances v2.7.1 and later. See the Threat Grid portal UI online help topic for additional information.

NFS

The Threat Grid Appliance (v2.2.4 or later) supports encrypted backups to NFS-backed storage, initialization of data from such storage, and reset to an empty-database state into which such a backup can be loaded.

Note Reset is different from the Wipe Appliance process; it is used to allow an appliance to be shipped off customer premises without information leakage, and is for backup preparation. The wipe process appropriate for that purpose already exists in the recovery bootloader, but is not suitable for preparing a system to restore a backup.

Content is encrypted with gocryptfs, a third-party open source product.

Note Filename encryption is disabled for performance reasons. Samples and other content in Threat Grid are not stored with their original names under any circumstances so this does not leak customer-owned data.

We strongly encourage consulting the documentation prior to use. Extended documentation regarding the backup functionality is available, and we strongly encourage consulting it prior to use. For additional technical information and instructions see the *Threat Grid Appliance Backup Notes and FAQ*.

NFS Requirements

The following NFS requirements must be met for encrypted backups to NFS-backed storage:

- Must be running the NFSv4 protocol over TCP, accessible from the Threat Grid Appliance admin interface.
- Configured directory must be writable by **nfsnobody** (UID 65534).
  - Exposing files for write by **nfsnobody** is secure. The only processes on the Threat Grid Appliance running as **nfsnobody** or with write to **nfsnobody**, are those responsible for encryption of data. Plain text data is exposed under distinct user accounts for different subtrees according to principal of least privilege; the PostgreSQL service on the appliance cannot access Elasticsearch data or the freezer; the Elasticsearch service cannot access PostgreSQL or freezer data.
  - Using the **nfsnobody** account simplifies configuration, preventing the need to build an **idmap.conf** for each customer site, mapping local and remote account names together.
- The NFSv4 server must be accessible via the Admin 10-Gb interface.
- Sufficient storage must be available (see Backup Storage Requirements).
- The system will use these parameters: `rw`, `sync`, `nfsvers=4`, `nofail`

Note Do not enter conflicting parameters. Manually entering any parameters that conflict with the above parameters is explicitly unsupported and may result in undefined behavior.

- Invalid NFS configuration (or configuration pointing the service to an incorrectly configured NFS server) will generally cause the process of applying configuration to fail. Correcting this configuration in the Admin UI and reapplying should result in success.

Backup Storage Requirements

Total storage required for a backup store should not require more than 5.6 TB. A backup store consists of the following components:

- **Object Store** - This is normally the bulk of the storage in use. Data retention for the bulk component of a backup store follows the same policies and limits documented for the Threat Grid Appliance release in use and places maximum storage use for this component as 4.1 TB. See the Threat Grid Appliance Data Retention Notes.
- **PostgreSQL database store** - This contains two full backups of the PostgreSQL store, and a chain of WAL logs sufficient to allow replay from the oldest of the retained full backups. This should be less than 500 GB in total.
- **Elasticsearch snapshot store** - This should be less than 1 TB in total.

Backup Expectations

The following backup expectations should be considered:

- **Included in Backup** - The initial release of the Threat Grid Appliance backup process includes the following customer-owned bulk data:
  - Samples
  - Analysis results, artifacts, flagging
  - Application-layer (not Admin UI) organization and user account data.
  - Databases (including users and organizations)
  - Configuration done within the Face or Mask portal UI
- **Not Included in Backup** - The following is not included in the initial release of the Threat Grid Appliance backup process:
  - System logs
  - Previously downloaded and installed updates
  - Configuration inside the appliance Admin UI, including SSL keys and CA certificates
- **Other Expectations** - Other considerations about the backup process include:
  - PostgreSQL base backup takes place on a 24-hour cycle. Database backup cannot be restored, and a warning will be displayed, until this has successfully completed at least once.
  - Elasticsearch backup takes place incrementally, once every 5 minutes.
  - Freezer backup takes place on an ongoing basis, with a job following behind every 24 hours to handle any objects which were missed from the ongoing backup.

- Generating a new key creates a new, independent backup store. Like the original, this new store is not valid until a base backup has taken place on a 24-hour cycle.

Backup Data Retention

During a backup, data is retained as follows:

- **PostgreSQL** - The last two successful backups and all WAL segments since those backups are retained.
- **Elasticsearch** - The last two 5-minute snapshots are retained.
- **Bulk Storage** - The same retention policy followed and documented for a single Threat Grid Appliance is used for the shared store.

If you want to retain historical data for longer periods, it is strongly recommended that you use a NFS server with filesystem- or block-layer snapshot support.

Database base backups are only retained until a new base backup has been successfully created.



Note Backup copies of the virtual images are created on the RAID-1 storage array, to be used in the event of a reset following a bulk-storage failure. Early Cisco Threat Grid Appliance models (based on the UCS C220-M3 platform) have less storage than later models, and are more likely than other units to have less than 25 percent of disk space remaining available on the RAID-1 file system after installing Threat Grid Appliance v2.9, which will trigger a service notice.

For later model hardware, being at less than 25 percent of remaining storage on the RAID-1 array after installing the v2.9 release is not normal and should be raised to customer support.

Strictly Enforce Retention Period Limits

The **strict_retention** option in **tgsh** (v2.6 or later) allows you to strictly enforce the retention period limit by not storing artifacts from analysis for more than fifteen (15) days. When this option is enabled, files are deleted during the first nightly pruning on which they are more than 15 days old.



Note The time period of 15 days cannot be configured or changed.

Artifacts refers to the samples themselves and other things generated from them. Artifacts do not include the analysis report HTML, which is subject to its original limits as otherwise documented. Artifacts also do not include database entries and search indexes.

The **strict_retention** option is disabled (false) by default. To enable the hard-pruning of artifacts after 15 days, set the option to true in **tgsh**:

configure set strict_retention true

Backup Frequency

The backup frequency of data is as follows:

- For bulk storage of samples, artifacts and reports, content is continuously backed up. Additionally, a pass is performed to look for and transfer missing content on a 24-hour cycle.

- For the PostgreSQL database, a base backup is created on a 24-hour cycle, and incremental content is continually added thereafter, either as soon as a 16-MB threshold of newly-written database content is reached, or not less than once every 5 minutes.
- For the Elasticsearch database, content is incrementally added to the backup store on a 5-minute cycle.

Backup frequency cannot be controlled or tuned because doing so would make estimates regarding storage usage, restore-process time, and performance overhead invalid.

Backup Related Service Notices

The following service notices may be displayed during the backup process:

- **Network storage not mounted** - Check that the network file system being used as a backend is fully operational, and then try reapplying configuration through the Admin UI or rebooting your appliance.
- **Network storage not working** - Check that the network file system being used as a backend is fully operational; if the system does not recover within 15 minutes of correcting any problems with the NFS server, try rebooting your appliance.
- **Backup file system access failure** - Contact customer support.
- **No PostgreSQL backup found** - This is a normal condition between the point in time when a backup store has been configured and the point in time when the first base backup (run automatically on a 24-hour cycle) takes place. Note that until this is complete, a backup is not considered complete and cannot be restored. If and only if this message persists for more than 48 hours, contact customer support.
- **Newest PostgreSQL base backup more than two days old** - This indicates that the system has not been successful in generating a new base backup for PostgreSQL. If not remediated, it can result in unbounded usage on the backup store (to retain a full chain of writes necessary to restore from an increasingly old backup point), and unacceptably long processing time needed for a restore to take place. Contact Support.
- **Backup Creation Messages** - These reflect errors detected when starting or triggering a backup.
- **ES Backup (Creation) Inactive** - Indicates that when Elasticsearch was started, the backup store was unavailable. This can be remediated by rebooting the appliance, or (if NFS and the encryption service are now functional) by logging into **tgsh** and running the command service `restart elasticsearch.service`.
- **Backup Maintenance Messages** - These reflect errors detected when checking status of previously created backups.
- **ES Backup (Maintenance) snapshot (...) status FAILED** - This indicates that in the most recent attempt to update the backup of the Elasticsearch database, no indices could be successfully written. Check that the NFS server is functional and has free space; if no issue can be identified and the issue persists, contact customer support.
- **ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE** - Should only occur immediately after an appliance upgrade installing a new version of Elasticsearch; will be displayed until the backup store has been upgraded to be compatible with this new release. Restoring from an incompatible backup may require customer service assistance, should a failure occur while in this state.
- **ES Backup (Maintenance) snapshot (...) status PARTIAL** - Contains one of two messages in the body: No prior successful backups seen, so retaining. (if we're keeping a partial backup as better than

none at all); or Prior successful backups exist, so removing. (if we're discarding that partial backup with the intent to retry later).

- **ES Backup (Maintenance) - Backup required (...) ms** - Occurs if a backup requires more than 60 seconds. This is not necessarily an error: Elasticsearch performs periodic maintenance which can cause significant write load even on idle systems. However, if it takes place consistently when under periods of low load, investigate storage performance or contact customer service for assistance.
- **ES Backup (Maintenance)** - Unable to query Elasticsearch snapshot status - Elasticsearch could not be contacted; and this failure took place after a backup creation was successfully started. Generally, this will occur in conjunction with other appliance failures, and remediation should focus on those issues. If this error is seen when the appliance is otherwise fully functional and does not go away of its own accord, contact customer support.

Appliance Backup

Perform the following steps to perform a backup of the Threat Grid Appliance:

Procedure

Step 1 Create the backup target directory according to the NFS.

Step 2 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Note
If you completed the NFS configuration during the initial appliance setup and you have the encryption key, you can skip step 3 through step 5. Otherwise, you must obtain an encryption key to restore the backup data.

Figure 33: NFS Configuration

Step 3 Enter the following information:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server under which files will be stored.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4. The default is **rw**.
- **FS Encryption Key Hash** - Click **Generate Key** to generate a new encryption key. You will need this key to restore backups later. (At that time, click **Upload** and upload the key required for the backup.)

Step 4 Click **Save**. The page refreshes and a **FS Encryption Password Key ID** is displayed.

The first time you configure this page, options to **Delete** or **Download** the encryption key become visible. The **Upload** option is available if you have NFS enabled but do not have a key created. Once you create a key, the **Upload** button changes to **Download**. (If you delete the key, the **Download** button becomes **Upload** again.)

Note
If the key correctly matches the one used to create a backup, the **Key ID** displayed in Admin UI after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 5 Click **Activate** to activate the key.

Important
The user is responsible for backing up the encryption key and securely storing it; Threat Grid does not retain a copy. Backup cannot be completed without this key.

Step 6 Reset the backup restore target as described in Reset Appliance as Backup Restore Target.

Step 7 Restore the backup data as described in Restore Backup Content, on page 70.

Reset Appliance as Backup Restore Target

Before an appliance can be used as a restore target, it must be in a preconfigured state. Appliances ship in this state. However, getting one back to the preconfigured state once it has been configured requires explicit administrative action.

Caution Performing this process will destroy customer-owned data. Read all of the documentation before performing any tasks, and be very careful before proceeding. .

Note Reset is not the same as the secure wipe that is available in recovery mode; only the recovery-mode secure wipe is appropriate to completely remove customer-owned data from an appliance before shipping it to a DLP reimaging center. However, the secure wipe in recovery mode is not a replacement for this reset: secure wipe renders an appliance unusable until reimaged, while this reset prepares an appliance to restore a backup.

Data Reset

The data reset process was updated in Threat Grid Appliance v2.7 and later and is now more comprehensive. While the Wipe process (in the recovery bootloader menu) is still required for a firm guarantee of the destruction of all customer-related data, the reset process now clears operating system logs and other state which was previously left in place.

A successfully reset Threat Grid Appliance now has a new randomly-generated password displayed on its console (identical to behavior in newly-installed state). This improved process now reboots multiple times, and can be invoked from recovery mode (as opposed to the prior process, which could only be successfully invoked when booted into regular operation).

The Threat Grid Appliance (v2.7 and later) uses XFS as the primary file system, instead of the ZFS file system that was used on older appliances that have not been reset. If a Threat Grid Appliance has its data reset, the datastore will be changed from a ZFS file system to a XFS file system. This improves forward compatibility and provides OS-level support for I/O usage monitoring on a per-service basis.

The data reset process now also requires sufficient storage to contain all content necessary for a fresh install on the system SSDs. Any pre-existing data is only deleted after the presence and validity of this content has been ensured. It is possible that systems that have been in use for an extended period (particularly first-generation hardware), may not have sufficient space immediately available. If this is the case, customer support can assist, if needed.

Returning a Target Appliance to Preconfigured State

If you are not restoring to a system fresh from manufacturing, the restore target appliance must be returned to the preconfigured state by clearing pre-existing data and NFS-related configuration from the system.

Procedure

Step 1 Access the TGSH Dialog via the Threat Grid Appliance TTY, or SSH.

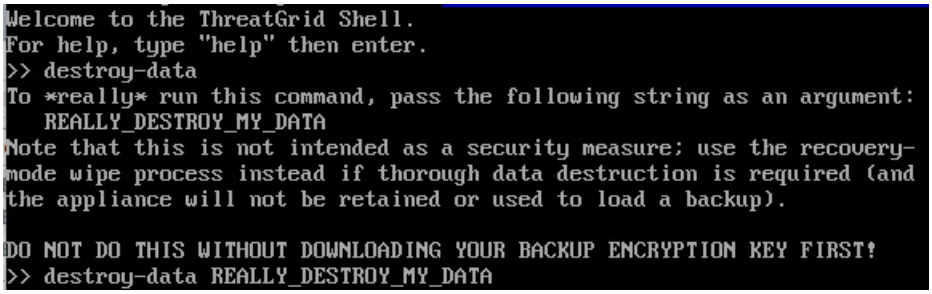
Step 2 Choose the **CONSOLE** option to enter **tgsh**.

Note
Entering **tgsh** via Recovery Mode is not suitable for this use case.

Step 3 At the **tgsh** prompt, enter the command `destroy-data`. Carefully read and follow the instructions provided with the prompt.

Caution
There is no Undo from this command. All data will be destroyed.

Figure 34: The destroy-data REALLY_DESTROY_MY_DATA Command and Argument



The following data is destroyed:

- Samples
- Analysis results, artifacts, flagging
- Application-layer (not the Admin UI) organization and user account data
- Databases (including users and organizations)
- Configuration done within the Face or Mask portal UI
- NFS configuration and credentials
- The local copy of the encryption key used for NFS

Returning Non-Target Appliance to Preconfigured State

If another system or Threat Grid Appliance is actively writing to the backup that is being restored, for example, a test restore of content being written by a second master Threat Grid Appliance actively used in production, return that Threat Grid Appliance to the preconfigured state.

Procedure

Step 1 Generate a consistent, writable copy of the datastore.

Step 2 Point the Threat Grid Appliance that is doing the test restore to the writable copy instead of to the store which is being continuously written.

Once the Threat Grid Appliance is in a preconfigured state, it can function as the target for the backup store as described in Restore Backup Content.

Restore Backup Content



Important

- The system is unavailable for sample submission during the restore process.
- Only one server can be running with data from a given backup store active at a time.
- Backups can only be restored from the Admin UI.
- Set up the same NFS store and encryption key, as previously used, with a process identical to the original process. Setting up a Threat Grid Appliance with a prior NFS store and encryption key will trigger a restore.
- To test the restore process on a different Threat Grid Appliance while the primary Threat Grid Appliance is still operational, make a copy of a consistent snapshot of the backup store and point the new Threat Grid Appliance (with the encryption key uploaded) to it.

Perform the following steps to restore the backup content:

Procedure

Step 1 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Step 2 Click **Upload** to retrieve the backup key previously generated when configuring the server on which the backup was created.

If the key correctly matches the one used to create a backup, the **Key ID** displayed in the Admin UI should match the name of a directory in the configured path. The install wizard checks for a directory matching the backup key, and if it finds one, begins restoring the data to that location.

Note
There is no progress bar. The amount of time required to restore data depends on the size of the backup and other factors. In testing, a 1.2-GB restore is quick, while a 1.2-TB restore required over 16 hours. For large restores it may appear that the install has hung so be patient. The Admin UI will report that the restore has succeeded, and the appliance will start up.

Step 3 Confirm that the restored data looks the same as the original data.

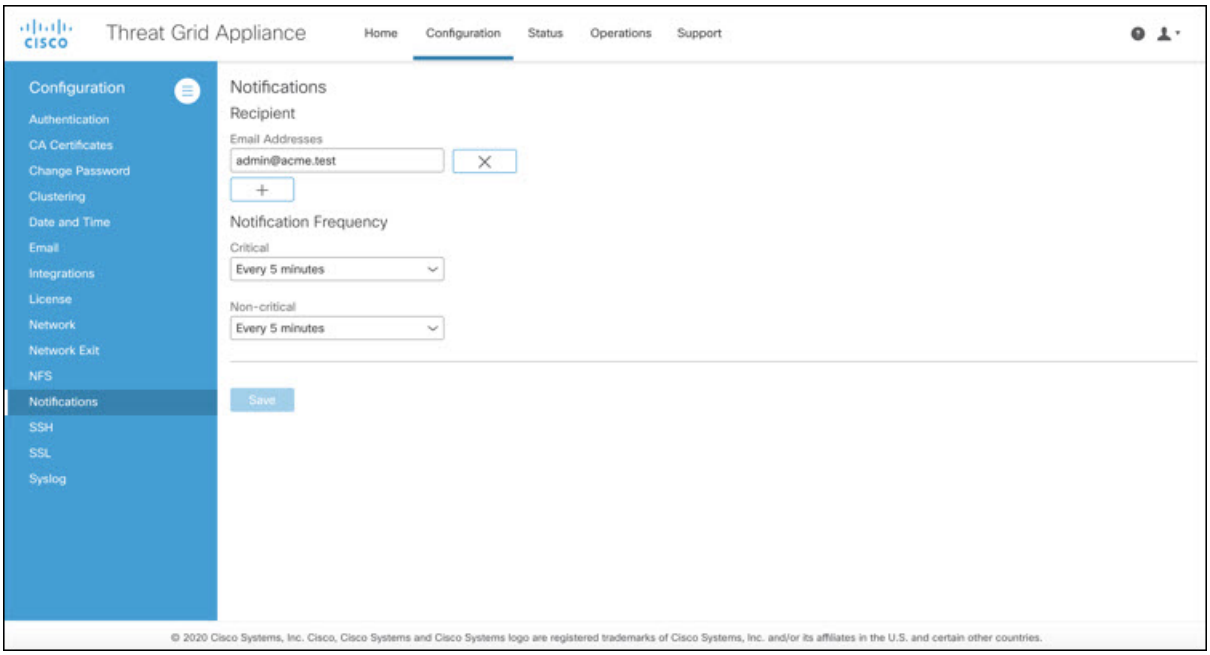
Notifications

When you initially set up the Threat Grid Appliance, you configure the notifications to be received via email. You can add or delete recipients, and change the notification frequency using the **Notifications** page.

Procedure

Step 1 Click the **Configuration** tab and choose **Notifications** to open the **Notifications** page.

Figure 35: Notifications



Step 2 Under **Recipients**, enter the **Email Address** for at least one notifications recipient. If you need to add multiple email addresses, click the + icon to add another field; repeat as needed.

Step 3 Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.

Step 4 Click **Save**.

SSH

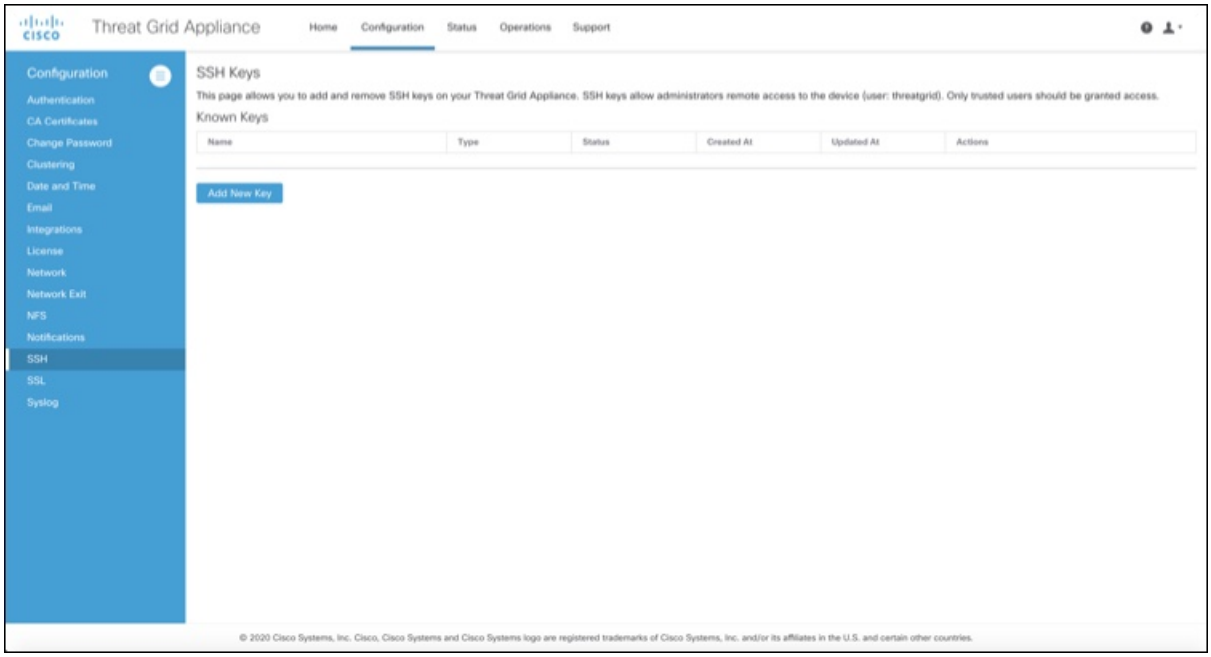
Setting up SSH keys provides the Threat Grid Appliance administrator with access to the TGSH Dialog via SSH (`threatgrid@<host>`); it does not provide root access or a command shell. You can add and remote SSH keys on your appliance using the **SSH Keys** page in the Admin UI.

Note Configuring a SSH public key for access to the Threat Grid Appliances disables password-based authentication via SSH (v2.7.2 and later); this makes SSH authentication methods one or the other, not both. After a successful SSH connection using key-based authentication, the TGSH Dialog prompts for a password, such that both tokens are required.

Procedure

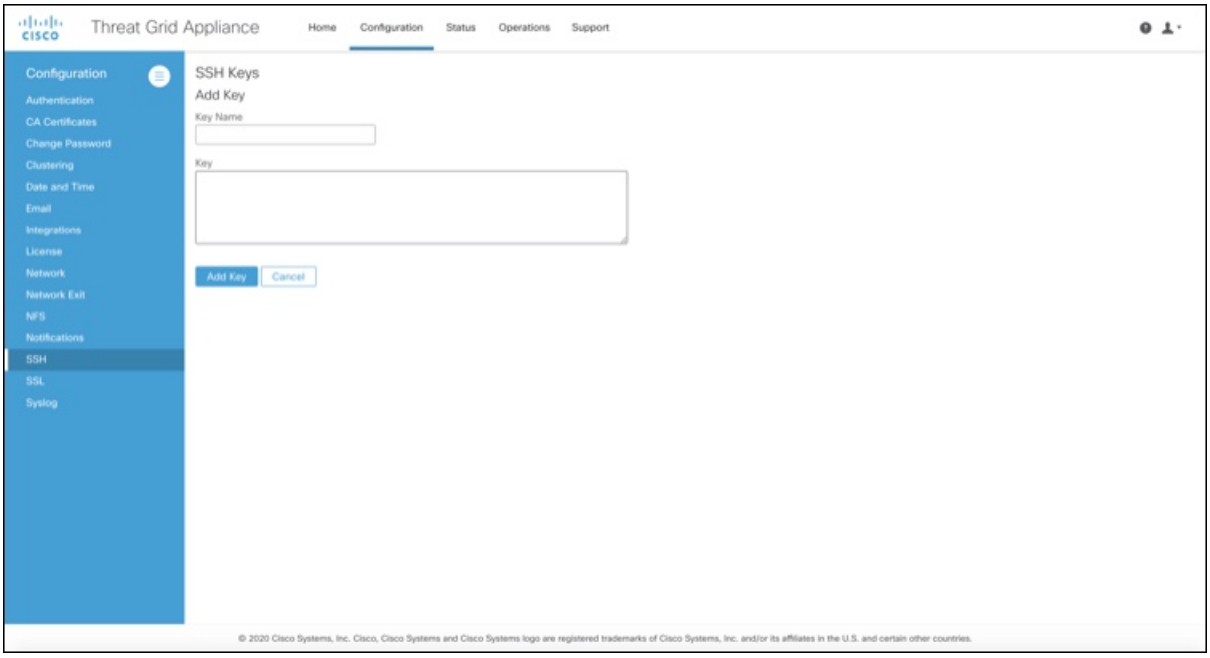
Step 1 Click the **Configuration** tab and choose **SSH** to open the **SSH Keys** page.

Figure 36: SSH Keys



Step 2 Click **Add New Key**.

Figure 37: Add Key



Step 3 Enter the **Key Name** and paste the key into the **Key** field.

Step 4 Click **Add Key**.

SSL

All network traffic passing to and from the Threat Grid Appliance is encrypted using SSL. The following information is provided to assist you through the steps for setting up SSL certificates to support Threat Grid Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), AMP for Endpoints Private Cloud, and other integrations.

Note A full description of how to administer SSL certificates is beyond the scope of this guide.

Interfaces Using SSL

There are two interfaces on the Threat Grid Appliance that use SSL:

- **Clean** interface for the Threat Grid Portal UI and API, and integrations (ESA, WSA, and AMP for Endpoints Private Cloud Disposition Update Service).
- **Admin** interface for the Admin UI.

Supported SSL/TLS Version

The following versions of SSL/TLS are supported on the Threat Grid Appliance:

- TLS v1.0 - Disabled in the Admin interface (v2.7 and later)
- TLS v1.1 - Disabled in the Admin interface (v2.7 and later)
- TLS v1.2



Note TLS v1.0 and TLS v1.1 are disabled in the Admin interface (v2.7 and later), and disabled by default for the main application. If one of these protocols is required for integration compatibility purposes, they can be re-enabled (for the main application only) from tgsh.

Supported Customer-Provided CA Certificates

Customer-provided CA certificates are supported (v2.0.3 and later) to allow customers to import their own trusted certificates or CA certificates.

Self-Signed Default SSL Certificates

The Threat Grid Appliance is shipped with a set of self-signed SSL certificates and keys already installed. One set is for the Clean interface and the other is for the Admin interface. These SSL certificates can be replaced by an administrator.

The default Threat Grid Appliance SSL certificate hostname (Common Name) is the appliance serial number (with an additional subjectAltName field for the IP address), and is valid for 10 years. For releases prior to v2.11, the default SSL certificate hostname is **pandem**.

If a different hostname was assigned to the Threat Grid Appliance during configuration, the hostname and the Common Name in the certificate will no longer match.

The hostname in the certificate must also match the hostname expected by a connecting an ESA or WSA, or other integrating Cisco device or service, as many client applications require SSL certificates where the Common Name used in the certificate matches the hostname of the connecting appliance.

Configuring SSL Certificates

Cisco security products, such as ESA, WSA, and AMP for Endpoints Private Clouds, can connect to a Threat Grid Appliance (inbound connection) and submit samples to it. To accomplish this, the connected appliance or other device must be able to trust the Threat Grid Appliance SSL certificate.

You must first validate that the hostname matches the Common Name; if it doesn't match, you must regenerate or replace it. You then must export the SSL certificate from the Threat Grid Appliance, and then import it into the connected appliance or device.

The certificates used for inbound SSL connections on the Threat Grid Appliance are configured on the **SSL Keys** page. The SSL certificates for the Clean and Admin interfaces can be configured independently.



Note For information about outbound SSL connections so that the Threat Grid Appliance can trust the Cisco AMP for Endpoints Private Cloud, see CA Certificates.

Procedure

Step 1 Click the **Configuration** tab and choose **SSL** to open the **SSL Keys** page.

Figure 38: SSL Keys Page



In this example, there are two SSL certificates: **OpAdmin** for the Admin interface, and **Pandem** for the Clean interface.

Step 2 Confirm that the hostname matches the SAN (Subject Alternative Name) used in the SSL. The hostname must match the SAN used in the SSL certificate on the Threat Grid Appliance. If they do not match, you can regenerate the SSL certificate. See Regenerating SSL Certificates.

Replacing SSL Certificates

SSL certificates usually need to be replaced at some point for various reasons, such as the certificate has expired, the hostname has changed, or to support integrations with other Cisco devices and services.

Cisco ESA, WSA, and other CSA Cisco integrating devices may require an SSL certificate in which the Common Name matches the Threat Grid appliance hostname. You must replace the default SSL certificate with a newly generated certificate that uses the same hostname to access the Threat Grid Appliance.

If integrating a Threat Grid Appliance with an AMP for Endpoints Private Cloud to use its Disposition Update Service, you must install the AMP for Endpoints Private Cloud SSL Certificate so the Threat Grid Appliance can trust the connection.

There are several ways to replace an SSL certificate on a Threat Grid Appliance:

- Regenerating SSL Certificates that uses the current hostname for the SAN.
- Downloading SSL Certificates
- Uploading SSL Certificates; this can be a commercial or enterprise SSL, or one you create using OpenSSL.
- Generating SSL Certificates Using OpenSSL

Regenerating SSL Certificates

You can regenerate a SSL certificate on the **SSL Keys** page if your hostname does not match the SAN in the certificate.

Procedure

Step 1 Click the **Configuration** tab and choose **SSL** to open the **SSL Keys** page.

Step 2 In the **Actions** column, click the (**...**) menu and choose **Regenerate** for the interface that needs a new certificate.

A new self-signed SSL certificate is generated on the Threat Grid Appliance that uses the current hostname of the appliance in the SAN field of the certificate. The regenerated certificate (.cert file) can be downloaded and installed on the integrating appliance.

Downloading SSL Certificate

The Threat Grid generated SSL certificates, but not the keys, can be downloaded. A downloaded certificate can be used when setting up a cluster. It can also be installed on integrating devices so they can trust connections from the Threat Grid appliance. (You will only need to .cert file for this step.)

Procedure

Step 1 Click the **Configuration** tab and choose **SSL** to open the **SSL Keys**page.

Step 2 From **Actions** (**...**) menu, choose **Download** for the appropriate interface. The SSL Certificate is downloaded.

Uploading SSL Certificates

If you already have a commercial or corporate SSL certificate in place for your organization, you can use that to generate a new SSL certificate for the Threat Grid Appliance and use the CA cert on the integrating device.

Procedure

Step 1 Click the **Configuration** tab and choose **SSL** to open the **SSL Keys** page.

Step 2 In the **Actions** column, click the (**...**) menu and choose **Upload** for the appropriate interface. The **Upload SSL Certificate** page opens.

Step 3 Complete the **Certificate** and **Private Keys** fields and then click **Add Certificate**.

Generating SSL Certificates Using OpenSSL

OpenSSL is a standard open-source SSL tool for creating and managing OpenSSL certificates, keys, and other files. You can manually generate a SSL certificate using OpenSSL when there is no SSL certificate infrastructure

already in place on your premises and upload it to the Threat Grid Appliance (as described in Uploading SSL Certificates). .

Note OpenSSL is not a Cisco product, therefore Cisco does not provide technical support for it. It is recommended that you search the Web for additional information on using OpenSSL. Cisco does offer a SSL library, *Cisco SSL*, for generating SSL certificates.

Procedure

Step 1 Run the following command to generate a new self-signed SSL certificate:

Note
The following example still uses the CN (Common Name) instead of the more contemporary SAN (Subject Alternative Name).

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout tgapp.key -nodes -out
tgapp.cert -subj "/C=US/ST=New York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl - OpenSSL

req - Specifies to use X.509 certificate signing request (CSR) management. X.509 is a public key infrastructure standard that SSL and TLS use for key and certificate management. In this example, this parameter is used to create a new X.509 cert.

-x509 - This modifies the req parameter X.509 to make a self-signed certificate instead of generating a certificate signing request.

-days 3650 - This option sets the length of time for which the certificate will be considered valid. In this example, it is set for 10 years.

-newkey rsa:4096 - This specifies to generate a new certificate and a new key at the same time. Because the required key was not previously created, it must be created with the certificate. The **rsa:4096** parameter indicates to make an RSA key that is 4096 bits long.

-keyout - This parameter indicates where OpenSSl should save the generated private key file that is being created.

-nodes - This parameter indicates that OpenSSL should skip the option to secure the certificate with a passphrase. The appliance needs to be able to read the file, without user intervention, when the server starts up. A certificate that is secured with a passphrase requires that the user enter the passphrase every time the server is restarted.

-out - This parameter indicates where OpenSSL should save the certificate that is being created.

-subj: (Example):

- **C=US** - Country
- **ST=New York** - State
- **L=Brooklyn** - Location
- **O=Acme Co** - Owner's name

- **CN=tgapp.acmeco.com** - Enter the Threat Grid Appliance FQDN (Fully Qualified Domain Name). This includes the HOSTNAME of the Threat Grid Appliance (in this example, **tgapp**) and the associated domain name (in this example, **acmeco.com**).

  Important
  You must at least change the Common Name to match the FQDN of the Threat Grid Appliance Clean interface.

Step 2 Once the new SSL certificate is generated, upload the certificate to the Threat Grid Appliance from the **SSL Keys** page (see Uploading SSL Certificates). You must also upload the certificate (**.cert** file only) to the Email Security Appliance or Web Security Appliance, if you are integrated with those devices.

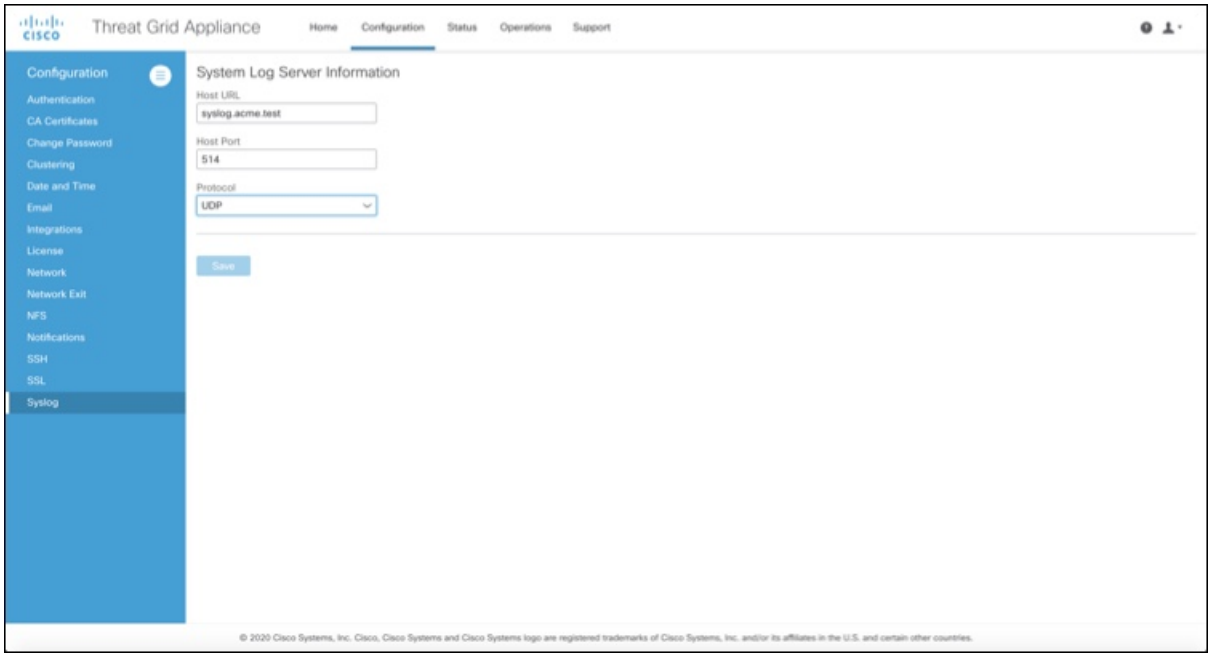
Syslog

The **System Log Server Information** page is used to configure a system log server to receive syslog messages and Thread Grid notifications.

Procedure

Step 1 Click the **Configuration** tab and choose **Syslog** to open the the **System Log Server Information** page.

Figure 39: System Log Server Information

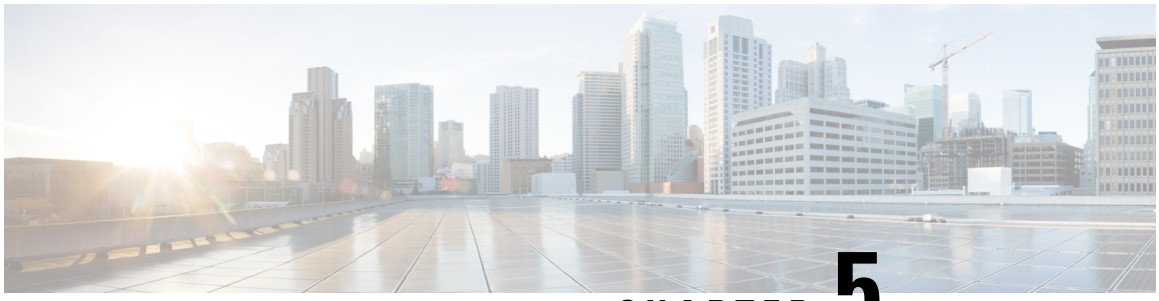


Step 2 Complete the fields on the page:

- **Host URL** - Enter the host name or URL for the system log server.
- **Host Port** - Enter the port number for the server.

- **Protocol** - Choose **TCP** or **UDP** from the drop-down list.

Step 3 Click **Save**.



CHAPTER 5

Status

The **Status** menu in the Admin UI is used by administrators to view system information, such as installed system packages and their version, detailed logs, and available storage.

- About, on page 81
- Backup Details, on page 82
- Logs, on page 83
- Storage, on page 83

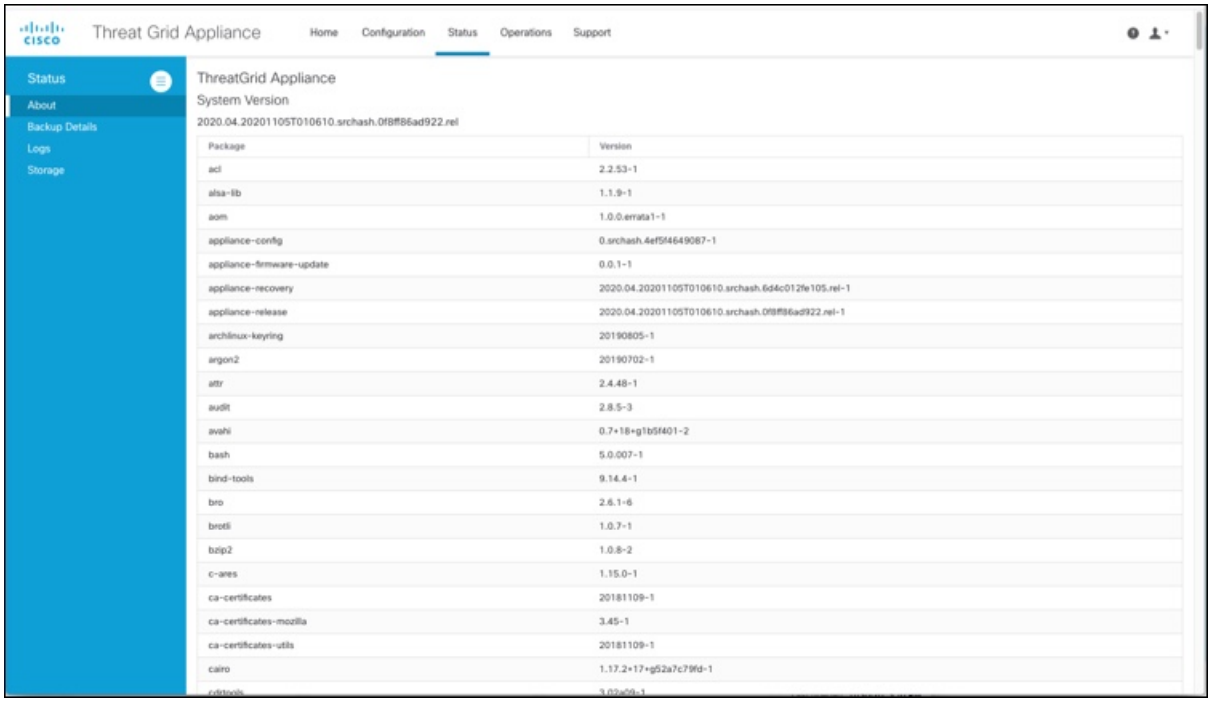
About

You can view the installed packages and their version on the **System Version** page in the Admin UI.

Procedure

Step 1 Click the **Status** tab and choose **About** to open the **System Version** page.

Figure 40: System Version



Step 2 View the packages that are installed and their versions. The release version is shown in the upper portion of the page.

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

Backup Details

You can view detailed backup information on the **Backup Details** page, which displays the most recent time at which complete, non-incremental (where applicable) backups of PostgreSQL, Elasticsearch, and Sand Castle freezer data were successfully completed.

Click the **Status** tab and choose **Backup Details** to open the **Backup Details** page.

Figure 41: Backup Details



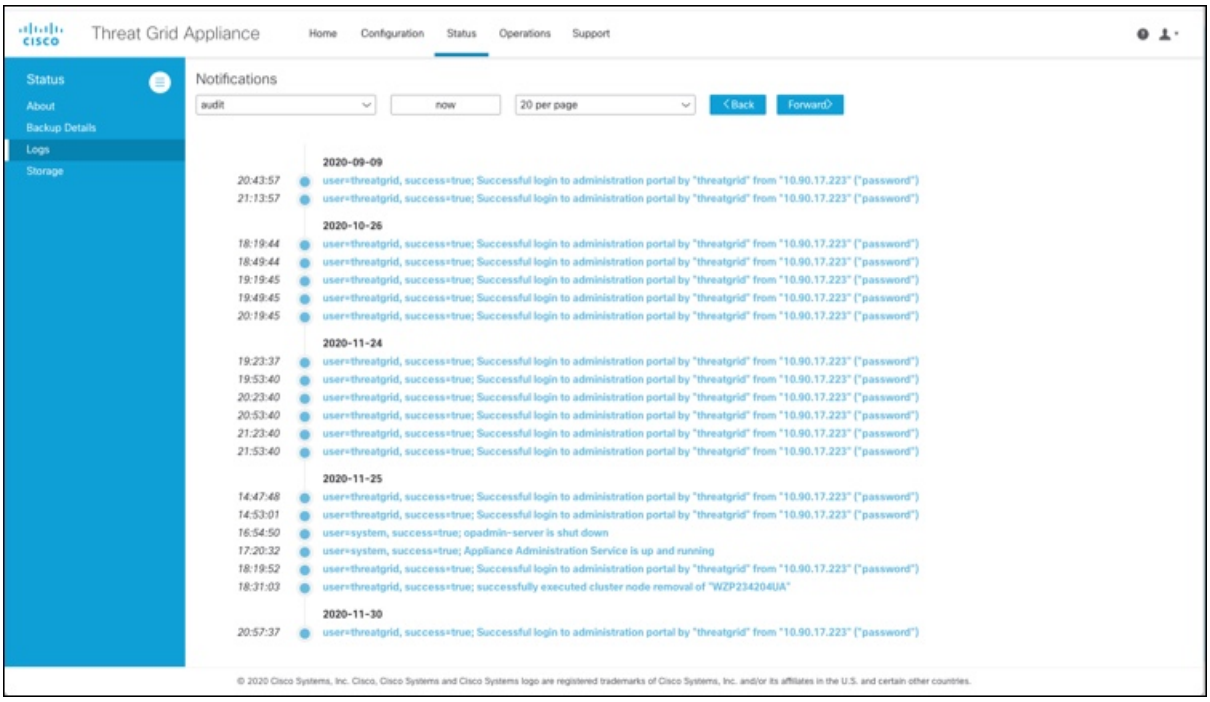
Logs

You can view detailed log information, including historical system logs, on the **Notifications** page.

Procedure

Step 1 Click the **Status** menu and choose **Logs** to open the **Notifications** page.

Figure 42: Notifications



Step 2 Filter the logs that are displayed by choosing the type of notification from the drop-down list, and specify the number of records to be displayed on the page.

Use the **Back** and **Forward** buttons to navigate between pages.

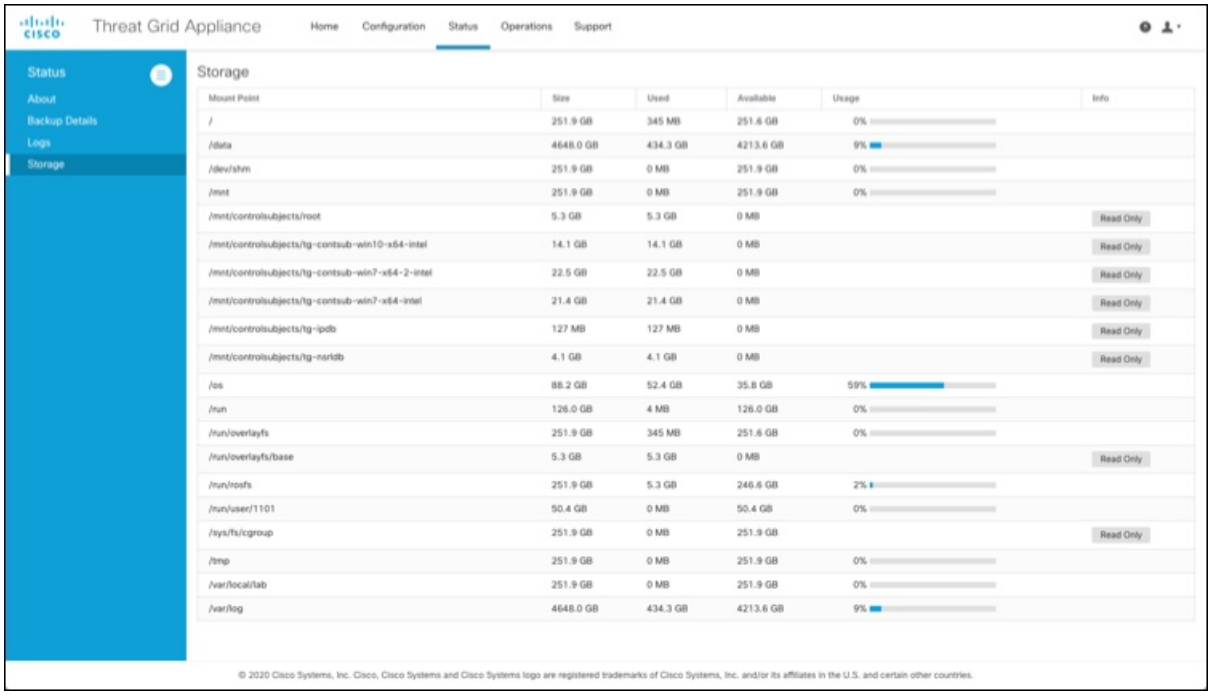
Storage

You can view the available storage on the Threat Grid Appliance from the **Storage** page.

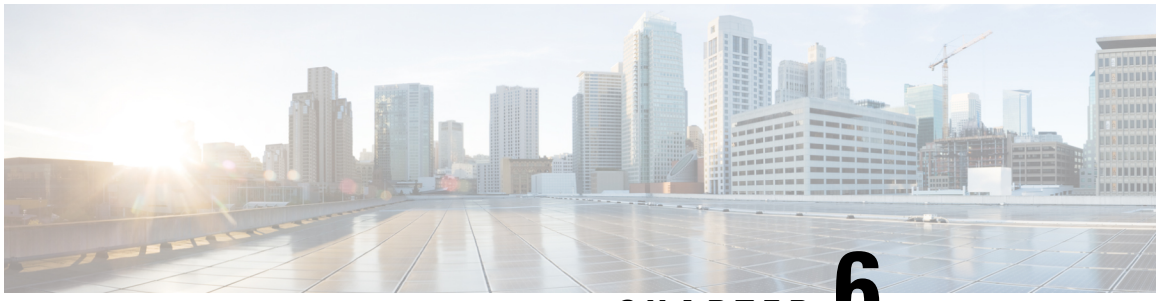
Procedure

Step 1 Click the **Status** tab and choose **Storage**.

Figure 43: Storage



Step 2 View the size of the directories, amount of used storage, and the amount of available storage.



CHAPTER 6

Operations

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

- Activate, on page 85
- Jobs, on page 86
- Power, on page 87
- Update, on page 88

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.

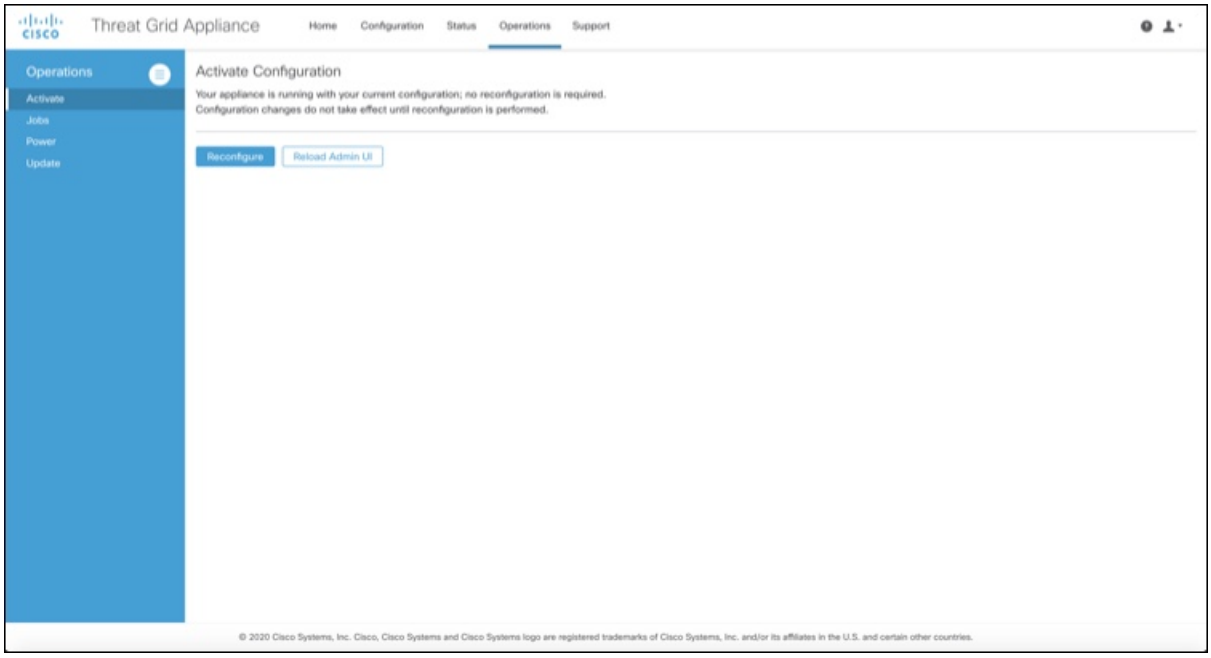
If a reconfiguration is required, a light orange alert message appears in a banner in the upper portion of the page. When you click the **Reconfigure** button on this banner, it takes you to **Activate Configuration** page in the **Operations** menu. From this page, you can apply the configuration changes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

Procedure

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 44: 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**.

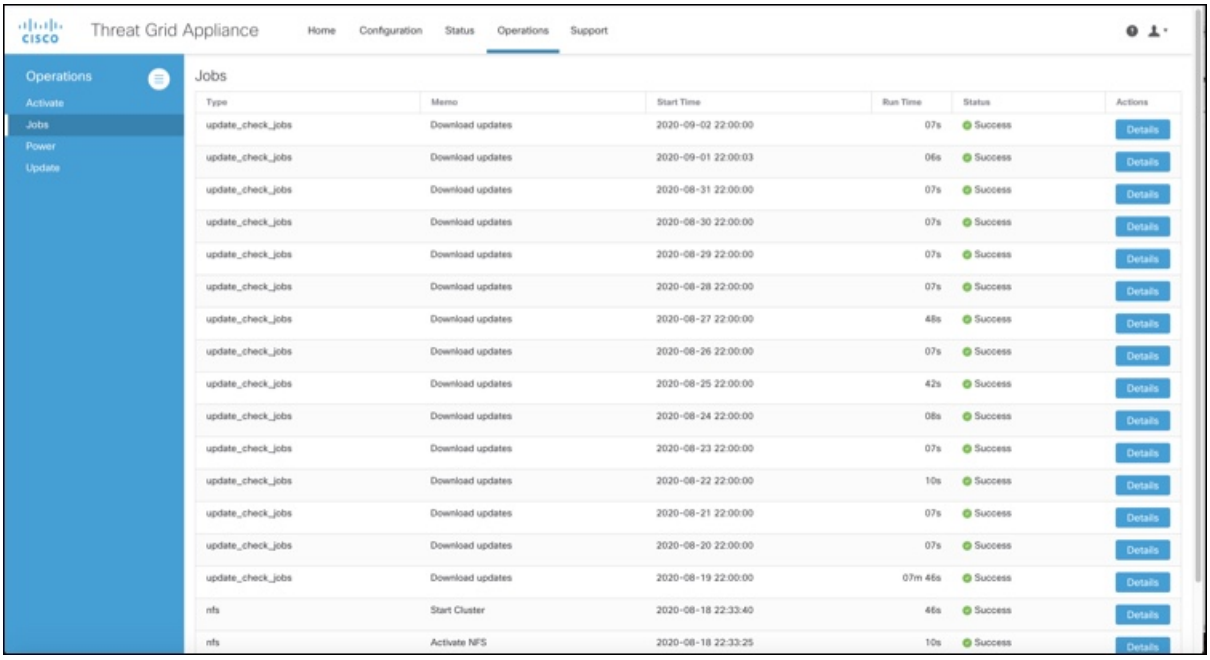
Jobs

You can view the jobs that have been run on the Threat Grid 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.

Procedure

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

Figure 45: 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

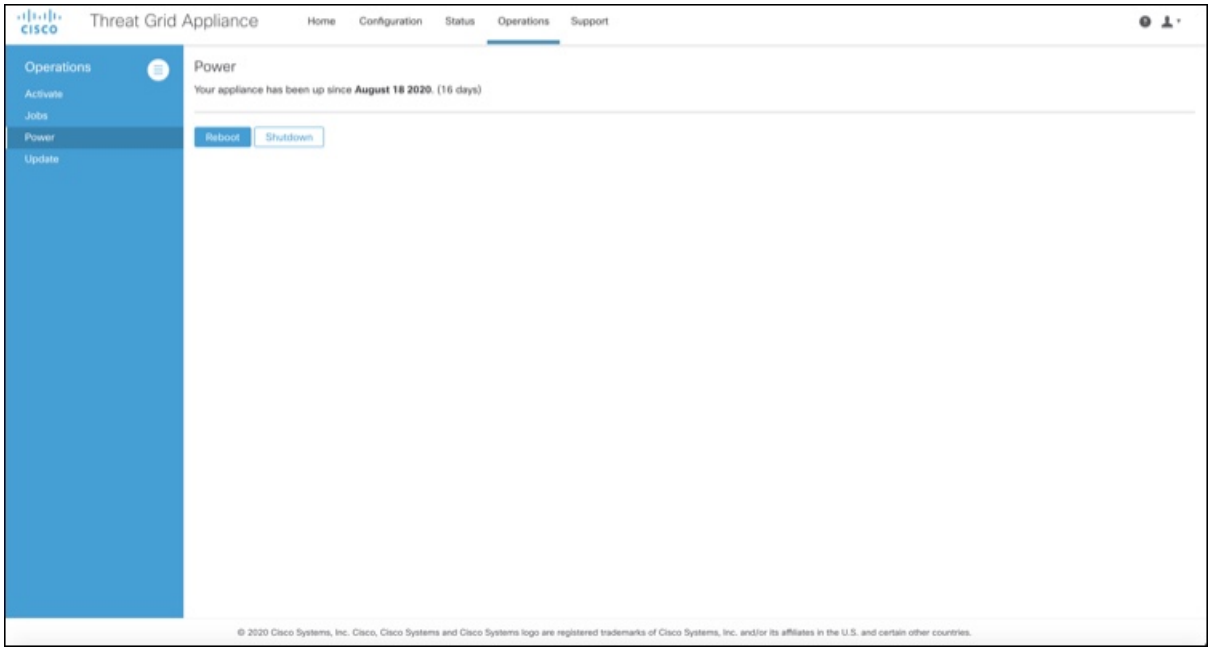
You can reboot or shut down the Threat Grid Appliance from the **Power** page in the Admin UI.

Note The GNU GRUB bootloader is completely removed from the Threat Grid 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.

Procedure

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

Figure 46: 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 Threat Grid Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the *Cisco Threat Grid Appliance Getting Started Guide*.

Note If you have a new Threat Grid 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 Threat Grid Appliance has not been fully configured, including the database.

The 2.12 release adds a new update process which is faster than the previous process and only requires a single reboot. Simply 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:

- Threat Grid 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.
- Users with air-gapped implementations may contact support (see Opening a Support Case) to request a downloadable update boot image.

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, 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.)

Threat Grid 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 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.

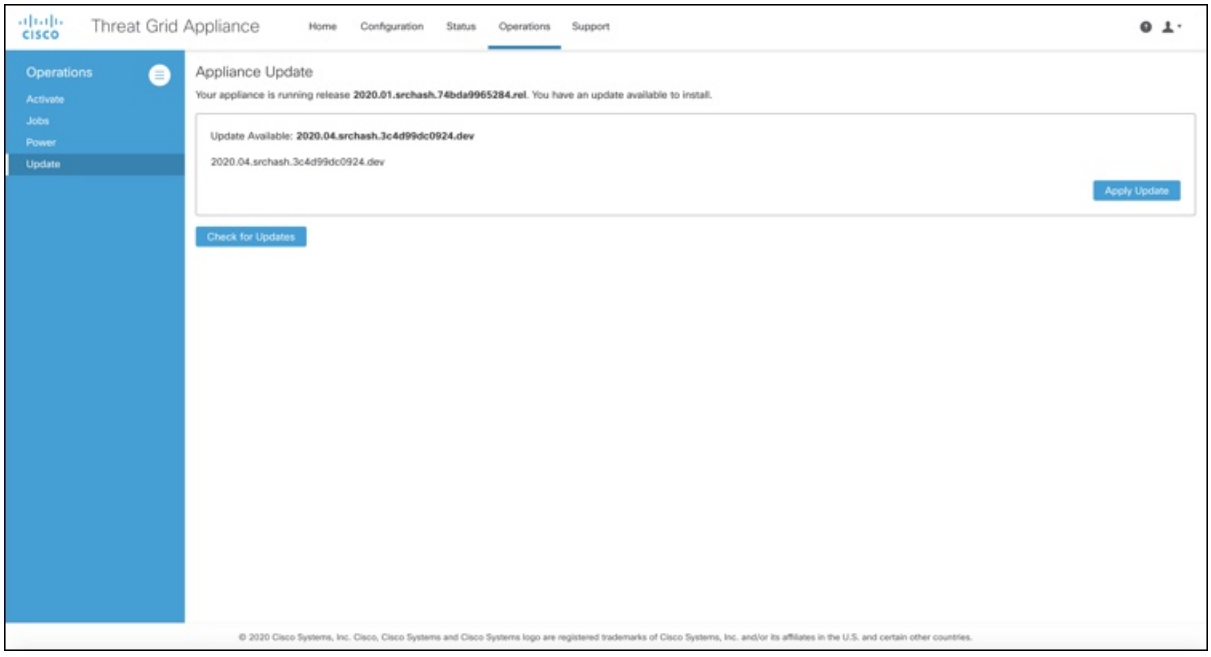
Installing Updates

Perform the following steps to check for updates and to update the Threat Grid Appliance.

Procedure

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

Figure 47: 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 Threat Grid 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 Threat Grid Appliance software, and if so, downloads it. This may take some time.

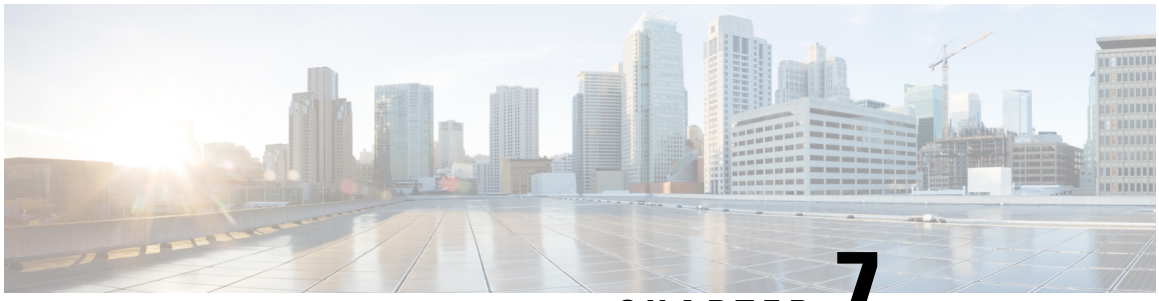
Step 3 Once the update has been downloaded, click **Apply Update** to install it.

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 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 *Cisco Threat Grid Appliance Release Notes v2.0.1* for more information.



CHAPTER 7

Support

This chapter provides instructions for starting a support session and taking support snapshots to aid in resolving issues with the Threat Grid Appliance.

- Opening a Support Case, on page 93
- Live Support Session, on page 95
- Support Snapshots, on page 97

Opening a Support Case

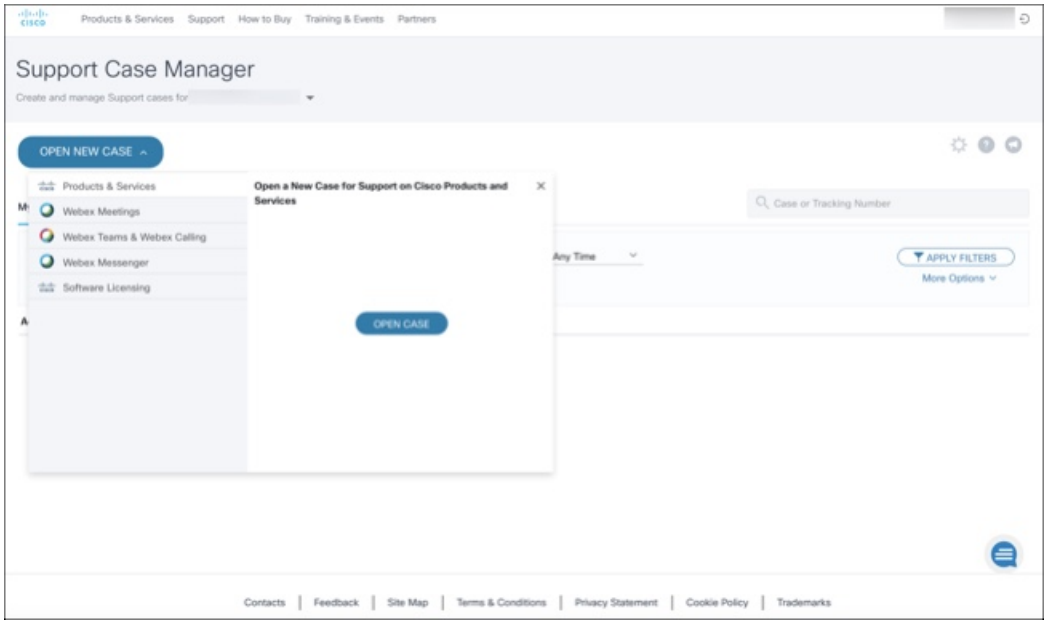
If you have questions or require assistance with Threat Grid, open a case in Support Case Manager, which is located at https://mycase.cloudapps.cisco.com/case.

Note If you are receiving support from a Cisco Threat Grid engineer, they may need remote access to your appliance. See Starting a Live Support Session to learn more about how to start a live support session, and take a snapshot of your appliance.

Procedure

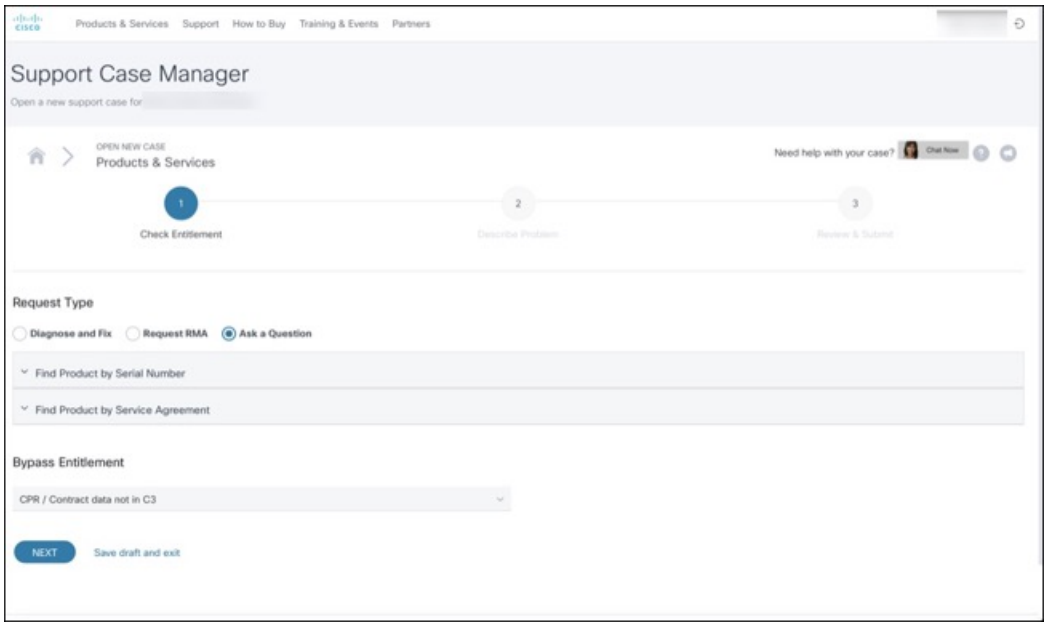
Step 1 In Support Case Manager, click **Open New Case** > **Open Case**.

Figure 48: Open New Case



Step 2 Click the **Ask a Question** radio button and search for your Cisco Security **Product Serial Number** or **Product Service Contract**. This should be the serial number or service contract for Threat Grid.

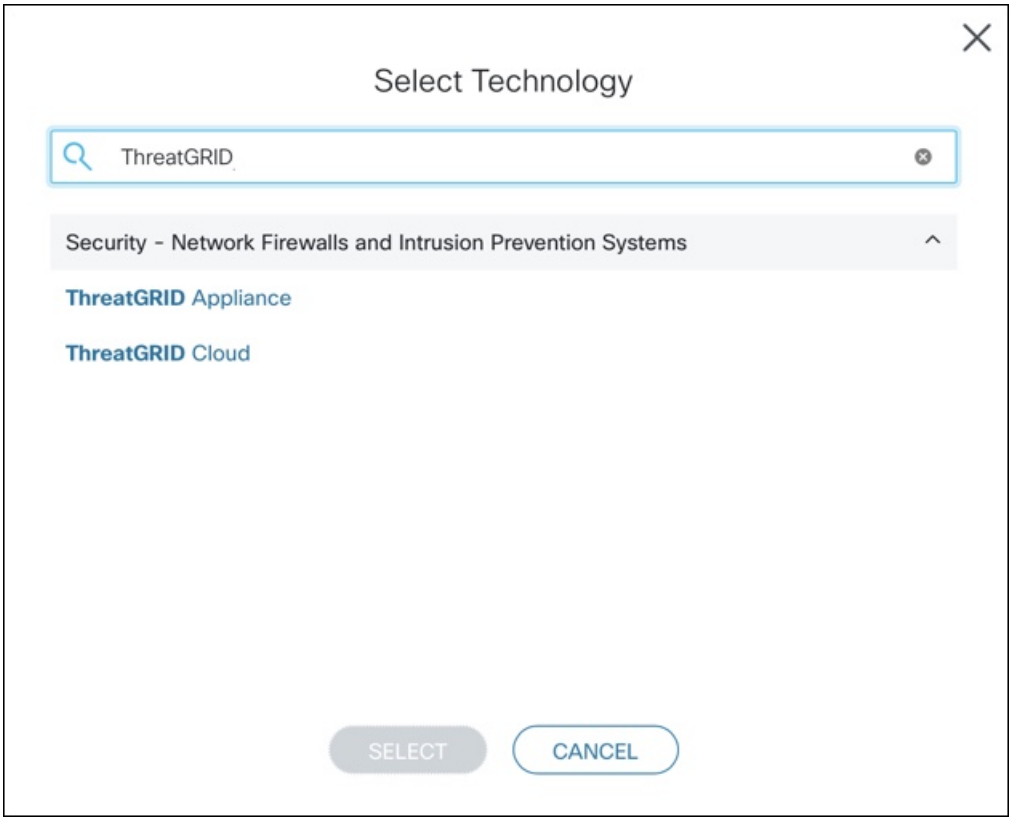
Figure 49: Check Entitlement



Step 3 On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Threat Grid in the title).

Step 4 Click **Manually select a Technology** and search for **ThreatGRID**.

Figure 50: Select Technology



Step 5 Choose **ThreatGRID Appliance** from the list and click **Select**.

Step 6 Complete the remainder of the form and click **Submit**.

If you are unable to open a case online, contact Cisco Support:

- **US and Canada**: 1-800-553-2447
- **Worldwide Contacts**: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

For additional information on how to request support:

- See the blog post: **Changes to the Cisco Threat Grid Support Experience** at https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407
- See the main **Cisco Support & Downloads** page at: https://www.cisco.com/c/en/us/support/index.html

Live Support Session

If you require support from a Threat Grid engineer, they may ask you to start a live support session that gives Threat Grid support engineers remote access to the appliance. Normal operations of the appliance will not be affected. You can start a live support session from the **Live Support Session** page.

Note You can also enable support mode from the TGSH Dialog, and when booting up in Recovery Mode (see Resetting the Administrator Password for instructions).

Support Servers

Establishing a live support session requires that the appliance be able to reach the following servers:

- **support-snapshots.threatgrid.com** - This allows you to directly upload a support snapshot for support, without the need to give Cisco support staff direct access to your appliance or to download the files and then upload/attach it to the support ticket.
- **rash.threatgrid.com** - This support mode allows Cisco support staff to log in and inspect the appliance directly.

Both servers should be allowed by the firewall during an active support session.

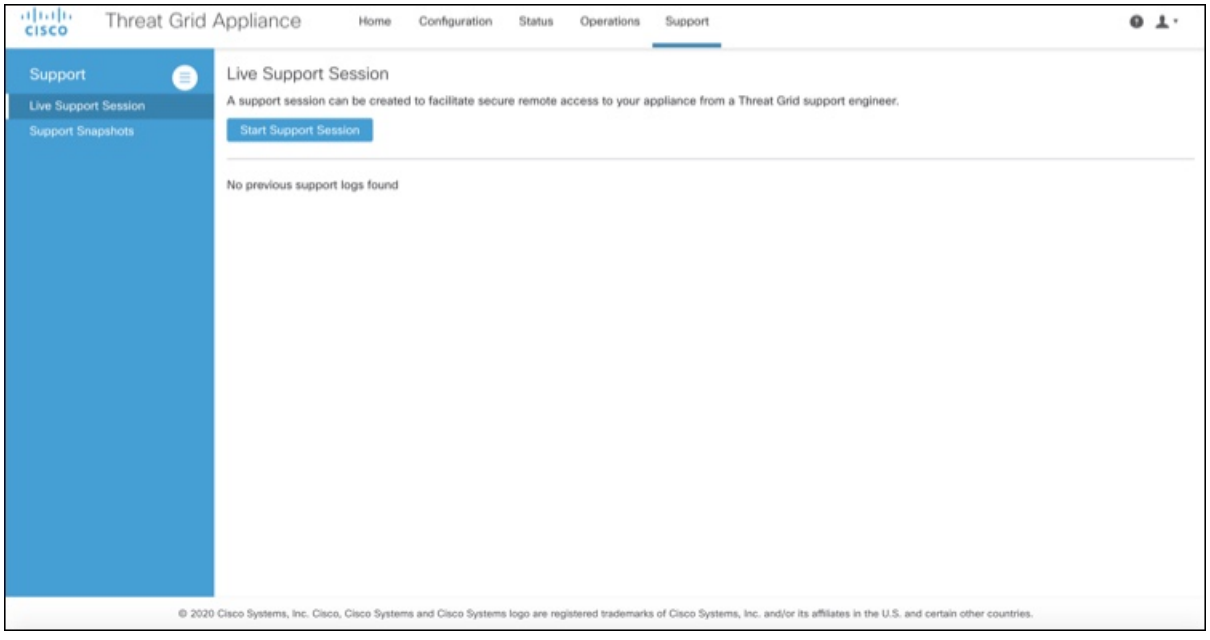
Starting a Live Support Session

You can start a live support session from the **Live Support Session** page.

Procedure

Step 1 Click the **Support** tab and choose **Live Support Session**.

Figure 51: Live Support Session



Step 2 Click **Start Support Session** and follow the prompts.

Step 3 To end the session, click **Terminate Support Session**.

Support Snapshots

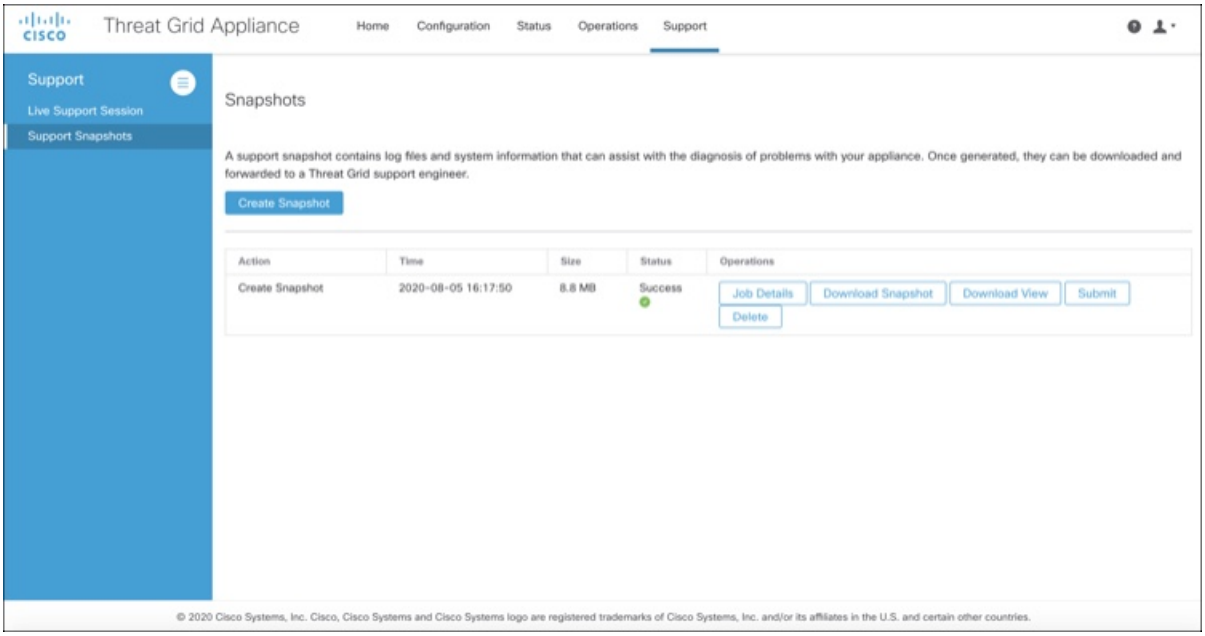
A support snapshot is basically a snapshot of the running system, which contains logs, psoutput, etc., to help Support staff troubleshoot any issues.

Note Snapshots taken before the v2.11 update may no longer have their content available to view or submit.

Procedure

Step 1 To take a snapshot, click the **Support** tab and choose **Support Snapshots**.

Figure 52: Support Snapshots



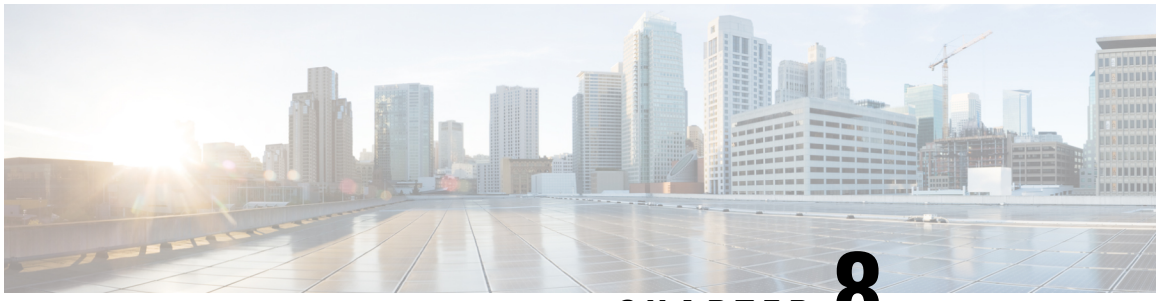
Step 2 Click **Create Snapshot**. The snapshot is taken and added to the page.

Step 3 Once you take the snapshot, you can view job details, download it as a **.tar** file, or click **Submit**, to automatically upload the snapshot to the Threat Grid snapshot server.

To remove a snapshot, click **Delete**.

Use Snapshots to Verify Backups

You can also use snapshots to test and verify that your backups are good. Take a snapshot of the backup store in your Production appliance or cluster, creating a new writable volume off of it, and then try to restore a non-production appliance or cluster from that snapshot.



CHAPTER 8

Organizations and Users

Threat Grid is installed on the Threat Grid Appliance with a default organization and Admin user. Once the set up and the network configuration is completed, you can create additional organization and user accounts, so users can log in and begin submitting malware samples for analysis.

Adding organizations, users, and administrators may require planning and coordination among multiple users and teams, depending on your organization. This chapter describes how to manage organizations and users in Threat Grid and includes the following topics:

- Creating a New Organization, on page 99
- Managing Users, on page 100
- Removing Organizations and Users, on page 101
- Activating a New Device User Account, on page 101

Creating a New Organization

Users are always affiliated with an organization; before you can add users, you must first create the organization so you can add them to it. You must be logged in as an Admin to create a new organization, which is performed on the **Managing Organizations** page in the Threat Grid portal UI.



Important You cannot delete an organization from this interface once it has been created so plan this task carefully.

Procedure

Step 1 Log into the Threat Grid portal as Admin.

Step 2 Click the **Administration** tab and choose **Manage Organization**. The **Organizations** page opens and shows all the organizations on the appliance.

Step 3 Click **New Organization** in the upper-right corner of the page to open the **New Organization** dialog.

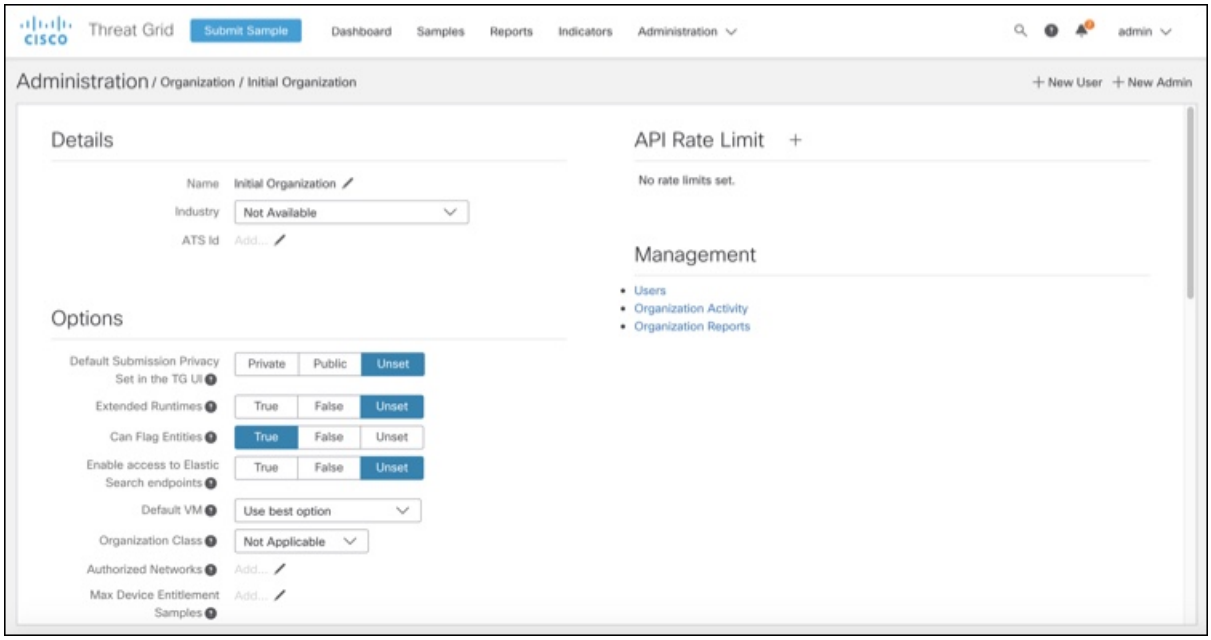
Step 4 Complete the following information:

- **Name** - Add a name for the organization (there is currently no size limit to the name).

- **Industry** - Choose the type of business from the **Industry** drop-down list. If none of the industries on the list are applicable, then leave it set to **Unknown**, and contact Threat Grid Opening a Support Case to request that an option be added.
- **ATS Id** - Enter the Advanced Threat Services ID.

Step 5 Click **Submit**. The new organization is created and is now visible in the list of Organizations.

Figure 53: Organization Page for the Default Initial Organization



Step 6 Edit the newly created organization and complete the following information:

- **Options** - Complete as appropriate.
- **Rate Limit** - Set the default user submission rate limit.

  The API rate limit is global for the Threat Grid Appliance under the terms of the license agreement. This affects API submissions only, not manual sample submissions. The rate limit in the license applies to the organization.

  You can also set sample submission rates on individual users, as documented in the Threat Grid portal online Help.

  Rate limits are based on a 24-hour window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error and a message about how long to wait before retrying.

Once the organization is created, the Admin or Organization Admin can manage it.

Managing Users

For instructions and documentation on creating and managing user accounts, including how to add users, see the Threat Grid Portal UI online help:

In the navigation bar, click **Help > Using Threat Grid Online Help > Managing Threat Grid Users**.



Note Users can only be removed via the API, and only if they have not submitted samples.

Managing device user accounts for integrating Email Security Appliances, Web Security Appliances, and other devices is described in Activating a New Device User Account.

Removing Organizations and Users

Organizations and users can be removed by an admin user with the Threat Grid API. An organization can only be removed if it has no users; if it has users, you must delete them before removing the organization. However, users can only be deleted if they have not submitted any samples.

- To remove an organization, use the Threat Grid API: /api/v3/organizations/:org-id and DELETE.
- To remove a user, use the Threat Grid API: /api/v3/users/:user-id and DELETE.

See the Threat Grid portal online help for API endpoint details.

Activating a New Device User Account

When the Cisco Email Security Appliance, Web Security Appliance, or other Cisco Sandbox API integration connects and registers itself with a Threat Grid Appliance, a new Threat Grid user account is automatically created. The initial status of the user account is de-activated. The device user account must be manually activated by a Threat Grid Appliance administrator before it can be used for submitting malware samples for analysis.

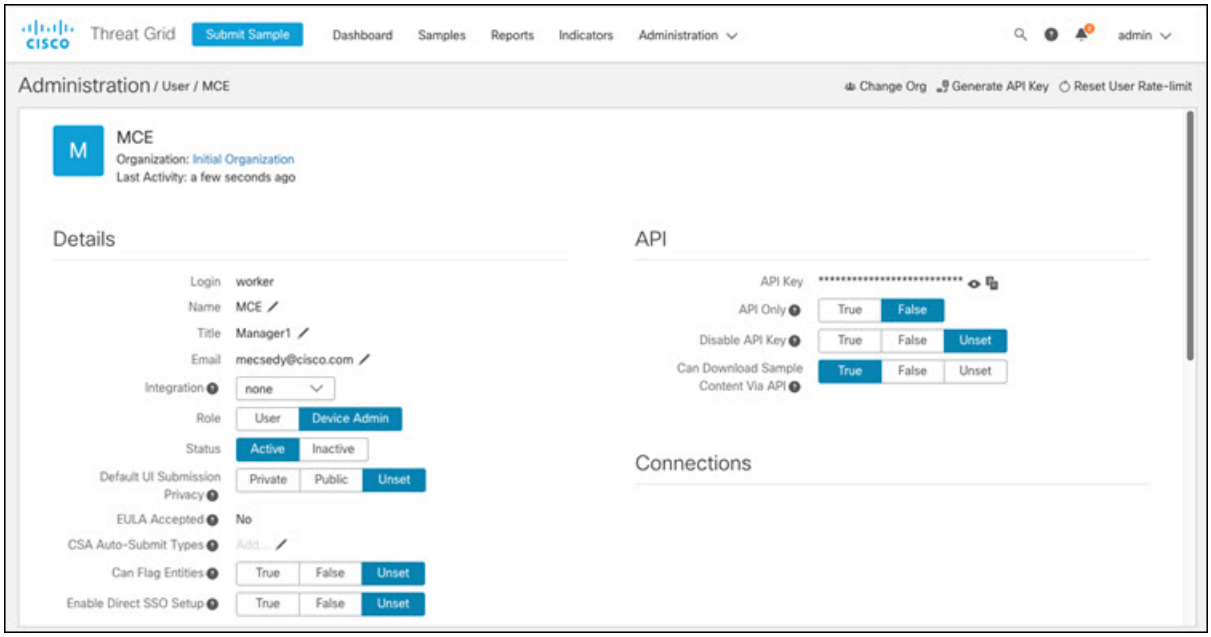
Procedure

Step 1 Log into the Threat Grid Portal UI as Admin.

Step 2 Click the **Administration** tab and choose **Manage Users**.

Step 3 Locate the device user account and open the **User Details** page.

Figure 54: User Details

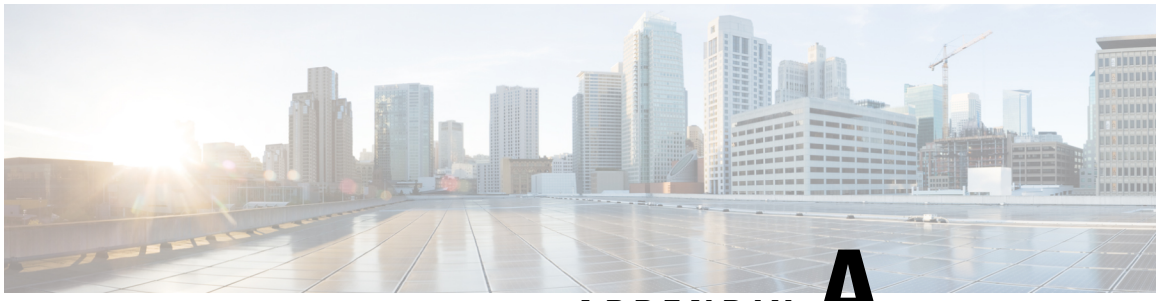


The user status is currently **Inactive**.

Step 4 Click **Activate**.

Step 5 On the confirmation dialog, confirm the action.

The integrating appliance or device can now communicate with the Threat Grid Appliance.



APPENDIX A

Inbound and Outbound Connections

You can set up Threat Grid Appliance to communicate with other Cisco appliances, devices, and services using inbound and outbound connections. Encrypted SSL connections allow other appliances (such as Email Security Appliance and Web Security Appliance) to submit possible malware samples to Threat Grid for analysis (inbound connections).

In addition, Threat Grid Appliance can be set up to communicate with AMP for Endpoints Private Cloud for the Disposition Update Service through an outbound connection.

This appendix provides instructions for setting up both inbound and outbound connections.

- Connecting ESA or WSA to Threat Grid Appliance, on page 103
- Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance, on page 105

Connecting ESA or WSA to Threat Grid Appliance

Connections between the Threat Grid Appliance and Cisco Email Security Appliances (ESA) or Web Security Appliances (WSA) are enabled by the Cisco Sandbox API (CSA API) and are often referred to as CSA Integrations. The ESA/WSA must be registered with the Threat Grid Appliance before it can submit samples for analysis.

Before the ESA/WSA can be registered with the Threat Grid Appliance, the ESA/WSA administrator must first set up the SSL certificate connection as appropriate for their appliance and their network environment.

ESA/WSA Documentation

See the instructions for Enabling and Configuring File Reputation and Analysis Services in the ESA/WSA product documentation:

- *Cisco Email Security Appliance User Guides*
- *Cisco Web Security Appliance User Guides*



Note The Threat Grid Appliance is often referred to as an analysis service, or private cloud file analysis server in these guides.

Inbound Connection Overview

When setting up an inbound connection, the following tasks must be performed:

- **Set Up SSL Certificate** - The Threat Grid Appliance SSL certificate SAN (Subject Alternative Name), or the CN (Common Name) needs to match the hostname and the ESA/WSA expectations; for a successful connection with an integrating ESA/WSA, this must be the same hostname by which the integrating ESA/WSA identifies the Threat Grid Appliance.

  Depending on your requirements, you may need to regenerate the self-signed SSL certificate on the Threat Grid Appliance so it uses the current hostname in the SAN/CN field, then download it to your working environment and upload and install it onto the integrating ESA/WSA.

  Alternatively, you may need to replace the current Threat Grid Appliance SSL certificate by uploading an enterprise or commercial SSL certificate (or a manually generated certificate). For detailed instructions, see Configuring SSL Certificates.

- **Verify Connectivity** - Once the SSL certificate setup is complete, the next step is to verify that the ESA/WSA can communicate with the Threat Grid Appliance. The ESA/WSA must be able to connect to the Clean interface of the Threat Grid Appliance over your network. Follow the instructions in the product documentation to verify that the Threat Grid Appliance and ESA/WSA can communicate with each other (see Connecting ESA or WSA to Threat Grid Appliance).

- **Complete the ESA/WSA File Analysis Configuration** - Enable the **File Analysis Security** service and configure the advanced settings.

- **Register ESA/WSA with Threat Grid Appliance** - An ESA/WSA that is configured according to the product documentation, registers itself automatically with the Threat Grid Appliance. Upon registration of the connecting device, a new Threat Grid user is automatically created with the Device ID as the login ID, and a new organization is created with a name based on the same ID. An administrator must activate the new Device user account.

- **Activate the New ESA/WSA Account on the Threat Grid Appliance** - When the ESA/WSA or other integration connects and registers itself with the Threat Grid Appliance, a new Threat Grid user account is automatically created. The initial status of the user account is de-activated. A Threat Grid Appliance administrator must manually activate the device user account before it can be used for submitting malware samples for analysis.

Configuring Inbound Connection

The connection between the ESA/WSA is incoming from the perspective of the Threat Grid Appliance, and uses the CSA API.

Note Refer to the ESA and WSA product documentation for more information about the tasks that must be performed.

Procedure

Step 1 Set up and configure the Threat Grid Appliance as normal (no integration yet).

Step 2 Check for updates and install, if necessary.

Step 3 Set up and configure the ESA/WSA as normal (no integration yet).

Step 4 The Threat Grid Appliance SSL certificate SAN or CN must match its current Hostname and ESA/WSA Expectations. If you are deploying a self-signed SSL certificate, generate a new SSL certificate (on the Threat Grid Application Clean interface), to replace the default if needed, and download it to install on the ESA/WSA (see Replacing SSL Certificates).

Note
Be sure to generate a certificate that has the hostname of your Threat Grid Appliance as the SAN or CN (the default certificate from the Threat Grid Appliance will not work). Use the hostname; not the IP address.

Step 5 Verify that the ESA/WSA can connect to the Clean interface of the Threat Grid Appliance over your network.

Step 6 Configure the ESA/WSA for Threat Grid Appliance integration. See the ESA/WSA product documentation for complete instructions.

Step 7 Submit and commit your changes.

Registration of your ESA/WSA with the Threat Grid Appliance occurs automatically when you submit the configuration for File Analysis.

Step 8 Activate the new device user account on the Threat Grid Appliance:

a) Log into the Threat Grid Portal UI as Admin.
b) Click the **Administration** tab and choose **Manage Users** to open the **Users** page.
c) Click the user name to open the **User Details** page for the device user account (you may need to use Search to find it).
d) The user status is currently **Inactive**. Click **Active** to activate th enew account.
e) On the confirmation dialog, confirm the action.

The ESA/WSA can now initiate connections with the Threat Grid Appliance.

Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance

The Threat Grid Appliance supports integration with AMP for Endpoints Private Cloud for the Disposition Update Service as an outbound connection.



Note The Threat Grid Appliance Disposition Update Service and AMP for Endpoints Private Cloud integration setup tasks must be performed on the devices in the specified order, particularly if you are setting up new appliances. If you are integrating appliances that are already set up and configured, the order is not as critical.

Refer to the AMP for Endpoints Private Cloud documentation for more detailed information on the tasks that must be performed.

Procedure

Step 1 Set up and configure the Threat Grid Appliance as normal (no integration yet). Check for updates and install, if necessary.

Step 2 Set up and configure the AMP for Endpoints Private Cloud as normal (no integration yet).

Step 3 In the Threat Grid Appliance Admin UI, click the **Configuration** tab and choose **SSL**.

Step 4 Regenerate the SSL certificate on the Clean interface to replace the default certificate, if needed, and make a copy of it to install on the AMP for Endpoints Private Cloud device (see Regenerating SSL Certificates for more information).

Step 5 Obtain the following information, which is needed to configure the integration in AMP for Endpoints Private Cloud device:

- **Hostname** - Click **Configuration** > **Hostname** and note the hostname.
- **API Key** - Copy the **API Key** from the **User Details** page in the Threat Grid portal (click the **Administration** tab and choose **Manage Users**, and then navigate to the integration user account to locate the API key on the **User Details** page).

  Note
  This does not need to be the Admin user; it can be a user that was specifically created for this purpose on the Threat Grid Appliance.

Step 6 Configure the AMP for Endpoints Private Cloud device for Threat Grid Appliance integration. See the ESA/WSA product documentation for complete instructions. The configuration will allow AMP to talk to the Threat Grid Appliance; you can now submit samples to Threat Grid.

Step 7 Complete the remaining steps to set up the Disposition Update Service to communicate disposition results to the Threat Grid Appliance (for more information, see the user documentation for AMP for Endpoints Private Cloud):

a) Configure DNS, if needed. See Configuring DNS.
b) Download or copy and paste the AMP for Endpoints Private Cloud SSL certificate to the Threat Grid Appliance so it can trust the integrating device. See CA Certificates.
c) In the Threat Grid portal UI, specify the AMP Disposition Update Service URL and credentials and click **Add** (see Managing Disposition Update Syndication Services).

Managing Disposition Update Syndication Services

You can manage the Disposition Update Syndication Service for AMP for Endpoints Private Cloud appliance integrations in the Threat Grid portal. URLs can be added, edited, and deleted from the **Disposition Update Syndication Service** page.

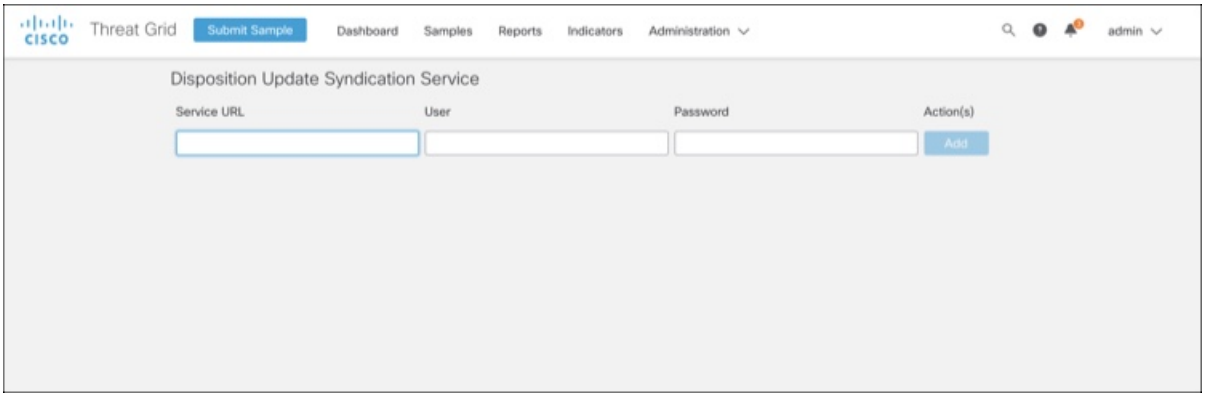


Note For more information about AMP for Endpoints Private Cloud appliance integrations, see Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance.

Procedure

Step 1 In the Threat Grid portal, click the **Administration** tab and choose **Manage AMP Private Cloud Integration** to open the **Disposition Update Syndication Service** page.

Figure 55: Disposition Update Syndication Service

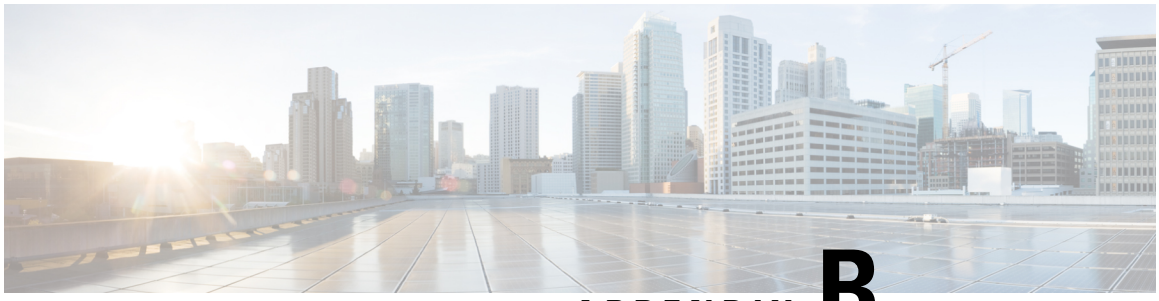


Step 2 Enter the following information:

- **Service URL** - The AMP for Endpoints Private Cloud URL.
- **User** - The admin user name.
- **Password** - The password provided by the AMP for Endpoints configuration portal.

Step 3 Click **Add**.

Inbound and Outbound Connections



APPENDIX B

Removing All Data with the Wipe Appliance Operation

This appendix describes how to use the Wipe Appliance operation to remove all data from the Threat Grid Appliance. It includes the following topics:

- About Wipe Appliance, on page 109
- Wipe Appliance Procedure, on page 109
- Wipe Appliance and Clusters, on page 110

About Wipe Appliance

The Wipe Appliance boot option enables you to wipe the disks on a Threat Grid Appliance to remove all data prior to decommissioning or returning it to the Cisco Demo Loan Program.

Note The Wipe Appliance boot option should not be confused with Data Reset, which prepares an appliance to restore a backup by clearing operating system logs and other state with the `destroy-data` command.

Important After performing the wipe appliance procedure, the Threat Grid Appliance will no longer operate without being returned to Cisco for reimaging.

Wipe Appliance Procedure

This operation is only available in recover-mode tgsh, not tgsh as started from TGSH Dialog. Perform the following steps to wipe all data from the appliance:

Procedure

Step 1 Reboot the appliance (click the **Operations** tab, choose **Power**, and then click the **Reboot** button).

Step 2 Press **F6** at the BIOS window for a list of possible boot targets, and choose **Recovery**.

The Threat Grid Shell opens in Recovery Mode. (See Figure 6 in Resetting the Administrator Password)

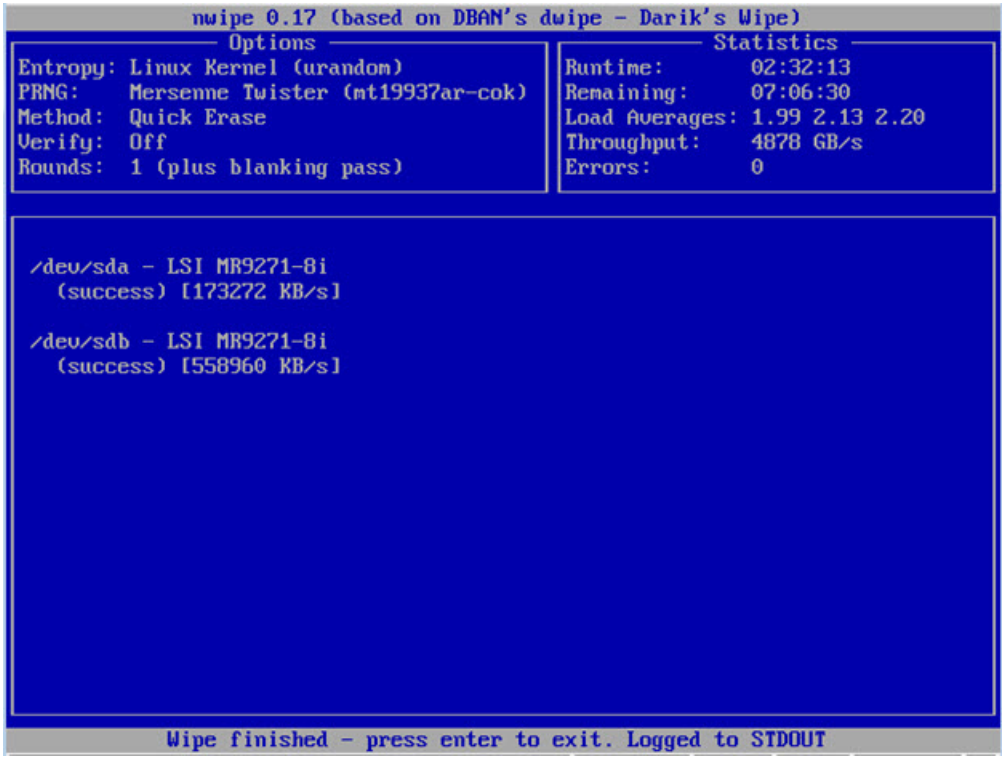
Step 3 Run one of the following commands in recovery-mode tgsh. These vary only in performance and (theoretically) level of security (although with modern drives, even the fast mechanism is likely to provide very good security).

- service start wipe-fast
- service start wipe-random
- service start wipe-3pass

Immediately after running any of these commands, the Wipe process will start.

The **Wipe Finished** window is displayed when the wipe operation is complete.

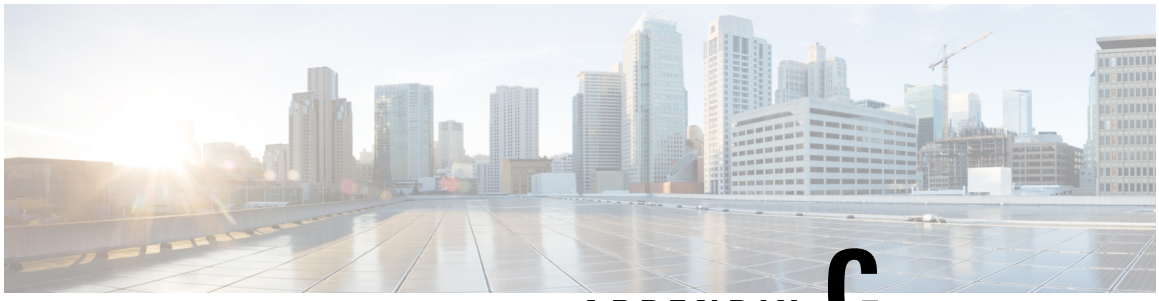
Figure 56: Wipe Finished



Step 4 Press **Enter** to exit.

Wipe Appliance and Clusters

After performing a wipe operation, the Threat Grid Appliance will no longer operate unless it is returned to Cisco for reimaging. Wipe should only be used on a cluster node after that node has been flagged in the Admin UI as permanently removed.



APPENDIX C

CIMC Configuration

The Ciisco Integrated Management Controller (CIMC) Configuration is the user interface used to manage the server. This appendix includes the following information about using the CIMC Utility to set up remote server management:

- Using CIMC Configuration Utility, on page 111

Using CIMC Configuration Utility

After booting the server, the Cisco screen is displayed, which allows you to enter the Cisco Integrated Management Controller (CIMC) Configuration Utility. The CIMC interface can be used for remote server management.

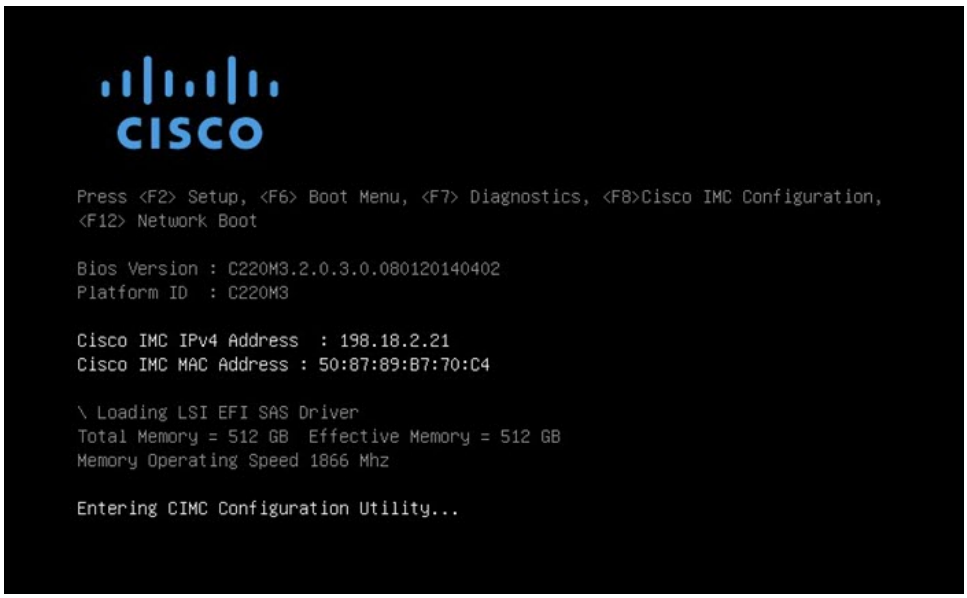
A monitor and keyboard must be attached directly to the Threat Grid Appliance to use this utility.

Note CIMC is not supported on Threat Grid M5 Appliance servers.

Procedure

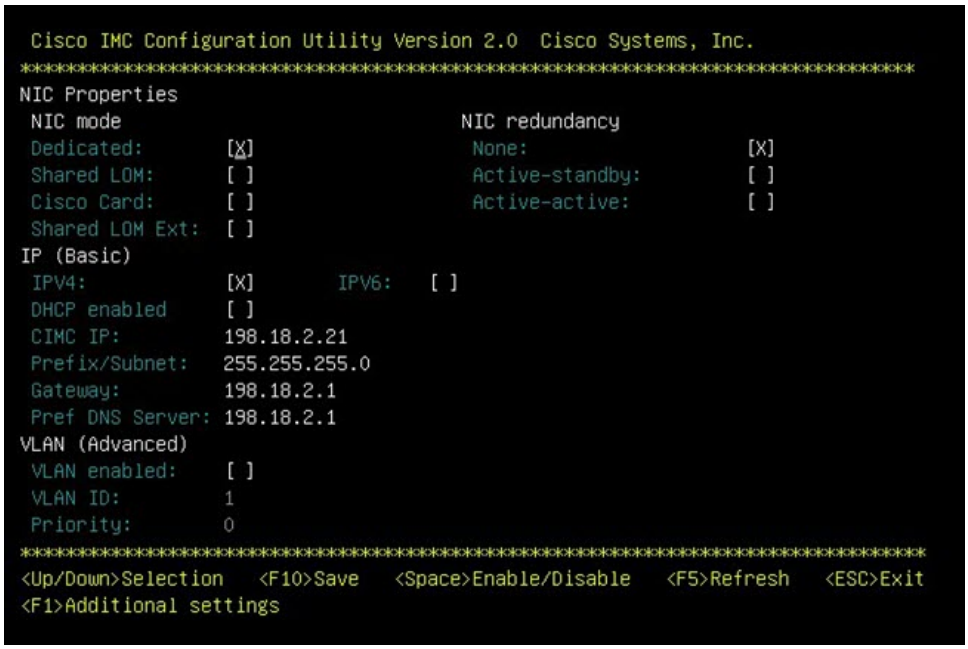
Step 1 Power on the server.

Figure 57: Cisco Screen



Step 2 After the memory check is completed, press **F8** to enter the CIMC Configuration Utility.

Figure 58: CIMC Configuration Utility



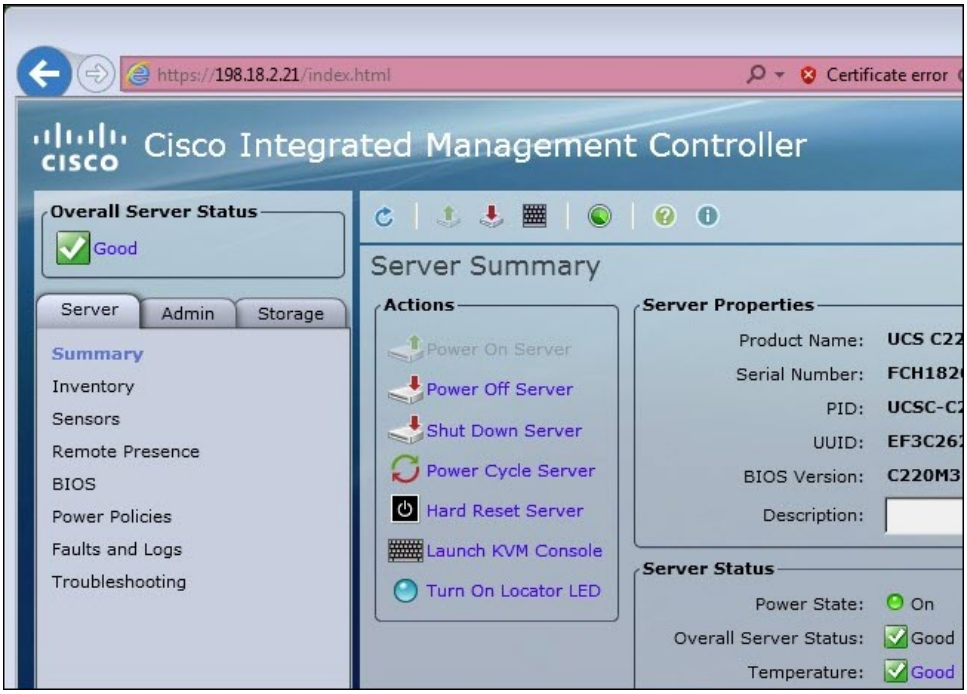
Step 3 In the CIMC configuration utility, set up an IP address that can be used for remote server management.

Step 4 Save the configuration and exit the utility.

Step 5 In a web browser, enter **https://<CIMC-IP address>/** to open the CIMC interface.

Step 6 Enter the initial **User Name** (admin) and **Password** (password).

Figure 59: Cisco Integrated Management Controller (CIMC) Interface



The CIMC interface can now be used to view the server health and open a KVM to complete the remaining setup steps remotely.

CIMC Configuration