Planning

A Cisco Threat Grid Appliance is a Linux server with Threat Grid software installed by Cisco Manufacturing prior to shipping. Once a new appliance is received, it must be set up and configured for your on-premises network environment. Before you begin, there are a number of issues to consider and plan. This chapter includes the following information about the environmental, hardware, and network requirements:

Supported Browsers

Threat Grid supports the following browsers:

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

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

Environmental Requirements

The Threat Grid Appliance is deployed on a UCS C220-M3 or UCS C220-M4 server. Before you set up and configure your appliance, make sure the necessary environment requirements for power, rack space, cooling, and other issues are met, according to the specification for your server.

Hardware Requirements

The form factor for the Admin interface is SFP+. If you are clustering appliances, each one will require an additional SFP+ module on the Cust interface.

Note The SFP+ modules must be connected *before* the 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 1: Cisco 1000BASE-T Copper SFP (GLC-T)

You can attach a monitor to the server, or, if CIMC (Cisco Integrated Management Controller) is configured, you can use a remote KVM.

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 appliance setup.
  - OpAdmin 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 appliance (requests). This includes integrated appliances. For example, the Cisco Email Security appliances and Web Security appliances connect to the IP address of the Clean interface.

Note The URL for the Clean network interface *will not work* until the OpAdmin portal configuration is complete.

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

- Remote syslog connections
- Email messages sent by the Threat Grid Appliance itself
- 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 appliance (including malware traffic).

Note We recommend using a dedicated external IP address (i.e., the Dirty interface) that is different from your corporate IP, in order to protect your internal network assets.

For network interface setup information and illustrations, see the Network Interfaces section, and the Network Interface Connections Setup sections.

DNS Server Access

The DNS server 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 itself needs to be accessible via the dirty network.

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 OpAdmin interface.

See the Cisco Threat Grid Appliance Administrator Guide for additional information.

NTP Server Access

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

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.

DHCP

If you are connected to a network configured to use DHCP, follow the instructions provided in the *Using DHCP* section of the Cisco Threat Grid Appliance Administrator Guide.

License

You will receive a license and password from Cisco Threat Grid.

For questions about licenses, contact support@threatgrid.com.

Rate Limits

The API rate limit is global for the 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 Threat Grid portal UI FAQ entry on rate limits for a more detailed description.

Organization and Users

Once you have completed the appliance setup and network configuration, you will need to create the initial Threat Grid Organizations and add user account(s), so 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.

Managing Threat Grid Organizations is documented in the Cisco Threat Grid Appliance Administrator Guide. Managing users is documented in the Threat Grid portal Help.

Updates

The initial 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 described in this guide (see Install Updates).

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

Note Verify that SSH is specified for updates.

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 OpAdmin with version 2.1.6.

TGSH Dialog

The **TGSH Dialog** interface is used to configure the Network Interfaces. TGSH Dialog is displayed when the appliance successfully boots up.

Reconnecting to the TGSH Dialog

TGSH Dialog will remain 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 will either be 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 OpAdmin Portal Configuration.

Threat Grid Shell - tgsh

The Threat Grid Shell (tgsh) is an administrator's interface that is used for executing a couple of commands (including destroy-data and forced backup), as well as for expert, low-level debugging. To access tgsh, select **CONSOLE** in the TGSH Dialog.

Note OpAdmin uses the same credentials as the Threat Grid user, so any password changes/updates made via tgsh will impact OpAdmin as well.

Caution Network configuration changes made with tgsh are NOT supported unless specifically directed by Threat Grid support; OpAdmin or TGSH Dialog should be used instead.

OpAdmin Portal

This is the primary Threat Grid GUI configuration tool. Much of the appliance configuration can ONLY be done via OpAdmin, 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.

Cisco Integrated Management Controller (CIMC)

Another user interface is the Cisco Integrated Management Controller (CIMC), which is used to manage the server.

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. • OpAdmin 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. **Note** The form factor for the Admin interface is SFP+. See Figure 2 - Cisco 1000BASE-T Copper SFP (GLC-T).
Clust	The non-Admin SFP+ port that was formerly reserved, is now being 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)
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 OpAdmin. • NTP • Updates • Support Session in Normal Operations Mode • Support Snapshots • Malware Sample-initiated Traffic • Recovery Mode Support Session (outbound) • OpenDNS, TitaniumCloud, Virus Total, ClamAV • SMTP Outbound connections are redirected to a built-in honeypot **Note** Although using IPv4LL address space (168.254.0.16) for the Dirty interface has never been documented as supported, from version 2.3.0 forward it is recognized as broken, and therefore explicitly unsupported.

Interface	Description
CIMC Interface	Recommended. If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. For more information see CICM Configuration.

Login Names and Passwords (Default)

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

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

Setup and Configuration Overview

The following setup and initial configuration steps are described in this guide:

- Server Setup
- Network Interface Connections Setup (Admin, Clust, Clean, Dirty)
- Initial Network Configuration - TGSH Dialog
- Main Configuration - OpAdmin Portal
- Install Updates
- Test the Appliance Setup - Submit a Sample for Analysis

Complete the remaining administrative configuration tasks (license installation, email server, SSL Certificates, etc.) in the OpAdmin Portal as documented in the Cisco Threat Grid Appliance Administrator Guide.

You should allow yourself approximately 1 hour to complete the server setup and initial configuration steps.