

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 1
- Environmental Requirements, on page 2
- Hardware Requirements, on page 2
- Network Requirements, on page 2
- DNS Server Access, on page 3
- NTP Server Access, on page 4
- Integrations, on page 4
- DHCP Requirements, on page 4
- License, on page 5
- Rate Limits, on page 5
- Organizations and Users, on page 5
- Updates, on page 5
- User Interfaces, on page 6
- Network Interfaces, on page 7
- Firewall Rules, on page 10
- Privacy and Sample Visibility, on page 12
- Wipe Appliance Boot Option, on page 14

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 1: 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.

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/WSA to Threat Grid Appliance for more information.

DHCP Requirements

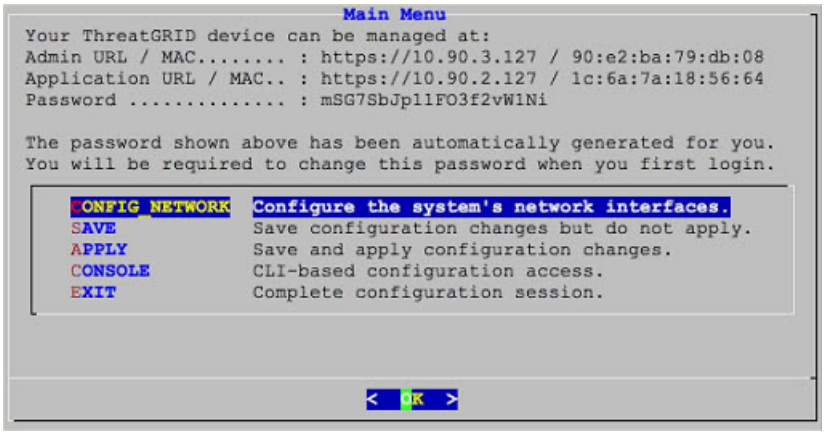
If you are connected to a network configured to use DHCP, it is important that you understand the requirements. Threat Grid Appliances that use DHCP need to explicitly specify DNS.

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 2: 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 Configuring Network and DHCP.

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 Support.

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 Create New Organizations 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.

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.

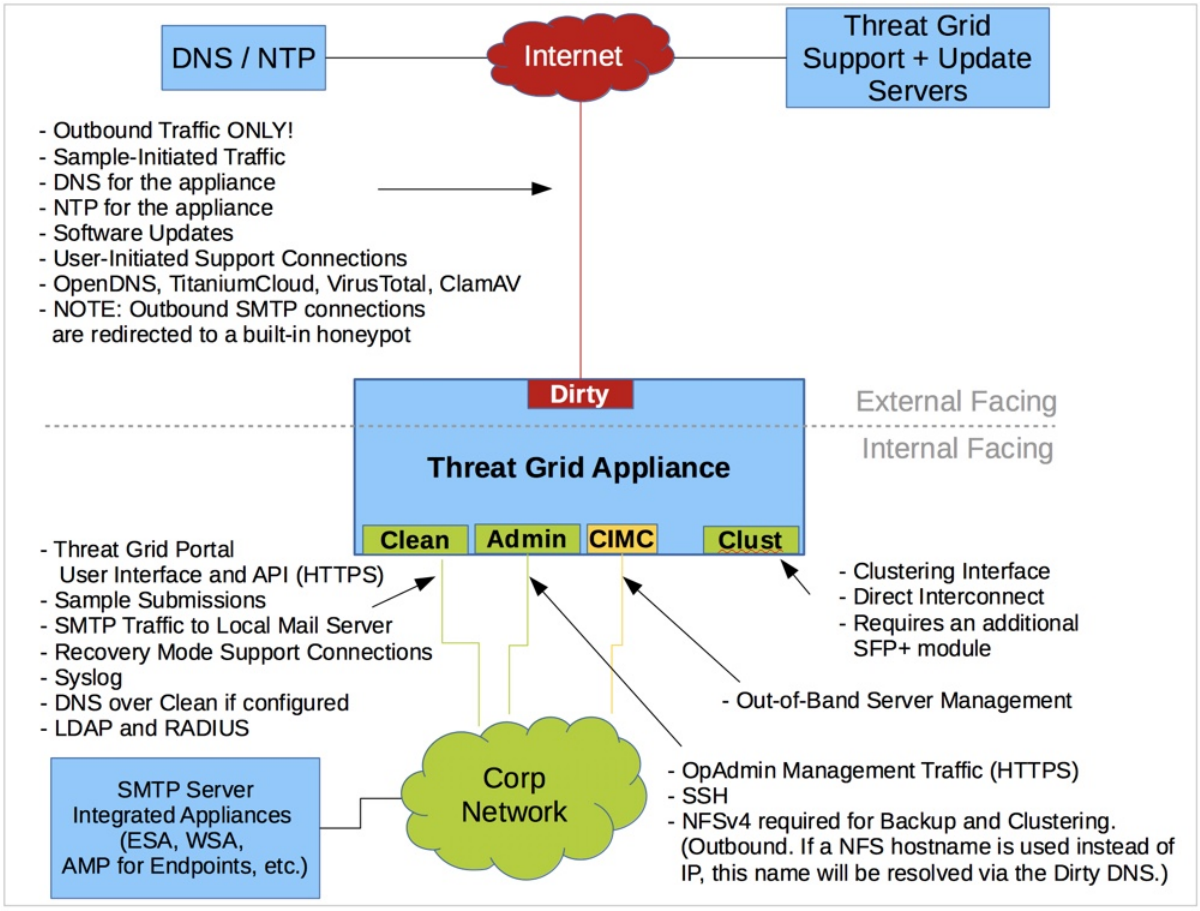
Interface	Description
Clean	• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. • UI and API traffic (inbound) • Sample submissions • SMTP (outbound connection to the configured mail server) • SSH (inbound for TGSH Dialog) • Syslog (outbound to configured syslog server) • ESA/WSA and CSA Integrations • AMP for Endpoints Private Cloud Integration • DNS optional • LDAP (outbound) • RADIUS (outbound)
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 • 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 3: 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 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 4: 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 Boot Option

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.



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 Wipe Appliance Procedure.