Connecting with a Threat Grid Appliance

Version 2.1.3

Last Updated: 8/11/2016

Cisco Systems, Inc. www.cisco.com

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

CONTENTS

LIST OF FIGURES

SSL CERTIFICATES AND THREAT GRID APPLIANCES

All network traffic passing to and from the Threat Grid Appliance is encrypted using SSL. A full description of how to administer SSL certificates is beyond the scope of this Guide. However, the following information is provided to assist you through the steps for setting up SSL certificates to support Threat Grid Appliance connections with ESA/WSA appliances, FireAMP Private Cloud, and other integrations.

Interfaces That Use SSL

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

- **Clean** interface for the Threat Grid Portal UI and API, as well as integrations (ESA/WSA appliances, FireAMP Private Cloud Disposition Update Service, etc.)

- **Admin** interface for the **OpAdmin Portal**.

SSL/TLS Versions Supported

- TLSv1.0

- TLSv1.1

- TLSv1.2

Customer-Provided CA Certificates Are Supported

With the 2.0.3 release we now support customer-provided CA certificates, allowing customers to import their own trusted certificates or CA certificates.

SSL Certificates - Self-Signed Default

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. The appliance SSL certificates can be replaced by an administrator.

The default Threat Grid Appliance SSL certificate hostname (Common Name) is "*pandem*", which is valid for 10 years. If a different hostname was assigned to the Threat Grid Appliance during configuration, then the hostname and the CN in the certificate will no longer match. The hostname in the certificate must also match the hostname expected by a connecting ESA or WSA appliance, or other integrating Cisco device or service, as many client applications require SSL certificates where the CN used in the certificate matches the hostname of the appliance.
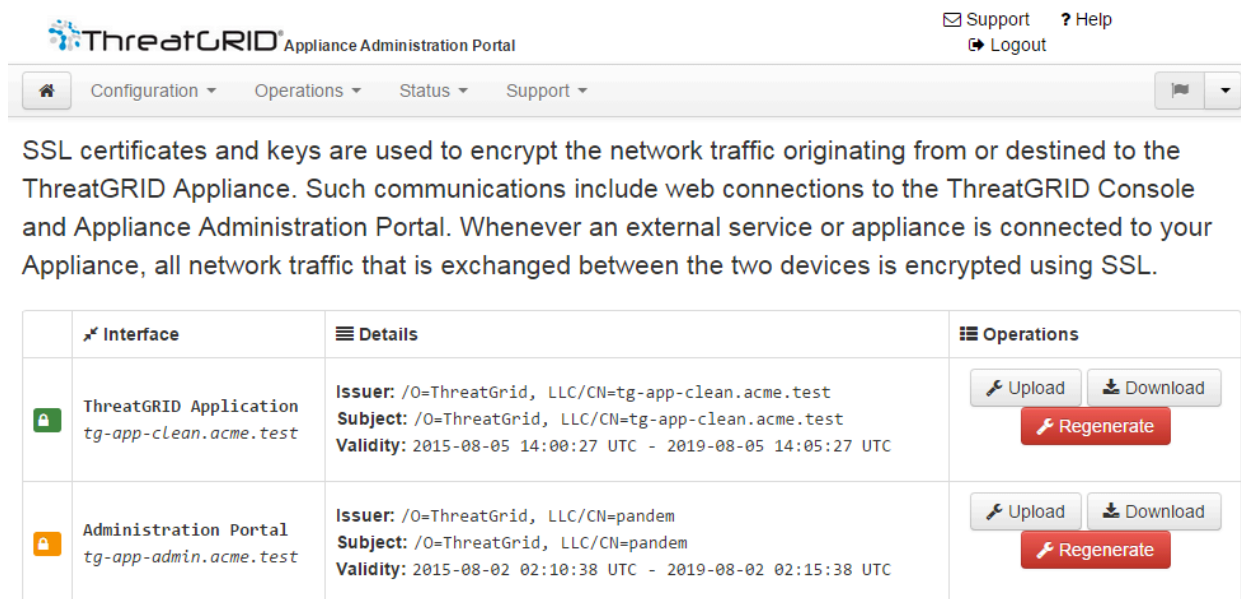
Configuring SSL Certificates for Inbound Connections

Other Cisco products, such as such as ESA and WSA appliances and FireAMP Private Clouds, can integrate with a Threat Grid Appliance and submit samples to it. These integrations are *Inbound* connections from the perspective of the Threat Grid Appliance. The integrating appliance or other device must be able to trust the Threat Grid Appliance's SSL certificate, so you will need to export it from the TGA (first making sure that it uses the correct hostname in the CN field and regenerating or replacing it if necessary), and then import it into the integrating appliance or service.

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

Select **OpAdmin > Configuration > SSL**. The SSL Certificate configuration page opens:

Figure 1 - SSL Certificate Configuration Page

There are two SSL certificates in the illustration above: "ThreatGRID Application" is the **Clean** interface, and "Administration Portal" is the **Admin** interface.

CN Validation

In the SSL Certificate Configuration page, a colored padlock icon indicates the status of the SSL certificates on the TG Appliance. The hostname must match the CN ("Common Name") used in the SSL certificate. If they do not match, you will need to replace the certificate with one that uses the current hostname. See Replacing an SSL Certificate below.

- The green padlock icon indicates that the Clean interface hostname matches the CN ("Common Name") used in the SSL certificate.

- The yellow padlock icon is a warning that the Admin interface hostname does NOT match the CN in that SSL certificate. You will need to replace the certificate with one that uses the current hostname.

Replacing an SSL Certificate

SSL certificates usually need to be replaced at some time, for a variety of reasons. For example, they expire, or the hostname changes. An SSL certificate may also need to be added or replaced in order to support integrations between the Threat Grid Appliance and other Cisco devices and services.

ESA/WSA appliances and other CSA Cisco integrating devices may require an SSL certificate in which the Common Name matches the Threat Grid Appliance hostname. In this case, you will need to replace the default SSL certificate and generate a new one using the same hostname from which you'll be accessing the Threat Grid Appliance.

In the case where you are integrating a Threat Grid Appliance with a FireAMP Private Cloud to use its Disposition Update Service, you will need to install the FireAMP 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 a new SSL Certificate, which will use the current hostname for the CN.

- Downloading an SSL Certificate

- Uploading a new SSL Certificate. This can be a commercial or enterprise SSL, or one you make yourself using OpenSSL.

- Generating Your Own SSL Certificate – an Example Using OpenSSL

These are described in the following sections.

Regenerating an SSL Certificate

This replaces the need in pre-v1.3 Threat Grid Appliances to generate a new SSL certificate manually using OpenSSL or other SSL tool. However, that method is still valid, as described in the section Generating Your Own SSL Certificate – an Example Using OpenSSL, below.

NOTE: The Threat Grid Appliance should be upgraded to 1.4.2 or higher before performing this task.

In the **OpAdmin SSL Certificate Configuration** page, click **Regenerate**. A new, self-signed SSL certificate is generated on the Threat Grid Appliance that uses the current hostname of the appliance in the CN field of the certificate. The CN validation padlock icon is green. The regenerated certificate (.cert file) can be downloaded as described in the next section, and installed on the integrating appliance.

Downloading an SSL Certificate

The Threat Grid SSL certificate, but not the key, can be downloaded, and installed on your integrating device so it can trust connections from the TG Appliance. You will only need the .cert file for this step.

1. In the OpAdmin SSL Certificate Configuration page, click **Download** next to the certificate you wish to obtain**.** The SSL Certificate is downloaded.

2. Next, install the downloaded SSL certificate on the ESA/WSA appliance, FireAMP Public Cloud, or other integrating Cisco products just as you would install any other SSL certificate.

Uploading an SSL Certificate

If you already have a commercial or corporate SSL certificate in place within your organization, you can use that to generate a new SSL certificate for the TGA, and use the CA cert on the ESA/WSA or other integrating device.

Generating Your Own SSL Certificate – an Example Using OpenSSL

Another alternative is to generate your own SSL certificate manually, such as when there is no SSL certificate infrastructure already in place on your premises, and you are unable to obtain one by other means. This can then be uploaded as described above.

This example illustrates the command for generating a new self-signed SSL certificate for the "Acme Company". The example uses OpenSSL, which is a standard open source SSL tool for creating and managing OpenSSL certificates, keys, and other files.

NOTE: OpenSSL is not a Cisco product, and Cisco provides no technical support for it. Search the Web for additional information on using OpenSSL. Cisco offers an SSL library, *Cisco SSL*, for generating SSL certificates.

```
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 that we want 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. We want to create a new X.509 cert, so we are using this subcommand.

- **-x509**: This modifies the previous subcommand by telling the utility that we want to make a self-signed certificate instead of generating a certificate signing request, as would normally happen.

- **-days 3650**: This option sets the length of time for which the certificate will be considered valid. Here we set it for 10 years.

- **-newkey rsa:4096**: This specifies that we want to generate a new certificate and a new key at the same time. We did not create the key that is required to sign the certificate in a previous step, so we need to create it along with the certificate. The rsa:4096 portion tells it to make an RSA key that is 4096 bits long.

- **-keyout**: This line tells OpenSSL where to place the generated private key file that we are creating.

- **-nodes**: This tells OpenSSL to skip the option to secure our certificate with a passphrase. The appliance needs to be able to read the file without user intervention, when the server starts up. A passphrase would prevent this from happening because we would have to enter it after every restart.

- **-out**: This tells OpenSSL where to place the certificate that we are creating.

- **-subj:** Example:

   C=US: Country.

   ST=New York: State.

   L=Brooklyn: Location.

   O=Acme Co: Owner's name.

   CN=tgapp.acmeco.com: Please enter the Threat Grid Appliance FQDN ("Fully Qualified Domain Name"). This includes the HOSTNAME of the Threat Grid Appliance ("tgapp" in our example), together with the associated domain name ("acmeco.com") appended to the end.

   IMPORTANT: You will need to change at the very least the Common Name to match the FQDN of the Threat Grid Appliance Clean interface.

Once the new SSL certificate is generated, use the SSL page **Upload** button to upload it to the Threat Grid Appliance, and also upload it to the ESA/WSA appliance (.cert only).

Configuring SSL Certificates for Outbound Connections

The Threat Grid Appliance release 2.0.3 includes features to support integrations with FireAMP Private Cloud for the Disposition Update Service.

Configure DNS

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

> In **OpAdmin**, select **Configuration > Network**, and complete the DNS fields for the Dirty and Clean networks, and click **Save**.

CA Certificate Management

One of the features added with release 2.0.3 is a new page for the CA Certificate Management truststore for the *Outbound* SSL connections, so the TGA can trust the FireAMP Private Cloud to notify it about analyzed samples that are considered to be malicious.

> In **OpAdmin**, select **Configuration > CA Certificates**. Select:

1. **Import from Host.** Retrieve the certificate from the server. The Retrieve certificates from server dialog opens.

2. Enter the **Host** and **Port** for the FireAMP Private Cloud and click **Retrieve**. The certificate is retrieved.

OR

> **Import from Clipboard.** Paste the PEM from the clipboard, and click **Add Certificate**.

3. Click **Import**.

Disposition Update Service Management

This task is performed from within the Threat Grid Portal UI.

1. From the **My Account** dropdown, select **Manage FireAMP Integration**. The Disposition Update Service page opens.

2. Enter the **FireAMP Private Cloud URL**, the **admin user name** and **password** provided by the FireAMP configuration portal, and click **Config**.

For more information on FireAMP Private Cloud appliance integrations, see Connecting a Threat Grid Appliance to a Cisco FireAMP Private Cloud:

Connecting ESA/WSA Appliances to a Threat Grid Appliance

Cisco products such as ESA/WSA and other appliances, devices, services, etc. may integrate with Threat Grid Appliances via connections encrypted with SSL, in order to submit possible malware samples to it for analysis. Integrations between the Threat Grid Appliance and ESA/WSA appliances are enabled by the Cisco Sandbox API ("CSA API"), are often referred to as "CSA Integrations".

In order for ESA/WSA appliances to connect to a Threat Grid Appliance, the Threat Grid Appliance's SSL certificate CNs must match its current hostname, which must also be the hostname expected by the integrating ESA/WSA appliance.

An integrating appliance must be registered with the Threat Grid Appliance before it can submit samples for analysis. Before an integrating ESA/WSA appliance can register 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.

This section describes the steps necessary for setting up a Threat Grid Appliance to communicate with integrating ESA/WSA appliances and other Cisco products.

Links to ESA/WSA Documentation

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

- The ESA user guides are located here:
  http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

- The WSA user guides are located here:
  http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

1. Hostname Must Match the CN and ESA/WSA Expectations

   The CN in the Threat Grid Appliance SSL certificate(s) must match its current hostname. For a successful connection with an integrating ESA/WSA appliance, this must also be the same hostname by which the integrating ESA/WSA appliance identifies the TGA.

   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 CN field, then download it to your working environment and upload and install it onto the integrating ESA/WSA appliance.

   Or, you may need to replace the current TGA SSL certificate by uploading an enterprise or commercial SSL certificate (or a certificate generated manually).

   For detailed instructions, see: Configuring SSL Certificates for Inbound Connections.

   Once the SSL certificate setup is complete, the next step is to verify that the Threat Grid Appliance and the ESA/WSA appliances can communicate with each other.

2. Verify Connectivity

   Cisco ESA/WSA appliances must be able to connect to the **Clean** interface of the Threat Grid Appliance over your network.

   Follow the instructions in the appropriate guide for your product to verify that the TGA and ESA/WSA Appliances can communicate with each other. (See links above.)

3. Register the Cisco ESA/WSA/other device with theThreat Grid Appliance.

   An ESA/WSA appliance that is configured according to the documentation for those products registers itself automatically with the Threat Grid appliance.

4.   Complete the ESA/WSA File Analysis Configuration.

Upon registration of the connecting device, a new Threat Grid user is created automatically with the Device ID as the login ID, and a new organization is created with a name based on the same ID. The new Device user account must be activated by an administrator, as described in the next section.

Activating a New Device User Account on the Threat Grid Appliance.

When the ESA/WSA appliance or other integration connects and registers itself with the Threat Grid Appliance, a new Threat Grid user account is created automatically. The initial status of this user account is "de-activated". Just like any other Threat Grid user, 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.

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

2.   From the navigation bar **Welcome** menu, select **Manage Users**. The **Threat Grid Users** page opens.

3.   Open the **User Details** page for the device user account (you may need to use Search to find it). The user status is currently "de-activated":

Figure 2 - User Details Page > Re-Activate User

4.   Click Re-**Activate User**. A dialog opens asking you to confirm.

5.   Click **Re-Activate** in the dialog to confirm.

The ESA/WSA or other integrating appliance or device can now communicate with the Threat Grid Appliance.

Connecting a Threat Grid Appliance to a Cisco FireAMP Private Cloud

The Threat Grid Appliance Disposition Update Service and FireAMP Private Cloud integration setup tasks must be performed on the devices in the following 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.

This connection is outgoing from the perspective of the Threat Grid Appliance. This integration does not use the CSA API.

Please refer to the FireAMP Private Cloud documentation for more detailed information on the tasks which must be performed on that side.

STEPS	Threat Grid Appliance ("TGA")	FireAMP Private Cloud
1	Set up and configure the Threat Grid Appliance ("TGA") as normal (i.e., no integration yet).	
2		Set up and configure the FireAMP Private Cloud as normal (i.e., no integration yet).
3		**Configure the FireAMP Private Cloud for the TGA Integration:** Select **Integrations > Threat Grid** and go to the **Connection to Threat Grid** section. To complete the connection with the Threat Grid Appliance, you have to trust it. You need its DNS hostname, SSL certificate, and API key. Go to step 3.1 in the TGA column to find this information.

STEPS	Threat Grid Appliance ("TGA")	FireAMP Private Cloud
3.1	**SSL Certificate: –** In the Threat Grid Appliance OpAdmin interface, select **Configuration > SSL** Regenerate a new SSL Certificate (on the "Threat Grid Application" – the Clean interface), to replace the default if needed, and download it to install in the FireAMP Private Cloud device.(TGA SSL Certificates are documented in SSL CERTIFICATES AND THREAT GRID APPLIANCES.) **Hostname** Select **Configuration > Hostname** **API Key**: The API Key may be found in the Threat Grid Face Portal UI, in the **User Details** page for the account that is going to be used for integrations: 1. Go to the **Threat Grid Portal UI**. 2. From the upper-right Welcome menu (located in the upper-right corner of the navigation bar), select **Manage Users**. 3. Navigate (use Search if necessary) to the **User Details** page for the integration's user account, and copy the **API Key**. Note that this does not need to be the "admin" user, but can be another user that was specifically created for this purpose on the Threat Grid Appliance.	

STEPS	Threat Grid Appliance ("TGA")	FireAMP Private Cloud
3.2		Complete the **Connection to Threat Grid** fields: 1. Enter the TGA Hostname 2. Enter the Threat Grid API Key for the account that is to be used for integrations. 3. Choose the TGA SSL Certificate file. 4. Click Save Configuration. 5. Click Test Connection. 6. Once the connection test passes, you will need to run the Reconfiguration on the FireAMP Private Cloud to apply the changes. Technically, this will allow AMP to talk to the Threat Grid Appliance, and you can now submit samples to TG at this point. However, you must complete the remaining steps to set up the Disposition Update Service, in order to communicate disposition results to the TGA. (For more information, please refer to the user documentation for the FireAMP Private Cloud.)
4	**Set up the Disposition Update Service** The following steps describe how to set up the Disposition Update Service	

STEPS	Threat Grid Appliance ("TGA")	FireAMP Private Cloud
4.1	**Configure DNS (if needed):** The Clean interface is used for the FireAMP integration. But by default, DNS uses the Dirty interface. If the FireAMP Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in OpAdmin. In OpAdmin, select **Configuration > Network**, and complete the fields for DNS on the **Dirty** and **Clean** networks, and click **Save**.	
4.2	**CA Certificate Management:** The next step is to download or copy/paste the FireAMP Private Cloud SSL certificate to the Threat Grid Appliance so it can trust the integrating device: 1. In OpAdmin, select **Configuration > CA Certificates**. You can select an SSL certificate to import from the FireAMP Private Cloud Host, or import from the clipboard. 2. Select the certificate to import and click **Import from Host**. The **Retrieve certificates from server** dialog opens. Enter the **Host** and **Port** for the FireAMP Appliance Disposition Service, and click **Retrieve**. 3. The certificate is retrieved. 4. Click **Import**. (OR click **Import from Clipboard.** Paste the PEM from the clipboard, and click **Add Certificate**.)	

STEPS	Threat Grid Appliance ("TGA")	FireAMP Private Cloud
4.3	**FireAMP Integration Management:** In the Threat Grid Face Portal UI, from the upper-right menu select **Manage FireAMP Integration**. The Disposition Update Service window opens. Enter the AMP Disposition Update Service URL (you can find this on the FireAMP appliance: select **Integrations > Threat Grid > FireAMP Private Cloud Details**). Enter your **admin user name** and **password**, and click **Config**.	

MANAGING THREAT GRID ORGANIZATIONS AND USERS

Threat Grid is installed on the appliance with a default organization and Admin user. Once the appliance is set up and the network configuration is completed, you may create additional organization and user accounts, so people can login 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.

For documentation on managing organizations, see the *Threat Grid Appliance Administrator's Guide*, which is located on the **Threat Grid Install and Upgrades** page on cisco.com.

For instructions and documentation on managing user accounts - including accounts for integrating Cisco ESA/WSA appliances and other devices - see the Threat Grid Portal UI online help. From the navigation bar select **Help > Using Threat Grid Online Help > Managing Users**.

PRIVACY AND SAMPLE VISIBILITY

When submitting samples to Threat Grid for analysis, an important consideration is the privacy of their contents. 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 Threat Grid, especially with the search API.

Privacy may be less of a concern when submitting samples to an on-premises Threat Grid Appliance than to the Threat Grid Cloud, but understanding the basics of privacy and sample visibility is still necessary for TGA administrators.

The privacy and sample visibility model for sample submissions to Threat Grid is relatively simple: Unless samples are designated as Private, they will be visible to users who are outside the submitter's Organization. In general, a sample designated as *Private* may only be seen by Threat Grid users within the same Organization as the user who submitted the sample.

Privacy and Visibility on Threat Grid Appliances

The privacy and sample visibility model is modified on Threat Grid Appliances for samples that are submitted by "CSA Integrations." CSA Integrations are Cisco products such as ESA/WSA appliances and other devices or services, which are integrated (registered) with Threat Grid Appliances via the CSA API.

All sample submissions on Threat Grid Appliances are Public by default, and can be viewed by any other appliance user, including CSA Integrations, regardless of which Organization they belong to.

All appliance users can see all details of samples submitted by all other users.

Non-CSA Threat Grid users may submit Private samples to the Threat Grid Appliance, in which case the samples are only visible to other Threat Grid Appliance users, including CSA Integrations, within the submitter's Organization.

Privacy and sample visibility model on Threat Grid Appliances illustrated in the table below, using the following terms:

CSA Integrations   CSA Integrations are ESA/WSA appliances and other Cisco devices or services that are registered on a Threat Grid Appliance via the CSA API. Samples submitted to Threat Grid Appliances by CSA Integrations are Public by default.

Threat Grid User - Public   Public samples submitted to a Threat Grid Appliance by normal Threat Grid users (i.e., non-CSA Integrations).

For example, appliance administrators or malware analysts who submit samples via the Threat Grid Portal UI, or by using the Threat Grid Native API.

Threat Grid User - Private   Private samples submitted to a Threat Grid Appliance by normal Threat Grid users.

In this case, the Private samples are invisible to all other users on the appliance who are outside of the submitter's Organization. (The samples will be visible to CSA Integrations within the same Organization as the submitter.)

Figure 3 - Privacy and Visibility on a Threat Grid Appliance

Samples Submitted by:	Sample Visibility when Accessed by:			
	Threat Grid Users from the Same Organization	Threat Grid Users from a Different Organization	CSA Integration from the Same Organization	CSA Integration from a Different Organization
Threat Grid User - Public	Full	Full	Full	Full
Threat Grid User - Private	Full	None	Full	None
CSA Integrations (ESA/WSA appliances, etc.) All CSA submissions to Threat Grid Appliance are Public by default	Full	Full	Full	Full

The same basic privacy rules apply to Threat Grid Appliance integrations with FireAMP Private Cloud.

For more information, see the documentation on the **Threat Grid Install and Upgrades** page on cisco.com.