



Connecting with a Threat Grid Appliance



Version 2.1.4

Last Updated: 11/17/2016

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.

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.

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: www.cisco.com/go/trademarks. 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.

Cover photo: Claret Cup cactus in bloom on a ridge high above the Arches National Park visitor's center. It takes good defenses and making the most of your resources to flourish in a harsh and hostile environment. Copyright © 2015 Mary C. Ecsedy. All rights reserved. Used with permission.

Connecting with a Threat Grid Appliance consists of sections in the *Cisco AMP Threat Grid Appliance Administrator's Guide*.

All contents are Copyright © 2015-2016 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

CONTENTS

CONTENTS	i
LIST OF FIGURES	i
SSL CERTIFICATES AND THREAT GRID APPLIANCES	1
Interfaces That Use SSL	1
SSL/TLS Versions Supported	1
Customer-Provided CA Certificates Are Supported	1
SSL Certificates - Self-Signed Default	1
Configuring SSL Certificates for Inbound Connections	1
CN Validation	2
Replacing an SSL Certificate	2
Regenerating an SSL Certificate	3
Downloading an SSL Certificate	3
Uploading an SSL Certificate	3
Generating Your Own SSL Certificate – an Example Using OpenSSL	3
Configuring SSL Certificates for Outbound Connections	5
Configure DNS.....	5
CA Certificate Management.....	5
Disposition Update Service Management	5
Connecting ESA/WSA Appliances to a Threat Grid Appliance	6
Links to ESA/WSA Documentation.....	6
Integration Process Overview	6
ESA/WSA Integration Process Steps	7
Connecting a Threat Grid Appliance to a Cisco FireAMP Private Cloud	11
MANAGING THREAT GRID ORGANIZATIONS AND USERS	16
Creating a New Organization	16
Managing Users	17
Activating a New Device User Account on the Threat Grid Appliance	17
PRIVACY AND SAMPLE VISIBILITY	18
Privacy and Visibility on Threat Grid Appliances	18

LIST OF FIGURES

Figure 1 - SSL Certificate Configuration Page.....	2
Figure 2 - User Details Page > Re-Activate User	17
Figure 3 - Privacy and Visibility on a Threat Grid Appliance.....	19

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



The screenshot shows the ThreatGRID Appliance Administration Portal. The page title is "ThreatGRID Appliance Administration Portal". The navigation menu includes "Configuration", "Operations", "Status", and "Support". The page content is titled "SSL certificates and keys are used to encrypt the network traffic originating from or destined to the ThreatGRID Appliance. Such communications include web connections to the ThreatGRID Console and Appliance Administration Portal. Whenever an external service or appliance is connected to your Appliance, all network traffic that is exchanged between the two devices is encrypted using SSL."

Interface	Details	Operations
 ThreatGRID Application tg-app-clean.acme.test	Issuer: /O=ThreatGrid, LLC/CN=tg-app-clean.acme.test Subject: /O=ThreatGrid, LLC/CN=tg-app-clean.acme.test Validity: 2015-08-05 14:00:27 UTC - 2019-08-05 14:05:27 UTC	 Upload  Download  Regenerate
 Administration Portal tg-app-admin.acme.test	Issuer: /O=ThreatGrid, LLC/CN=pandem Subject: /O=ThreatGrid, LLC/CN=pandem Validity: 2015-08-02 02:10:38 UTC - 2019-08-02 02:15:38 UTC	 Upload  Download  Regenerate

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](#), below.

Connecting ESA/WSA Appliances to a Threat Grid Appliance

Other 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.

"CSA Integrations": Integrations between ESA/WSA appliances and Threat Grid appliances are enabled by the Cisco Sandbox API ("CSA API"), and are often referred to as "CSA Integrations".

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

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

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

- 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>

Integration Process Overview

Before you begin: This section provides an overview of the steps in setting up a connection between an ESA/WSA appliance or other CSA integration (inbound) with a Threat Grid Appliance.

A table containing more detailed descriptions of each step follows this section.

Threat Grid Appliance SSL Certificate SAN or CN Must Match its Current Hostname and ESA/WSA Expectations:

The Threat Grid appliance SSL certificate SAN ("Subject Alternative Name" – if defined), or the CN ("Common Name") needs to match the hostname, and also the ESA/WSA expectations: for a successful connection with an integrating ESA/WSA appliance, this must be the same hostname by which the integrating ESA/WSA appliance 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 appliance.

Alternatively, 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 the section above: *Configuring SSL Certificates for Inbound Connections*.

Verify Connectivity:

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

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

Connecting with a Threat Grid Appliance

SSL CERTIFICATES AND THREAT GRID APPLIANCES

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.)

Complete the ESA/WSA File Analysis Configuration:

Enable the File Analysis security service, and configure the advanced settings.

Register the Cisco ESA/WSA/other device with the Threat Grid Appliance:

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

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. An administrator, as described in the next section, must activate the new Device user account.

Activate the New ESA/WSA 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, a Threat Grid Appliance administrator must manually activate the device user account before it can be used for submitting malware samples for analysis.

ESA/WSA Integration Process Steps

This connection is *incoming* from the perspective of the Threat Grid Appliance.

This integration uses the CSA API.

Please refer to the ESA and WSA User Guides for more detailed information on the tasks that must be performed on that side.

STEPS	Threat Grid Appliance ("TGA")	ESA/WSA/Other CSA API Integrations
1	Set up and configure the Threat Grid Appliance ("TGA") as normal (i.e., no integration yet). Check for updates and install if found.	
2		Set up and configure the ESA/WSA appliance as normal (i.e., no integration yet).

Connecting with a Threat Grid Appliance

SSL CERTIFICATES AND THREAT GRID APPLIANCES

STEPS	Threat Grid Appliance (“TGA”)	ESA/WSA/Other CSA API Integrations
3	<p>The TGA SSL Certificate SAN or CN Must Match its Current Hostname and ESA/WSA Expectations</p> <p>If you will deploy a self-signed SSL certificate:</p> <p>Generate 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 ESA/WSA appliance device. (TGA SSL Certificates are documented in the section above, SSL CERTIFICATES AND THREAT GRID APPLIANCES.)</p> <p>Be sure to generate a certificate that has the hostname of your AMP Threat Grid appliance as the SAN or CN. The default certificate from the AMP Threat Grid appliance does NOT work.</p> <p>Use the hostname, not the IP address.</p>	
4		<p>Verify Connectivity</p> <p>Cisco ESA/WSA appliances must be able to connect to the Clean interface of the Threat Grid Appliance over your network.</p>

STEPS	Threat Grid Appliance (“TGA”)	ESA/WSA/Other CSA API Integrations
5		<p>Configure the ESA/WSA appliance for the TG Appliance Integration:</p> <p>Please refer to the ESA/WSA guides for complete instructions. The following steps are specific to the ESA, as this is currently the most common type of integration</p> <ol style="list-style-type: none"> 1. Select Security Services > File Reputation and Analysis. 2. Click Enable. 3. Click Edit Global Settings. <p>File Analysis is enabled by default. If you do not uncheck Enable File Analysis, the File Analysis feature key will be activated after the next commit.</p> <ol style="list-style-type: none"> 4. In the File Analysis section, select the file types to send to the Cloud for analysis. 5. Configure the Advanced Settings for File Analysis as needed, according to the ESA or WSA guides: <p>File Analysis Server URL:</p> <p>Select Private Cloud.</p> <p>Server:</p> <p>URL of the on-premises Cisco AMP Threat Grid Appliance.</p> <p>Use the hostname, not the IP address, for this value and for the certificate.</p> <p>SSL Certificate:</p> <p>Upload a self-signed certificate that you have generated from your on-premises Cisco AMP Threat Grid Appliance.</p> <p>The most recently uploaded self-signed certificate is used. It is not possible to access a certificate uploaded prior to the most recent certificate; if needed, upload the desired certificate again.</p> 6. Submit and commit your changes. <p>Note the File Analysis Client ID that appears at the bottom of the page. This identifies the “user” that you will need to activate in step 7.</p>

STEPS	Threat Grid Appliance (“TGA”)	ESA/WSA/Other CSA API Integrations
		<p>Registration with the Threat Grid Appliance is Automatic</p> <p>Registration of your Email Security appliance or Web Security appliance with your Threat Grid appliance occurs automatically when you submit the configuration for File Analysis. However, you must activate the registration as described in step 7, below.</p>
7	<p>Activate the New Device User Account on the Threat Grid Appliance</p> <ol style="list-style-type: none"> 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". 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 initiate connections 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). Check for updates and install if found.	
2		Set up and configure the FireAMP Private Cloud as normal (i.e., no integration yet).
3		<p>Configure the FireAMP Private Cloud for the TGA Integration:</p> <p>Select Integrations > Threat Grid and go to the Connection to Threat Grid section.</p> <p>To complete the connection with the Threat Grid Appliance, you have to trust it. You need its DNS hostname, SSL certificate, and API key.</p> <p>Go to step 3.1 in the TGA column to find this information.</p>

STEPS	Threat Grid Appliance (“TGA”)	FireAMP Private Cloud
3.1	<p>SSL Certificate: –</p> <p>In the Threat Grid Appliance OpAdmin interface, select Configuration > SSL</p> <p>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.)</p> <p>Hostname</p> <p>Select Configuration > Hostname</p> <p>API Key:</p> <p>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:</p> <ol style="list-style-type: none"> 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		<p>Complete the Connection to Threat Grid fields:</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>(For more information, please refer to the user documentation for the FireAMP Private Cloud.)</p>
4	<p>Set up the Disposition Update Service</p> <p>The following steps describe how to set up the Disposition Update Service</p>	

STEPS	Threat Grid Appliance (“TGA”)	FireAMP Private Cloud
4.1	<p>Configure DNS (if needed):</p> <p>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.</p> <p>In OpAdmin, select Configuration > Network, and complete the fields for DNS on the Dirty and Clean networks, and click Save.</p>	
4.2	<p>CA Certificate Management:</p> <p>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:</p> <ol style="list-style-type: none"> 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. <p>(OR click Import from Clipboard. Paste the PEM from the clipboard, and click Add Certificate.)</p>	

Connecting with a Threat Grid Appliance

SSL CERTIFICATES AND THREAT GRID APPLIANCES

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

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.

Creating a New Organization

Users are always affiliated with an organization; before you can add users, you must first create the Organization to add them to.

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

1. Log into the Threat Grid portal as Admin.
2. Click the **Welcome** dropdown link located in the upper-left corner, and select **Manage Orgs**. The Organizations page opens, listing all of the Organizations on the appliance.
3. Click the **Add Organization** button, located in the upper-right corner of the screen. The Properties dialog opens.
4. All fields are required.

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

Industry. Select the type of business from the Industry dropdown. If none of the industries on the list are applicable, then leave it set to Unknown, and contact Threat Grid support (support@threatgrid.com) to request that an option be added.

Complete the other Options.

Rate Limit:

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. The rate limit in the license applies to the Organization.

Set the default *user* submission rate limit. You can also set sample submission rates on individual users - as documented in *Using Threat Grid*, the Threat Grid Portal online Help (From the navigation bar select **Help > Using Threat Grid 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, plus a message about how long to wait before retrying.

The **Priority** field is going away; for now just enter "50".

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

Managing Users

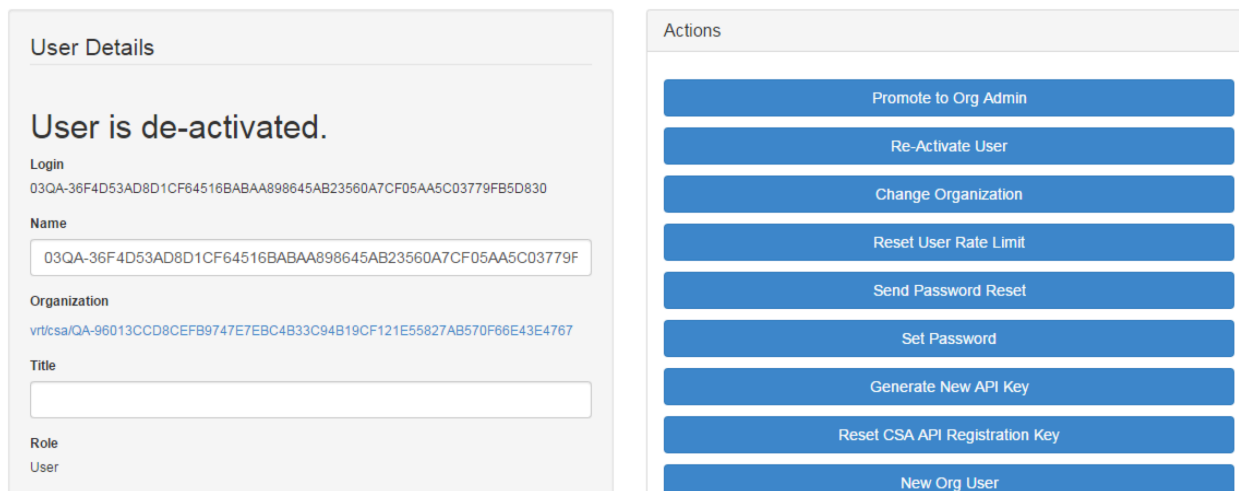
For instructions and documentation on managing user accounts - including accounts for integrating Cisco ESA/WSA appliances and other devices - see the Threat Grid Portal UI online help. From the navigation bar select **Help > Using Threat Grid Online Help > Managing Users**.

Activating a New Device User Account on the Threat Grid Appliance

When the ESA/WSA appliance or other CSA (“Cisco Sandbox API”) integration connects and registers itself with a 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.

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

	Sample Visibility when Accessed by:			
Samples Submitted 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.