Manage SSL Certificates

This chapter provides information about managing SSL certificates for your Threat Grid Appliance and integrated appliances and devices. It includes the following topics:

About SSL Certificates and Threat Grid Appliance

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

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

Interfaces Using SSL

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

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

Supported SSL/TLS Version

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

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

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

Supported Customer-Provided CA Certificates

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

Self-Signed Default SSL Certificates

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

The default Threat Grid Appliance SSL certificate hostname (Common Name) is **pandem**, and is valid for 10 years. If a different hostname was assigned to the Threat Grid appliance during configuration, then the hostname and the Common Name in the certificate will no longer match.

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

Configure SSL Certificates for Inbound Connections

Cisco security products, such as Email Security Appliance, Web Security Appliance, and AMP for Endpoints 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 SSL certificate. You must first validate that the hostname matches the Common Name; if it doesn't match, you must regenerate or replace it. You then must export the SSL certificate from the Threat Grid Appliance, and then import it into the 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.

Procedure

Step 1 In the OpAdmin portal, click **Configuration > SSL** to open the SSL Certificate configuration page.

Figure 1: SSL Certificate Configuration Page

In this example, there are two SSL certificates: **ThreatGRID Application** is the Clean interface, and **Administration Portal** is the Admin interface.

Step 2 Validate that the hostname matches the Common Name used in the SSL certificate (green padlock icon). See Validate Common Name in SSL Certificate.

Validate Common Name in SSL Certificate

The hostname must match the Common Name used in the SSL certificate on the Threat Grid Appliance.

On the SSL Certificate Configuration page, the padlock icon in the column to the left of the interface name indicates the status of the SSL certificates:

- **Green** - Indicates the interface hostname matches the Common Name used in the SSL certificate.
- **Yellow** - Indicates that the interface hostname does not match the Common Name in the SSL certificate. You must replace the certificate with one that uses the current hostname.

If the hostname and Common Name do not match, you must replace the certificate with one that uses the current hostname (see Replace SSL Certificate).

Replace SSL Certificate

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

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

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

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

- Regenerate SSL Certificate that uses the current hostname for the Common Name.
- Download SSL Certificate.
- Upload SSL Certificate; this can be a commercial or enterprise SSL, or one you create using OpenSSL.
- Generate SSL Certificate Using OpenSSL

Regenerate SSL Certificate

You can regenerate a SSL certificate from the SSL Certificate Configuration page (v1.4.2 or later required) if your hostname does not match the Common Name in the certificate.

In the OpAdmin SSL Certificate Configuration page, click Regenerate.

Procedure

Step 1 In the OpAdmin portal, click **Configuration > SSL** to open the SSL Certificate configuration page.

Step 2 In the Operations column, click **Regenerate** for the interface that needs a new certificate.

A new self-signed SSL certificate is generated on the Threat Grid Appliance that uses the current hostname of the appliance in the Common Name field of the certificate. The Common Name validation padlock icon next to the interface name changes to green.

You can now Download SSL Certificate the regenerated certificate (.cert file) and install it on the integrating appliance.

Download SSL Certificate

The Threat Grid Appliance SSL certificate can be downloaded and installed on your integrating device so it can trust connections from the Threat Grid Appliance.

Procedure

Step 1 In the OpAdmin portal, click **Configuration > SSL** to open the SSL Certificate configuration page.

Step 2 In the Operations column, click **Download** for the interface certificate. The SSL certificate **.cert** file is downloaded.

Step 3 Install the downloaded SSL certificate (**.cert** file) on the Email Security Appliance, Web Security Appliance, AMP for Endpoints Private Cloud, or other integrating Cisco products per the product documentation.

Upload 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 Threat Grid Appliance and use the CA cert on the integrating device.

Procedure

Step 1 In the OpAdmin portal, click **Configuration > SSL** to open the SSL Certificate configuration page.

Step 2 In the Operations column, click **Upload** for the appropriate interface.

The Common Name validation padlock icon next to the interface name changes to green.

Generate SSL Certificate Using OpenSSL

You can manually generate a SSL certificate using OpenSSL when there is no SSL certificate infrastructure already in place on your premises and upload it to the Threat Grid Appliance (as described in Upload SSL Certificate). OpenSSL is a standard open-source SSL tool for creating and managing OpenSSL certificates, keys, and other files.

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

Procedure

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

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

- **openssl** - OpenSSL
- **req** - Specifies to use X.509 certificate signing request (CSR) management. X.509 is a public key infrastructure standard that SSL and TLS use for key and certificate management. In this example, this parameter is used to create a new X.509 cert.
- **-x509** - This modifies the req parameter X.509 to make a self-signed certificate instead of generating a certificate signing request.
- **-days 3650** - This option sets the length of time for which the certificate will be considered valid. In this example, it is set for 10 years.
- **-newkey rsa:4096** - This specifies to generate a new certificate and a new key at the same time. Because the required key was not previously created, it must be created with the certificate. The **rsa:4096** parameter indicates to make an RSA key that is 4096 bits long.

- **-keyout** - This parameter indicates where OpenSSl should save the generated private key file that is being created.
- **-nodes** - This parameters indicates that OpenSSL should skip the option to secure the certificate with a passphrase. The appliance needs to be able to read the file, without user intervention, when the server starts up. A certificate that is secured with a passphrase requires that the user enter the passphrase every time the server is restarted.
- **-out** - This parameter indicates where OpenSSL should save the certificate that is being created.
- **-subj:** (Example):
  - **C=US** - Country
  - **ST=New York** - State
  - **L=Brooklyn** - Location
  - **O=Acme Co** - Owner's name
  - **CN=tgapp.acmeco.com** - Enter the Threat Grid Appliance FQDN (Fully Qualified Domain Name). This includes the HOSTNAME of the Threat Grid Appliance (in this example, **tgapp**) and the associated domain name (in this example, **acmeco.com**).

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

Step 2 Once the new SSL certificate is generated, upload the certificate to the Threat Grid Appliance from the SSL Certificate Configuration page (see Upload SSL Certificate). You must also upload the certificate (**.cert** file only) to the Email Security Appliance or Web Security Appliance.

Configure SSL Certificates for Outbound Connections

The Threat Grid Appliance (v2.0.3 and later) supports integration with Cisco AMP for Endpoints Private Cloud for the Disposition Update Service. This integration is a *Outbound* connection from the perspective of the Threat Grid Appliance.

Configure DNS

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

Procedure

Step 1 In OpAdmin, click **Configuration** > **Network**.

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

Step 3 Click **Save**.

Manage CA Certificates

The CA Certificate page (v2.0.3 or later) in the OpAdmin portal is used to manage the CA Certificate trust store for outbound SSL connections so that the Threat Grid Appliance can trust the Cisco AMP for Endpoints Private Cloud to notify it about analyzed samples that are considered malicious.

Procedure

Step 1 In the OpAdmin portal, click **Configuration > CA Certificates**.

Step 2 Choose one of the following import options:

- **Import from Host** to retrieve the certificate from the server. Enter the **Host** and **Port** for the AMP for Endpoints Private Cloud and then click **Retrieve**.
- **Import from Clipboard**, paste the PEM from the clipboard, and then click **Add Certificate**.

Step 3 Click **Import**.

Manage Disposition Update Syndication Service

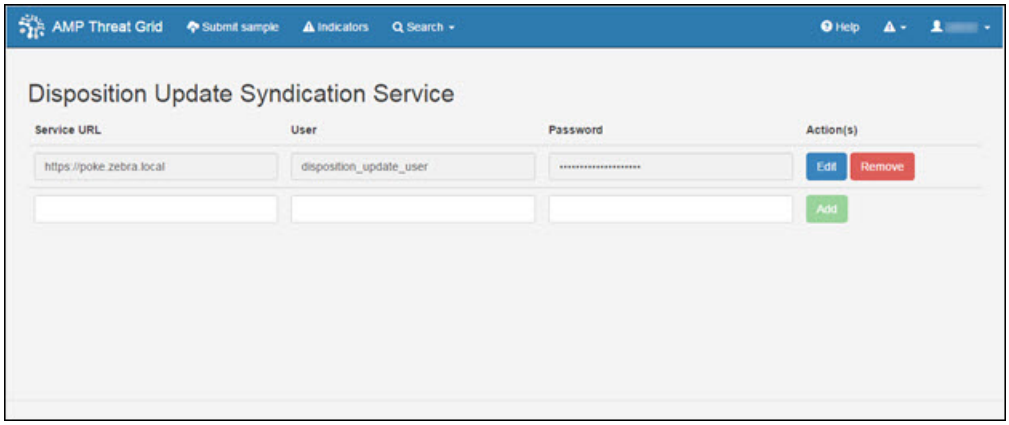
You can manage the Disposition Update Syndication Service for AMP for Endpoints Private Cloud appliance integrations in the Threat Grid portal user interface (v2.2 or later). URLs can be added, edited, and deleted from the Disposition Update Syndication Service page.

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

Procedure

Step 1 In the Threat Grid portal, click the drop-down on the navigation bar next to your login name and choose **Manage FireAMP Integration** to open the Disposition Update Syndication Service page.

Figure 2: Disposition Update Syndication Service



Step 2 Enter the following information:

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

Step 3 Click **Config**.

Connect ESA/WSA to Threat Grid Appliance

Cisco products such as Email Security Appliance (ESA), Web Security Appliance (WSA), and other appliances, devices, and services, can integrate with Threat Grid Appliances through connections encrypted with SSL to submit possible malware samples for analysis.

Integration between ESA/WSA and Threat Grid Appliance are enabled by the Cisco Sandbox API (CSA API) and are often referred to as CSA Integrations.

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

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

ESA and 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.

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

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

ESA and WSA Integration Process Overview

This section provides an overview of the steps in setting up a connection between an ESA/WSA or other CSA integration (inbound) with a Threat Grid Appliance. See ESA/WSA Integration Process Steps for more detailed descriptions and steps.

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), or the CN (Common Name) needs to match the hostname and the ESA/WSA expectations; for a successful connection with an integrating ESA/WSA, this must be the same hostname by which the integrating ESA/WSA identifies the Threat Grid Appliance.

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

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

Verify Connectivity

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

The ESA/WSA must be able to connect to the Clean interface of the Threat Grid Appliance over your network. Follow the instructions in the appropriate guide for your product to verify that the Threat Grid Appliance and ESA/WSA can communicate with each other (see Connect ESA/WSA to Threat Grid Appliance).

Complete the ESA/WSA File Analysis Configuration

Enable the **File Analysis Security** service and configure the advanced settings.

Register ESA/WSA with Threat Grid Appliance

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

Activate the New ESA/WSA Account on the Threat Grid Appliance

When the ESA/WSA or other integration connects and registers itself with the Threat Grid Appliance, a new Threat Grid user account is automatically created. The initial status of the user account is *deactivated*. 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

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

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

Procedure

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

Step 2 Set up and configure the ESA/WSA as normal (no integration yet).

Step 3 The TGA SSL Certificate SAN or CN Must Match its Current Hostname and ESA/WSA Expectations. If you are deploying a self-signed SSL certificate, generate a new SSL Certificate (on the Threat Grid Application the Clean interface), to replace the default if needed, and download it to install in the ESA/WSA appliance device (see Replace SSL Certificate).

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

Step 4 Verify that the ESA/WSA can connect to the Clean interface of the Threat Grid Appliance over your network.

Step 5 Configure the ESA/WSA for Threat Grid Appliance integration. See 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:

a) Select **Security Services > File Reputation and Analysis**.
b) Click **Enable**.
c) Click **Edit Global Settings**.
d) In the File Analysis section, File Analysis is enabled by default. If you do not uncheck the **Enable File Analysis** check box, the File Analysis feature key will be activated after the next commit. Select the file types to send to the Cloud for analysis.
e) Configure the **Advanced Settings** for File Analysis as needed, according to the ESA or WSA guides:

- **File Analysis Server URL** - Choose Private Cloud.
- **Server** - URL of the on-premises Cisco Threat Grid appliance. Use the hostname, not the IP address, for this value and for the certificate.
- **SSL Certificate** - Upload a self-signed certificate that you have generated from your on-premises Cisco Threat Grid Appliance. 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.

Step 6 Submit and commit your changes.

Note the **File Analysis Client ID** that appears at the bottom of the page. This identifies the user that will be activated.

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

Step 7 Activate the new device user account on the Threat Grid Appliance:

a) Log into the Threat Grid Portal UI as Admin.
b) From the navigation bar drop-down menu next to your login name, choose Manage Users to open the Threat Grid Users page.
c) Open the User Details page for the device user account (you may need to use Search to find it).
d) The user status is currently *de-activated*. Click **Re-Activate User**.
e) On the confirmation dialog, click **Re-Activate** to confirm the action.

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

Connect AMP for Endpoints Private Cloud to Threat Grid Appliance

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

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

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

Procedure

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

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

Step 3 In the Threat Grid Appliance OpAdmin interface, Regenerate SSL Certificate on the Clean interface), to replace the default if needed, and download it to install on the AMP for Endpoints Private Cloud device.

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

- **Hostname** - Click **Configuration** > **Hostname** and note the hostname.
- **API Key** - Copy the **API Key** from the User Details page in the Threat Grid Portal (click the drop-down next to your login name and choose Manage Users, then navigate to the integration user account).

Note
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.

Step 4 Configure the AMP for Endpoints Private Cloud device for Threat Grid Appliance integration:

a) Select **Integrations > Threat Grid** and go to the **Connection to Threat Grid** section.
b) Complete the following fields:

- **Hostname** - Enter the Threat Grid Appliance hostname (obtained in previous step).
- **API Key** - Enter the Threat Grid API Key for the account to be used for integrations (obtained in previous step).
- **SSL Certificate** - Choose the Threat Grid Appliance SSL Certificate file.

c) Click **Save Configuration**.
d) Click **Test Connection**.

Once the connection test passes, you must run the Reconfiguration on the AMP for Endpoints Private Cloud to apply the changes. This allows AMP to talk to the Threat Grid Appliance, and you can now submit samples to Threat Grid.

However, you must complete the remaining steps to set up the Disposition Update Service to communicate disposition results to the Threat Grid Appliance. (For more information, see the user documentation for AMP for Endpoints Private Cloud.)

Step 5 In the Threat Grid Appliance, set up the Disposition Update Syndication Service:

a) Configure DNS, if needed.
b) Download or copy and paste the AMP for Endpoints Private Cloud SSL certificate to the Threat Grid Appliance so it can trust the integrating device. See Manage CA Certificates.
c) From the upper-right menu, choose **Manage FireAMP Integration** and specify the AMP Disposition Update Service URL and credentials (see Manage Disposition Update Syndication Service).
d) Click **Config**.