



Inbound and Outbound Connections

You can set up Threat Grid Appliance to communicate with other Cisco appliances, devices, and services using inbound and outbound connections. Encrypted SSL connections allow other appliances (such as Email Security Appliance and Web Security Appliance) to submit possible malware samples to Threat Grid for analysis (inbound connections).

In addition, Threat Grid Appliance can be set up to communicate with AMP for Endpoints Private Cloud for the Disposition Update Service through an outbound connection.

This appendix provides instructions for setting up both inbound and outbound connections.

- [Connecting ESA or WSA to Threat Grid Appliance, on page 1](#)
- [Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance, on page 3](#)

Connecting ESA or WSA to Threat Grid Appliance

Connections between the Threat Grid Appliance and Cisco Email Security Appliances (ESA) or Web Security Appliances (WSA) are enabled by the Cisco Sandbox API (CSA API) and are often referred to as CSA Integrations. The ESA/WSA must be registered with the Threat Grid Appliance before it can submit samples for analysis.

Before the 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.

ESA/WSA Documentation

See the instructions for Enabling and Configuring File Reputation and Analysis Services in the ESA/WSA product documentation:

- [Cisco Email Security Appliance User Guides](#)
- [Cisco Web Security Appliance User Guides](#)



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

Inbound Connection Overview

When setting up an inbound connection, the following tasks must be performed:

- **Set Up SSL Certificate** - 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 [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 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 product documentation to verify that the Threat Grid Appliance and ESA/WSA can communicate with each other (see [Connecting ESA or 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 de-activated. A Threat Grid Appliance administrator must manually activate the device user account before it can be used for submitting malware samples for analysis.

Configuring Inbound Connection

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



Note Refer to the ESA and WSA product documentation for more information about the tasks that must be performed.

Procedure

- Step 1** Set up and configure the Threat Grid Appliance as normal (no integration yet).
- Step 2** Check for updates and install, if necessary.

- Step 3** Set up and configure the ESA/WSA as normal (no integration yet).
- Step 4** The Threat Grid Appliance 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 Clean interface), to replace the default if needed, and download it to install on the ESA/WSA (see [Replacing SSL Certificates](#)).
- 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 will not work). Use the hostname; not the IP address.
- Step 5** Verify that the ESA/WSA can connect to the Clean interface of the Threat Grid Appliance over your network.
- Step 6** Configure the ESA/WSA for Threat Grid Appliance integration. See the ESA/WSA product documentation for complete instructions.
- Step 7** Submit and commit your changes.

Registration of your ESA/WSA with the Threat Grid Appliance occurs automatically when you submit the configuration for File Analysis.
- Step 8** Activate the new device user account on the Threat Grid Appliance:
- Log into the Threat Grid Portal UI as Admin.
 - Click the **Administration** tab and choose **Manage Users** to open the **Users** page.
 - Click the user name to open the **User Details** page for the device user account (you may need to use Search to find it).
 - The user status is currently **Inactive**. Click **Active** to activate the new account.
 - On the confirmation dialog, confirm the action.
- The ESA/WSA can now initiate connections with the Threat Grid Appliance.

Connecting 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 setup 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 that must be performed.

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 Admin UI, click the **Configuration** tab and choose **SSL**.
- Step 4** Regenerate the SSL certificate on the Clean interface to replace the default certificate, if needed, and make a copy of it to install on the AMP for Endpoints Private Cloud device (see [Regenerating SSL Certificates](#) for more information).
- Step 5** 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 **Administration** tab and choose **Manage Users**, and then navigate to the integration user account to locate the API key on the **User Details** page).
- Note**
This does not need to be the Admin user; it can be a user that was specifically created for this purpose on the Threat Grid Appliance.
- Step 6** Configure the AMP for Endpoints Private Cloud device for Threat Grid Appliance integration. See the ESA/WSA product documentation for complete instructions. The configuration will allow AMP to talk to the Threat Grid Appliance; you can now submit samples to Threat Grid.
- Step 7** 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):
- a) Configure DNS, if needed. See [Configuring DNS](#).
 - 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 [CA Certificates](#).
 - c) In the Threat Grid portal UI, specify the AMP Disposition Update Service URL and credentials and click **Add** (see [Managing Disposition Update Syndication Services](#)).

Managing Disposition Update Syndication Services

You can manage the Disposition Update Syndication Service for AMP for Endpoints Private Cloud appliance integrations in the Threat Grid portal. URLs can be added, edited, and deleted from the **Disposition Update Syndication Service** page.

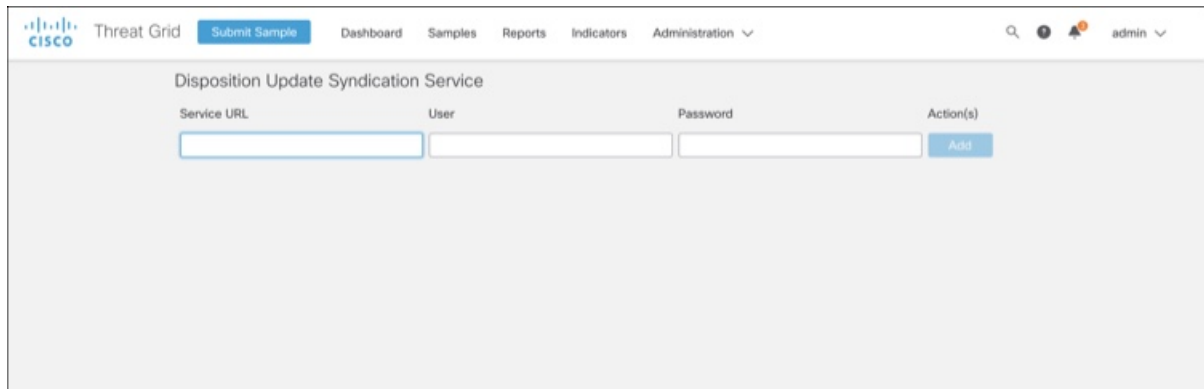


Note For more information about AMP for Endpoints Private Cloud appliance integrations, see [Connecting AMP for Endpoints Private Cloud to Threat Grid Appliance](#).

Procedure

- Step 1** In the Threat Grid portal, click the **Administration** tab and choose **Manage AMP Private Cloud Integration** to open the **Disposition Update Syndication Service** page.

Figure 1: Disposition Update Syndication Service



The screenshot shows the Cisco Threat Grid web interface. The top navigation bar includes the Cisco logo, 'Threat Grid', a 'Submit Sample' button, and links for 'Dashboard', 'Samples', 'Reports', 'Indicators', and 'Administration'. On the right, there are search, user, and notification icons, along with the 'admin' user name. The main content area is titled 'Disposition Update Syndication Service'. It contains a form with three input fields: 'Service URL', 'User', and 'Password'. To the right of these fields is an 'Add' button. Below the form, there is a large empty space.

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 **Add**.
