Inbound and Outbound Connections

You can set up Secure Malware Analytics 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 Secure Malware Analytics for analysis (inbound connections).

In addition, Secure Malware Analytics Appliance can be set up to communicate with Secure Endpoint 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 Secure Malware Analytics Appliance, on page 1
- Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance, on page 3

Connecting ESA or WSA to Secure Malware Analytics Appliance

Connections between the Secure Malware Analytics 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 Secure Malware Analytics Appliance before it can submit samples for analysis.

Before the ESA/WSA can be registered with the Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics Appliance.

  Depending on your requirements, you may need to regenerate the self-signed SSL certificate on the Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics Appliance. The ESA/WSA must be able to connect to the Clean interface of the Secure Malware Analytics Appliance over your network. Follow the instructions in the product documentation to verify that the Secure Malware Analytics Appliance and ESA/WSA can communicate with each other (see Connecting ESA or WSA to Secure Malware Analytics Appliance).

- **Complete the ESA/WSA File Analysis Configuration** - Enable the **File Analysis Security** service and configure the advanced settings.

- **Register ESA/WSA with Secure Malware Analytics Appliance** - An ESA/WSA that is configured according to the product documentation, registers itself automatically with the Secure Malware Analytics Appliance. Upon registration of the connecting device, a new Secure Malware Analytics 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 Secure Malware Analytics Appliance** - When the ESA/WSA or other integration connects and registers itself with the Secure Malware Analytics Appliance, a new Secure Malware Analytics user account is automatically created. The initial status of the user account is de-activated. A Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics 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 Secure Malware Analytics Appliance as the SAN or CN (the default certificate from the Secure Malware Analytics 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 Secure Malware Analytics Appliance over your network.

Step 6   Configure the ESA/WSA for Secure Malware Analytics 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 Secure Malware Analytics Appliance occurs automatically when you submit the configuration for File Analysis.

Step 8   Activate the new device user account on the Secure Malware Analytics Appliance:

a) Log into the Secure Malware Analytics Portal UI as Admin.

b) Click the **Administration** tab and choose **Manage Users** to open the **Users** page.

c) Click the user name to 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 **Inactive**. Click **Active** to activate th enew account.

e) On the confirmation dialog, confirm the action.

The ESA/WSA can now initiate connections with the Secure Malware Analytics Appliance.

Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance

The Secure Malware Analytics Appliance supports integration with Secure Endpoint Private Cloud for the Disposition Update Service as an outbound connection.

> **Note**   The Secure Malware Analytics Appliance Disposition Update Service and Secure Endpoint 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 Secure Endpoint Private Cloud documentation for more detailed information on the tasks that must be performed.

Procedure

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

Step 2 Set up and configure the Secure Endpoint Private Cloud as normal (no integration yet).

Step 3 In the Secure Malware Analytics 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 Secure Endpoint Private Cloud device (see Regenerating SSL Certificates for more information).

Step 5 Obtain the following information, which is needed to configure the integration in Secure Endpoint Private Cloud device:

- **Hostname** - Click **Configuration > Hostname** and note the hostname.

- **API Key** - Copy the **API Key** from the **User Details** page in the Secure Malware Analytics 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 Secure Malware Analytics Appliance.

Step 6 Configure the Secure Endpoint Private Cloud device for Secure Malware Analytics Appliance integration. See the ESA/WSA product documentation for complete instructions. The configuration will allow AMP to talk to the Secure Malware Analytics Appliance; you can now submit samples to Secure Malware Analytics.

Step 7 Complete the remaining steps to set up the Disposition Update Service to communicate disposition results to the Secure Malware Analytics Appliance (for more information, see the user documentation for Secure Endpoint Private Cloud):

  a) Configure DNS, if needed. See Configuring DNS.

  b) Download or copy and paste the Secure Endpoint Private Cloud SSL certificate to the Secure Malware Analytics Appliance so it can trust the integrating device. See CA Certificates.

  c) In the Secure Malware Analytics 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 Secure Endpoint Private Cloud appliance integrations in the Secure Malware Analytics portal. URLs can be added, edited, and deleted from the **Disposition Update Syndication Service** page.
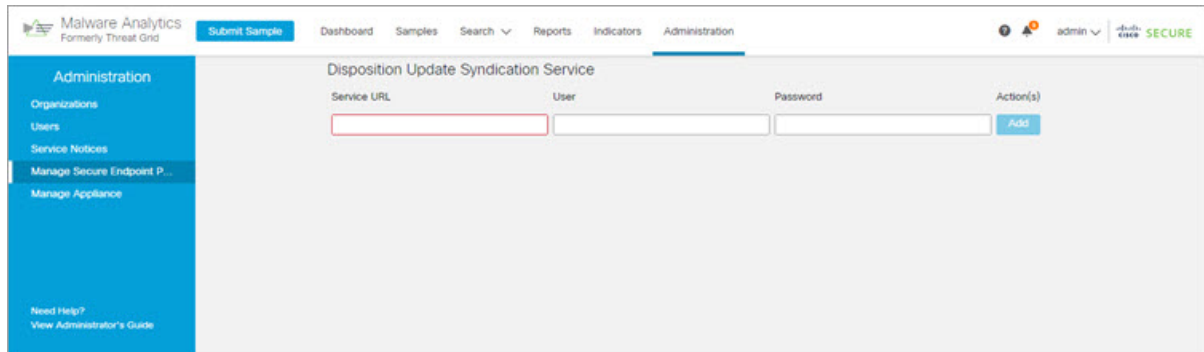
Note For more information about Secure Endpoint Private Cloud appliance integrations, see Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance.

Procedure

Step 1 In the Secure Malware Analytics portal, click the **Administration** tab and choose **Manage Secure Endpoint Private Cloud Integration** to open the **Disposition Update Syndication Service** page.

Figure 1: Disposition Update Syndication Service

Step 2 Enter the following information:

- **Service URL** - The Secure Endpoint Private Cloud URL.

- **User** - The admin user name.

- **Password** - The password provided by the Secure Endpoint configuration portal.

Step 3 Click **Add**.