Integration Guide for Cisco IronPort ESA
EventTracker v9.x and later

Publication Date: Feb 24, 2020
Abstract

This guide provides instructions to retrieve the Cisco ESA events by REST API. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Cisco ESA.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and Cisco ESA version 13.0 and later.

Audience

Administrators who are assigned the task to monitor Cisco ESA events using EventTracker.
Table of Contents

1. Overview ............................................................................................................................................ 3
2. Prerequisites ....................................................................................................................................... 3
3. Integrating Cisco ESA with EventTracker ....................................................................................... 3
   3.1 Enabling AsyncOS API .................................................................................................................. 3
   3.2 Enabling Message Tracking............................................................................................................ 4
   3.3 Creating New User .......................................................................................................................... 5
4. Forwarding logs from Cisco ESA REST API .................................................................................... 5
5. EventTracker Knowledge Packs ...................................................................................................... 7
   5.1 Saved Searches .............................................................................................................................. 7
   5.2 Alerts ............................................................................................................................................. 7
   5.3 Reports .......................................................................................................................................... 7
   5.4 Dashboards ................................................................................................................................... 8
6. Importing knowledge pack into EventTracker .................................................................................. 11
   6.1 Saved Searches ............................................................................................................................. 12
   6.2 Alerts ............................................................................................................................................ 13
   6.3 Parsing Rules ................................................................................................................................ 14
   6.4 Reports ......................................................................................................................................... 15
   6.5 Knowledge Objects ....................................................................................................................... 16
   6.6 Dashboards .................................................................................................................................. 17
7. Verifying knowledge pack in EventTracker ...................................................................................... 19
   7.1 Saved Searches ............................................................................................................................. 19
   7.2 Alerts ............................................................................................................................................ 19
   7.3 Parsing Rules ............................................................................................................................... 20
   7.4 Reports ......................................................................................................................................... 20
   7.5 Knowledge Objects ....................................................................................................................... 21
   7.6 Dashboards .................................................................................................................................. 22
1. Overview

The Cisco Email Security Appliance (ESA) is an email security gateway product. It is designed to detect and block a wide variety of email-borne threats, such as malware, spam and phishing attempts.

EventTracker, when integrated with Cisco ESA, collects logs from Cisco ESA and creates detailed reports, alerts, dashboards and saved searches. These attributes of EventTracker helps users to view the most critical and important information on a single platform.

Reports contain detailed overview of the activities like, incoming message summary, (Data, Loss and Protection) DLP and AMP (Advance Malware Protection) event summary, malicious or suspicious URL’s summary, and many more.

Alerts occur as soon as any critical events are triggered by Cisco ESA. With alerts, users will be able to get real time occurrences of events such as, DLP or AMP message detection, directly into their email services.

Major events such as DLP or AMP violation or messages blocked by Content Filters can be viewed on the EventTracker ‘dashboard’. These services will include information such as suspicious email attachments, Sender Base Reputation Scores (SBRS), Sender Domain Reputation (SDR), message risk Factor, etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- EventTracker knowledge packs are required.
- Microsoft PowerShell v5.0 or above.
- Create a new user profile to allow it to collect message tracking logs.

3. Integrating Cisco ESA with EventTracker

Although, there are various methods to export the Cisco ESA events, EventTracker recommends using: REST API.

(Note - The syslog push method generates multiline/event logs for a single event. As such log volume from ‘n’ number of events might not be a good option to collect and then co-relate logs with specific event.)

3.1 Enabling AsyncOS API

1. Log in to the web interface.

2. Choose Network > IP Interfaces.
3. Edit the Management interface.

**Note** You can enable AsyncOS API on any IP interface. However, Cisco recommends that you enable AsyncOS API on the Management interface.

You must not enable APIs on multiple management interface.

4. Under the AsyncOS API (Monitoring) section, depending on your requirements, select HTTP and the ports to use.

**Note** AsyncOS API communicates using HTTP / 1.1.

5. Submit and commit your changes.

### 3.2 Enabling Message Tracking

1. Click **Security Services > Message Tracking**.

   Use this path even if you do not plan to centralize this service.

2. Select **Enable Message Tracking Service**.

3. If you are enabling message tracking for the first time after running the System Setup Wizard, review the end-user license agreement, and click **Accept**.

4. Choose a Message Tracking Service:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Tracking</strong></td>
<td>Use message tracking on this appliance.</td>
</tr>
<tr>
<td><strong>Centralized Tracking</strong></td>
<td>Use a Security Management appliance to track messages for multiple Email Security appliances including this one.</td>
</tr>
</tbody>
</table>

5. (Optional) Select the check box to save information for rejected connections.

6. Submit and commit your changes.

**If you selected Local Tracking, choose who can access content related to DLP violations.**

1. Go to the **System Administration > Users** page.

2. Under **Access to Sensitive Information in Message Tracking**, click **Edit Settings**.
3. Select the roles for which you want to grant access to each type of sensitive information.

**Note** - Custom roles without access to Message Tracking can never view this information and thus are not listed.

4. Submit and commit your changes.

### 3.3 Creating New User

**(Note** - When you create a new user account, you assign the user to a predefined user role. E.g.: Help Desk User to help monitor the Message-Tracking events.)

1. Choose **System Administration > Users**.
2. Click **Add User**.
3. Enter a login name for the user. E.g. “EventTracker”.
4. Enter the user’s full name.
5. Select a predefined or custom user role. E.g. “Help Desk User”.
6. Enter a passphrase.
7. Submit and commit your changes.

### 4. Forwarding logs from Cisco ESA REST API

Contact the [EventTracker support](#) team and get the “Cisco_ESA_Integrator” executable file.

Once the executable application is received, right click on the file and select “Run as Administrator”.

Upon Running the Integrator, fill-in the given fields.

Follow the below procedures to configure Cisco ESA for EventTracker:

1. Right click the “EventTracker (Cisco_ESA)” executable file and “Run as administrator”.
2. Enter the **Username** and **Passcode**:
3. Enter “Base URL” and click “Add”.
(Note - If you have multiple ESA device platform (hence, multiple URL’s) repeat the process to add all the ESA devices you want EventTracker to monitor.) e.g.

4. Click “Validate” to verify the entered credentials.
5. Once validation success message pops-up, click “Submit” to finalize the configuration.
5. EventTracker Knowledge Packs

5.1 Saved Searches

- **Cisco ESA - AMP Messages**: Allows user to filter and search events specific to AMP messages/emails.
- **Cisco ESA - DLP Messages**: Allows user to filter and search events specific to DLP messages/emails.
- **Cisco ESA - Rejected Connections**: Allows user to filter and search events specific to rejected connections by Cisco ESA.
- **Cisco ESA - Content Filters**: Allows user to filter and search events specific to messages/emails flagged by Content filters.

5.2 Alerts

- **Cisco ESA - DLP Event has been detected**: This alert is triggered when a message/email content is flagged under DLP.
- **Cisco ESA - Message has been dropped by AMP**: This alert is triggered when a message/email content is flagged under AMP.
- **Cisco ESA - Message has been dropped by Content Filters**: This alert is triggered when a message/email content is flagged under Content Filters.
- **Cisco ESA - Message has been rejected**: This alert is triggered when a message/email is rejected by Cisco ESA.

5.3 Reports

- **Cisco ESA - AMP Messages**: This report will provide the summary of advanced malware protection (AMP) messages as detected in Cisco ESA. It will include details such as, Event log Time, Email direction, sender/recipient address, AMP details, etc.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>Email Direction</th>
<th>Sender Address</th>
<th>Recipient Address</th>
<th>Email Subject</th>
<th>Attachment</th>
<th>AMP Details</th>
<th>Sender Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>16/11/2018 11:01:08 AM</td>
<td>Cisco ESA 2 &amp; NIP/PLDT ELRA0</td>
<td>1753042</td>
<td>outgoing</td>
<td>cf_d rop_r@vm 30be00004.ibq a</td>
<td>6408@vm30be 0004.ibqa</td>
<td>Testing</td>
<td>ESA_AMP.ppr</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- **Cisco ESA – DLP Messages**: This report will provide the summary of Data Loss and Prevention (DLP) messages as detected in Cisco ESA. It includes details such as Event Log Time, Sender/recipient address, types of attachments with the specific email, DLP details, and so on.

- **Cisco ESA – Rejected connections**: Rejected connection report includes the details on emails/messages that have been rejected by Cisco ESA. This report has information such as for what reason a message was rejected.

---

### Cisco ESA – DLP Messages

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Message ID</th>
<th>Email Direction</th>
<th>Sender Address</th>
<th>Recipient Address</th>
<th>Email Subject</th>
<th>Attachment</th>
<th>DLP Details</th>
<th>DLP Risk Factor</th>
<th>Violation Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>16/11/2013 11:01:00 PM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>050</td>
<td>Outgoing</td>
<td>de_dscp_in@vm 300sd0004.bca</td>
<td>6406@vm:300sd0004.bca</td>
<td>Testing</td>
<td>dlvry_license</td>
<td>violationSeverity = HIGH</td>
<td>6</td>
<td>HIGH</td>
</tr>
<tr>
<td>16/11/2013 11:05:00 AM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>1763042</td>
<td>Incoming</td>
<td>de_dscp_in@vm 300sd0004.bca</td>
<td>6406@vm:300sd0004.bca</td>
<td>Testing</td>
<td>Zombies.pdf</td>
<td>violationSeverity = HIGH</td>
<td>6</td>
<td>HIGH</td>
</tr>
<tr>
<td>16/11/2013 11:01:00 AM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>850</td>
<td>Outgoing</td>
<td>de_dscp_in@vm 300sd0004.bca</td>
<td>6406@vm:300sd0004.bca</td>
<td>Testing</td>
<td>Lab_Guide.doc</td>
<td>violationSeverity = HIGH</td>
<td>6</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

---

### Cisco ESA – Rejected connections

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Host Name</th>
<th>Device Serial Number</th>
<th>Sender IP Address</th>
<th>Sender Group</th>
<th>Message Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/05/2020 04:39:04 PM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>Name unresolved</td>
<td>848F86B5EEF-BR50TW1</td>
<td>10.76.73.112</td>
<td>UNKNOWNLIST</td>
<td>REJECTED</td>
<td>(1/140) SMTP authentication failed for user fail using AUTH mechanism PLAIN with profile failAuthServer/exists.</td>
</tr>
<tr>
<td>02/05/2020 04:39:05 PM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>Name unresolved</td>
<td>848F86B5EEF-BR50TW1</td>
<td>205.100.20.253</td>
<td>UNKNOWNLIST</td>
<td>REJECTED</td>
<td>(1/175) REJECT sender group BLACKLIST match host [-10.0.2.0] SBS-44 country None</td>
</tr>
<tr>
<td>02/05/2020 04:39:12 PM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>Name unresolved</td>
<td>848F86B5EEF-BR50TW1</td>
<td>192.165.89.27</td>
<td>UNKNOWNLIST</td>
<td>REJECTED</td>
<td>(1/1651) TLS failed. Response: (336190761, error 1408A0C1:SSL routines SSL3_GET_CIPHER_LIST 0 no shared cipher).</td>
</tr>
<tr>
<td>02/05/2020 04:51:57 PM</td>
<td>CSCO_ESA2@1NTPL0TDLR48</td>
<td>Name unresolved</td>
<td>848F86B5EEF-BR50TW1</td>
<td>172.16.1.226</td>
<td>UNKNOWNLIST</td>
<td>REJECTED</td>
<td>(1/1690) Message 276 contains invalid recipient address: Invalid character in address: &quot; &quot;</td>
</tr>
</tbody>
</table>

---

### 5.4 Dashboards

- **Cisco ESA Events by email direction**
- **Cisco ESA DLP Events**

  ![Cisco ESA DLP Events](image)

  **Figure 4**
• Cisco ESA incoming email by Source IP address

![Cisco ESA incoming email by Source IP address](image1)

**Figure 5**

• Cisco ESA message tracking events

![Cisco ESA message tracking events](image2)

**Figure 6**
6. Importing knowledge pack into EventTracker

How to get Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

1. Press “\ + R”.
2. Now, type “%et_install_path%\Knowledge Packs” and press “Enter”.
   (Note – If, not able to locate the file path as mentioned above, please contact EventTracker support to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the EventTracker Control Panel.
2. Double click Export-Import Utility.

Figure 7
3. Click the **Import** tab.

### 6.1 Saved Searches

1. Once you have opened “**Export Import Utility**” via “**EventTracker Control Panel**”, click the **Category** option, and then click **Browse** ...
2. Navigate to the knowledge pack folder and select the file with extension “.iscat”, e.g. “Categories_Cisco_ESA.iscat” and then click “**Import**”.
EventTracker displays a success message:

![Image](image1.png)

**Figure 10**

### 6.2 Alerts

1. Once you have opened “**Export Import Utility**” via “**EventTracker Control Panel**”, click **Alert** option, and then click **Browse** …
2. Navigate to the knowledge pack folder and select the file with extension “.isalt”, e.g. “**Alerts_Cisco_ESA.isalt**” and then click **“Import”**:

![Image](image2.png)

**Figure 11**
Integration Guide for Cisco IronPort ESA

EventTracker displays a success message:

![Success Message](image)

Figure 12

6.3 Parsing Rules

1. Once you have opened “Export Import Utility” via “EventTracker Control Panel”, click the “Token Value” option, and then click Browse ...

2. Navigate to the knowledge pack folder and select the file with extension “.istoken”, e.g. “Parsing Rules_Cisco_ESA.istoken” and then click “Import”:

![Import Utility](image)

Figure 13
6.4 Reports

1. In EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and choose “New (*.etcrx)”: 

![Figure 14](image)

2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click “Select File” button and navigate to knowledge pack folder and select file with extension “.etcrx”, e.g. “Reports_Cisco_ESA.etcrx”.

![Figure 15](image)
3. Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import**.

![Image of Import Button](image1.png)

**Figure 26**

EventTracker displays a success message:

![Image of Success Message](image2.png)

**Figure 17**

### 6.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager web interface.

![Image of Admin Option](image3.png)

**Figure 38**

2. Next, click “**import object**”: 
3. A pop-up box will appear, click “Browse” in that and navigate to knowledge packs folder (type “%et_install_path%\Knowledge Packs” in navigation bar) with the extension “.etko”, e.g. “KO_Cisco_ESA.etko” and then click “Upload”.

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click “Import”:

6.6 Dashboards

1. Login to EventTracker manager web interface.
2. Navigate to Dashboard → My Dashboard.
3. In “My Dashboard”, Click Import:
4. Select the **browse** button and navigate to knowledge pack folder (type “%et_install_path%\Knowledge Packs” in navigation bar) where “.etwd”, e.g. “Dashboards_Cisco_ESA.etwd” is saved and click “Upload”.

5. Wait while EventTracker populates all the available dashboards. Now, choose “**Select All**” and click “**Import**”.

---

**Figure 22**

**Figure 23**

**Figure 24**
7. Verifying knowledge pack in EventTracker

7.1 Saved Searches

1. Login to EventTracker manager web interface.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand “Cisco ESA” group folder to view the imported categories:

![Category Tree](image)

7.2 Alerts

1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.
2. In search box enter “<search criteria> e.g. “Cisco ESA” and then click Search.
   EventTracker displays an alert related to “Cisco ESA”: 
7.3 Parsing Rules

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rule.
2. In the Parsing Rule tab, click on the “Cisco ESA” group folder to view the imported Token Values.

7.4 Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.
2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the “**Cisco ESA**” group folder to view the imported reports.

![Figure 30](image)

**7.5 Knowledge Objects**

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the “**Cisco ESA**” group folder to view the imported Knowledge objects.

![Figure 31](image)
7.6 Dashboards

1. In the EventTracker web interface, Click Home and select “**My Dashboard**”.

![Figure 9](image)

2. Select “**Customize daslets**” and type “**ESA**” in the search bar.

![Figure 33](image)

![Figure 34](image)