Introduction

By integrating the Cisco® Web Security Appliance (WSA) and Cisco Cognitive Threat Analytics (CTA) you can reduce the time to discover the spread of attacks. This integration helps to spot the symptoms of infection using both trust modelling and algorithms that detect behavioral anomalies. It also uses machine learning to adapt over time. Therefore, no rule sets are required, as it discovers threats on its own. CTA license is in built WSA-AMP-LIC= one can accomplish integration of WSA and CTA which in turn will take care of the after phase of the attack continuum.
This document describes how to configure a Cisco Web Security Appliance to upload log files to the Cisco Cognitive Threat Analytics system. When the log files have been uploaded to the system, CTA analyzes the data and reports findings to the CTA portal.

**Note:** The Cisco Content Security Management Appliance doesn’t support W3C logs. Therefore, we need to configure all the WSA appliances individually.

**Cisco Software/Solution Requirements**

- Cognitive Threat Analytics
- Web Security Appliance
- Security Management Appliance
For Cognitive Threat Analytics, you need:

- Access to the CTA Portal (https://cognitive.cisco.com/)
- Customer login credentials (you can submit a request for an evaluation if needed)
- Login credentials for Cloud Web Security, AMP for Endpoints, or Cisco SSO

Note:

- The username and password are case sensitive.
- In order to get user information in CTA portal please make sure that WSA is integrated with Active Directory or LDAP Server.
For the Web Security Appliance, you need:

- Admin access
- Host name or IP address of the WSA
- WSA software version 8.8 or later

All hardware and virtual platforms are supported. The WSA must be connected directly to the Internet without any additional upstream proxy. The SCP host (etr.cloudsec.sco.cisco.com with SCP port 22) should be accessible.

**Note:** When creating subscription logs on the WSA for CTA, the proxy process will restart and authentication cache will be cleared. Therefore, it is advisable to make the changes during a scheduled maintenance window.

## Configuration

**Configuring Cognitive Threat Analytics:**

- Login in to [https://cognitive.cisco.com/](https://cognitive.cisco.com/)
- Click the customer login on the top right
- Log in with your credentials
- As a first-time user, you will get an option to choose either SCP or HTTPS
Select SCP, or go to Options > Device Account > Add Device Account

Give a meaningful device name such as “WSA-Lab” and click on ADD ACCOUNT.

Note: Now we need to log in to the Cisco Web Security Appliance and use this information to create a connection to CTA.
Configuring the Web Security Appliance:

1. Log in to the Cisco WSA: https://wsa_hostname:8443
2. If needed, accept the insecure HTTPS certificate to proceed.
3. Log in as admin.
5. Click Add Log Subscription.
6. In the Log Type pull-down menu, select W3C Logs.
7. In the Log Name field, enter a descriptive name for the log directory.
8. If your WSA is running software older than AsyncOS 11.0
   a. Remove the pre-selected Log Fields by selecting all items in the Selected Log Fields box and clicking Remove
   b. In the Available Log Fields box, select the following items. If not available, in the Custom Fields box, enter the following items, using line breaks to separate them:

   timestamp
cs-bytes
x-elapsed-time
sc-bytes
c-ip
c-body-size
cs-username
cs(User-Agent)
c-port
cs-mime-type
s-ip
cs-method
s-port
cs-http-status
cs-url
cs(Referer)
cs(User-Agent)
cs-mime-type
cs-method
sc-bytes
sc-body-size
sc-http-status
cs(User-Agent)
cs-mime-type
cs-method
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
cs(Referer)
sc(byes)
sc-title
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
   c. When all the items are entered, click Add >> to add them to the Selected Log Fields box
   d. In the File Name field, enter w3c_log.
   e. Enable compression by checking Log Compression.
   f. For Retrieval Method, select SCP on Remote Server.
g. In the SCP Host field, enter the SCP host provided in Cisco CTA console: `etr.cloudsec.sco.cisco.com`

h. In the SCP Port field, enter 22.

i. In the Directory field, enter `/upload`.

j. In the Username field, enter the username generated for your device in Cisco CTA. The device username is case sensitive and different for each proxy device.

k. Proceed to Step 10.
9. If your WSA is running AsyncOS 11.0:
   a. Select the CTA Template check box to automatically configure most of the remaining settings:
b. Ensure that the following fields appear in the selected Log Fields box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Field</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>cs-bytes</td>
<td>sc(Location)</td>
</tr>
<tr>
<td>x-elapsed-time</td>
<td>sc-bytes</td>
<td>sc-result-code</td>
</tr>
<tr>
<td>c-ip</td>
<td>sc-body-size</td>
<td>x-amp-sha</td>
</tr>
<tr>
<td>cs-username</td>
<td>cs(User-Agent)</td>
<td>x-amp-verdict</td>
</tr>
<tr>
<td>c-port</td>
<td>cs-mime-type</td>
<td>x-amp-malware-name</td>
</tr>
<tr>
<td>s-ip</td>
<td>cs-method</td>
<td>x-amp-score</td>
</tr>
<tr>
<td>s-port</td>
<td>sc-http-status</td>
<td></td>
</tr>
<tr>
<td>cs-url</td>
<td>cs(Referer)</td>
<td></td>
</tr>
</tbody>
</table>

c. For Retrieval Method, in the Username field, enter the Username field generated for your device in the Cisco ScanCenter. The device username is case sensitive and different for each proxy device.

10. Select the Enable Host Key Checking checkbox, and select the Automatically Scan radio button.

11. In the Rollover by File Size field, enter 500M.

12. In the Rollover by Time pull-down, select Custom Time Interval.

13. In the Rollover every field, enter 55m (as an example).

<table>
<thead>
<tr>
<th>Number of Users Behind Proxy</th>
<th>Recommended Upload Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown or less than 2000</td>
<td>55 minutes</td>
</tr>
<tr>
<td>2000 to 4000</td>
<td>30 minutes</td>
</tr>
<tr>
<td>4000 to 6000</td>
<td>20 minutes</td>
</tr>
<tr>
<td>More than 6000</td>
<td>10 minute</td>
</tr>
</tbody>
</table>

14. Click Submit.
15. The WSA Management console displays a public SSH key. Copy and paste the whole key, including the “ssh-dss" at the beginning, into the device account in Cisco ScanCenter. Successful authentication between your proxy device and CTA System will allow log files from your proxy device to be uploaded to the CTA system for analysis.

```
Log Subscriptions
```

16. Copy the SSH Key in a notepad file

**Note:** Please make sure that you do the same in the maintenance window.

```
Uncommitted Changes
```

17. Give a meaningful comment and commit the changes.

**Switch to CTA Console:**

- Switch to the CTA console and copy the SSH keys. Then click **Finish**.
• This will provision the WSA.

• After the device is provisioned you will be able to see the status change from Provisioning to READY.

• After correlating the logs, CTA will be able to show Confirmed and Detected Incidents with a complete analysis.
Troubleshooting

To test your connection, force the WSA to attempt an immediate uploading of the logs:

1. Navigate to the Log Subscriptions page.
2. For the subscription you want to test, select the Rollover checkbox.
3. Click the Rollover Now button.

This concludes our configuration on Cisco Web Security Appliance and Cisco Cognitive Threat Analytics.