Integrate Cisco IronPort Web Security Appliance (WSA)
Abstract

This guide provides instructions to configure Cisco IronPort Web Security Appliance (WSA) to send the events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise and Cisco IronPort Web Security Appliance AsyncOS v7.1 and later.

Audience

Cisco IronPort Web Security Appliance users, who wish to forward events to EventTracker manager.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract.................................................................................................................................................. 1  
Scope.................................................................................................................................................. 1  
Audience............................................................................................................................................. 1  
About Cisco WSA.................................................................................................................................... 3  
Prerequisites.......................................................................................................................................... 3  
Syslog Configuration for forwarding logs to EventTracker................................................................. 3  
EventTracker Knowledge Pack (KP)....................................................................................................... 5  
  Categories .......................................................................................................................................... 6  
  Alerts .................................................................................................................................................. 6  
  Flex reports ...................................................................................................................................... 6  
Import Cisco IronPort WSA Knowledge pack into EventTracker .......................................................... 8  
  Categories .......................................................................................................................................... 9  
  Alerts ................................................................................................................................................ 11  
  Templates ........................................................................................................................................ 12  
  Flex Reports ................................................................................................................................... 13  
Verify Cisco IronPort WSA knowledge pack in EventTracker............................................................... 15  
  Categories ........................................................................................................................................ 15  
  Alerts ................................................................................................................................................ 16  
  Templates ........................................................................................................................................ 16  
  Reports ........................................................................................................................................... 17  
Create Dashboards in EventTracker........................................................................................................ 19  
  Schedule Reports............................................................................................................................. 19  
  Create Dashlets............................................................................................................................... 22  
  Sample dashboard ........................................................................................................................... 27
About Cisco WSA

Cisco WSA provides enhanced threat defense, malware protection, application visibility and control, insightful reporting, and secure mobility. The Cisco Web Security Appliance (WSA) is an appliance combining all of these forms of protection and more in a single solution. The WSA also helps to secure and control web traffic, while simplifying deployment and reducing costs.

EventTracker monitors the allowed and blocked web traffic of Cisco WSA and gives us alert when blocked web traffic is generated. It also provides report for allowed web traffic which will help you to analyze the web usage of users.

Prerequisites

- EventTracker Enterprise should be installed.
- Firewall between EventTracker enterprise and Cisco WSA should be closed or made exception for port 514.
- You should have administrator access to Cisco WSA for changes in syslog configuration.

Syslog Configuration for forwarding logs to EventTracker

1. Connect to your Iron Port device.
2. Click the System Administration tab.
3. In the left pane, click Log Subscriptions.
4. In the center pane, click Add Log Subscription.
5. In the Log Type field, select Access Logs.
6. In the Log Style section, select Squid.
7. Provide a File Name if one is not provided by default.
8. In the **Retrieval Method** section, select **Syslog Push**, and then supply the following information for your LEM appliance:
   - **Hostname**: Enter the hostname of EventTracker Manager Machine.
   - **Protocol**: Select UDP.
   - **Facility**: Select a Facility and note it. You will use this when you configure the connector on your LEM Manager.
NOTE: The "logging facility" in Cisco products is equivalent to the local facility on the logging destination plus 16. For example, the default local facility used in the IronPort Web Security connector is local 7, so the corresponding logging facility in Iron Port would be 23.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker, Alerts and Reports can be configured.

The following Knowledge Packs are available in EventTracker v7.x to support Cisco IronPort WSA monitoring:
Categories

- **Cisco IronPort WSA: Web access allowed**: All Syslog messages logged by Cisco WSA occurs, when user accesses the website properly.

- **Cisco IronPort WSA: Web access blocked**: All Syslog messages logged by Cisco WSA occurs, when the user access is blocked for the website.

- **Cisco IronPort WSA: URL filtering**: All Syslog messages logged by Cisco WSA occurs when website access is blocked by URL content filtering module of Cisco WSA.

- **Cisco IronPort WSA: Incomplete requests**: All Syslog messages logged by Cisco WSA occurs, when incomplete requests are received by Cisco WSA.

Alerts

- **Cisco IronPort WSA: Web access blocked**: This alert is generated when Web access is blocked from Cisco IronPort WSA.

Flex reports

- **Cisco IronPort WSA-Web access allowed**: This flex report provides information related to web access allowed by Cisco WSA. This report gives information of user (Client IP address and authentication user), requested URL details (URL, HTTP method, HTTP status code) and server accessed details.

![Figure 3](image3.png)

![Figure 4](image4.png)
• **Cisco IronPort WSA-Web access blocked:** This flex report provides information related to web access blocked by Cisco WSA. This report gives information of user (Client IP address, authenticated users and identity) and requested URL details (URL, HTTP methods).

![Figure 5](image1)

<table>
<thead>
<tr>
<th>Event Date</th>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/16/2010</td>
<td>22:06:59</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td>syslog</td>
</tr>
</tbody>
</table>

![Figure 6](image2)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Client IP</th>
<th>HTTP Method</th>
<th>HTTP Status Code</th>
<th>Authenticated User</th>
<th>Requested URL</th>
<th>Identity</th>
<th>Data Security Policy</th>
<th>External DLP Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/01/2018 05:30:48 PM</td>
<td>144.146.104.79</td>
<td>CONNECT</td>
<td>403</td>
<td><a href="mailto:james@contoso.com">james@contoso.com</a></td>
<td><a href="https://facebook.com">https://facebook.com</a></td>
<td>Conference_Rooms</td>
<td>DSFPolicy_01</td>
<td>eUPPolicy_01</td>
</tr>
<tr>
<td>09/01/2018 05:30:48 PM</td>
<td>144.146.104.79</td>
<td>CONNECT</td>
<td>403</td>
<td><a href="mailto:jones@contoso.com">jones@contoso.com</a></td>
<td><a href="https://yahoo.com">https://yahoo.com</a></td>
<td>Conference_Rooms</td>
<td>DSFPolicy_02</td>
<td>eUPPolicy_02</td>
</tr>
<tr>
<td>09/01/2018 05:30:48 PM</td>
<td>144.144.11.524</td>
<td>CONNECT</td>
<td>403</td>
<td><a href="mailto:dave@contoso.com">dave@contoso.com</a></td>
<td><a href="https://https://www.google.com">https://https://www.google.com</a></td>
<td>Conference_Rooms</td>
<td>DSFPolicy_03</td>
<td>eUPPolicy_03</td>
</tr>
<tr>
<td>09/01/2018 05:30:48 PM</td>
<td>144.144.11.524</td>
<td>CONNECT</td>
<td>403</td>
<td><a href="mailto:phil@contoso.com">phil@contoso.com</a></td>
<td><a href="https://https://www.google.com">https://https://www.google.com</a></td>
<td>Conference_Rooms</td>
<td>DSFPolicy_04</td>
<td>eUPPolicy_04</td>
</tr>
<tr>
<td>09/01/2018 05:30:48 PM</td>
<td>144.146.104.79</td>
<td>CONNECT</td>
<td>403</td>
<td><a href="mailto:Mickey.g@contoso.com">Mickey.g@contoso.com</a></td>
<td><a href="https://microsoft.com">https://microsoft.com</a></td>
<td>Conference_Rooms</td>
<td>DSFPolicy_05</td>
<td>eUPPolicy_05</td>
</tr>
</tbody>
</table>

• **Cisco IronPort WSA: URL filtering:** This flex report provides information related to web access blocked by URL filtering module of Cisco WSA. This report gives information about user (authenticated user, client IP), requested URL and its category (like social networking, advertisement, etc).

![Figure 7](image3)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Client IP</th>
<th>HTTP Method</th>
<th>HTTP Status Code</th>
<th>Authenticated User</th>
<th>Requested URL</th>
<th>URL category</th>
<th>HTTP Method</th>
<th>HTTP Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>10.78.33.20</td>
<td>GET</td>
<td>403</td>
<td>Branch_HomeBanking_PCs</td>
<td><a href="https://microsoft.com">https://microsoft.com</a></td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>10.78.33.20</td>
<td>GET</td>
<td>403</td>
<td>Branch_HomeBanking_PCs</td>
<td><a href="https://microsoft.com">https://microsoft.com</a></td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>10.78.33.20</td>
<td>GET</td>
<td>403</td>
<td>Branch_HomeBanking_Pcs</td>
<td><a href="https://microsoft.com">https://microsoft.com</a></td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>10.78.33.20</td>
<td>GET</td>
<td>403</td>
<td>Branch_HomeBanking_PCs</td>
<td><a href="https://microsoft.com">https://microsoft.com</a></td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
</tbody>
</table>

![Figure 8](image4)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Requested URL</th>
<th>URL category</th>
<th>HTTP Method</th>
<th>HTTP Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>Branch_HomeBanking_PCs</td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>Branch_HomeBanking_PCs</td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>Branch_HomeBanking_PCs</td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
<tr>
<td>09/16/2018 05:22:52 PM</td>
<td>Branch_HomeBanking_PCs</td>
<td>NV_comp</td>
<td>GET</td>
<td>403</td>
</tr>
</tbody>
</table>

• **Cisco IronPort WSA: Incomplete requests:** This flex report provides information related to incomplete requests captured by Cisco WSA which gives information about URL requested and client details (user and IP address details).
Import Cisco IronPort WSA Knowledge pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click the Import tab.
Figure 11

Import Category, Alert, Template and Flex Reports as given below sequence.

Category > Alert > Template > Flex Reports

Categories

1. Click Category option, and then click the browse button.
2. Locate All Cisco IronPort WSA group of Categories.iscat file, and then click the Open button.

3. Click the Import button to import the categories.

EventTracker displays success message.

4. Click OK, and then click the Close button.
Alerts

1. Click **Alert** option, and then click the browse button.

![Image of Export Import Utility]

**Figure 14**

2. Locate **All Cisco IronPort WSA group of Alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.

EventTracker displays success message.

![Image of Success Message]

**Figure 15**
4. Click **OK**, and then click the **Close** button.

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on the **Import** icon.

3. Click on the **Browse** button.

4. Locate **Cisco IronPort WSA token template.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Flex Reports**

1. Click **Report** option, and then click the browse button.
2. Locate **All Cisco IronPort WSA group of Flex Report.issch** file, and then click the **Open** button.

3. To import reports, click the **Import** button.

   EventTracker displays success message.

   ![Figure 20](image)

4. Click **OK**, and then click the **Close** button.
Verify Cisco IronPort WSA knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In Category Tree, expand IronPort WSA group folder to view the imported categories.

![Figure 22](image-url)
EventTracker: Integrating Cisco IronPort Web Security Appliance (WSA)

Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search field, enter ‘Cisco IronPort WSA’, and then click the Go button.

Alert Management page will display all the imported Cisco IronPort WSA alerts.

4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays message box.

Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab.
3. In Token Value Group Tree to view imported token values, scroll down and click Cisco IronPort WSA group folder.

Imported token template is displayed in the template pane.
Reports

1. Logon to EventTracker Enterprise.

2. Click the Reports menu, and then select Configuration.

3. In Reports Configuration pane, select Defined option.

4. In search box enter ‘Cisco IronPort WSA’, and then click the Search button.

   (OR)

   In Report groups pane, select Cisco IronPort WSA folder, and then select Defined option.

   EventTracker displays Flex reports of Cisco IronPort WSA.
Here you can find imported defined reports such as 'Cisco IronPort WSA – Web access allowed, Web access blocked' report.
Create Dashboards in EventTracker

Schedule Reports

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

1. Open **EventTracker** in browser and logon.

2. Navigate to **Reports>Configuration**.

![Figure 27](image-url)
3. Select **Cisco IronPort WSA** in report groups. Check **Defined** dialog box.

4. Click on ‘**schedule**’ icon to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check “Persist data in Eventvault Explorer” box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

### Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to **Dashboard>Flex**. Flex Dashboard pane is shown.

4. Click to add a new dashboard. Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.

6. Click the icon  to configure a new Flex dashlet.
   Widget configuration pane is shown.
7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.
   Evaluated chart is shown.
16. If satisfied, click **Configure** button.

17. Click ‘customize’ 📦 to locate and choose created dashlet.

18. Click 📦 to add dashlet to earlier created dashboard.
Sample dashboard

1. Cisco WSA-Web access by HTTP method

   Configuration-

   **DATA SOURCE:** Cisco IronPort WSA-Web access allowed report  
   **WIDGET TITLE:** Cisco WSA Web access by HTTP method  
   **CHART TYPE:** Donut  
   **AXIS LABELS [X-AXIS]:** HTTP Method

![Cisco WSA Web access by HTTP method](image-url)

*Figure 37*
2. Cisco WSA-Web access by URL

**Configuration:**

**DATA SOURCE:** Cisco IronPort WSA-Web access allowed report

**WIDGET TITLE:** Cisco WSA-Web access by URL

**CHART TYPE:** Donut

**AXIS LABELS [X-AXIS]:** Requested URL

![Cisco WSA Web Access by URL Chart](image-url)

*Figure 38*
3. Cisco WSA-Web access by user

Configuration-

DATA SOURCE: Cisco IronPort WSA-Web access allowed report
WIDGET TITLE: Cisco WSA-Web access by URL
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: authenticated users

Figure 39
4. Cisco WSA-Web access by client IP

Configuration-

DATA SOURCE: Cisco IronPort WSA-Web access allowed report
WIDGET TITLE: Cisco WSA Web access by client IP
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Client IP

Figure 40