

# Integrate Cisco IronPort Web Security Appliance (WSA)

---

*EventTracker Enterprise*

# 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.

Log Subscription	
Log Type:	<input type="text" value="Access Logs"/>
Log Name:	<input type="text"/> <small>(will be used to name the log directory)</small>
Rollover by File Size:	<input type="text"/> Maximum <small>(Add a trailing K or M to indicate size units)</small>
Rollover by Time:	<input type="text" value="None"/>
Log Style:	<input checked="" type="radio"/> Squid <input type="radio"/> Apache <input type="radio"/> Squid Details
Custom Fields (optional):	<input type="text"/> <a href="#">Custom Fields Reference</a>
File Name:	<input type="text"/>
Log Compression:	<input type="checkbox"/> Enable
Log Exclusions (Optional):	<input type="text"/> <small>(Enter the HTTP status codes of transactions that should not be included in the Access Log)</small>

Figure 1

- 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.

The screenshot shows the configuration page for Syslog Push in the EventTracker interface. The page has a breadcrumb trail: Netsuite > Orange > IronPort fr > Air France > Key Request Form. On the left, there is a navigation menu with categories: Feature Keys, Shutdown/Reboot, Upgrades (with sub-items: Upgrade Settings, System Upgrade), System Setup (with sub-items: System Setup Wizard, Next Steps). The main content area is titled 'Retrieval Method:' and contains three sections: 'FTP on blabber.run' (with 'Maximum Number of Files' set to 10), 'FTP on Remote Server' (with 'Maximum Time Interval Between Transferring' set to 3600 seconds and fields for FTP Host, Directory, Username, and Password), and 'SCP on Remote Server' (with 'Maximum Time Interval Between Transferring' set to 3600 seconds, 'Protocol' set to SSH1, and fields for SCP Host, Directory, and Username). Below these is an 'Enable Host Key Checking' section with options 'Automatically Scan' (selected) and 'Enter Manually'. At the bottom, the 'Syslog Push' section is highlighted with a red box and contains: 'Syslog Push' (checked), 'Hostname' (192.168.1.118), 'Protocol' (UDP selected, TCP unselected), and 'Facility' (LOCAL 23). 'Cancel' and 'Submit' buttons are at the bottom.

Figure 2

9. Click **Submit**.

**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.

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 2:26:58 PM	12	PNPL-2-KP / Contoso...	N/A	N/A	syslog
<b>Event Type:</b> Warning <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Aug 18 01:10:15 md-hq-wsa1 Aug 18 01:10:14 Access_Logs_to_Slater: Info: 1471497014.683 75 10.78.33.28 TCP_MISS/200 3022 POST http://10.16.14.10/scs:RPC.rpc_pullAPI - DIRECT/10.16.14.10 application/octet-stream DEFAULT_CASE_12-inLighten_Appliances-inLighten_Appliances-DefaultGroup-NONE-NONE-DefaultGroup <nc,-3.5,0,-,0,0,1,-,-,-,0,0,-,-,-,nc,-,Unknown,-,Unknown,Unknown,-,322.35,0,-,Unknown,-,-,-,-,-> -			

Figure 3

Cisco IronPort WSA: Web access allowed									
LogTime	Client IP	Requested URL	HTTP Method	HTTP Status Code	Authenticated User	Server Accessed	Server Name	Response Size	MIME Type
09/01/2016 05:20:46 PM	144.145.27.28	https://forbes.com	POST	200	john@contoso.com	DIRECT	forbes.com	324	text/html
09/01/2016 05:20:46 PM	144.145.30.28	https://google.com	POST	200	mike@contoso.com	DIRECT	google.com	3034	application/octet-stream
09/01/2016 05:20:46 PM	144.146.104.79	https://bankofamerica.com	CONNECT	200	james@contoso.com	DIRECT	bankofamerica.com	39	-
09/01/2016 05:20:46 PM	144.145.27.28	http://eventtracker.com	POST	200	jones@contoso.com	DIRECT	eventtracker.com	348	text/html
09/01/2016 05:20:46 PM	144.145.19.28	http://yahoo.com	GET	200	daniel@contoso.com	DIRECT	yahoo.com	34397	image/png

Figure 4

- 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).

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 2:26:58 PM	12	PNPL-2-KP / Contoso...	N/A	N/A	syslog

**Event Type:** Warning  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 Aug 18 01:10:15 md-hq-wsa1 Aug 18 01:10:14 Access\_Logs\_to\_Slater: Info: 1471497004.759 9 144.146.103.72 TCP\_DENIED/407 0 CONNECT tunnel://urs.microsoft.com:443/ - NONE/ - - OTHER-NONE-Conference\_Rooms-NONE-NONE-NONE-NONE <.....0.00,0.....>

Figure 5

Cisco IronPort WSA: Web access blocked									
LogTime	Client IP	HTTP Method	HTTP Status Code	Authenticated User	Requested URL	Identity	Data Security Policy	External DLP Policy	
09/01/2016 05:20:46 PM	144.146.104.79	CONNECT	407	james@contoso.com	https://facebook.com	Conference_Rooms	DSPPolicy_01	eDLPPolicy_01	
09/01/2016 05:20:46 PM	144.146.104.79	CONNECT	407	jones@contoso.com	https://yahoo.com	Conference_Rooms	DSPPolicy_02	eDLPPolicy_02	
09/01/2016 05:20:48 PM	144.144.11.124	CONNECT	407	daniel@contoso.com	tunnel//hangouts.google.com:443/	Conference_Rooms	DSPPolicy_03	eDLPPolicy_03	
09/01/2016 05:20:48 PM	144.144.11.124	CONNECT	407	phil.b@contoso.com	tunnel//hangouts.google.com:443/	Conference_Rooms	DSPPolicy_04	eDLPPolicy_04	
09/01/2016 05:20:49 PM	144.146.103.72	CONNECT	407	mickey.g@contoso.com	tunnel//urs.microsoft.com:443/	Conference_Rooms	DSPPolicy_05	eDLPPolicy_05	

Figure 6

- 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).

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 2:26:54 PM	12	PNPL-2-KP / Contoso...	N/A	N/A	syslog

**Event Type:** Warning  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 Aug 18 01:10:47 md-hq-wsa1 Aug 18 01:10:46 Access\_Logs\_to\_Slater: Info: 1471497046.785 59 10.78.31.20 TCP\_DENIED\_SSL/403 0 GET https://leo.nline.microsoft.com:443/iedomainsuggestions/ie11/suggestions.en-US - NONE/ - - BLOCK\_WEBCAT\_12-Branch\_HomeBanking\_PCs-Branch\_HomeBanking\_PCs-DefaultGroup-NONE-NONE-NONE <IW\_comp,4.0.....IW\_comp,....Unknown,Unknown,....0.00,0.....>

Figure 7

Cisco WSA-URL filtering							
LogTime	Authenticated User	Client IP	Identity	Requested URL	URL category	HTTP Method	HTTP Status Code
09/01/2016 05:21:22 PM	james@contoso.com	10.78.34.20	Branch_HomeBanking_PCs	https://microsoft.com	IW_comp	GET	403
09/01/2016 05:22:29 PM	jones@contoso.com	10.78.33.20	Branch_HomeBanking_PCs	https://gmail.com	IW_pem	GET	403
09/01/2016 05:22:52 PM	phil.brook@contoso.com	10.78.33.20	Branch_HomeBanking_PCs	https://outlook.com	IW_pem	GET	403
09/01/2016 05:22:54 PM	daniel.c@contoso.com	10.78.31.20	Branch_HomeBanking_PCs	https://facebook.com	IW_snet	GET	403
09/01/2016 05:22:54 PM	nike.d@contoso.com	10.78.31.20	Branch_HomeBanking_PCs	https://forbes.com	IW_busi	GET	403

Figure 8

- 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).



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
9/16/2016 2:26:58 PM	12	PNPL-2-KP / Contoso...	N/A	N/A	syslog

**Event Type:** Warning  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 Aug 18 01:10:15 md-hq-wsa1 Aug 18 01:10:14 Access\_Logs\_to\_Slater: Info: 1471497014.281 0 144.146.104.79 TCP\_DENIED/407 0 CONNECT tunne  
 //scs-prod-ue1-notif.24.adobesc.com:443/ - NONE/ - OTHER-NONE-Conference\_Rooms-NONE-NONE-NONE-NONE <.....>  
 .....0.00.0.....>-

Figure 9

LogTime	Client IP	HTTP Method	HTTP Status Code	Identity	Requested URL
09/01/2016 05:20:46 PM	144.146.104.79	CONNECT	407	Conference_Rooms	https://sxyrfj.com
09/01/2016 05:20:46 PM	144.146.104.79	CONNECT	407	Conference_Rooms	https://letsc.forbes.com
09/01/2016 05:20:48 PM	144.144.11.124	CONNECT	407	Conference_Rooms	tunnel://hangouts.google.com:443/
09/01/2016 05:20:48 PM	144.144.11.124	CONNECT	407	Conference_Rooms	tunnel://hangouts.google.com:443/
09/01/2016 05:20:49 PM	144.146.103.72	CONNECT	407	Conference_Rooms	tunnel://urs.microsoft.com:443/
09/01/2016 05:20:49 PM	144.146.103.72	CONNECT	407	Conference_Rooms	tunnel://urs.microsoft.com:443/

Figure 10

# 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.

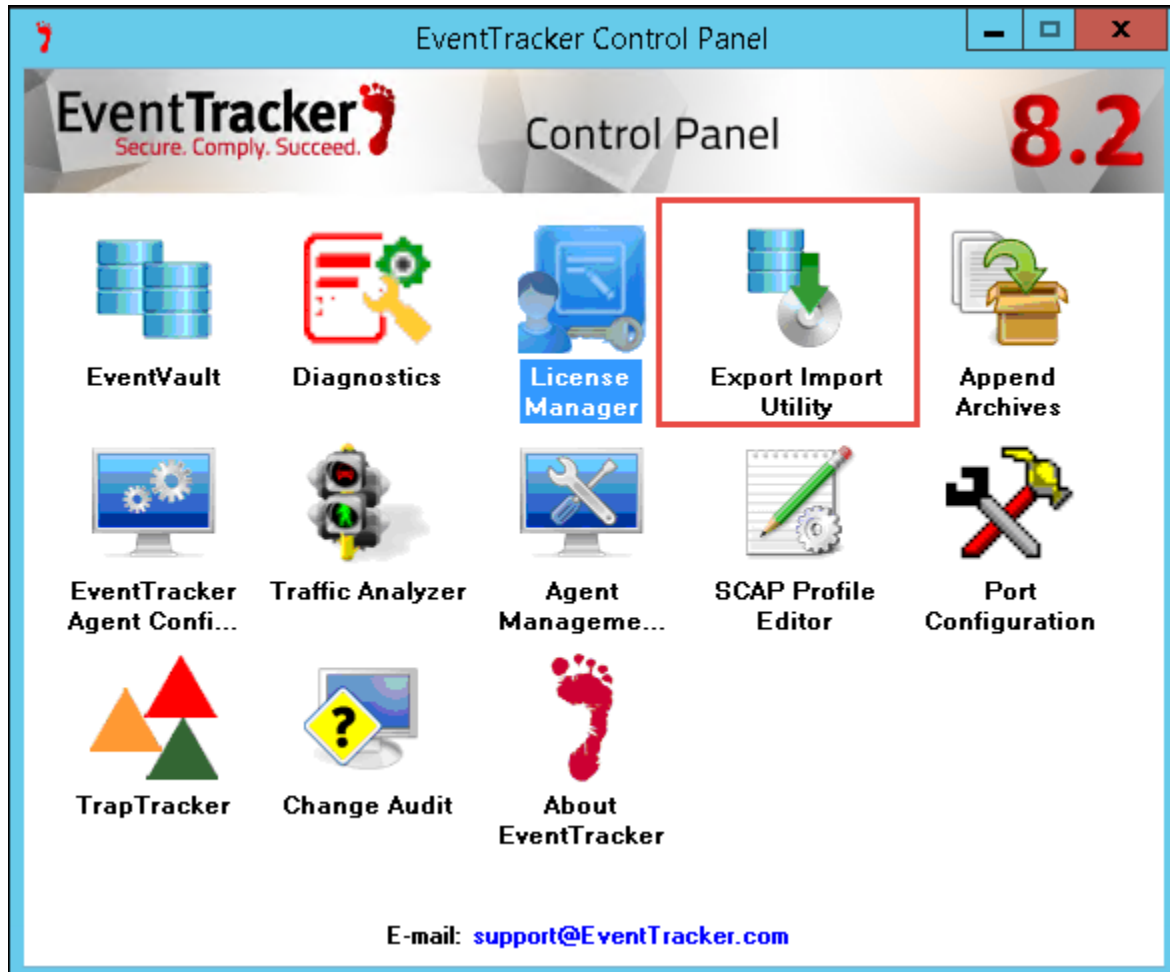



Figure 11

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.

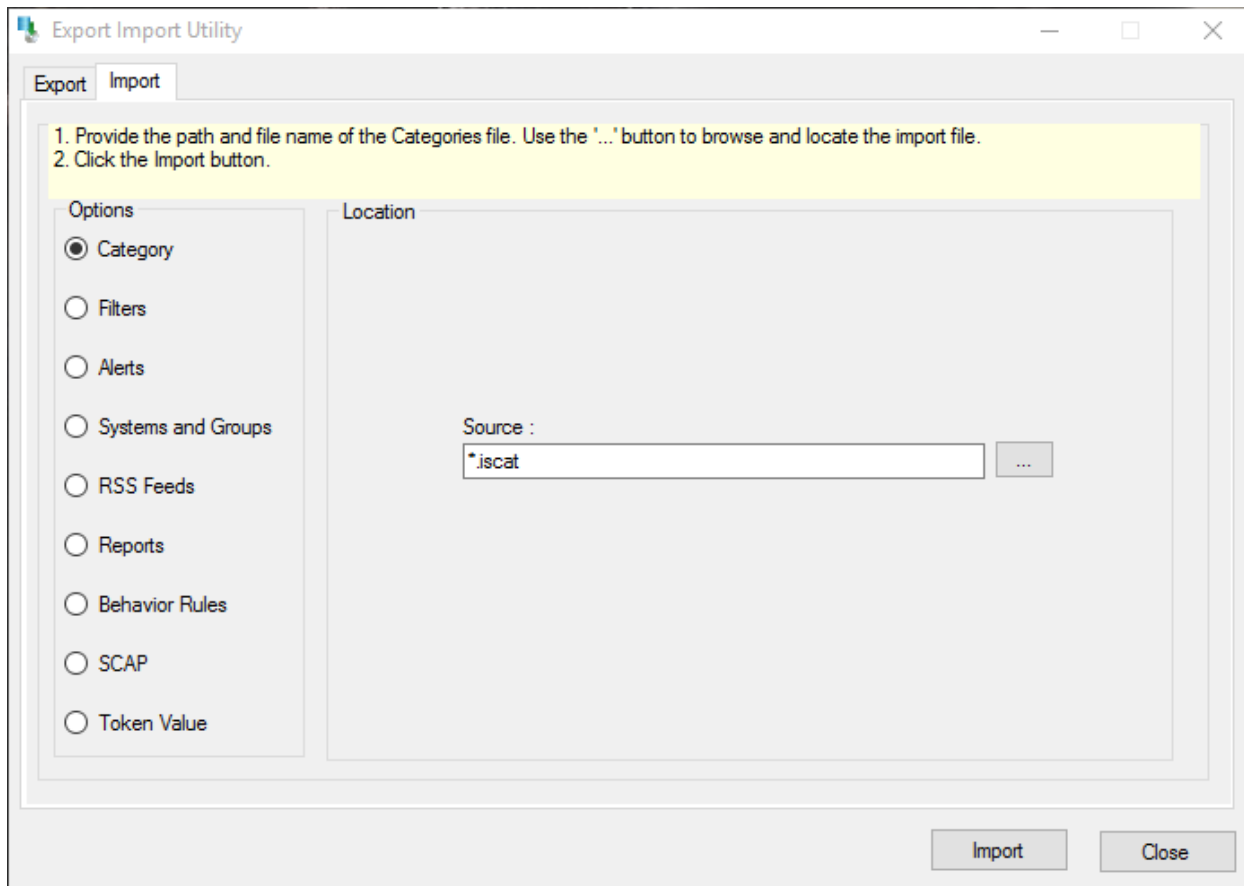


Figure 12

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.

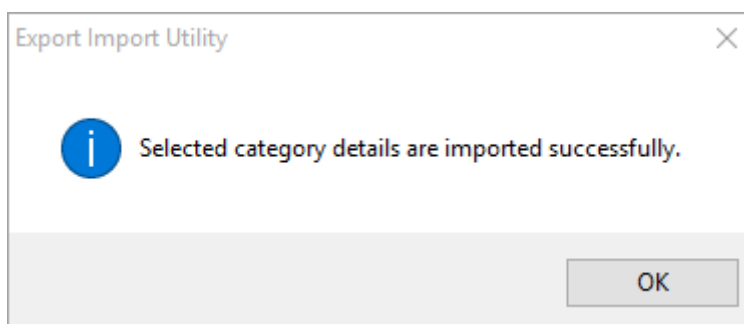


Figure 13

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

# Alerts

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

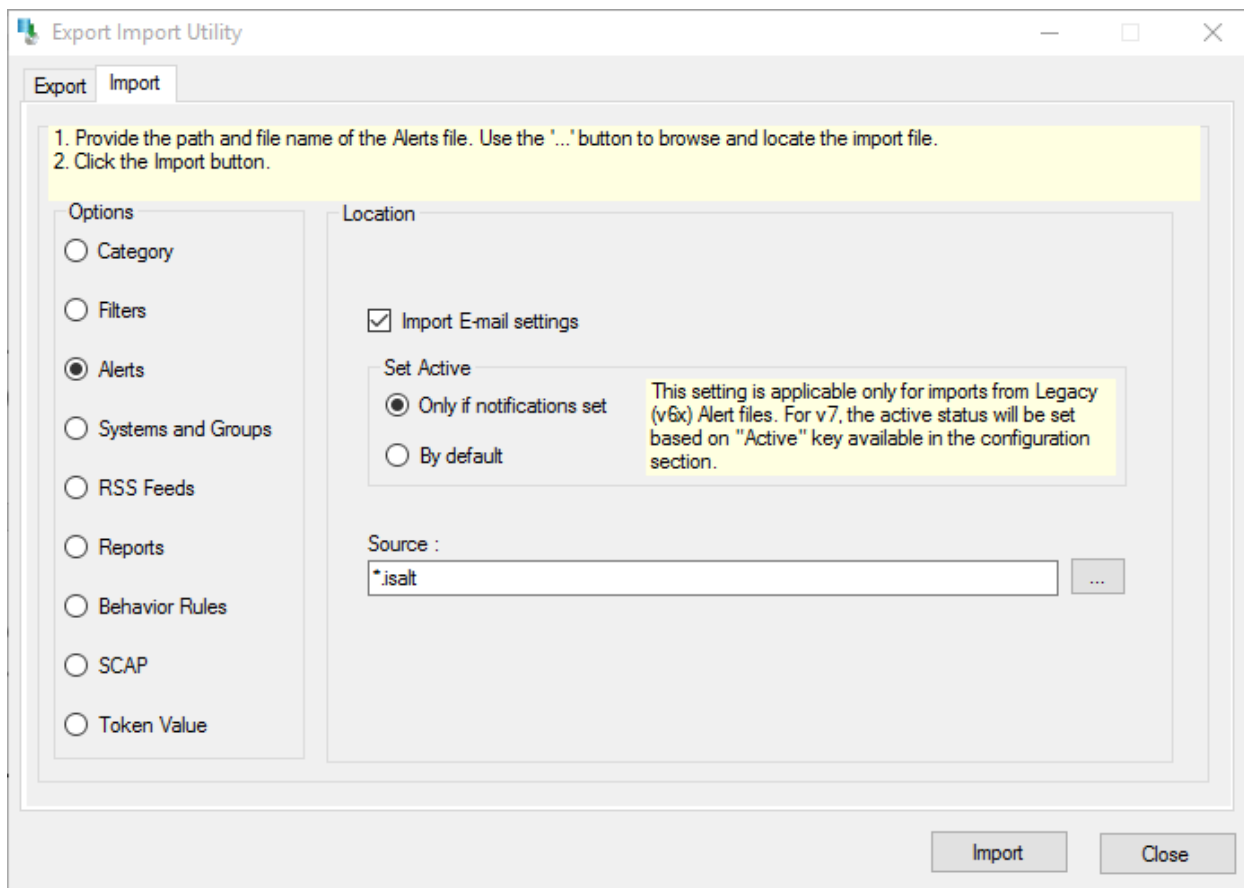


Figure 14

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.

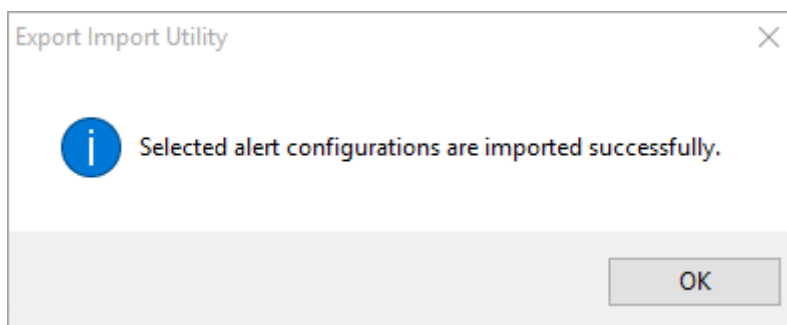



Figure 15

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  'Import' icon.

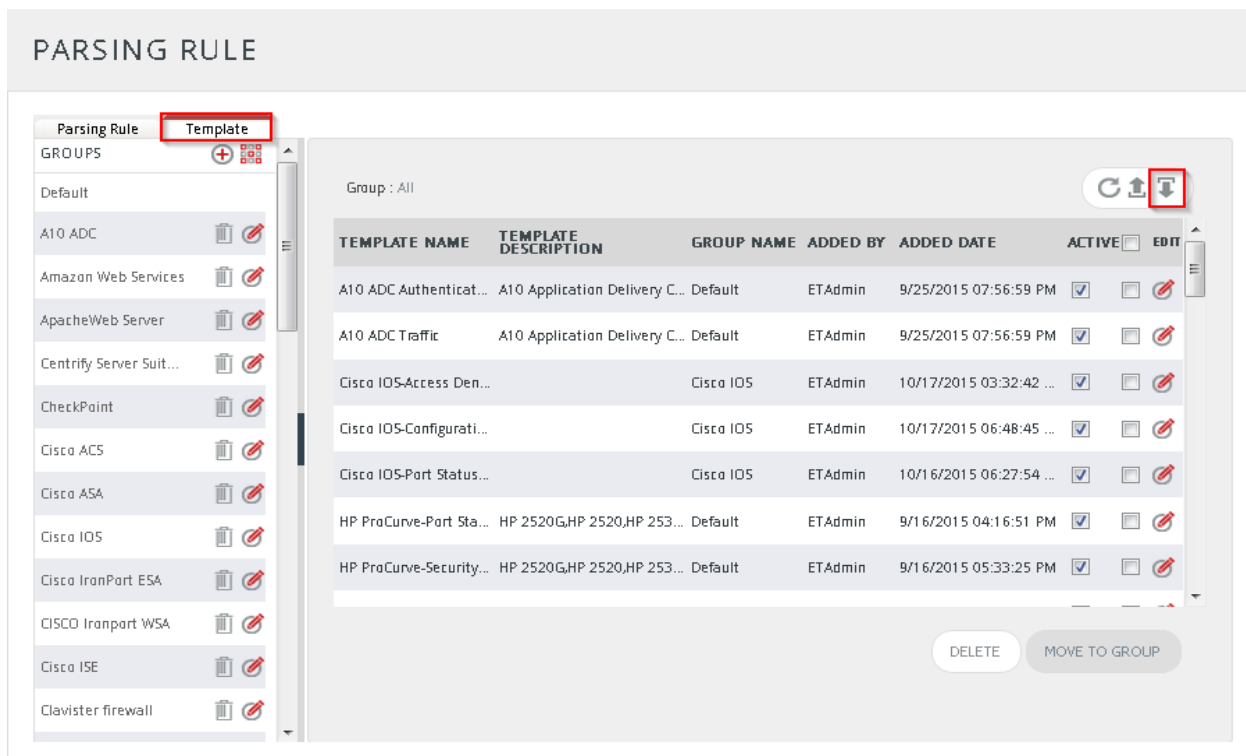


Figure 16

3. Click on **Browse** button.

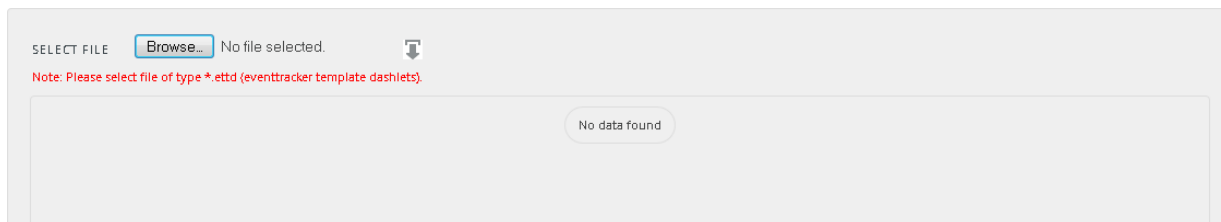


Figure 17

4. Locate **Cisco IronPort WSA token template.ettd** file, and then click the **Open** button.

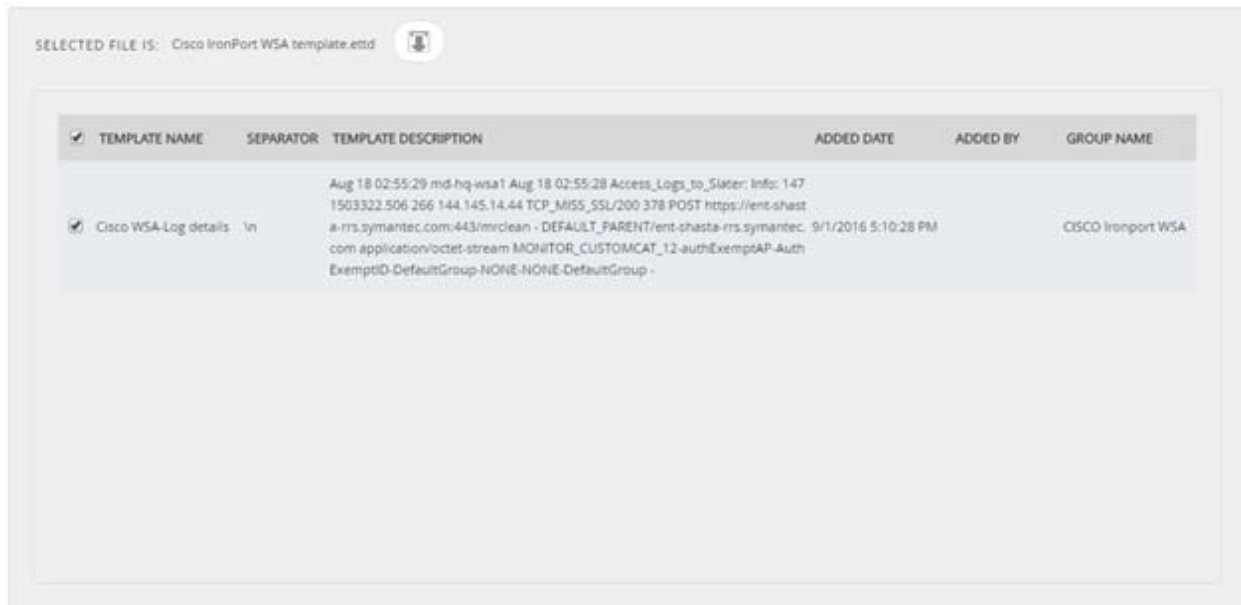



Figure 18

- Now select the check box and then click on  **'Import'** option. EventTracker displays success message.

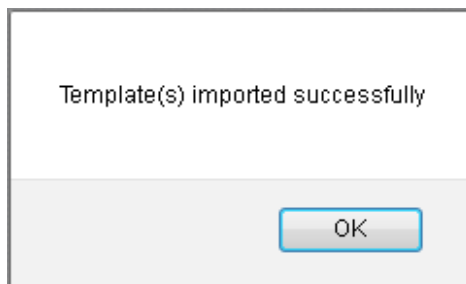



Figure 19

- Click on **OK** button.

## Flex Reports

- Click **Report** option, and then click the browse  button.

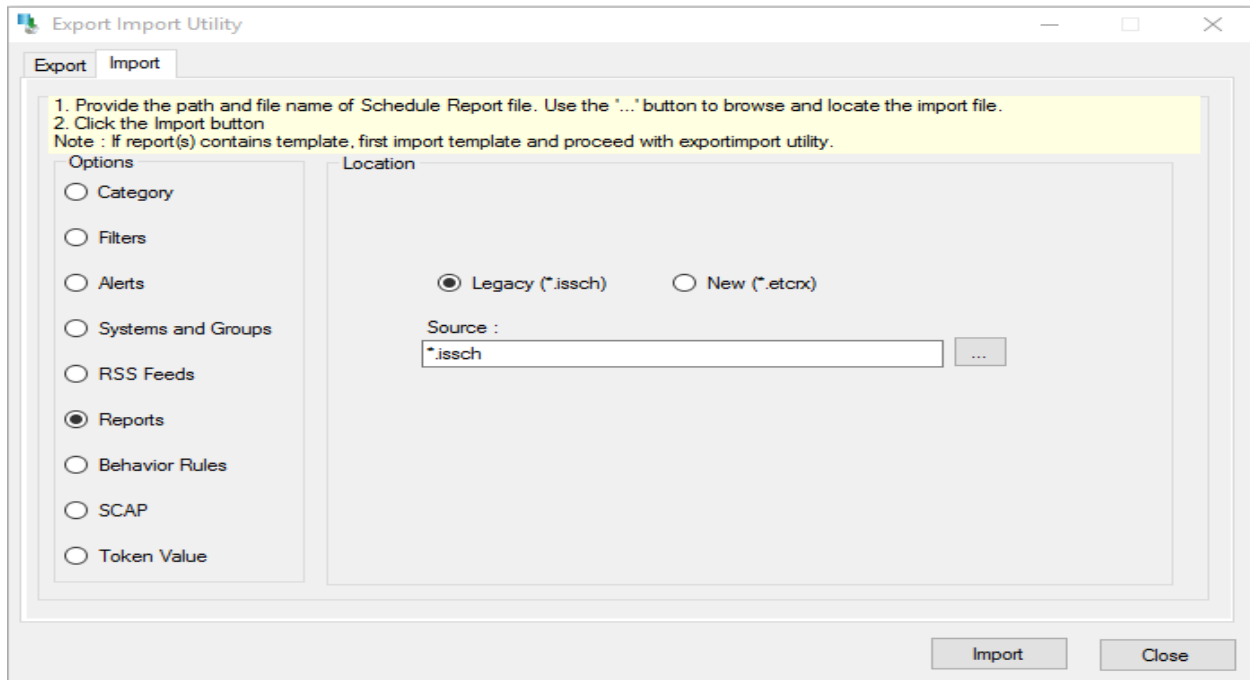


Figure 20

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.

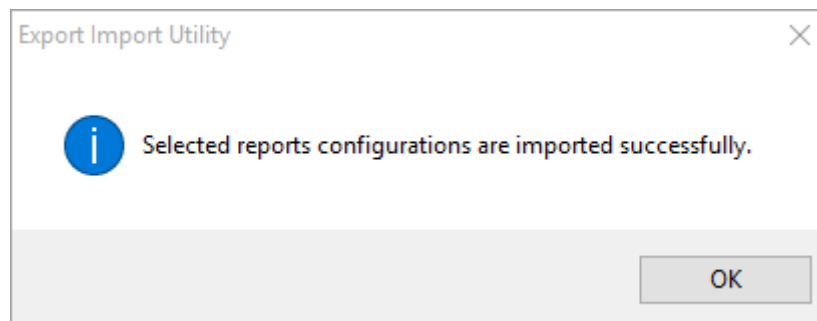


Figure 21

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.

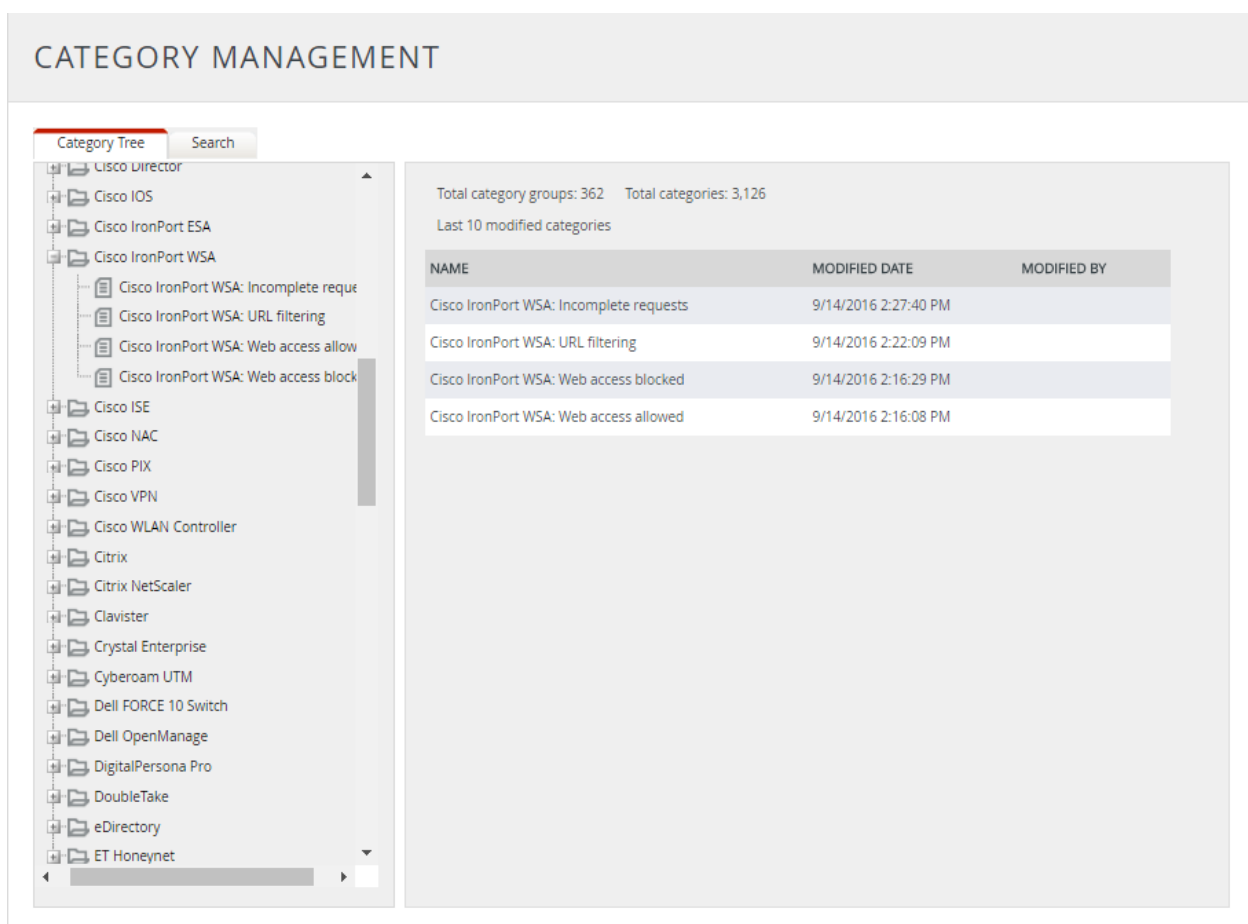


Figure 22



## 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.

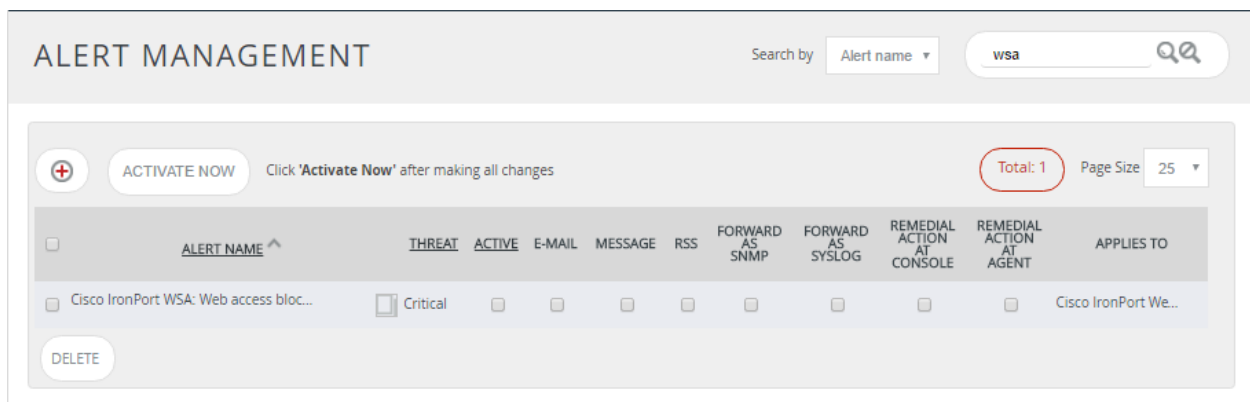


Figure 23

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

EventTracker displays message box.

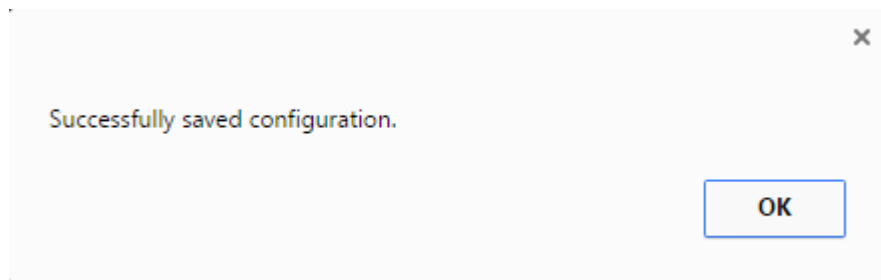


Figure 24

## 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.

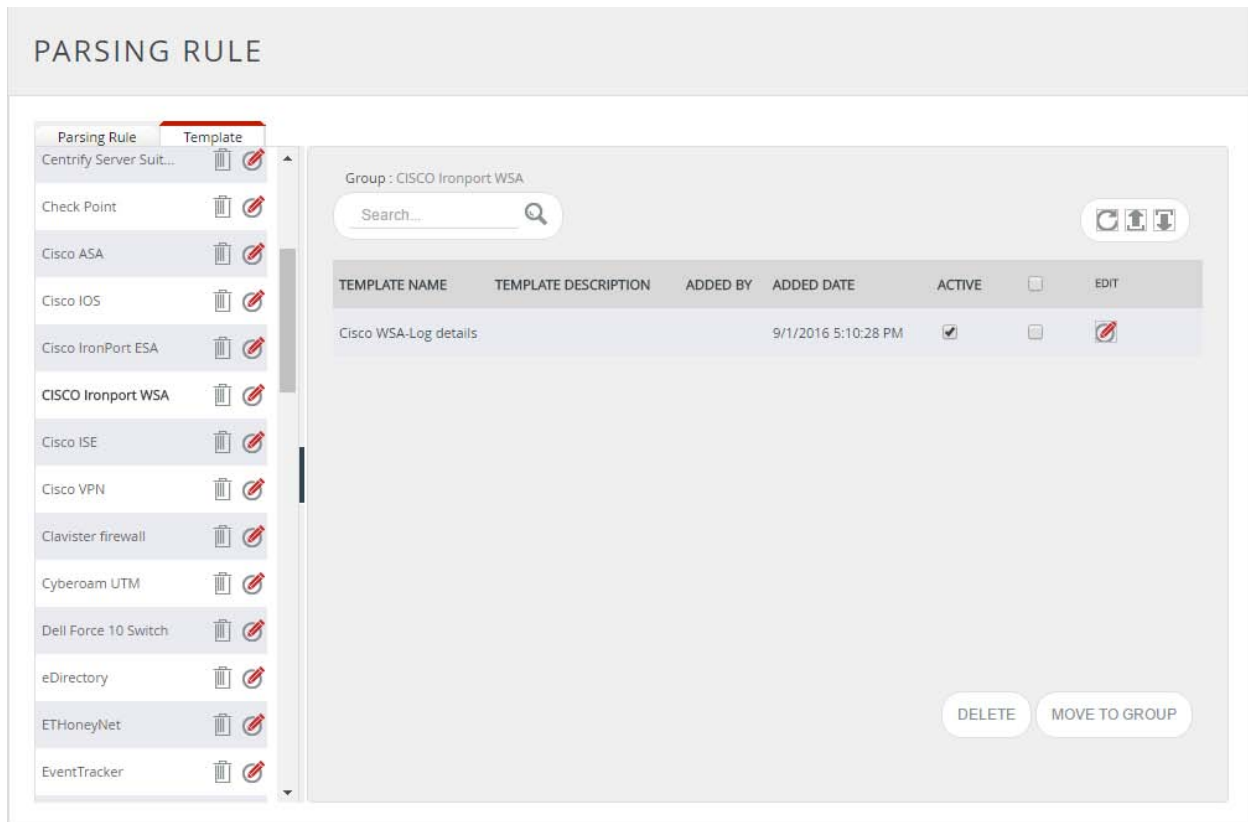


Figure 25

## 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.

REPORTS CONFIGURATION

Scheduled Queued **Defined**

Search

REPORT GROUPS

- Cisco Firewall
- Cisco IOS
- Cisco IronPort ESA
- Cisco IronPort WSA
- Cisco ISE
- Cisco VPN
- Cisco WSA
- Clavister
- Cyberoam UTM
- Dell FORCE 10 Switch
- eDirectory
- ETHoneyNet

REPORTS CONFIGURATION : CISCO IRONPORT WSA

Total: 4

TITLE	CREATED ON	MODIFIED ON
Cisco WSA-Incomplete requests	9/6/2016 12:58:01 PM	9/14/2016 2:55:36 PM
Cisco WSA-URL filtering	9/6/2016 12:35:16 PM	9/14/2016 2:55:13 PM
Cisco IronPort WSA-Web access allowed	11/20/2013 6:35:29 PM	11/20/2013 6:35:29 PM
Cisco IronPort WSA-Web access blocked	11/20/2013 5:51:36 PM	11/20/2013 5:51:36 PM

Figure 26

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.

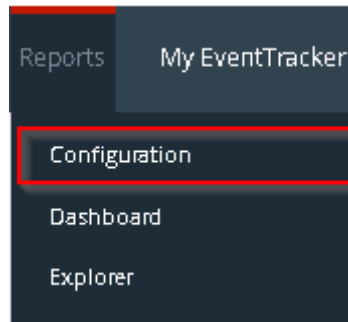


Figure 27

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

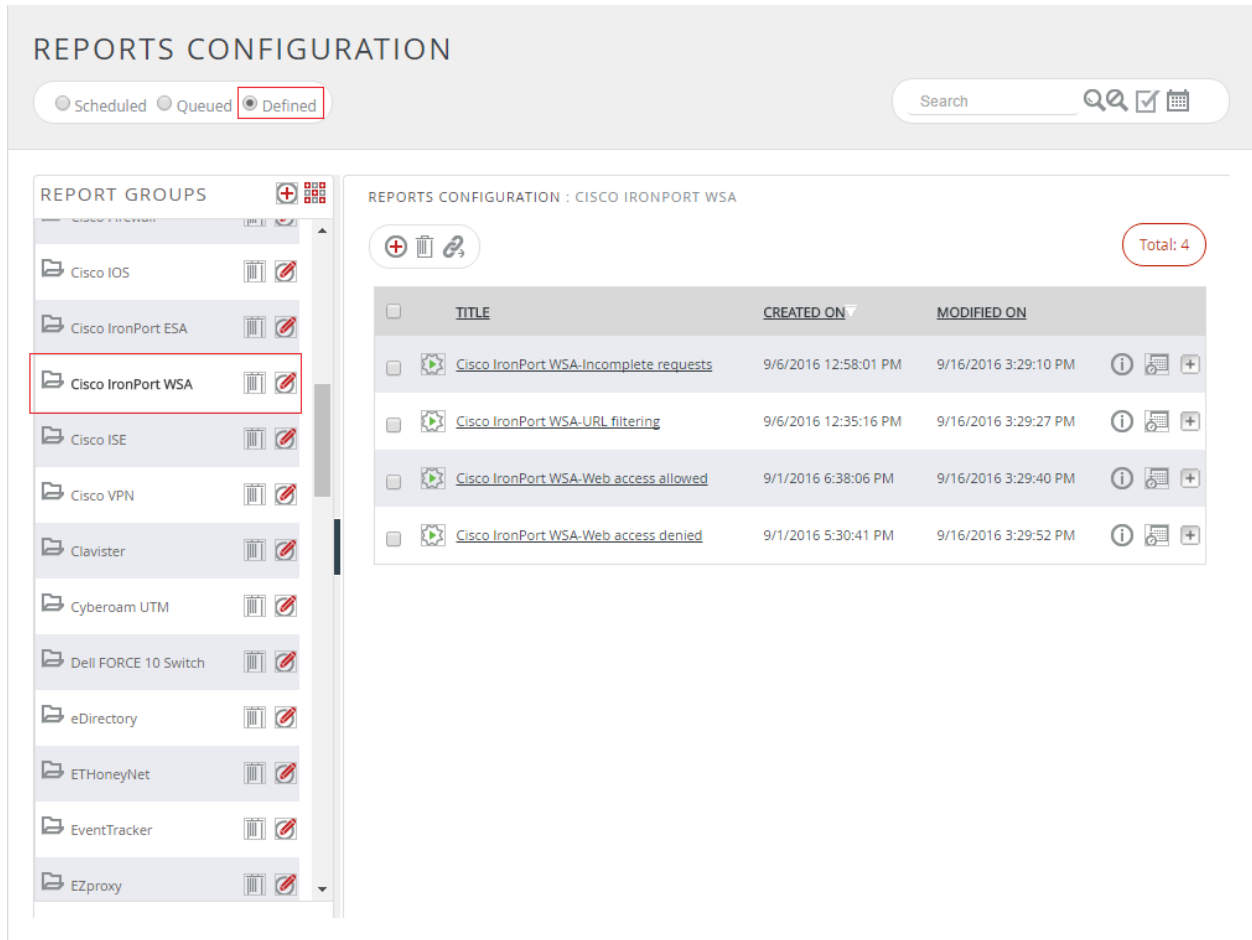



Figure 28

3. Select **Cisco IronPort WSA** in report groups. Check **Defined** dialog box.
4. Click on 'schedule'  icon to plan a report for later execution.

**REPORT WIZARD** CANCEL < BACK NEXT >

TITLE:  
LOGS

Review cost details and configure the publishing options. Step 8 of 10

**DISK COST ANALYSIS**

Estimated time for completion: **Unknown**  
Number of cab(s) to be processed: **Unknown**  
Available disk space: **Unknown**  
Required disk space: **Unknown**

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)  
 Deliver results via E-mail  
 Notify results via E-mail

To E-mail:  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:  ▼

Show in:  ▼

Persist data in Eventvault Explorer

Figure 29

5. Choose appropriate time for report execution and in **Step 8** check **"Persist data in Eventvault Explorer"** box.

## REPORT WIZARD

TITLE: CISCO IRONPORT WSA-WEB ACCESS ALLOWED  
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

### RETENTION SETTING

Retention period:  days ⓘ

Persist in database only [Reports will not be published and will only be stored in the respective database]

### SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Client IP	<input checked="" type="checkbox"/>
Requested URL	<input checked="" type="checkbox"/>
HTTP Method	<input checked="" type="checkbox"/>
HTTP Status Code	<input checked="" type="checkbox"/>
Authenticated User	<input checked="" type="checkbox"/>
Server Accessed	<input checked="" type="checkbox"/>

Figure 30

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.

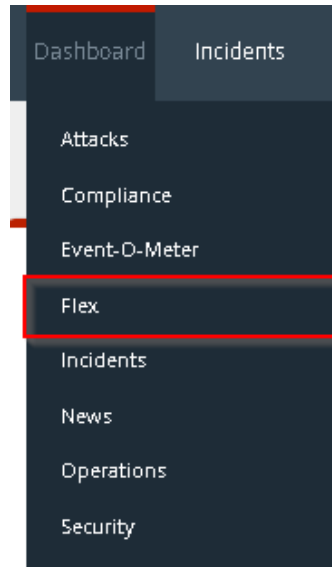


Figure 31

3. Navigate to **Dashboard>Flex**.  
Flex Dashboard pane is shown.

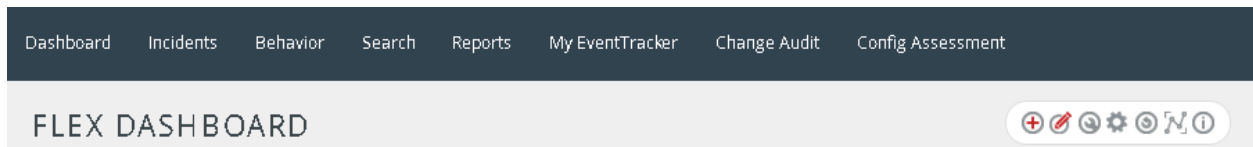

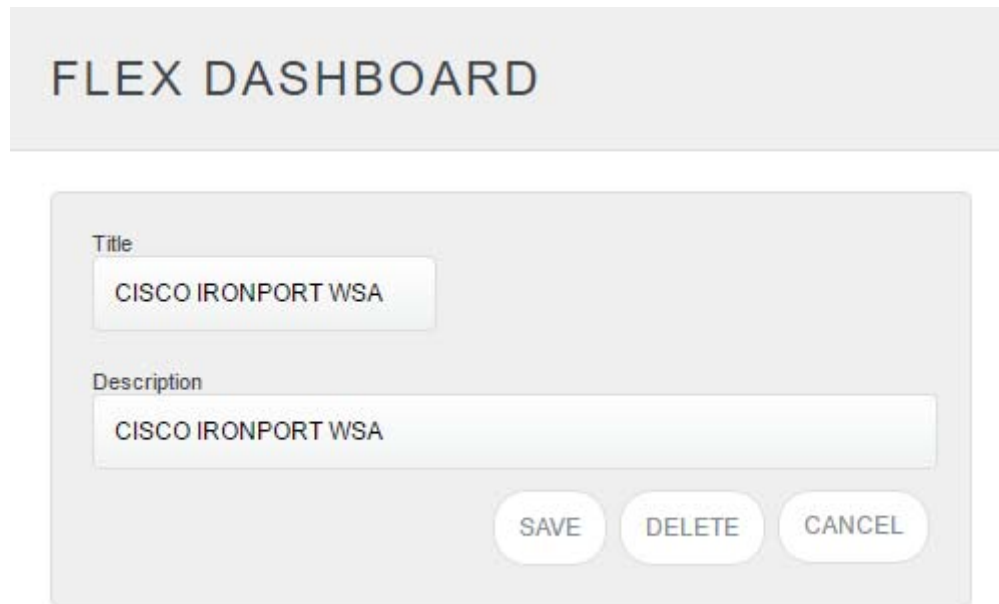


Figure 32


4. Click  to add a new dashboard.  
Flex Dashboard configuration pane is shown.





The image shows a configuration form titled "FLEX DASHBOARD". It contains two input fields: "Title" and "Description", both containing the text "CISCO IRONPORT WSA". Below the input fields are three buttons: "SAVE", "DELETE", and "CANCEL".

Figure 33

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.

## WIDGET CONFIGURATION

The screenshot shows a 'WIDGET CONFIGURATION' dialog box. It contains the following fields and options:

- WIDGET TITLE:** Cisco WSA web access by client IP
- NOTE:** (Empty text area)
- DATA SOURCE:** Cisco WSA-TCP allowed traffic
- CHART TYPE:** Donut
- DURATION:** 12 Hours
- VALUE FIELD SETTING:** COUNT
- AS OF:** Now
- AXIS LABELS [X-AXIS]:** Client IP
- LABEL TEXT:** (Empty text area)
- VALUES [Y-AXIS]:** Select column
- VALUE TEXT:** (Empty text area)
- FILTER:** Select column
- FILTER VALUES:** (Empty dropdown)
- LEGEND [SERIES]:** Select column
- SELECT:** All

At the bottom right, there are three buttons: TEST, CONFIGURE, and CLOSE.

Figure 34

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.

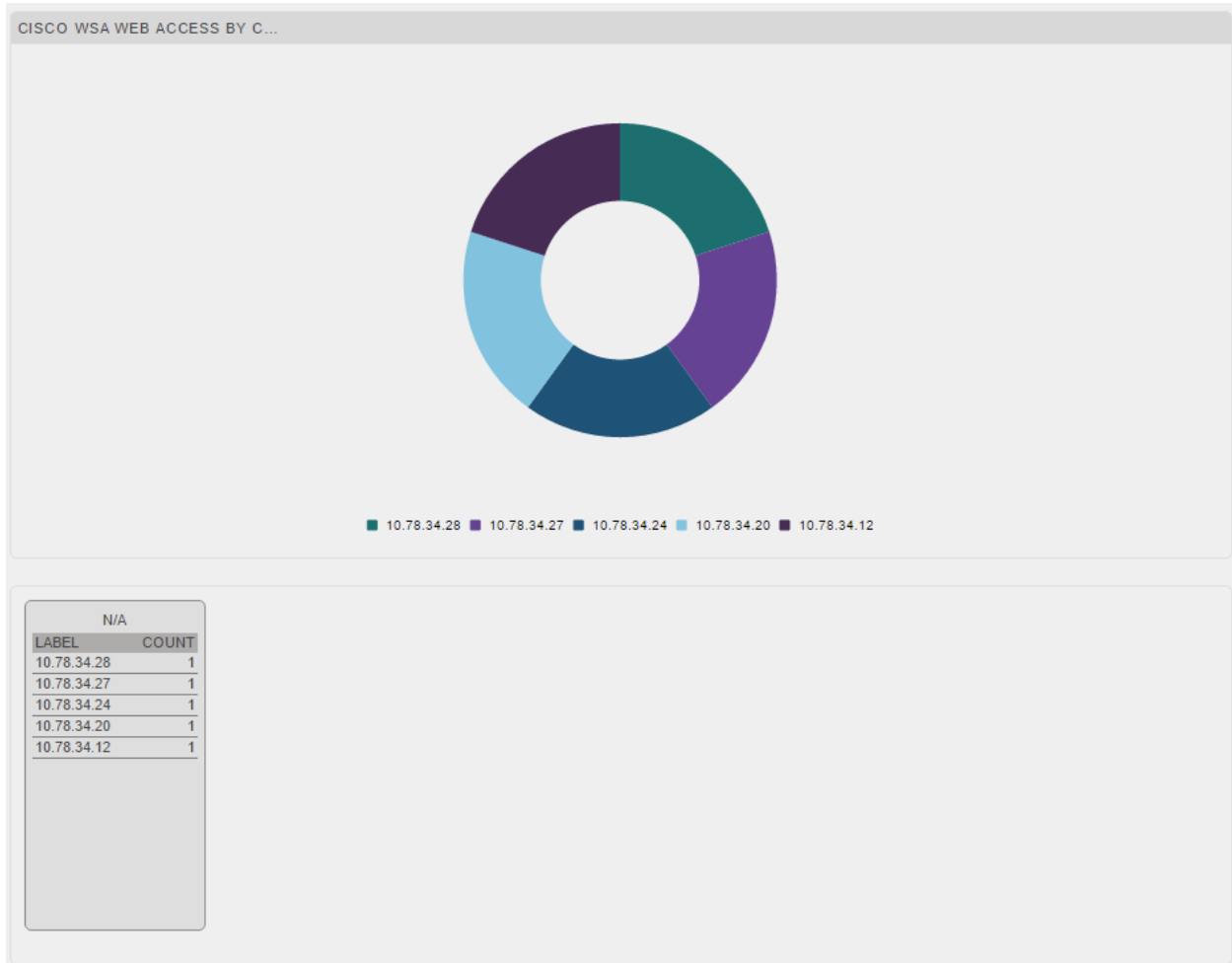



Figure 35

16. If satisfied, click **Configure** button.



Figure 36

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

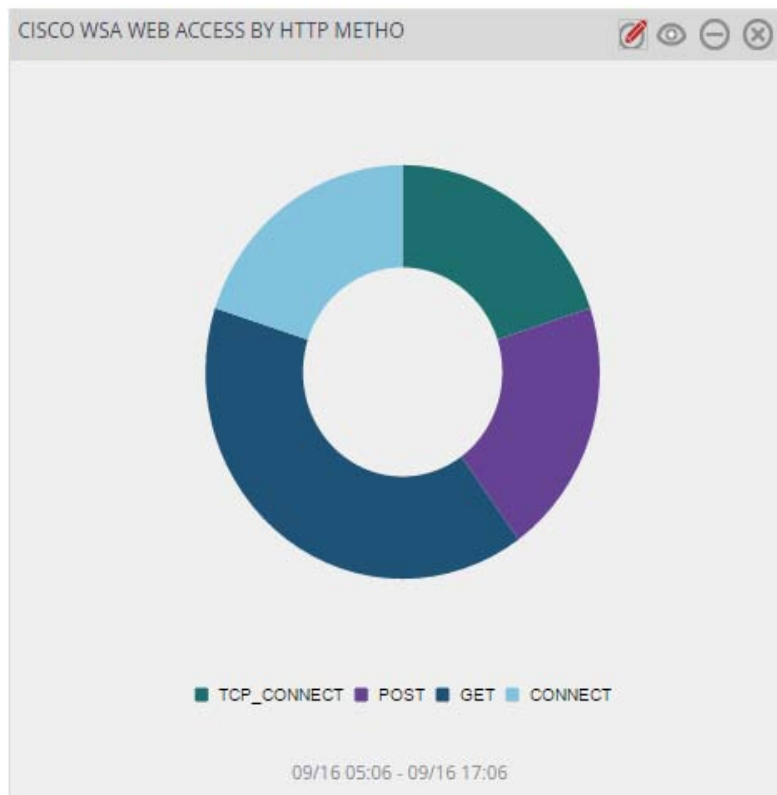


Figure 37

## 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

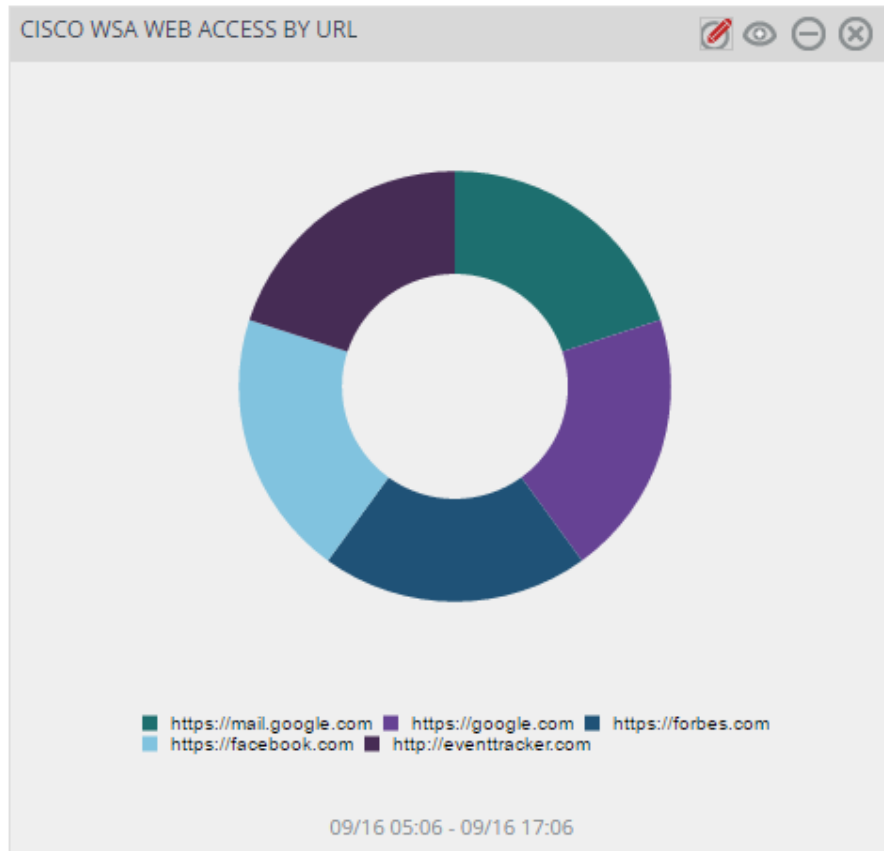


Figure 38

### 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

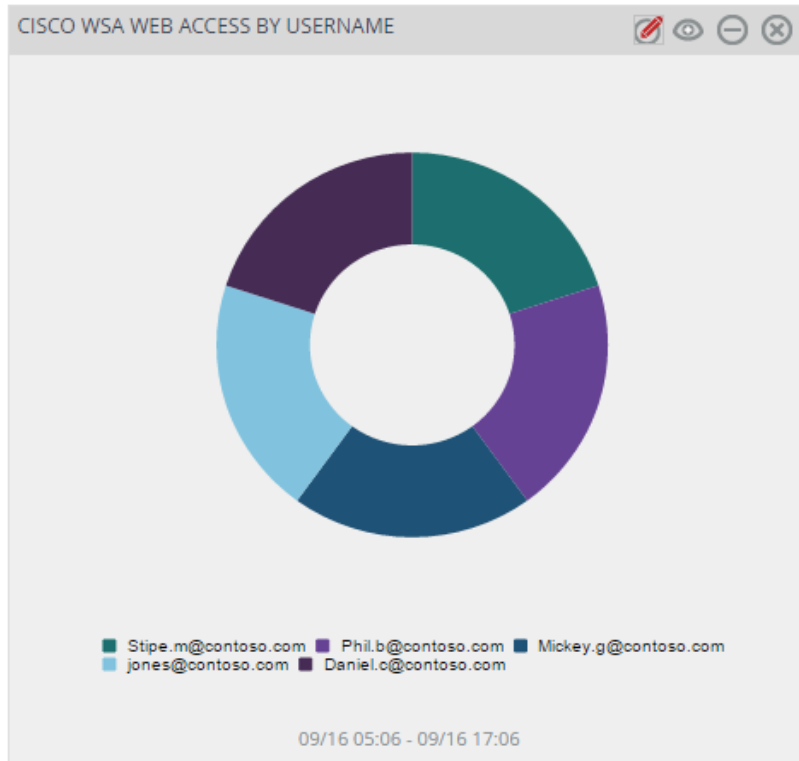


Figure 39

#### 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

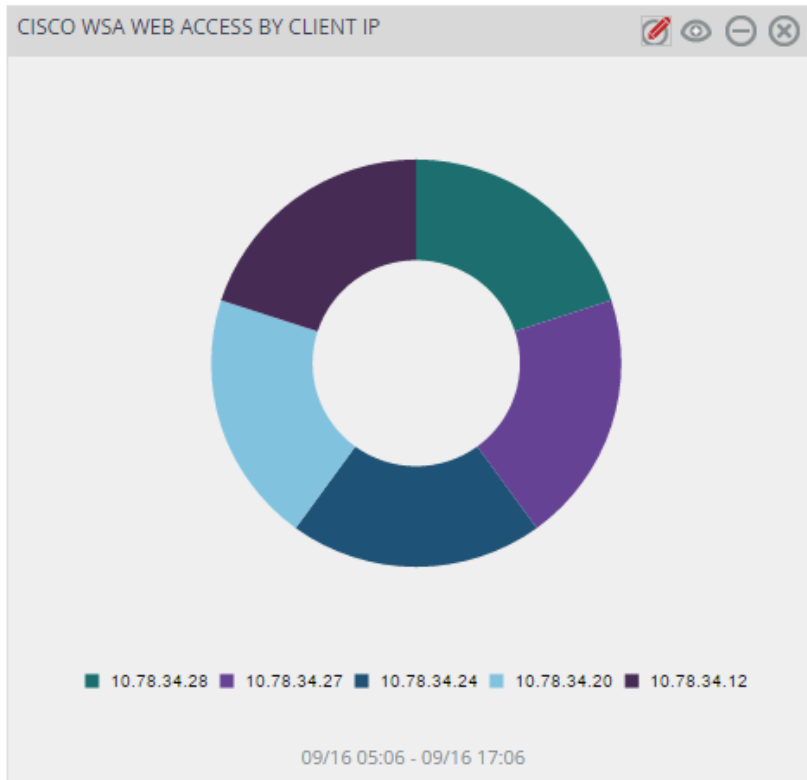


Figure 40