

Integration Guide

Integrating Cisco Email and Web Security with EventTracker

Publication Date:

February 24, 2022

Abstract

This guide provides instructions to retrieve the Cisco Email and Web Security (Cisco Secure Email, Cisco Secure Web Appliance, Cisco Secure Email, and Web Manager) events using the REST API. After EventTracker is configured to collect and parse these logs, then the dashboard and reports can be configured to monitor the Cisco Email and Web Security.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and Cisco Email and Web Security v13.0 (Cisco Secure Email, Cisco Secure Web Appliance, Cisco Secure Email and Web Manager) and later.

Audience

Administrators who are assigned the task to monitor Cisco Email and Web Security (Cisco Secure Email, Cisco Secure Web Appliance, Cisco Secure Email, and Web Manager) events using EventTracker.

Table of Contents

Table of Contents	3
1. Overview	4
2. Prerequisites.....	4
3. Configuring Cisco Email and Web Security to Forward Logs to EventTracker	4
3.1 Enable AsyncOS API	4
3.2 Enable Message Tracking (Applicable for Cisco Secure Email)	5
3.3 Create New User.....	5
3.4 Integrate Cisco Email and Web Security with EventTracker.....	6
4. EventTracker Knowledge Packs	8
4.1 Categories.....	8
4.2 Reports	9
4.3 Dashboards.....	10
5. Importing Cisco Email and Web Security Knowledge Pack into EventTracker.....	15
5.1 Categories.....	16
5.2 Knowledge Objects.....	16
5.3 Reports	19
5.4 Dashboards.....	19
6. Verifying Cisco Email and Web Security Knowledge Pack in EventTracker	21
6.1 Categories.....	21
6.2 Knowledge Objects.....	22
6.3 Reports	23
6.4 Dashboards.....	24
About Netsurion	26
Contact Us.....	26

1. Overview

Cisco Email and Web Security (formerly known as Cisco Security Appliance) centralizes management and reporting functions across multiple Cisco email and web security appliances. Its email security gateway (Cisco secure email gateway) product is designed to detect and block a wide variety of email-borne threats, such as malware, spam, and phishing attempts. Cisco Secure Web Appliance protects your organization by automatically blocking risky sites and testing unknown sites before allowing users to click on them.

EventTracker, when integrated with Cisco Email and Web Security collects logs from Cisco secure email gateway and Cisco Secure Web Appliance creates detailed reports, alerts, dashboards, and saved searches. These attributes of EventTracker help the user to view the critical information on a single platform.

Secure Email Reports contain a detailed overview of activities like incoming message summary, (Data, Loss, and Protection) DLP, and AMP (Advanced Malware Protection) event summary, malicious or suspicious URLs summary, and many more. The Secure Web Appliance reports contain Proxy, Layer 4, SOCKS Proxy monitored allowed, and blocked traffic event summary.

2. Prerequisites

- **EventTracker v9.3** or **above** should be installed.
- A user with administrator access for Cisco Email and Web Security (Secure Email & Secure Web)
- Port should be allowed in the firewall.
- Microsoft PowerShell v5.0 or above.

3. Configuring Cisco Email and Web Security to Forward Logs to EventTracker

Cisco Email and Web Security can be integrated with EventTracker by Integrator based on the API Integration to forward logs to the EventTracker Manager.

3.1 Enable AsyncOS API

In the cloud, the API is enabled by default.

Follow the steps below to enable the API on the On-Premises instance.

1. Login to the web interface.
2. Choose **Network > IP Interfaces**.
3. Edit the **Management** interface.
 - **Note:** You can enable the AsyncOS API on any IP address interface. However, Cisco recommends that you enable the AsyncOS API on the Management interface.
4. You must not enable the APIs on multiple management interfaces.
5. Under the AsyncOS API (Monitoring) section, depending on your requirements, select the HTTP and the ports to use.

AsyncOS API	
The Next Generation portal of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerconfig command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.	
<input checked="" type="checkbox"/> AsyncOS API HTTP	6080
<input checked="" type="checkbox"/> AsyncOS API HTTPS	6443

- Save the HTTPS port, it will be required later during the Integration.

Note: AsyncOS API communicates using HTTP / 1.1.

- Submit and commit your changes.

3.2 Enable Message Tracking (Applicable for Cisco Secure Email)

- Click **Security Services** > Message Tracking.
Use this path even if you do not plan to centralize this service.
- Select **Enable Message Tracking Service**.
- If you are enabling the message tracking for the first time, after running the **System Setup Wizard**, review the end-user.
- Choose a Message Tracking Service.

Option	Description
Local Tracking	Use message tracking on this appliance.
Centralized Tracking	Use a Security Management appliance to track messages for multiple Email Security appliances including this one.

- (Optional) Select the check box to save information for the rejected connections.
- Submit** and commit your changes.

If you select the **Local Tracking**, choose who can access the contents related to the DLP violations.

- Go to the System Administration > Users page.
- Under Access to Sensitive Information in Message Tracking, click **Edit Settings**.
- Select the roles for which you want to grant access to each type of sensitive information.

Note: Custom roles without access to the Message Tracking can never view this information and hence they are not listed.

- Submit and commit your changes.

3.3 Create New User

Note: When you create a new user account, you assign the user to a predefined user role.

E.g.: **Read-Only User** to help monitor the Message-Tracking events.

- Choose **System Administration** > **Users**.
- Click **Add User**.
- Enter a login name for the user. E.g., **EventTracker**.
- Enter the user's full name.

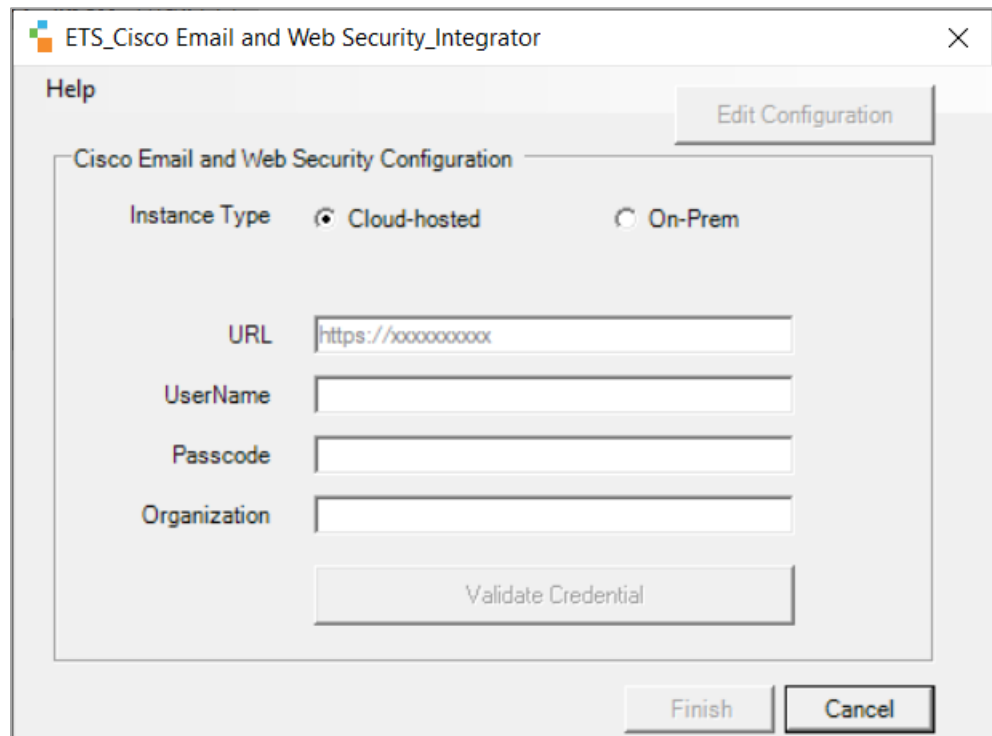
5. Select a predefined or custom user role. E.g., **Help Desk User**.
6. Enter a passphrase.
7. Submit and commit your changes.

3.4 Integrate Cisco Email and Web Security with EventTracker

1. Download the Cisco Email and Web Security (applicable for Cisco Secure Email, Cisco Secure Web Appliance, Cisco Secure Email, and Web Manager) integrator on the EventTracker Manager/EventTracker Agent machine from [here](#).
2. Run the downloaded “ETS_Cisco Email and Web Security_Integrator.exe” file. The Integration window will open.
3. To check the Integrator version, go to **Help > About**. Make sure you are using the latest version of the integrator.

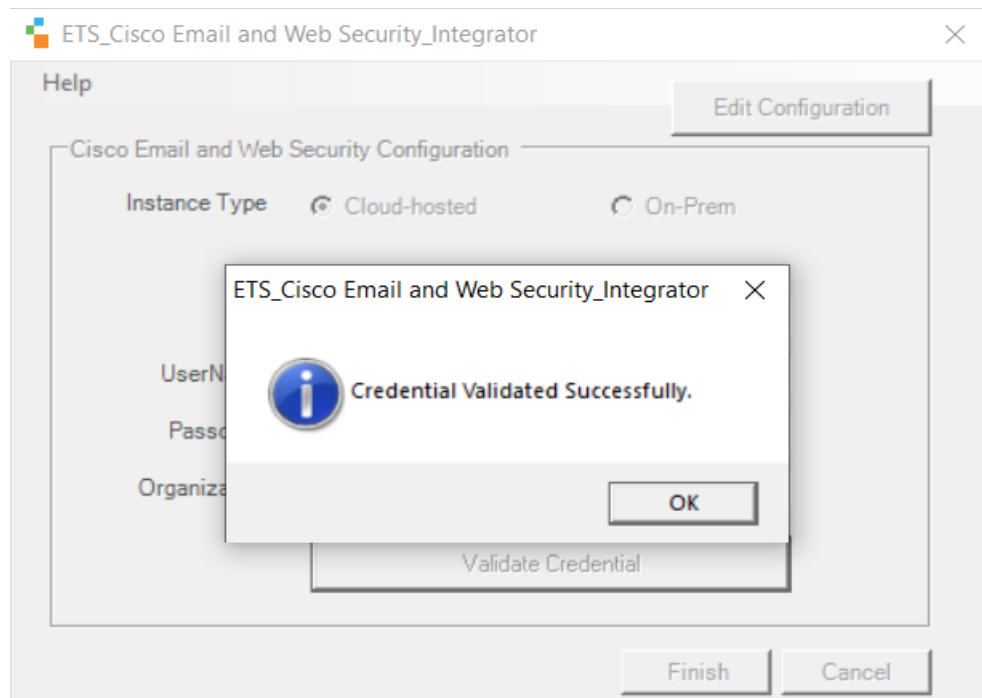
Note: In case both cloud and on-prem integration is needed, finish the cloud integration, and create a new folder inside the Integrator folder (under Agent). Copy all the files present in the “Cisco Email and Web Security” folder and launch the ETS_Cisco Email and Web Security_Configure.exe with administrator access.

Cloud Based Integration



1. Select the **Instance Type** as **Cloud-hosted** (Default selected)
2. Provide the **URL** (e.g., https://dhxxx.xxx.com)
3. Provide the **Username** and **Passcode** which was created for Integration.
4. Provide your **Organization** name which will get displayed under the EventTracker Manager.
5. Click **Validate Credential**.

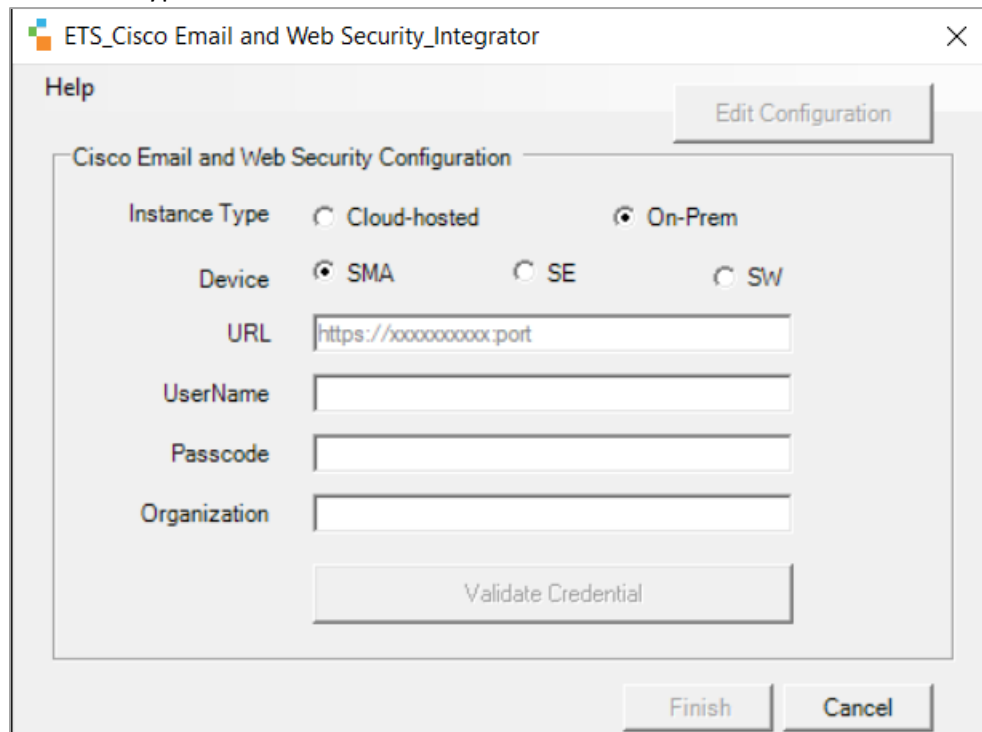
- A message window will pop up stating **Credentials Validated Successfully**. Click **OK**.



- Click **Finish** to complete the integration.

On-Premises Integration

- Select the Instance Type as On-Premises.



2. Select the Device Type.
 - **SMA**: Centralized email and web manager
 - **SE**: Secure Email
 - **SW**: Secure Web Appliance
3. Provide the **URL** with the port which was saved during enabling the AsyncOS API (eg: <https://dhxxx.xxx.com:6443>)
4. Provide the **Username** and **Passcode** which was created for the Integration.
5. Provide your **Organization** name which will get displayed under the EventTracker Manager.
6. Click **Validate Credential**.
7. A message window will pop up stating **Credentials Validated Successfully**. Click **OK**.
8. Click **Finish** to complete the integration.

4. EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, then the Knowledge Packs can be configured into EventTracker.

4.1 Categories

- **Cisco SE - AMP Messages**: This allows the user to filter and search events specific to the AMP messages/ emails.
- **Cisco SE - DLP Messages**: This allows the user to filter and search events specific to the DLP messages/ emails.
- **Cisco SE - Emails quarantined by Anti-spam/graymail**: This allows the user to quickly filter, and search events related to spam emails or graymail.
- **Cisco SE - Emails quarantined by Content Filters**: This allows the user to quickly filter, and search events related to the emails quarantined by the content filters.
- **Cisco SE - Incoming Emails**: This allows the user to quickly filter and search all the inbound/ incoming emails.
- **Cisco SE - Outgoing Emails**: This allows the user to quickly filter and search all the outbound/ outgoing emails.
- **Cisco SWA - Layer 4 Traffic Events**: This allows the user to quickly filter and retrieve transactions processed by the Layer 4 traffic monitor.
- **Cisco SWA - Proxy Traffic Events**: This allows the user to quickly filter and retrieve transactions processed by the Proxy services.
- **Cisco SWA - SOCKS Proxy Traffic Events**: This allows the user to quickly filter and retrieve transactions processed by the SOCKS Proxy services.

4.2 Reports

- Cisco ES – AMP and DLP Messages:** This report will provide a summary of the Advanced Malware Protection (AMP) and Data Loss and Prevention (DLP) messages as detected in the Cisco Secure Email. It will include details such as event log time, email direction, sender/recipient address, and many more.

LogTime	Computer	Message	Email Direction	Sender Address	Recipient Address	Email Subject	Attachments	AMP Details	Sender Group
16/11/2018 11:01:08 AM	CISCO_ESA2@NTPLDTBLR48	1763042	outgoing	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	ESA_AMP.pptx	timestamp = 16 Nov 2018 13:01:08	RELAYLIST
16/11/2018 11:05:08 AM	CISCO_ESA2@NTPLDTBLR48	22124	outgoing	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	Zombies.pdf	timestamp = 16 Nov 2018 11:05:08	RELAYLIST
16/11/2018 11:01:08 AM	CISCO_ESA2@NTPLDTBLR48	22124	outgoing	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	Lab_Guide.docx	timestamp = 16 Nov 2018 11:01:08	RELAYLIST
16/11/2018 11:01:08 AM	CISCO_ESA2@NTPLDTBLR48	1763042	incoming	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	ESA_AMP.pptx	timestamp = 16 Nov 2018 11:01:08	RELAYLIST
16/11/2018 11:01:08 AM	CISCO_ESA2@NTPLDTBLR48	856	incoming	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	Zombies.pdf	timestamp = 16 Nov 2018 11:01:08	RELAYLIST
16/11/2018 11:01:08 AM	CISCO_ESA2@NTPLDTBLR48	22124	incoming	cf_drop_in@vm30bsd0004.ibqa	6406@vm30bsd0004.ibqa	Testing	driver_license_germany.txt	timestamp = 16 Nov 2018 11:01:08	RELAYLIST

- Cisco ES - Emails Reports** – This report outlines the summary of spam email/ graymail and delivered activity that includes, source/recipient address, email direction, SBRS (SenderBase Reputation Score) score, and so on.

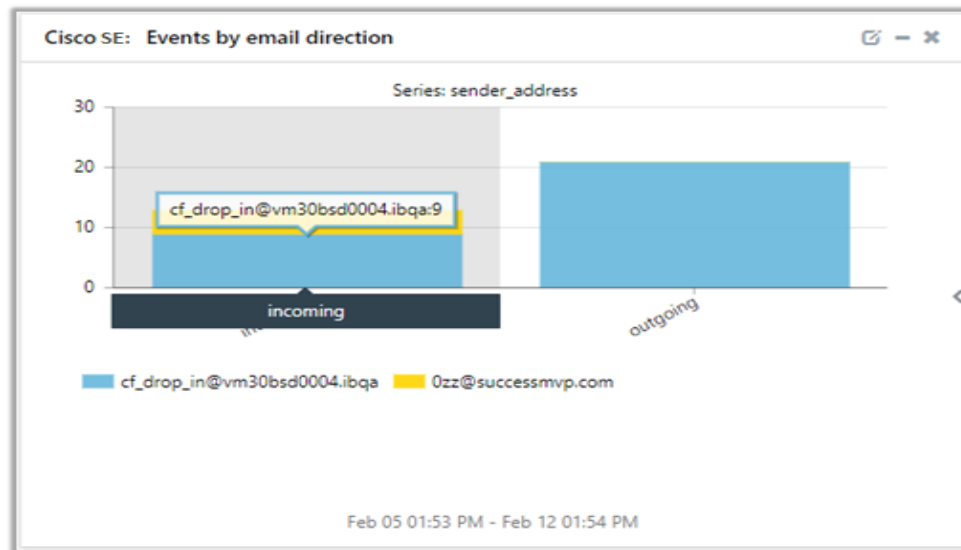
LogTime	Computer	Email Direction	Email Subject	Sender IP Address	Sender Address	Recipient Address	SBRS
05/04/2020 06:36:46 AM	IRONPORTMGMT.TestBed.COM	incoming	Uh-oh, your prescription is expiring	69.68.117.197	kayvont@yahoo.com	florin.anita@specnondse.cf	0.1
05/04/2020 06:38:03 AM	IRONPORTMGMT.TestBed.COM	incoming	Startups face an existential threat	131.154.73.151	drezet@hotmail.com	florin.anita@specnondse.cf	2.3
05/04/2020 06:39:06 AM	IRONPORTMGMT.TestBed.COM	incoming	25% off your favorites	149.222.120.155	cantu@att.net	florin.anita@specnondse.cf	3.4
05/04/2020 06:49:33 AM	IRONPORTMGMT.TestBed.COM	incoming	? a surprise gift for you! (unwrap)	173.245.78.108	specprog@aol.com	florin.anita@specnondse.cf	0.4
05/04/2020 06:50:01 AM	IRONPORTMGMT.TestBed.COM	incoming	Grow your email list 10X faster with these 30 content upgrade ideas	12.130.137.18	ianbuck@optonline.net	demailn.wayne@specnondse.cf	4.1

- Cisco SWA – Traffic Report** – This report generates a summary of all the traffic monitored by the proxy services, SOCKS proxy, and Layer 4. It includes source IP address, destination IP address, URL, policy type, application name, web category, username, and many more.

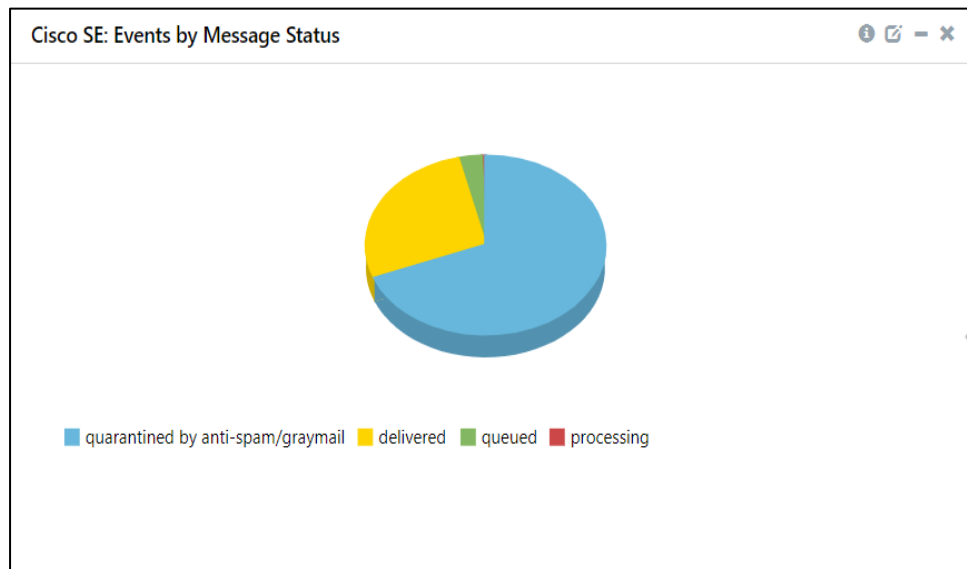
LogTime	Bandwidth	Content Type	Decision Source	Destination IP	Domain Name	Lee Flag	Page Resource	Page View	Policy Name	Policy Type
11-15-2021 04:36:02 AM	695	application/plax-crt	DEFAULT	23.192.60.120	lencr.org		http://x1.c.lencr.org/		DefaultGroup	Access
11-15-2021 04:36:03 AM	16183	-	WEBCAT	52.225.136.36	52.225.136.36		52.225.136.36;443;52.225.136.36;443		DefaultGroup	Decryption
11-15-2021 04:36:03 AM	608	application/vnd.ms-cab-compressed	WEBCAT	72.22.185.209	windowsupdate.com		http://cldl.windowsupdate.com/msdo...wloadupdate/v3/statictrusted/en/di...sallowedcertstl.cab?sa3d4fcdf985d67c		Skype	Access

4.3 Dashboards

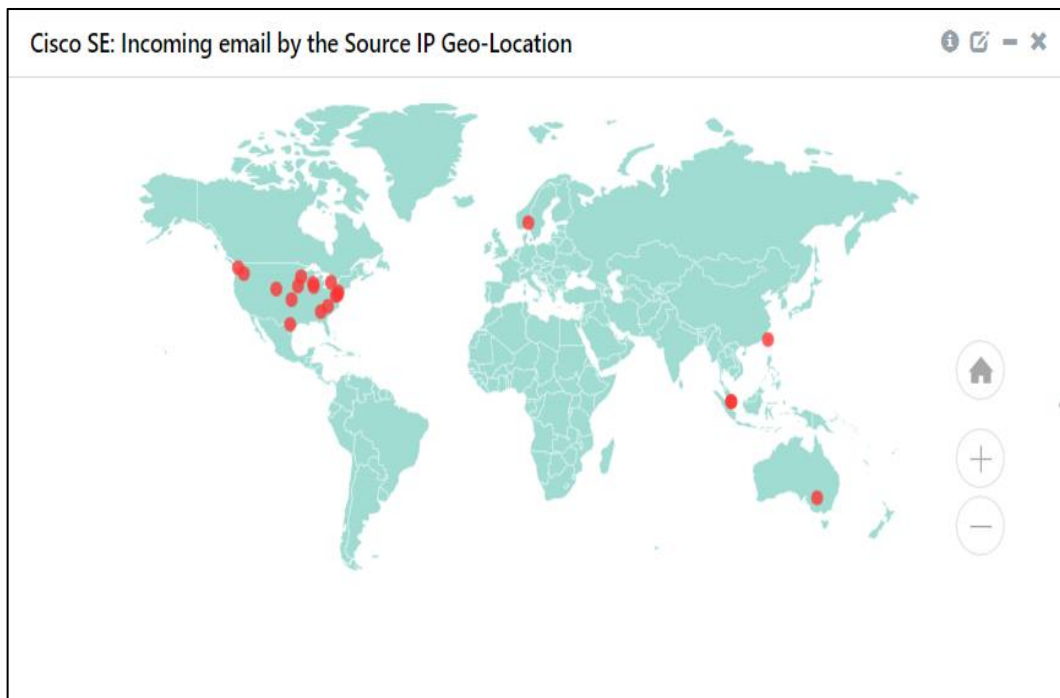
- Cisco SE: Events by email direction



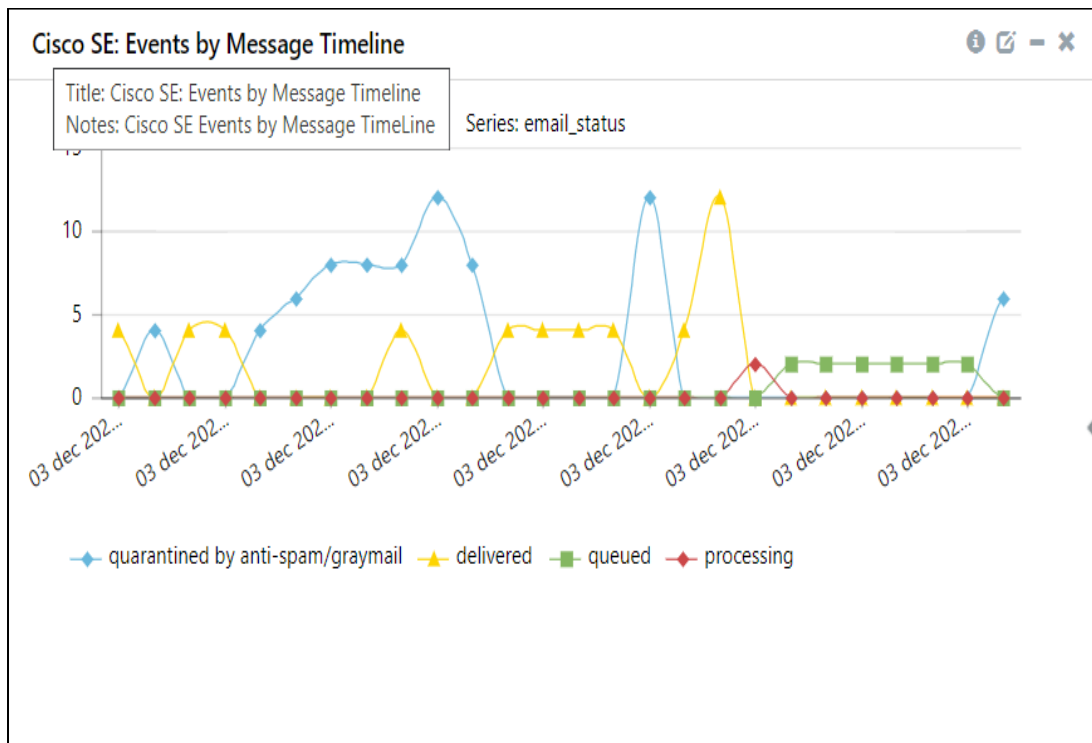
- Cisco SE: Events by the Message Status



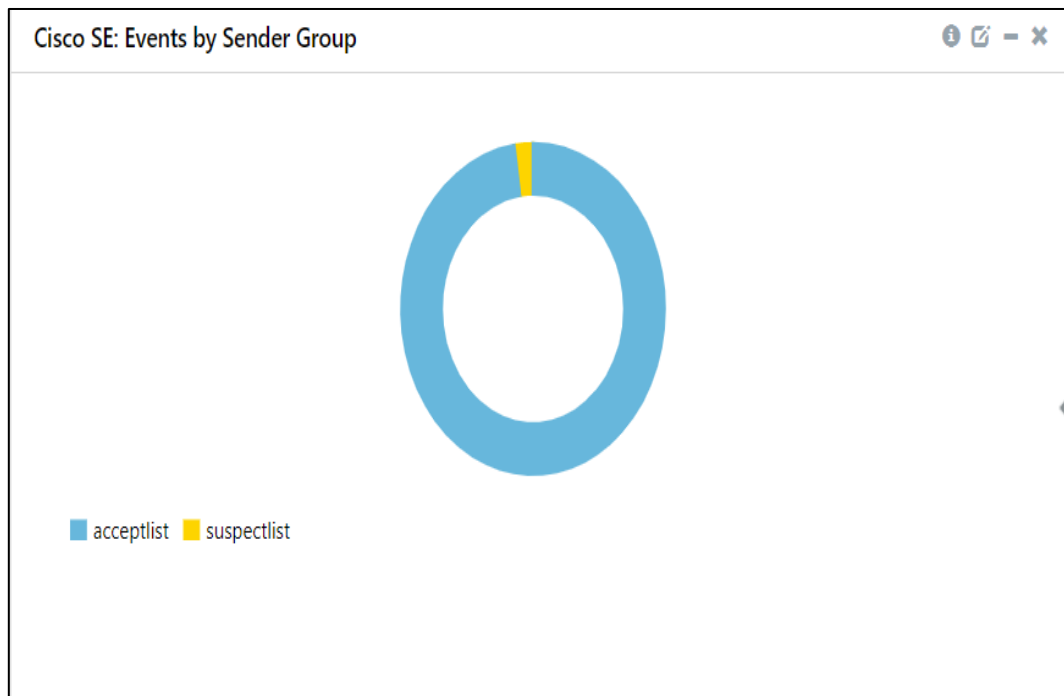
- Cisco SE: Incoming email by the Source IP address Geo-Location



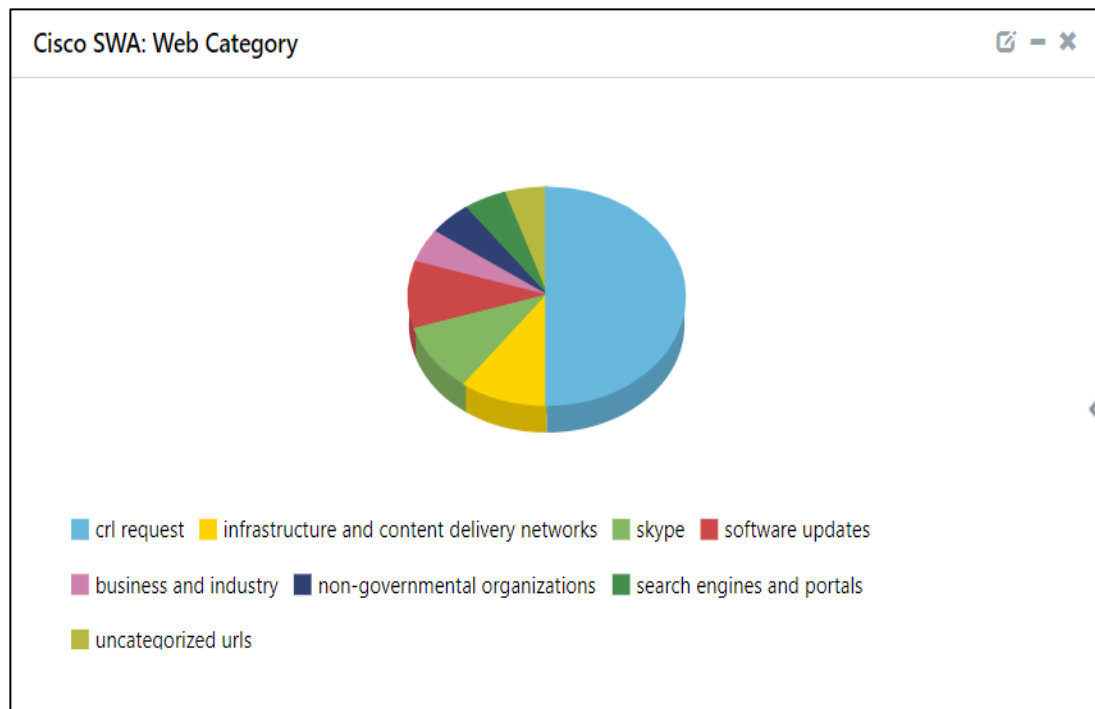
- Cisco SE: Events by the Message Timeline



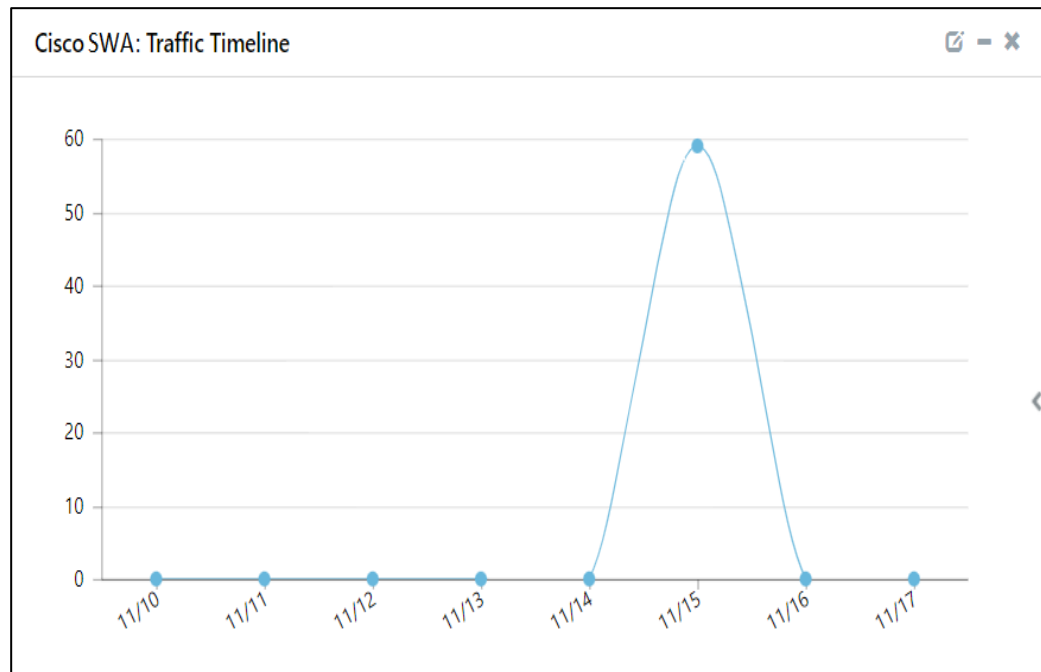
▪ Cisco SE: Events by the Sender Group



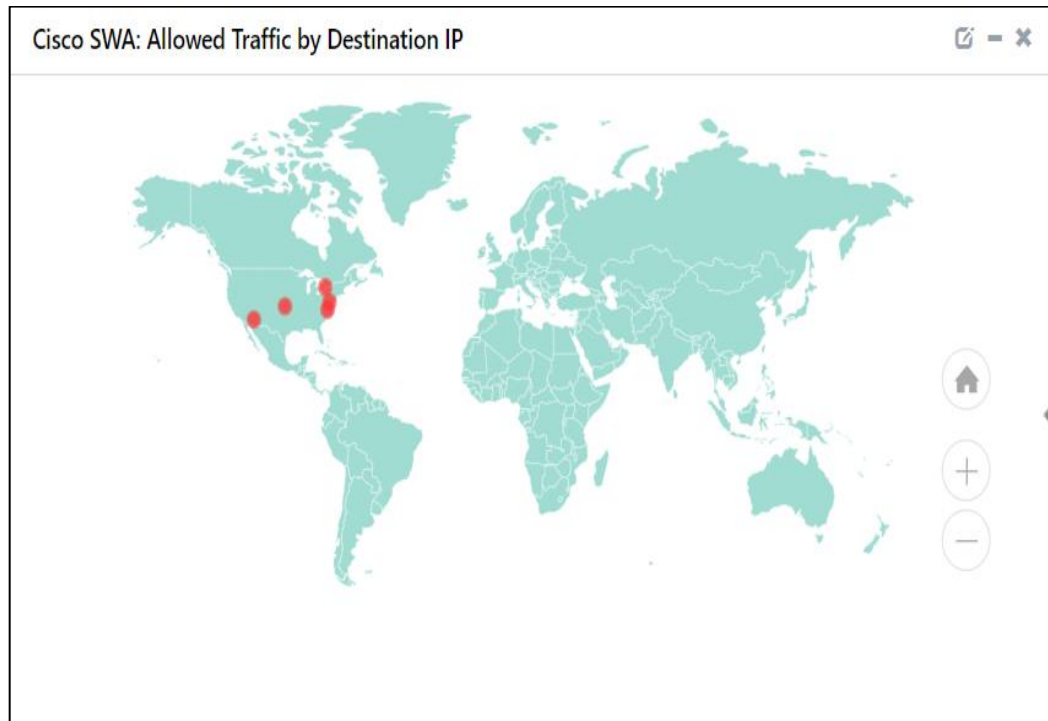
▪ Cisco SWA: Web Category



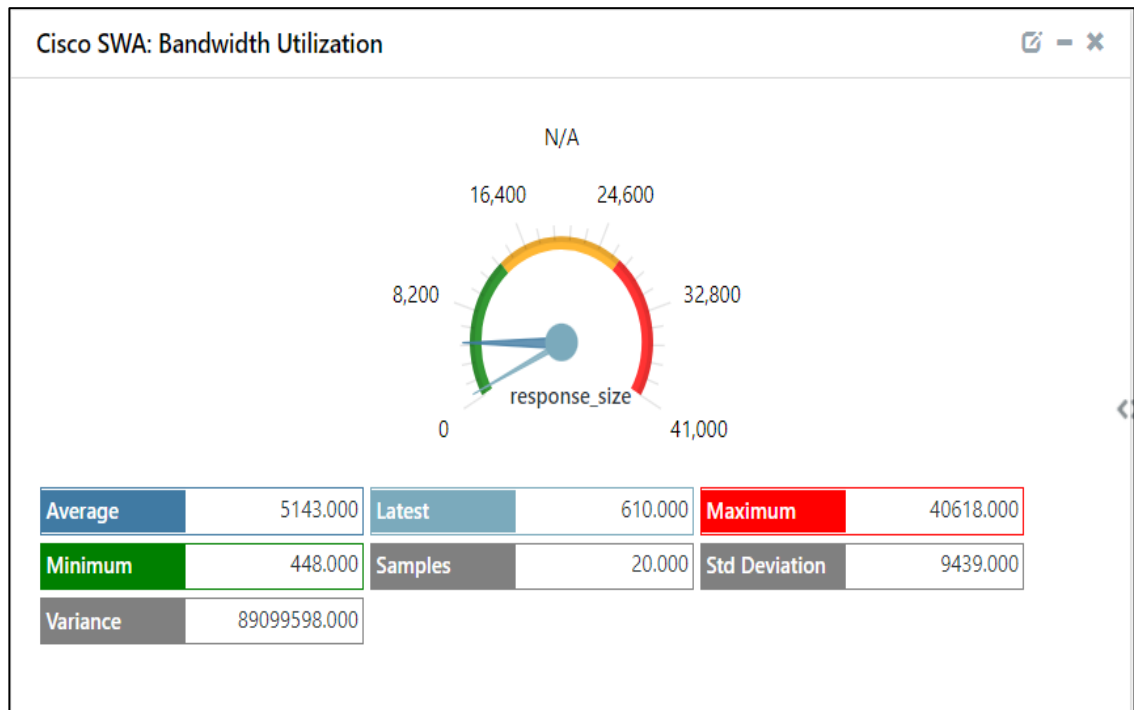
- Cisco SWA: Traffic Timeline



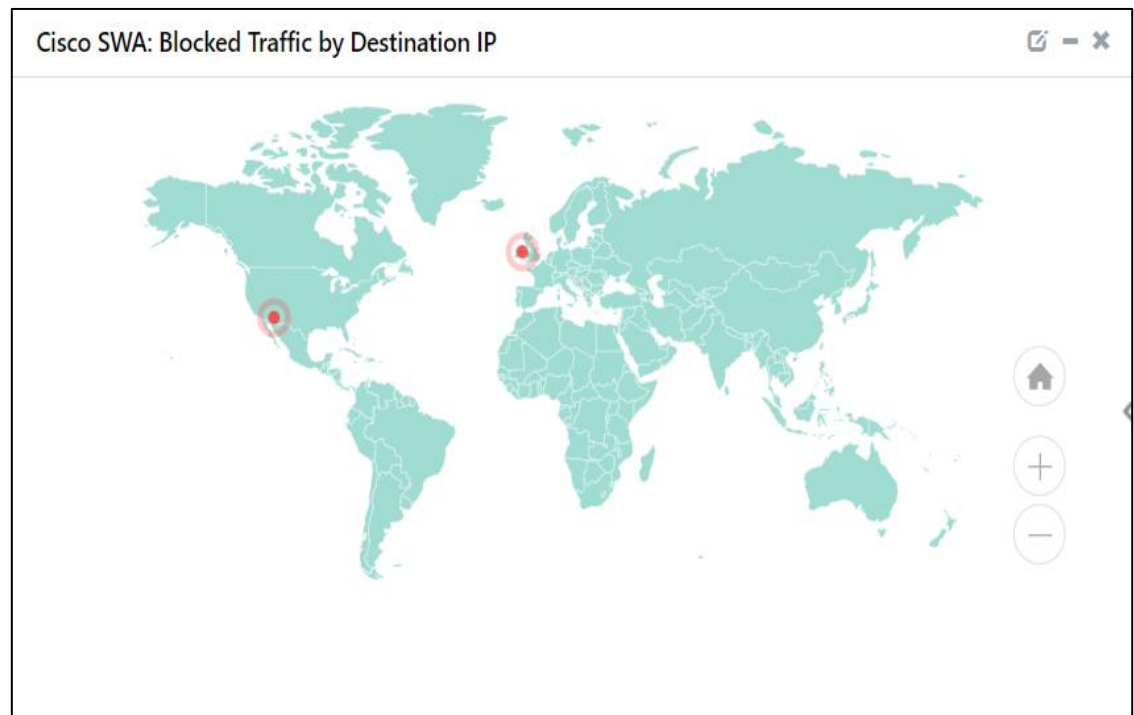
- Cisco SWA: Allowed Traffic by the Destination IP address



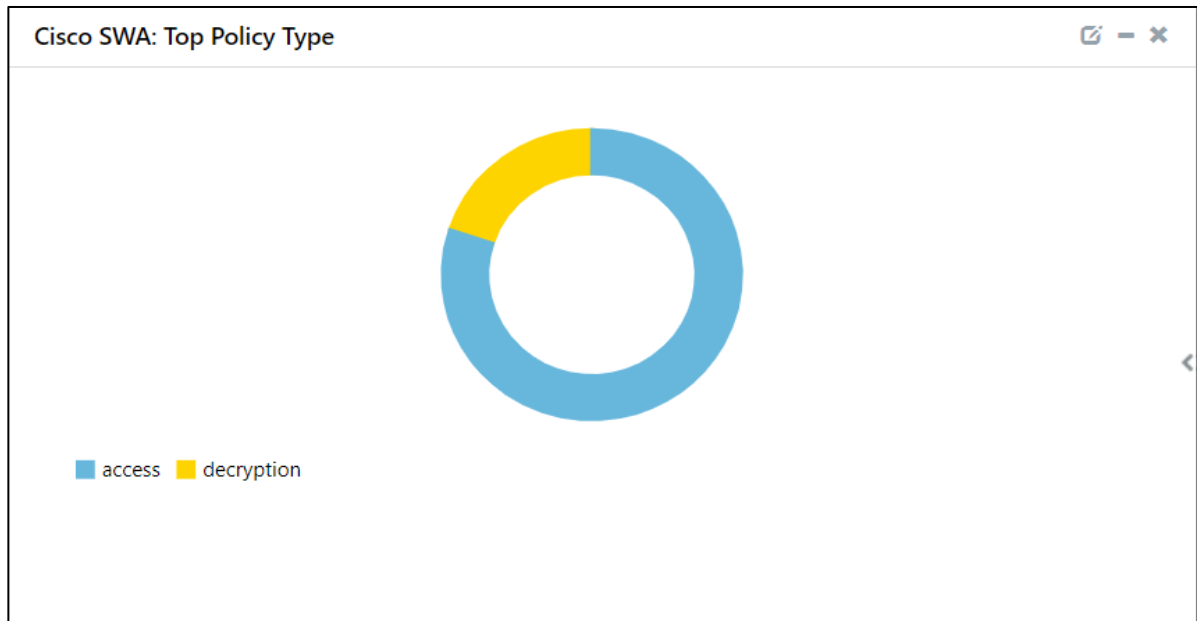
- Cisco SWA: Bandwidth Utilization



- Cisco SWA: Blocked Traffic by the Destination IP address

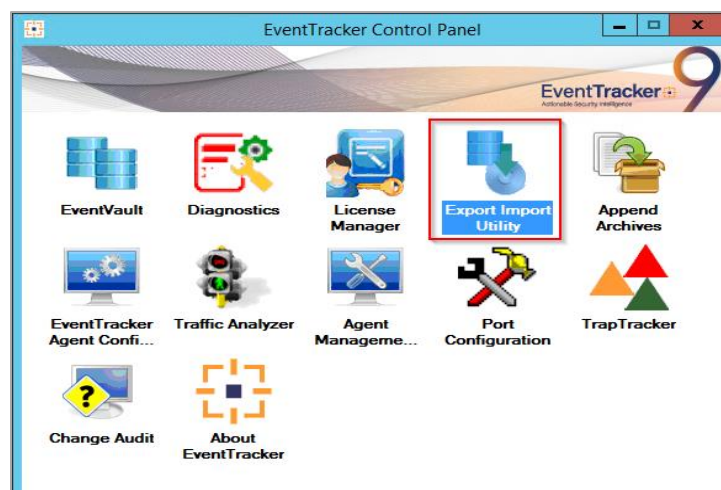


▪ Cisco SWA: Top Policy Type




5. Importing Cisco Email and Web Security Knowledge Pack into EventTracker

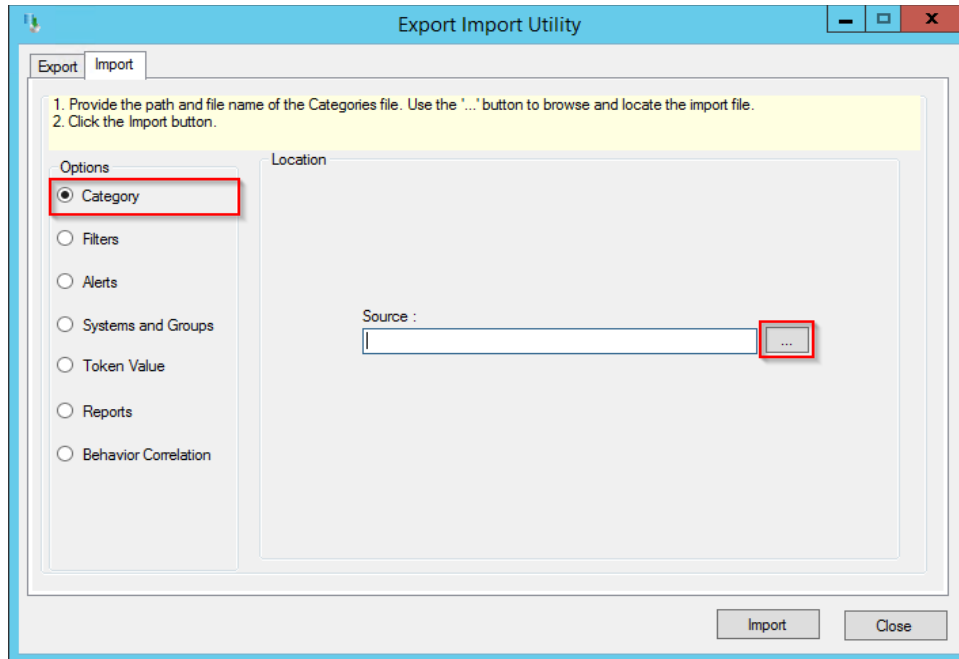
1. Launch the **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

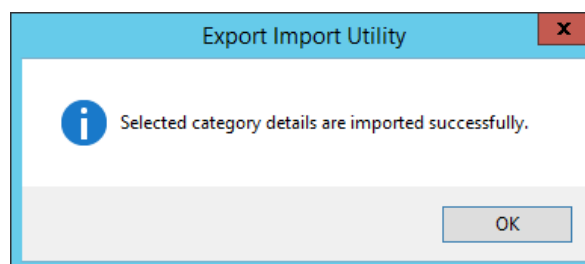
5.1 Categories

1. Click the **Category** option, and then click the **Browse**  button.



2. Locate the **Categories_Cisco SE.iscat** and **Categories_Cisco SWA.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

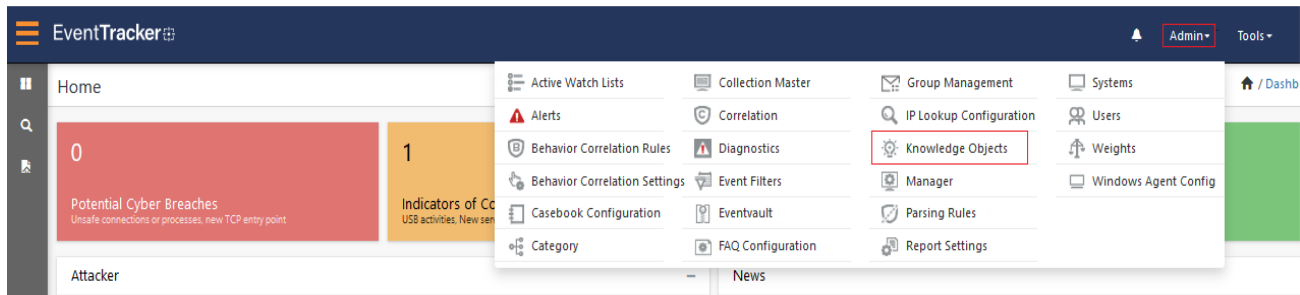
EventTracker displays a success message.



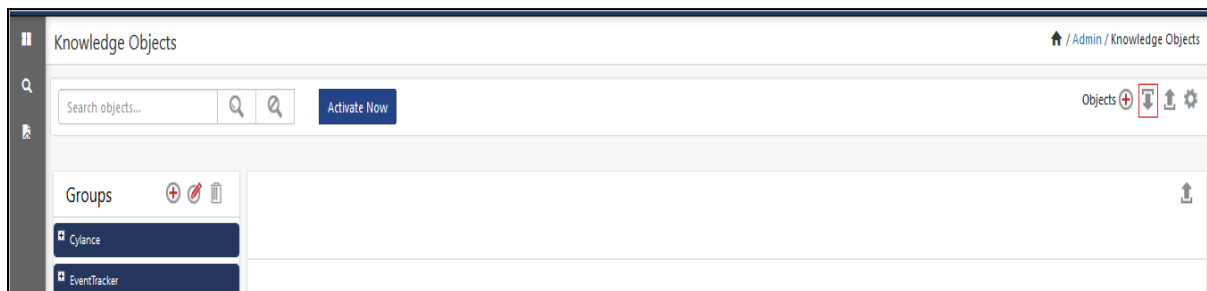
4. Click **OK**, and then click the **Close** button.

5.2 Knowledge Objects

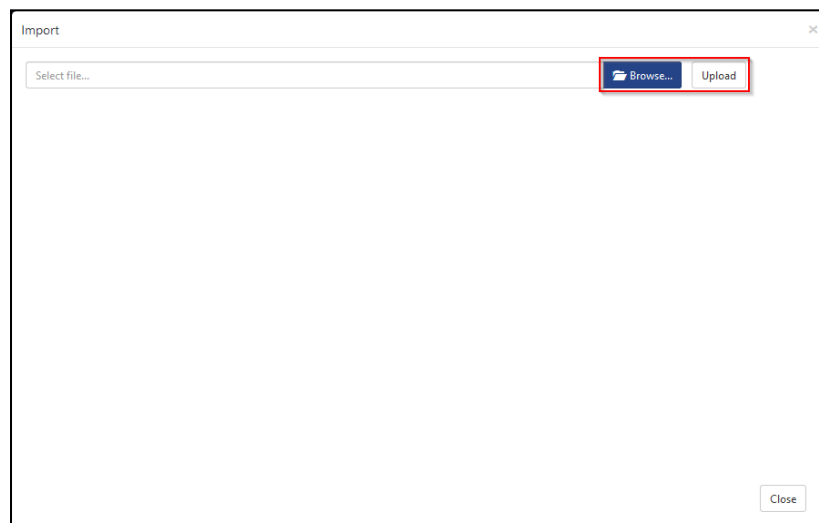
1. Click the **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.



2. Click the **Import** button as highlighted in the below image.



3. Click **Browse**.



4. Locate the file named **KO_Cisco SE.etko** and **KO_Cisco SWA.etko**.
5. Select the check box and then click the **Import** option.
6. Knowledge Objects (KO) are now imported successfully.

Import

Select file...

Browse...

Upload

<input checked="" type="checkbox"/>	Object name	Applies to	Group name
<input checked="" type="checkbox"/>	Cisco SWA	Cisco Email and Web Security	Cisco Email and Web Security

Import

Close

Import

Select file...

Browse...

Upload

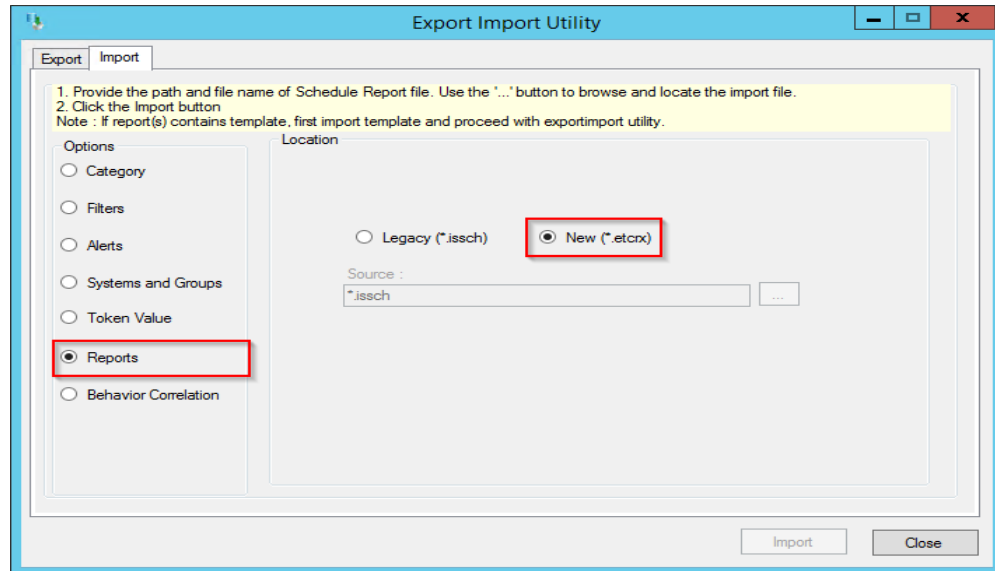
<input type="checkbox"/>	Object name	Applies to	Group name
<input type="checkbox"/>	Cisco SE Events	Cisco Secure Email v13.0	Cisco Email and Web Security

Import

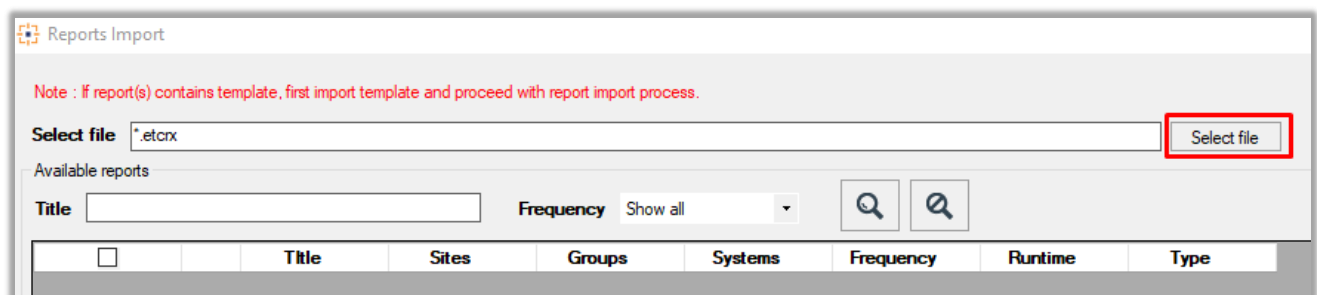
Close

5.3 Reports

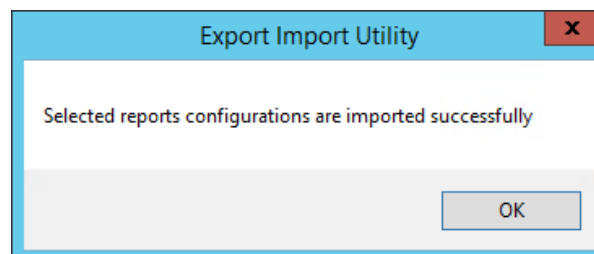
1. Click the **Reports** option and select the **New (*.etcrx)** option.



2. Locate the file named **Reports_Cisco SE.etcrx** and **Reports_Cisco SWA.etcrx**, select all the check boxes.



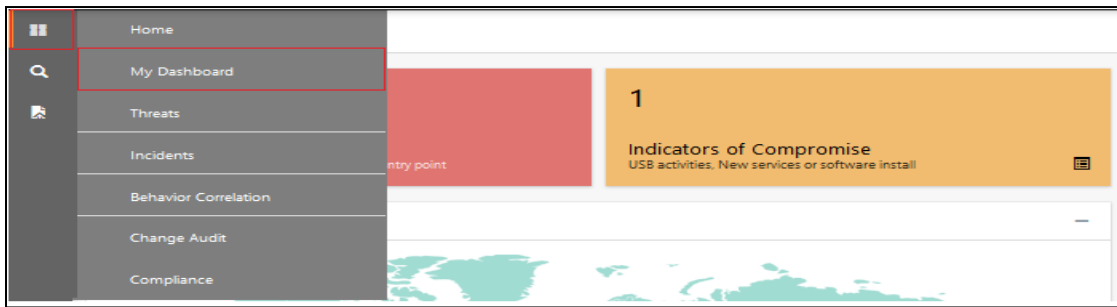
3. Click the **Import** button to import the report. EventTracker displays a success message.



5.4 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

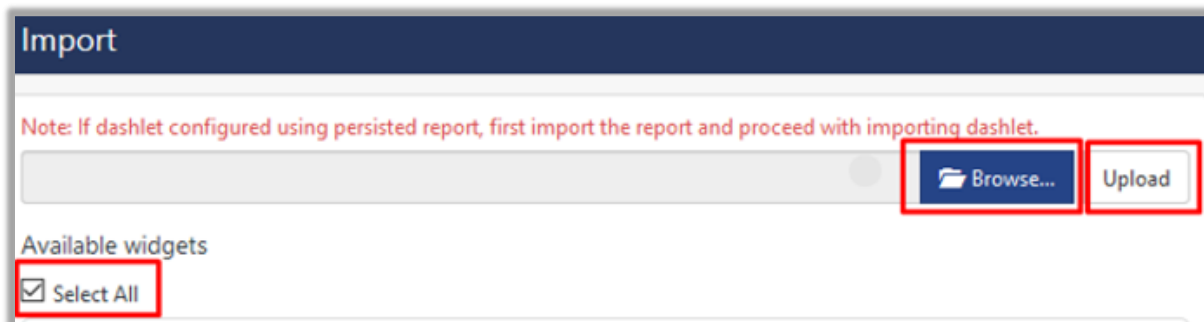
1. Open **EventTracker** in a browser and log on.



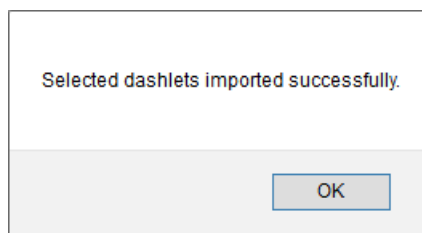
2. Navigate to the **My Dashboard** option as shown above.
3. Click the **Import** button.



4. Import the dashboard file **Dashboards_Cisco SE.etwd** and **Dashboards_Cisco SWA.etwd**, select the **Select All** checkbox.
5. Click the **Import** as shown below.




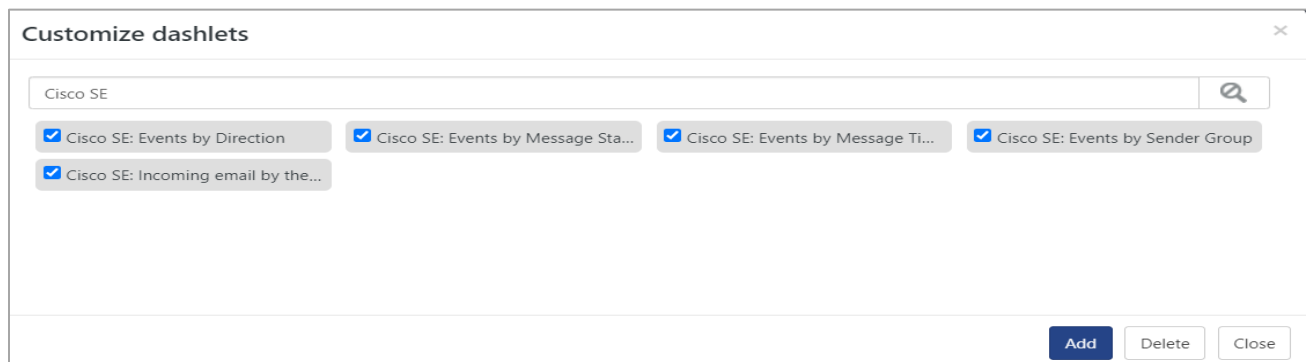
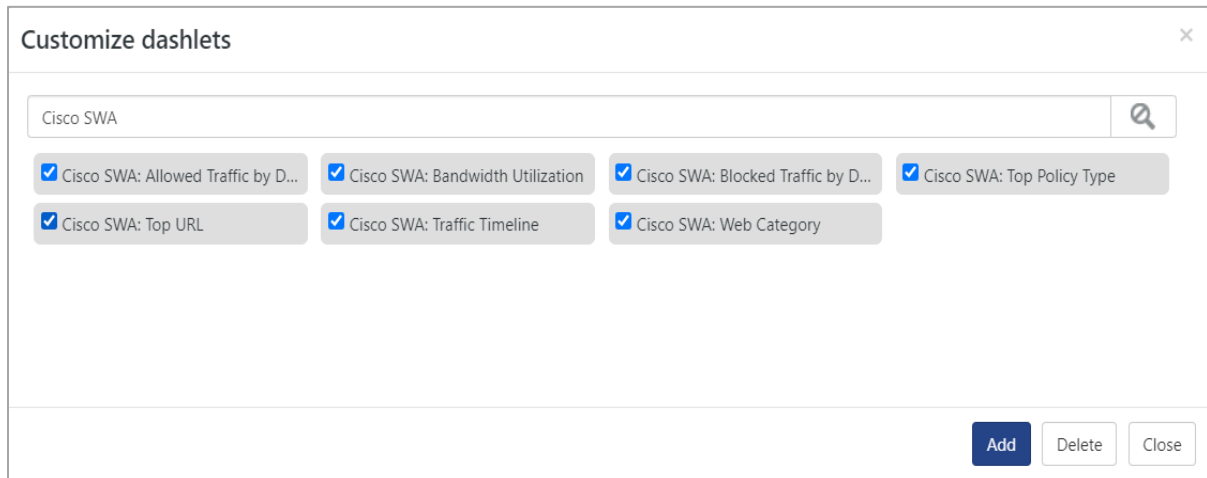
6. Import is now completed successfully.



7. In the **My Dashboard** page select **+** to add dashboard.



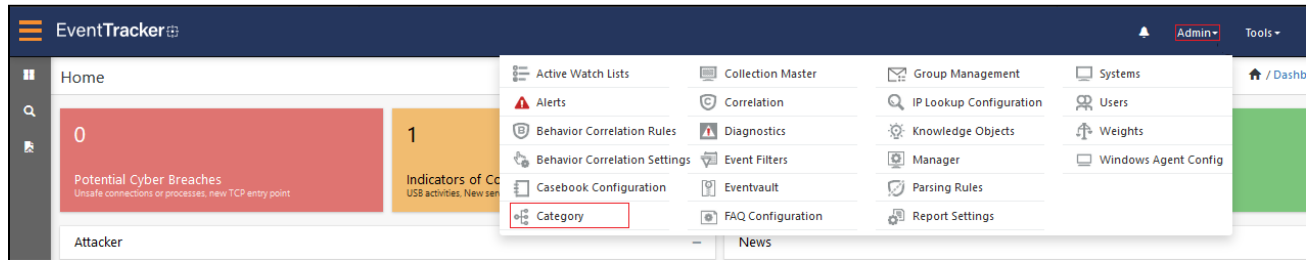
8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.
9. In the **My Dashboard** page select  to add dashlets.
10. Select the imported dashlets and click **Add**.



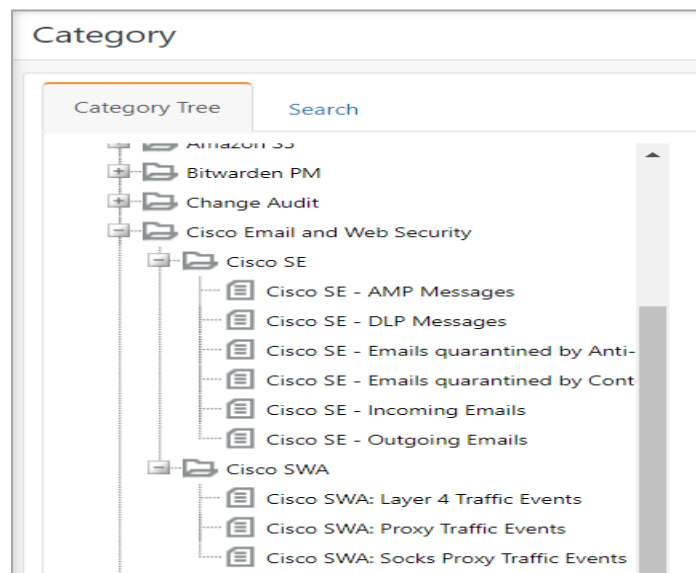
6. Verifying Cisco Email and Web Security Knowledge Pack in EventTracker

6.1 Categories

1. Logon to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Category**.

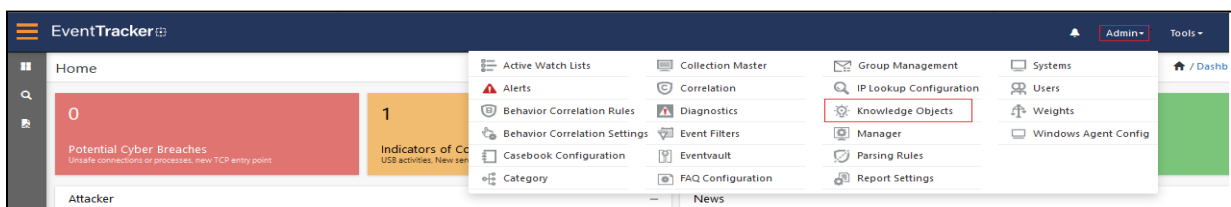


3. In the **Category Tree** to view the imported category, scroll down and expand the **Cisco Email and Web Security** group folder to view the imported category.

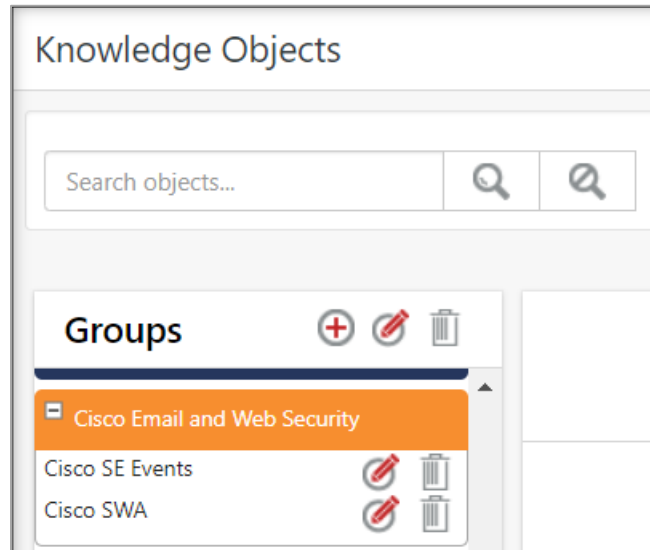


6.2 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select the **Knowledge Objects**.



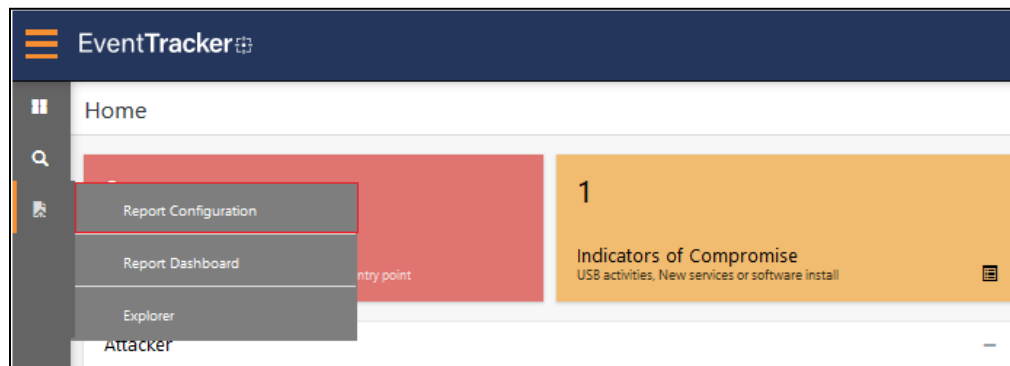
2. In the Knowledge Object tree, expand the **Cisco Email and Web Security** folder to view the imported Knowledge Object.



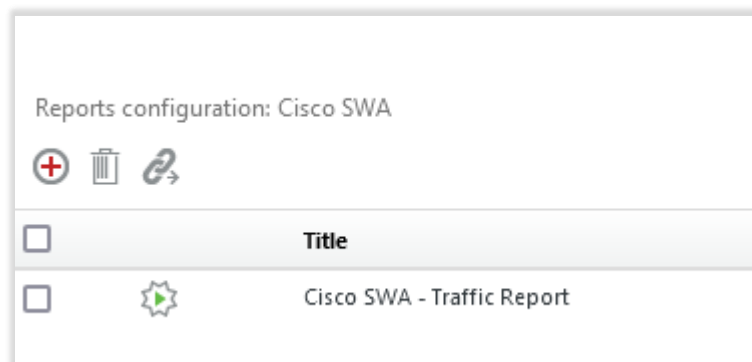
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.3 Reports




1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.





2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Cisco SWA** and **Cisco SE** group folders to view the imported reports.



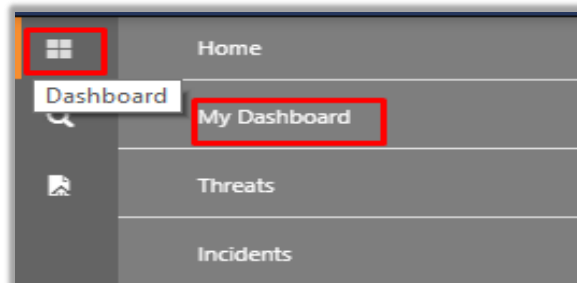
Reports configuration: Cisco SE






<input type="checkbox"/>		Title
<input type="checkbox"/>		Cisco SE - Emails Report
<input type="checkbox"/>		Cisco SE - AMP and DLP Messages


6.4 Dashboards

1. In the EventTracker web interface, click the **Home** button and select **My Dashboard**.



2. In the **My Dashboard** page select  to add dashlets.
3. Search for **Cisco SWA** or **Cisco SE**, you can see the imported dashlets.

Customize dashlets
×



☒ Cisco SWA: Allowed Traffic by D...

☒ Cisco SWA: Bandwidth Utilization

☒ Cisco SWA: Blocked Traffic by D...

☒ Cisco SWA: Top Policy Type

☒ Cisco SWA: Top URL

☒ Cisco SWA: Traffic Timeline

☒ Cisco SWA: Web Category

Add
Delete
Close

Customize dashlets
×

☒ Cisco SE: Events by Direction

☒ Cisco SE: Events by Message Sta...

☒ Cisco SE: Events by Message Ti...

☒ Cisco SE: Events by Sender Group

☒ Cisco SE: Incoming email by the...

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both.

Netsurion [Managed Threat Protection](#) combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion [Secure Edge Networking](#) delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#).

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
<https://www.netsurion.com/eventtracker-support>