How-To Guide

# Configuring Cisco Email and Web Security to Forward Logs to EventTracker

Author: Marketing

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

# 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 to create detailed reports, alerts, dashboards, and saved searches. These attributes of EventTracker help the user to view the critical information on a single platform.

The 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 contains 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.

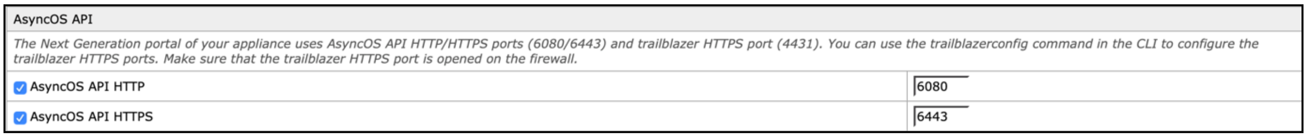
## 3.1 Enable AsyncOS API

In the cloud, the API is enabled by default.
Follow the below steps to enable 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.*

|  |  |
|---|---|
| ☑ AsyncOS API HTTP | 6080 |
| ☑ AsyncOS API HTTPS | 6443 |

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

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

7. Submit and commit your changes.

## 3.2 Enable Message Tracking (Applicable for Cisco Secure Email)

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 the message tracking for the first time, after running the **System Setup Wizard**, review the end-user.
4. 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. |

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

**If you select the Local Tracking, choose who can access the contents related to the 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 the Message Tracking can never view this information and hence they are not listed.

4. 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.

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.

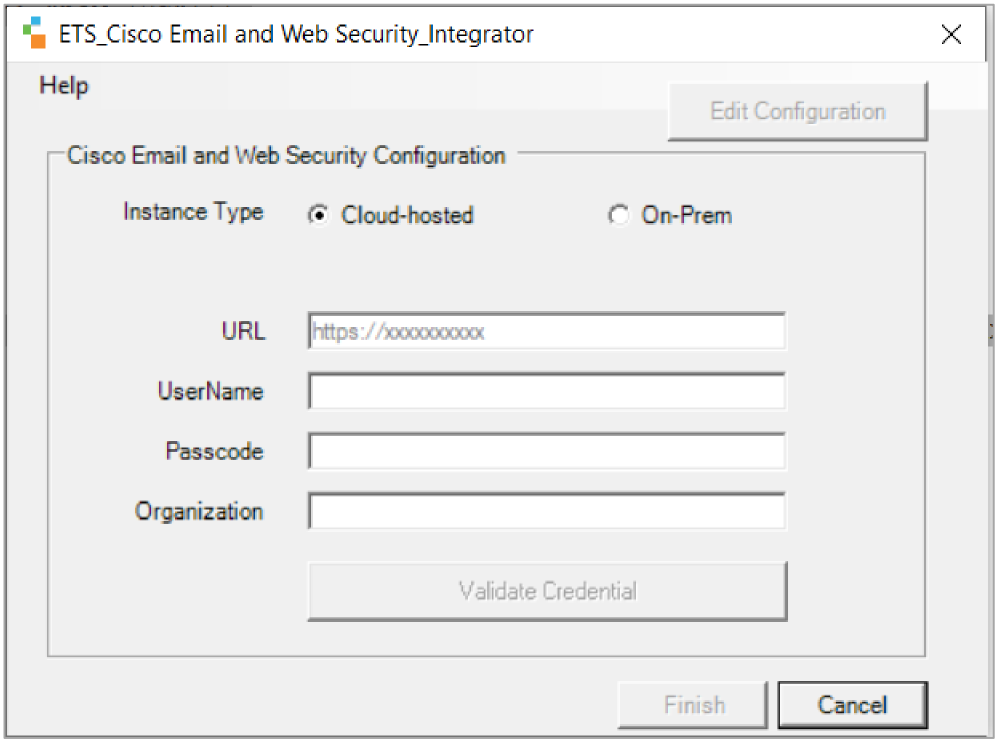
5. Select a predefined or custom user role. E.g., **Help Desk User**.
6. Enter a passphrase.
7. Submit and commit your changes.

## 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 "Cisco Email and Web Security" folder and launch the ETS_Cisco Email and Web Security_Configure.exe with administrator access.

**Cloud Based Integration**


ETS_Cisco Email and Web Security_Integrator
Help
Edit Configuration
Cisco Email and Web Security Configuration
Validate Credential
Finish
Cancel

Instance Type ● Cloud-hosted ○ On-Prem

URL https://xxxxxxxxxx

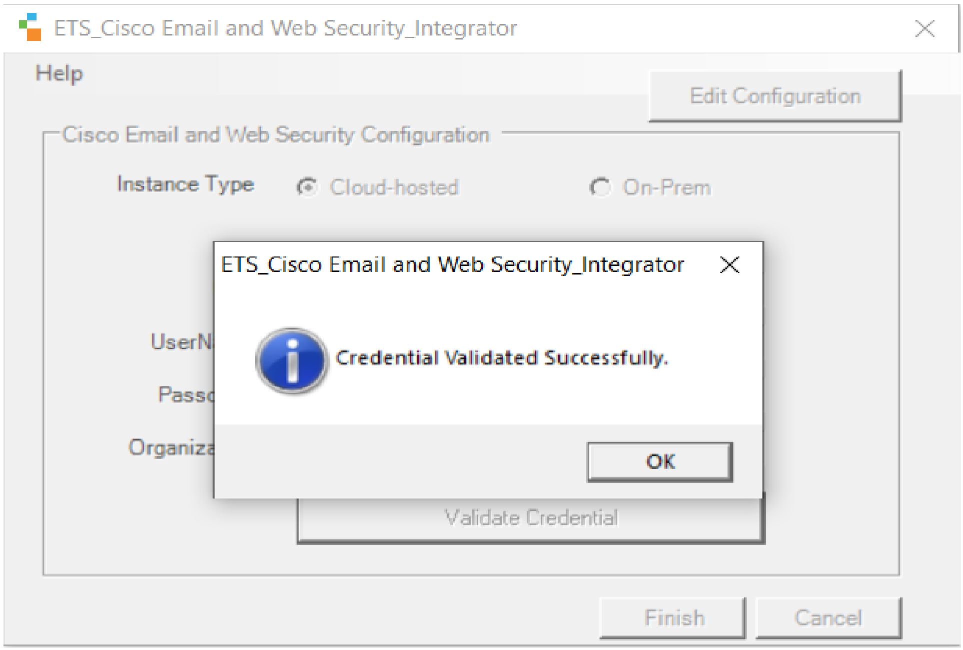
UserName

Passcode

Organization

1. Select the **Instance Type** as **Cloud-hosted** (**Default** selected)
2. Provide the **URL** (e.g., https://dhxxx.xxxx.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.**

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


ETS_Cisco Email and Web Security_Integrator

Instance Type ● Cloud-hosted ○ On-Prem

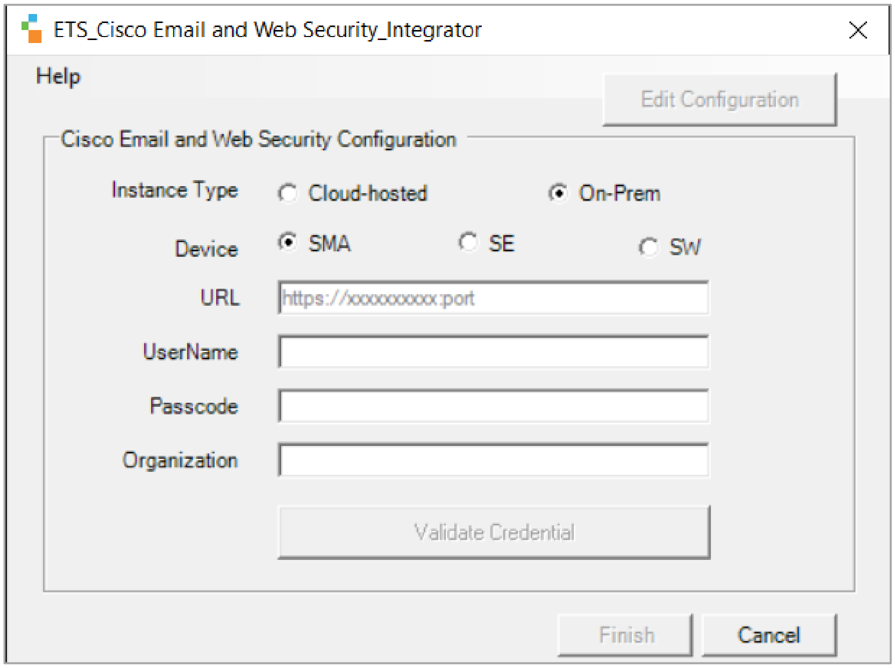
Credential Validated Successfully.

Help
Edit Configuration
Cisco Email and Web Security Configuration
UserN
Passc
Organiza
ETS_Cisco Email and Web Security_Integrator
OK
Validate Credential
Finish
Cancel

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

**On-Premises Integration**

1. Select the Instance Type as On-Premises.


ETS_Cisco Email and Web Security_Integrator

Instance Type ○ Cloud-hosted ● On-Prem

Device ● SMA ○ SE ○ SW

URL https://xxxxxxxxxx:port

UserName

Passcode

Organization

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.

## 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 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 MSP's 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