Troubleshoot XDR and Secure Email Appliance (Formerly ESA) Integration

Contents

Introduction

This document describes the steps to perform a basic analysis and how to troubleshoot the XDR and Insights and Secure Email Appliance integration module.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- XDR
- Security Services Exchange
- Secure Email

Components Used

The information in this document is based on these software and hardware versions:

- Security Services Exchange
- XDR
- Secure Email C100V on software version 13.0.0-392

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Cisco Secure Email Appliance (formerly Email Security Appliance) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secure important information in transit with end-to-end encryption. Once configured, the Secure Email Appliance module provides details associated with observables. You can:

- View the email reports and message tracks data from multiple appliances in your organization
- Identify, investigate and remediate threats observed in the email reports and message tracks
- Resolve the identified threats rapidly and provide recommended actions to take against the identified

threats
- Document the threats to save the investigation, and enable collaboration of information among other devices

The integration of a Secure Email Appliance module requires the use of Security Services Exchange (SSE). SSE allows a Secure Email Appliance to register with the Exchange and you provide explicit permission to access the registered devices.

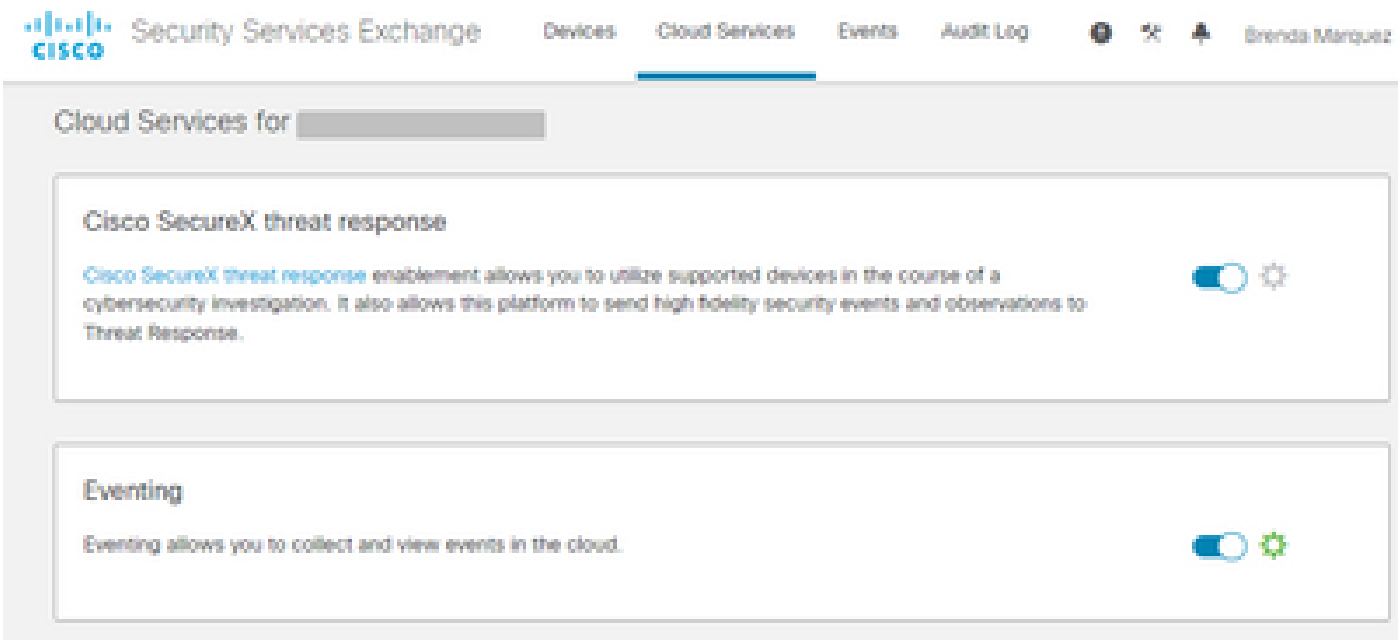
If you want to know more about the configuration, please review, this article here the integration module details.

Troubleshoot

In order to troubleshoot common issues with the XDR and Secure Email Appliance integration, you can verify these steps.

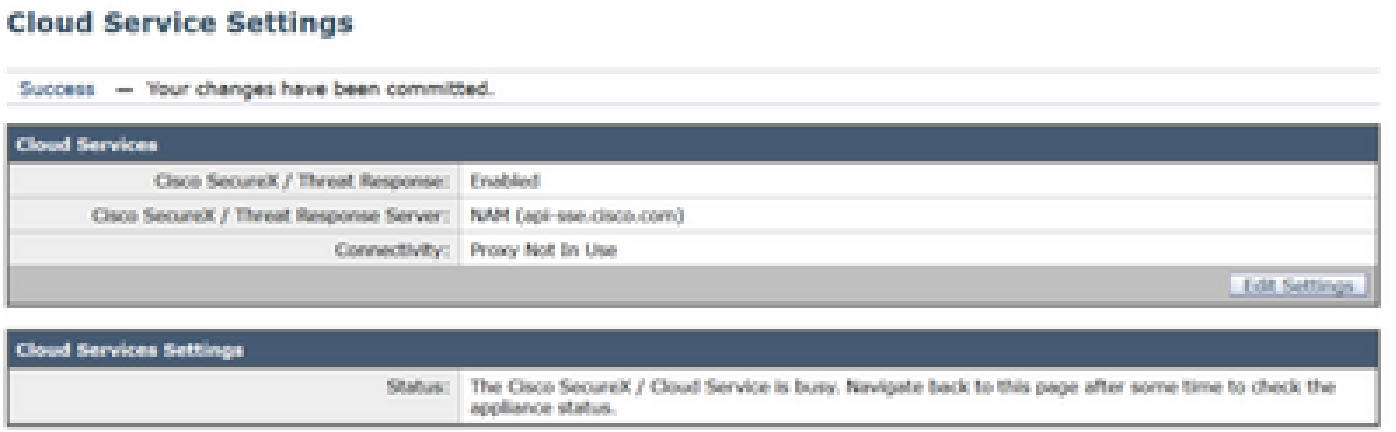
Secure Email device is not shown in the XDR nor Security Services Exchange portal

If your device is not shown in the SSE portal, please ensure to have enabled the **XDR Threat Response** and **Event** Services in the SSE portal, navigate to **Cloud Services**, and enable the services, as the image below:



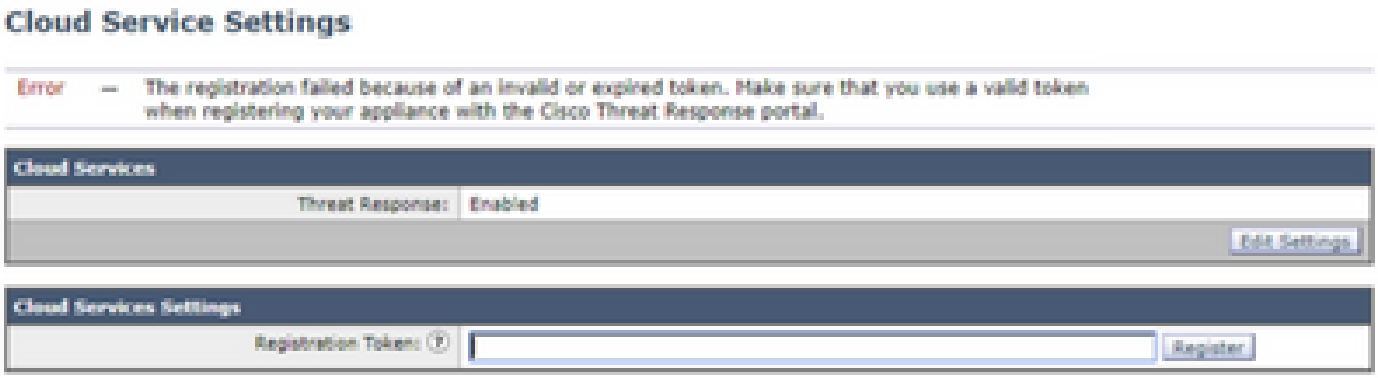
Secure Email does not request the Registration token

Please ensure to commit the changes, once the Cisco XDR / Threat Response service has been enabled, otherwise, the changes will not applied to the Cloud Service section in the Secure Email, see the image below.



Registration failed because of an invalid or expired token

If you see the error message: "The registration failed because of an invalid or expired token. Ensure that you use a valid token for your appliance with the Cisco XDR Threat Response portal" in the Secure Email GUI, as in the image below:



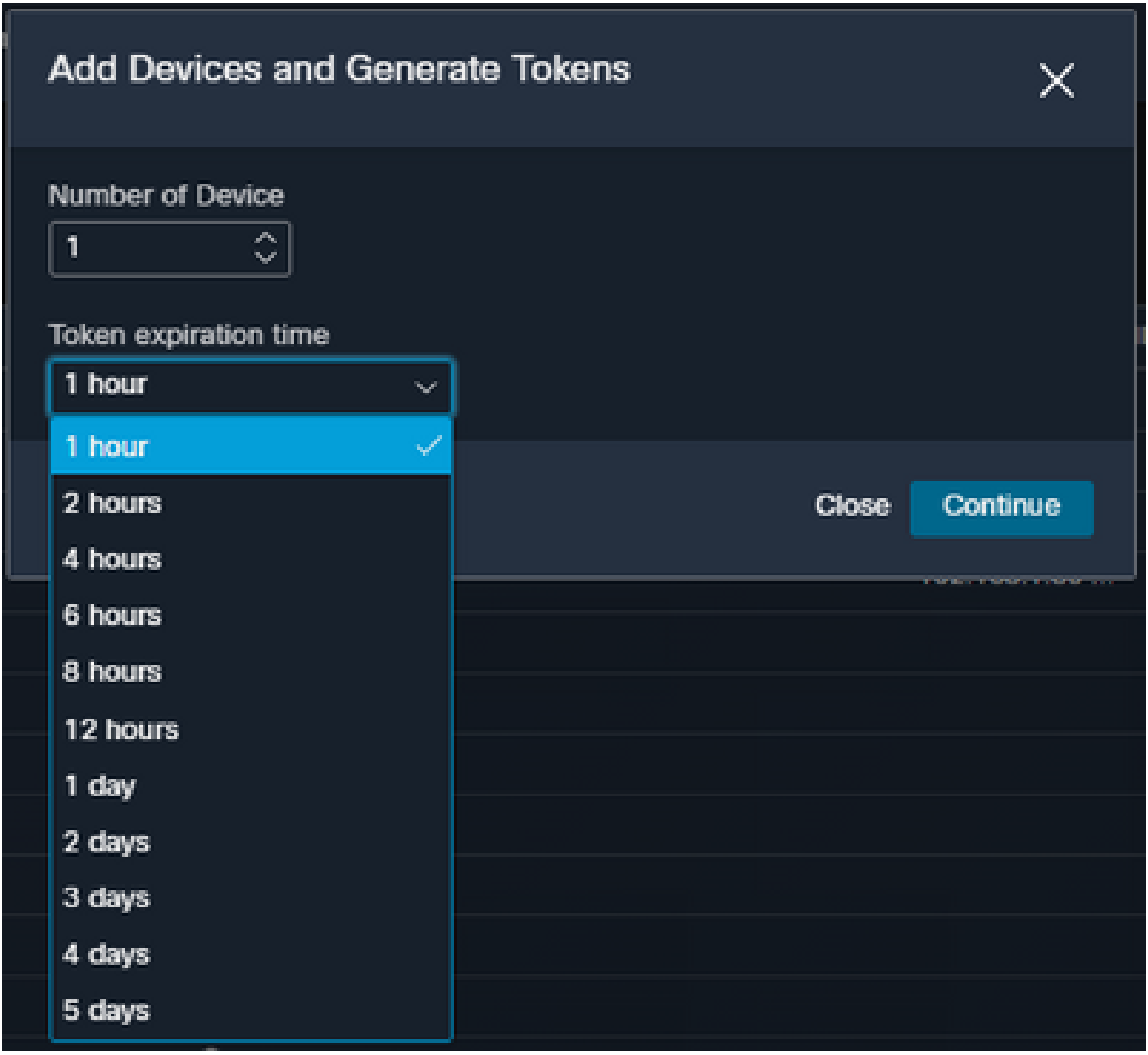
Please ensure that the token is generated from the correct Cloud:

If you use Europe (EU) Cloud for Secure Email, generate the token from https://admin.eu.sse.itd.cisco.com/

If you use Americas (NAM) Cloud for Secure Email, generate the token from https://admin.sse.itd.cisco.com/

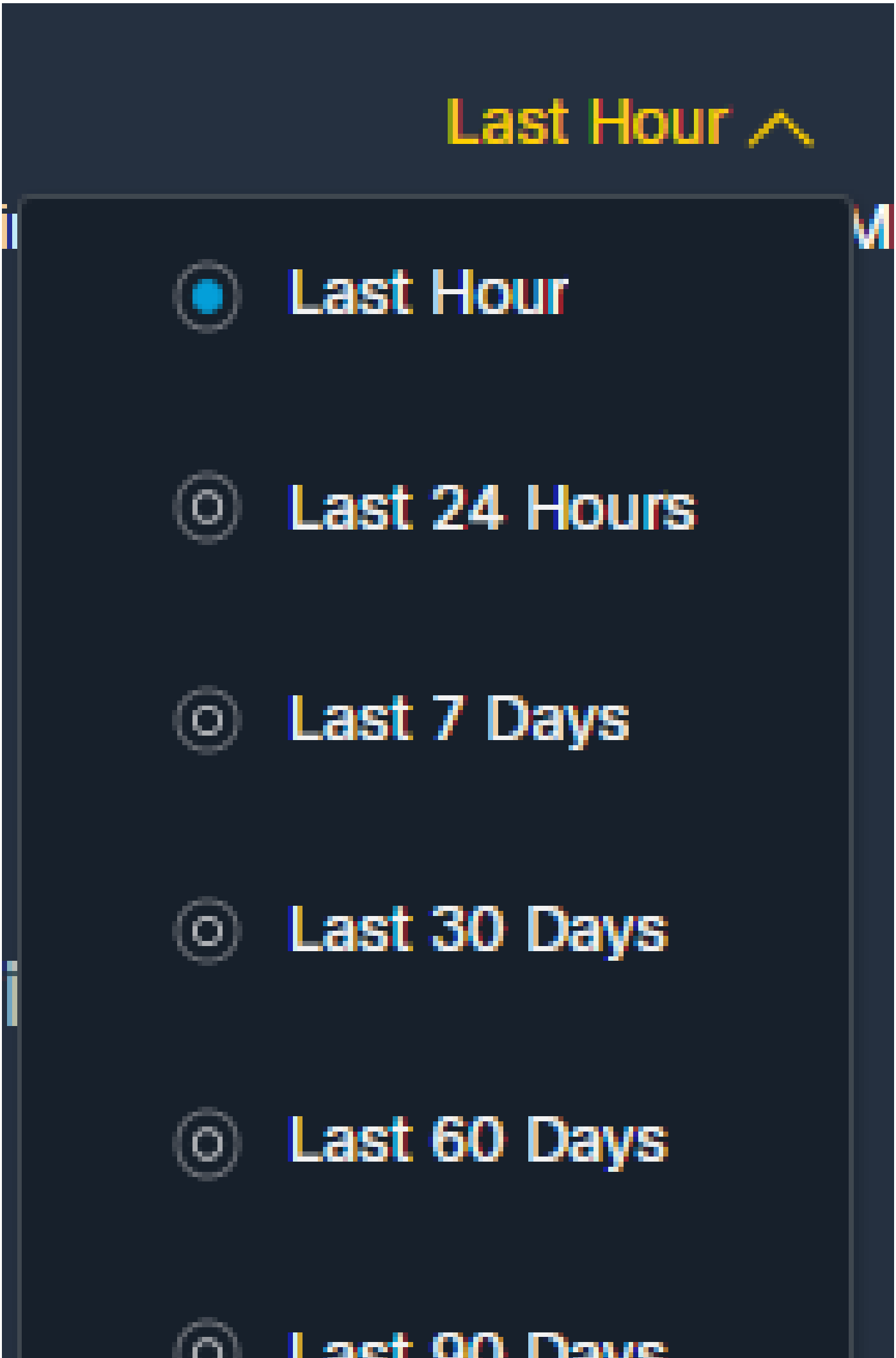
Security Services Exchange (SSE) portal:	NAM: https://admin.sse.itd.cisco.com/ EU: https://admin.eu.sse.itd.cisco.com/
Cisco XDR portal	NAM: https://XDR.us.security.cisco.com/ EU: https://XDR.eu.security.cisco.com/
Secure Email Cisco XDR / Threat Response Server:	NAM: api-sse.cisco.com EU: api.eu.sse.itd.cisco.com

Also, remember that the Registration token has an expiration time (select the most convenient time to complete the Integration in time), as shown in the image.



XDR Dashboard does not display information about the Secure Email module

You can select a wider time range in the available tiles, from **Last Hour** to **Last 90 Days**, as in the image below.


Last Hour
Last Hour
Last 24 Hours
Last 7 Days
Last 30 Days
Last 60 Days