Integrate WSA with CTR

Contents

Introduction

This document describes the steps to integrate Web Security Appliance (WSA) with Cisco Threat Response (CTR) portal.

Contributed by Shikha Grover and Edited by Yeraldin Sanchez Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- WSA access
- CTR portal access
- Cisco Security Account

Components Used

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

- Async Operating System version 12.x or later

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.

Configure

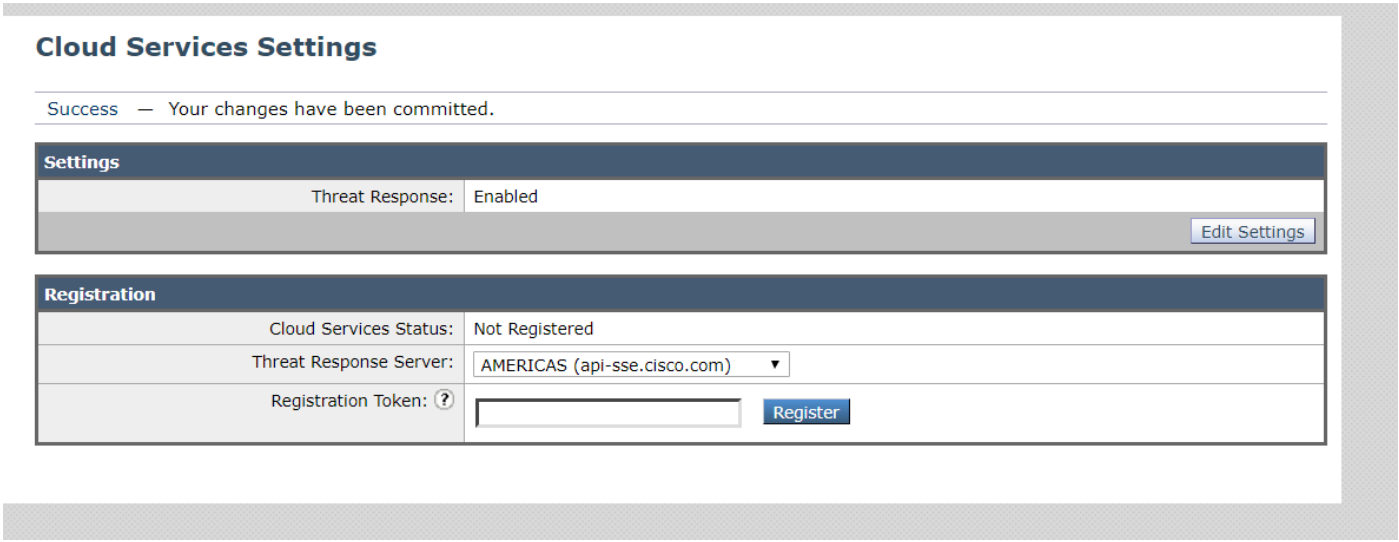
> **Caution**: If you access to CTR with a regional Asia Pacific, Japan, and China URL (https://visibility.apjc.amp.cisco.com/), the integration with your appliance is not currently supported.

Step 1. Enable **CTROBSERVABLE** under REPORTINGCONFIG in the CLI and commit the changes, as shown in the image.

```
WSA-12-0-1-173.COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

Step 2. Configure the Security Service Exchange (SSE) cloud portal, navigate to **Network >Cloud Services Settings > Edit settings**, click **Enable** and **Submit**, as shown in the image.

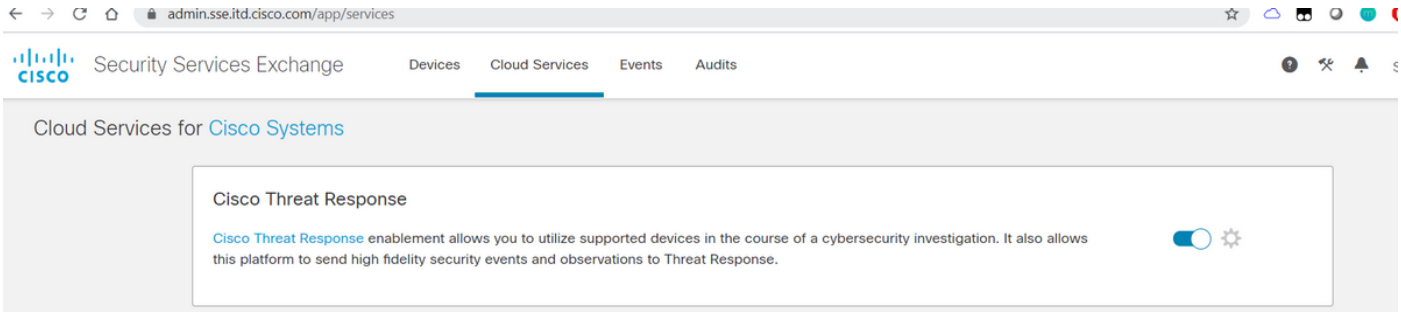
Chose the cloud as per your location, as shown in the image.



Step 3. If you do not have a Cisco Security account, you can create a user account in the Cisco Threat Response portal with admin access rights.

In order to create a new user account, navigate to the Cisco Threat Response portal login page.

Step 4. Enable Cisco Threat Response under Cloud Services on the SSE portal, as shown in the image.



Step 5. Make sure WSA has reachability on port 443 to the SSE portal:

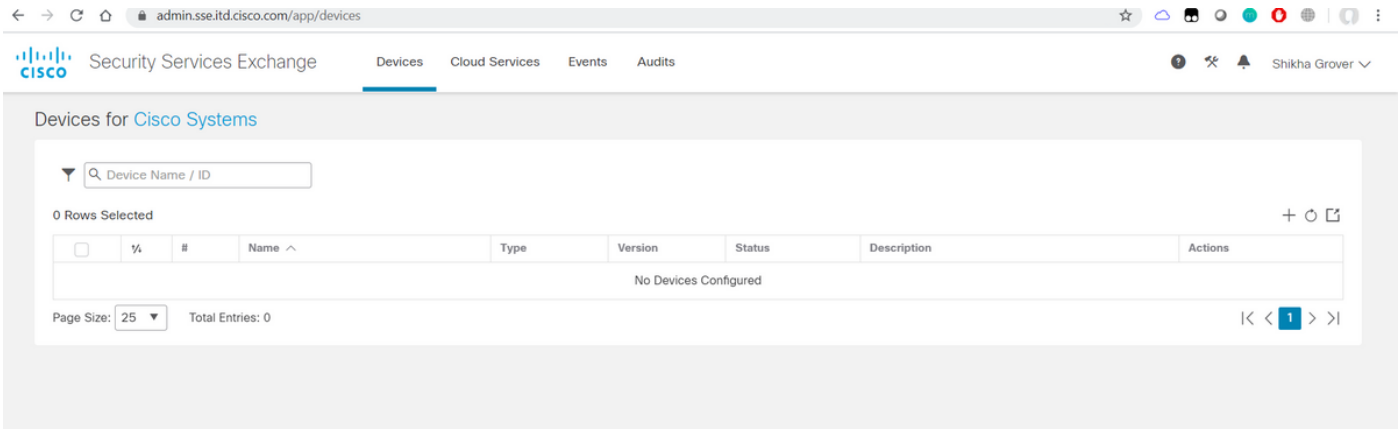
- api.eu.sse.itd.cisco.com (Europe)
- api-sse.cisco.com (America)

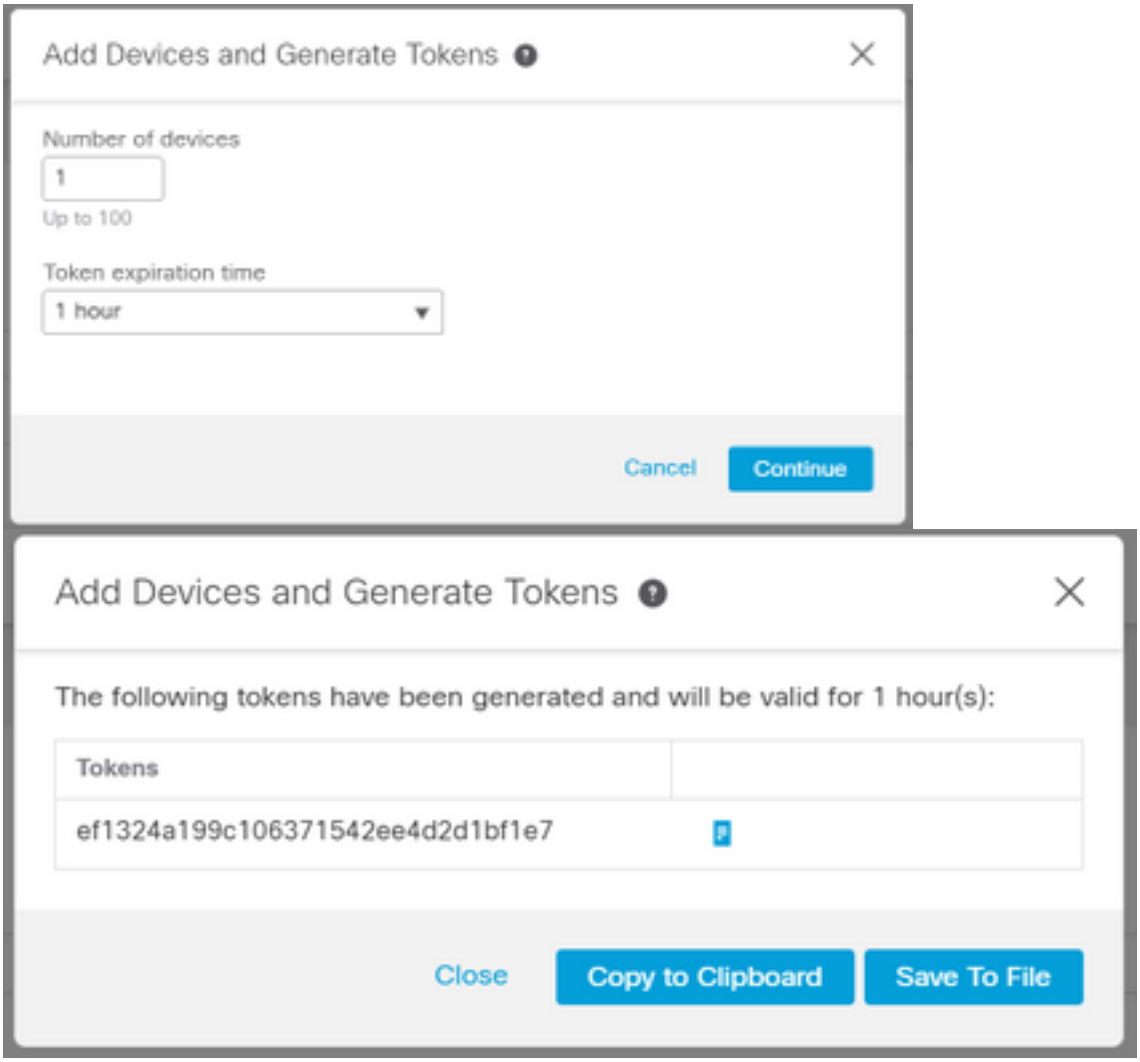
Register the Appliance

Step 1. Obtain a registration token from the Security Services Exchange (SSE) portal to register your appliance with the Security Services Exchange portal.

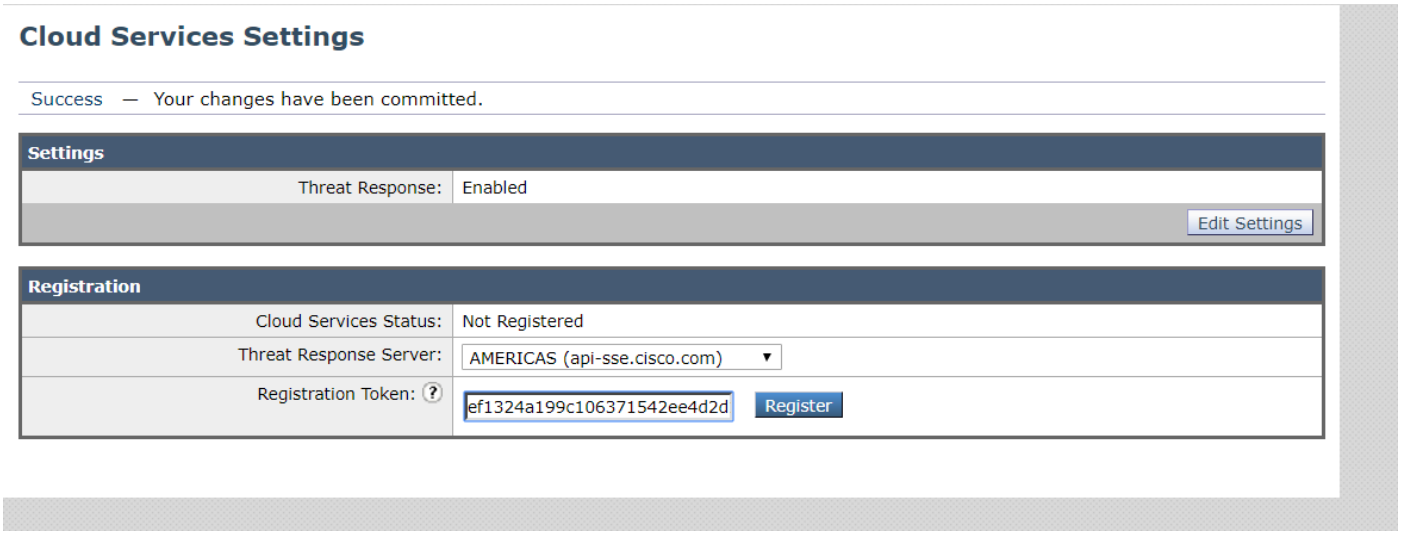
SSE portal link is https://admin.sse.itd.cisco.com/app/devices.

> **Note**: Use CTR account credentials to login to SSE portal.



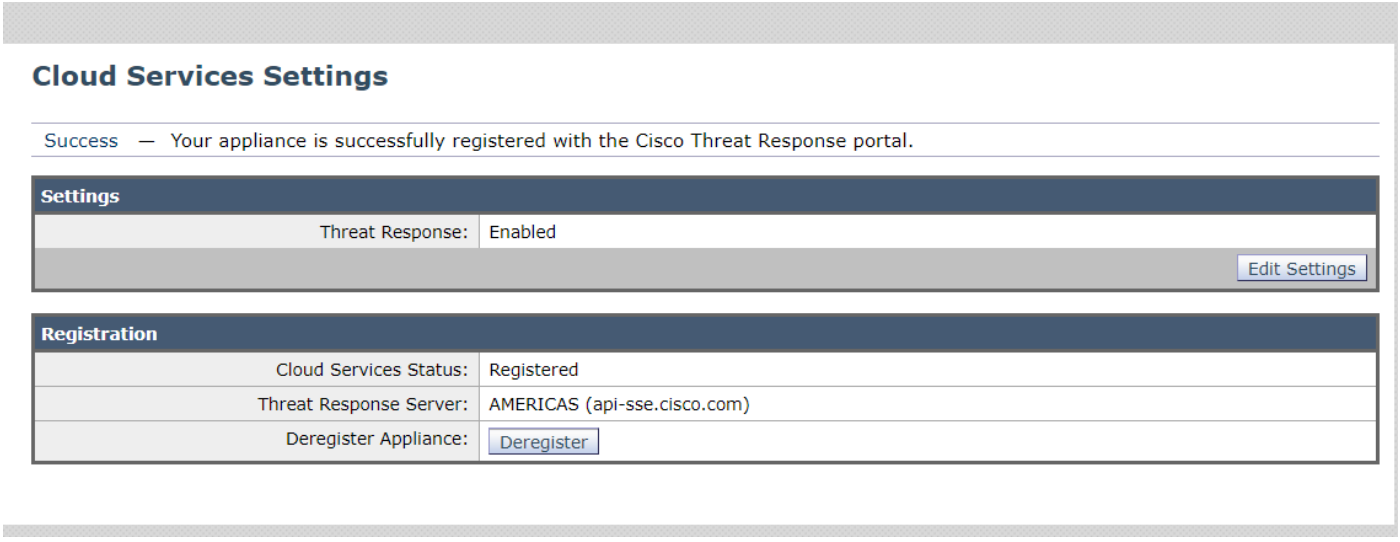


Step 2. Enter the registration token obtained from the Security Services Exchange portal in WSA and click **Register**, as shown in the image.

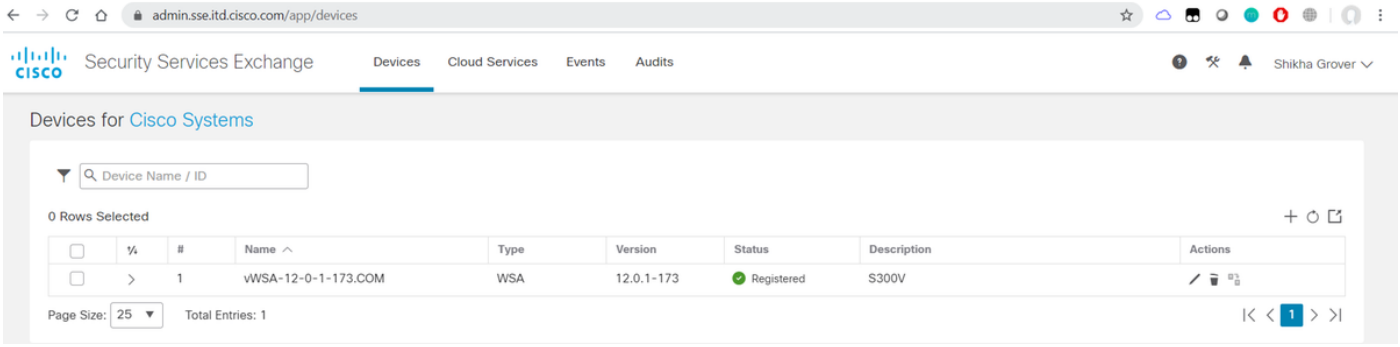


Step 3. After a few seconds, you would see registration is successful.

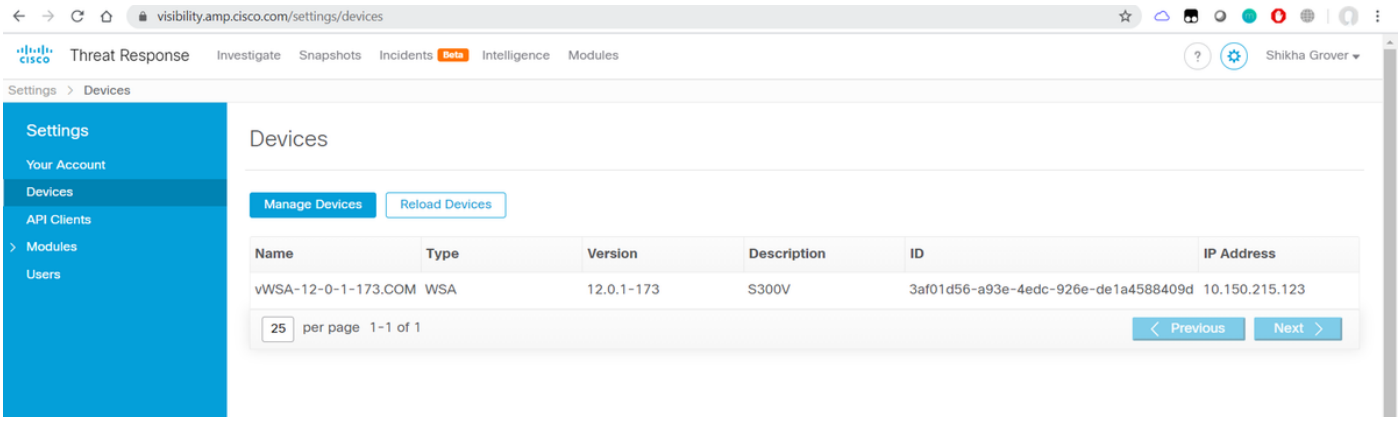
Caution: Make sure the token generated is used before it expires.



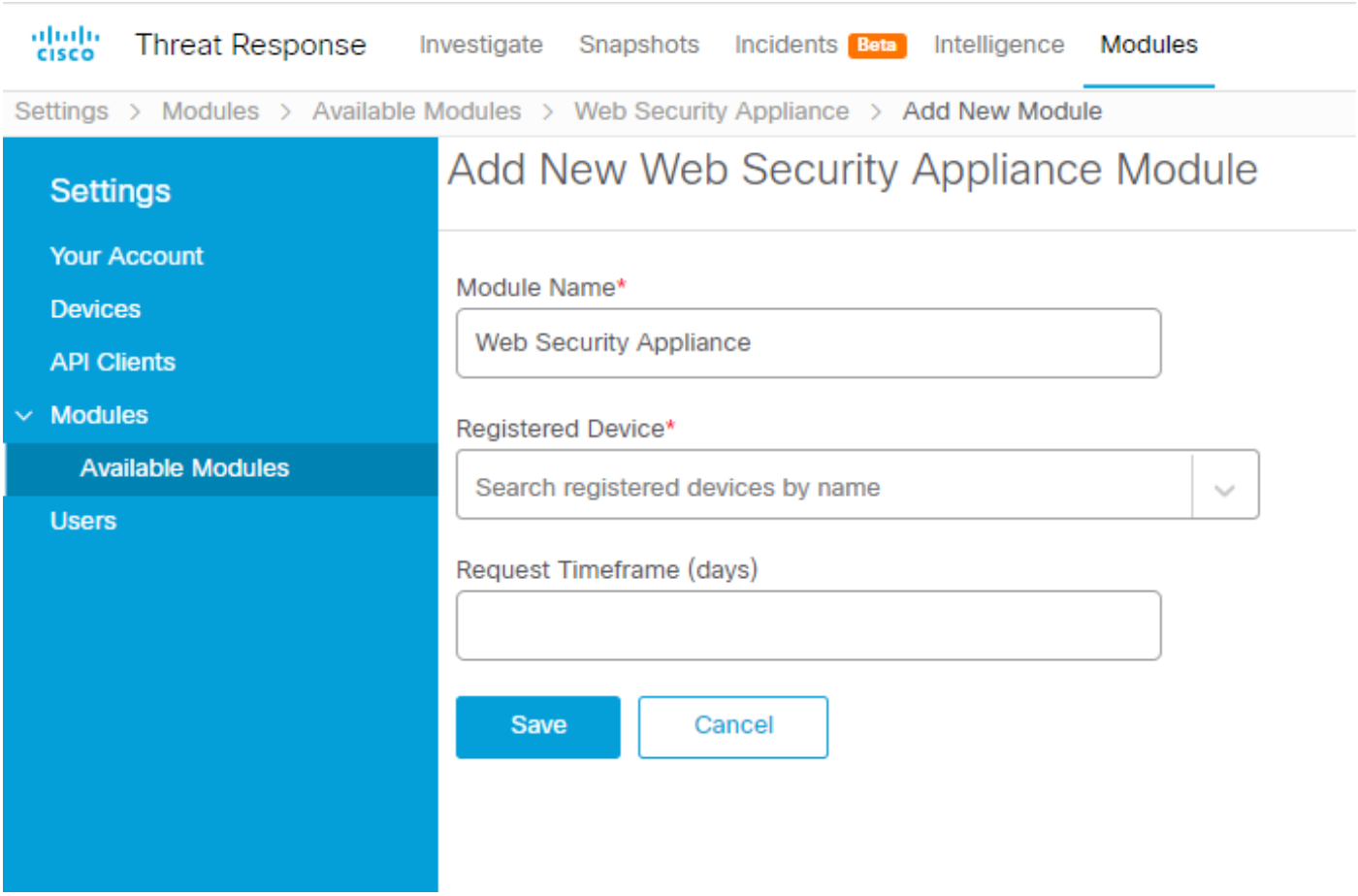
Step 4. On the SSE portal, you can see the device status.



Step 5. On the CTR portal appears the device registered.



You can associate this device to a module, navigate to **Modules > Add New Module > Web Security Appliance**, as shown in the image.



The device is now integrated. You can pass through traffic from the WSA and investigate threats on the CTR portal.

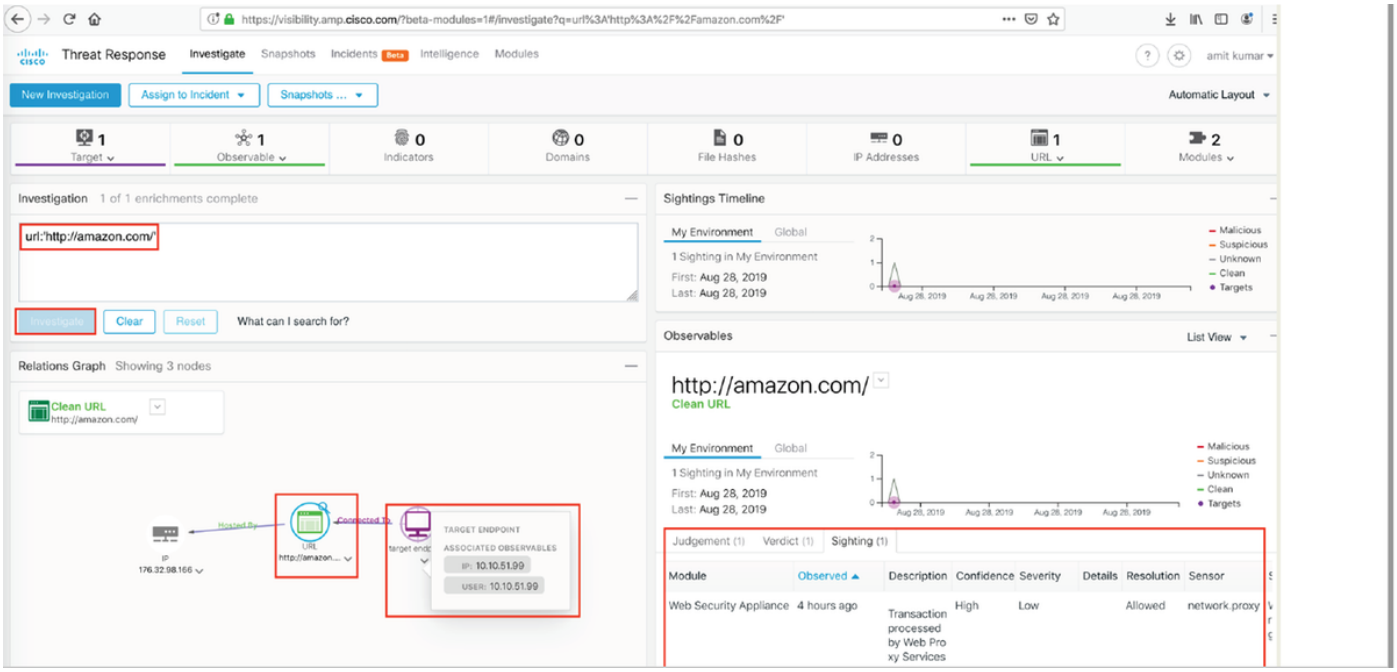
Verify

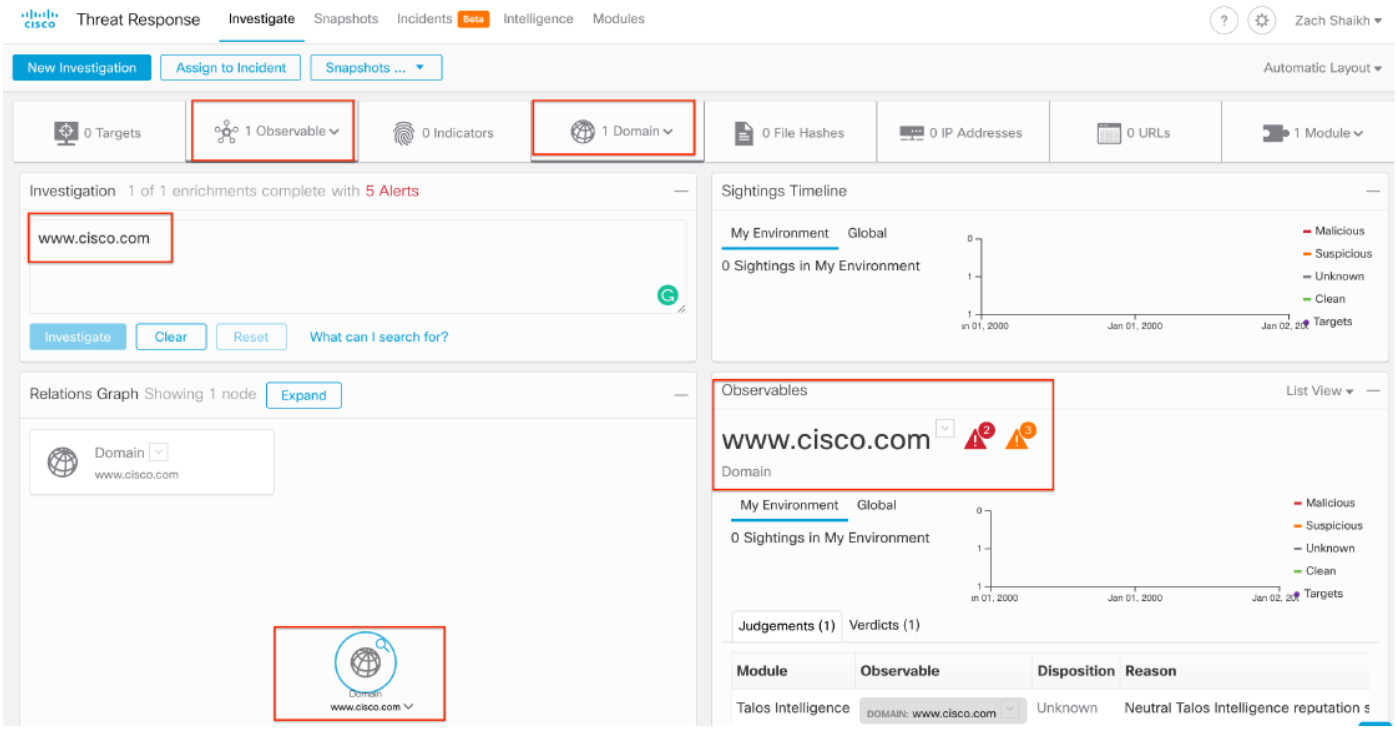
Use this section to confirm that your configuration works properly.

Enrichments(Querying the WSA logs) available for the WSA module and their supported format for running the query from the CTR portal:

- Domain – domain:"com"
- URL – url:"http://www.neverssl.com"
- SHA256 – sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP – ip:"172.217.26.164"
- Filename – file_name:"test.txt"

Enrichments in use as an example:





Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included. Feel free to let me know if I have missed something that should be included.