将WSA与CTR集成

目录

简介

本文档介绍将网络安全设备(WSA)与思科威胁响应(CTR)门户集成的步骤。

供稿：Shikha Grover，编辑者：Yeraldin Sanchez Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- WSA访问
- CTR门户访问
- 思科安全帐户

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 异步操作系统版本12.x或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

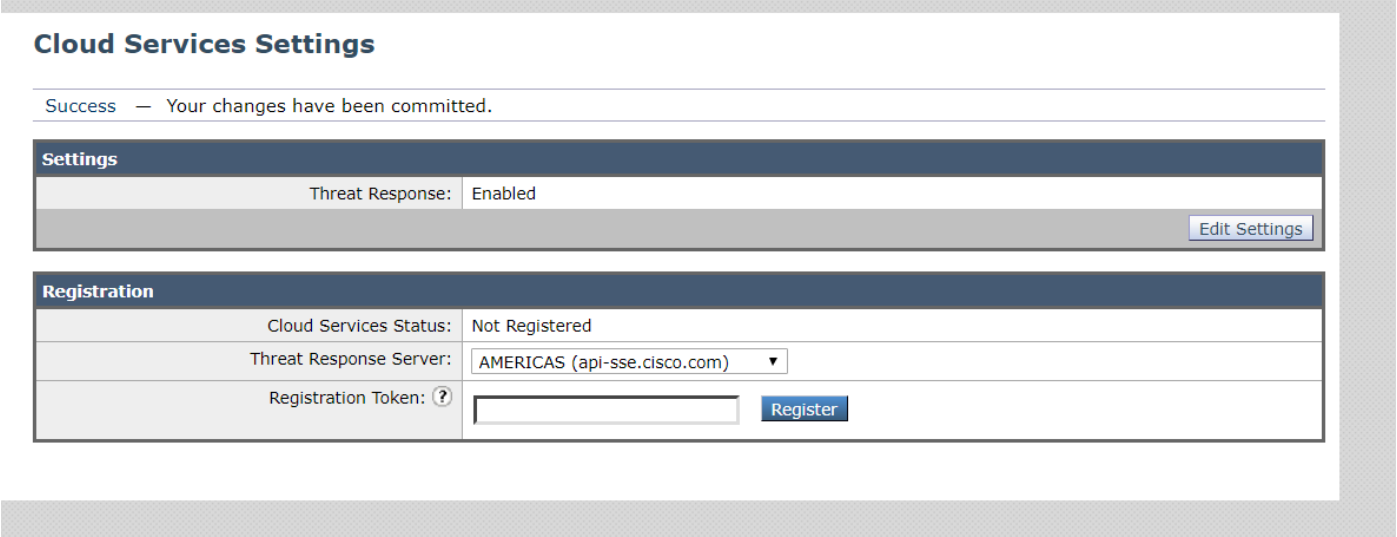
> **警告**：如果您使用亚太地区、日本和中国地区URL(https://visibility.apjc.amp.cisco.com/)访问CTR，则目前不支持与您的设备集成。

步骤1.在CLI中的REPORTINGCONFIG下启用POSERVABLE并提交更改，如图所示。

```
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.
```

步骤2.配置安全服务交换(SSE)云门户，导航至**网络>云服务设置>编辑设置**，单击**启用**并提交，**如图所示。**

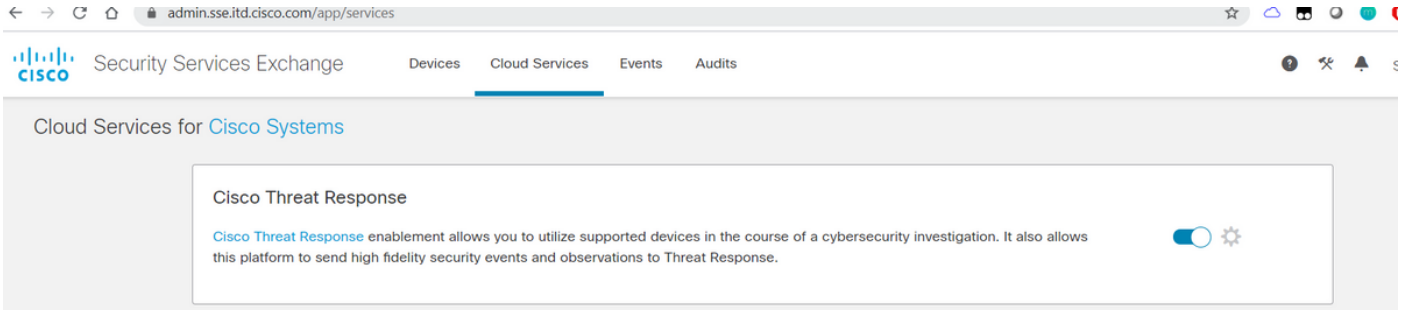
根据您的位置选择云，如图所示。



步骤3.如果您没有思科安全帐户，则可以在具有管理员访问权限的思科威胁响应门户中创建用户帐户。

要创建新用户帐户，请导航至思科威胁响应门户登录页。

步骤4.在SSE门户上的云服务下启用思科威胁响应，如图所示。



第五步： 确保WSA在端口443上具有到SSE门户的可达性：

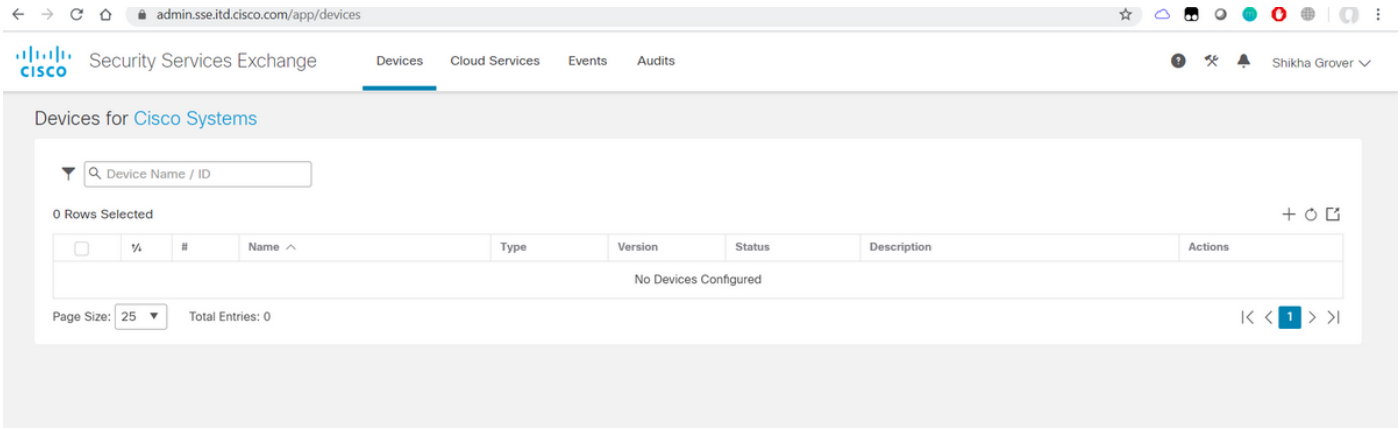
- api.eu.sse.itd.cisco.com（欧洲）
- api-sse.cisco.com（美国）

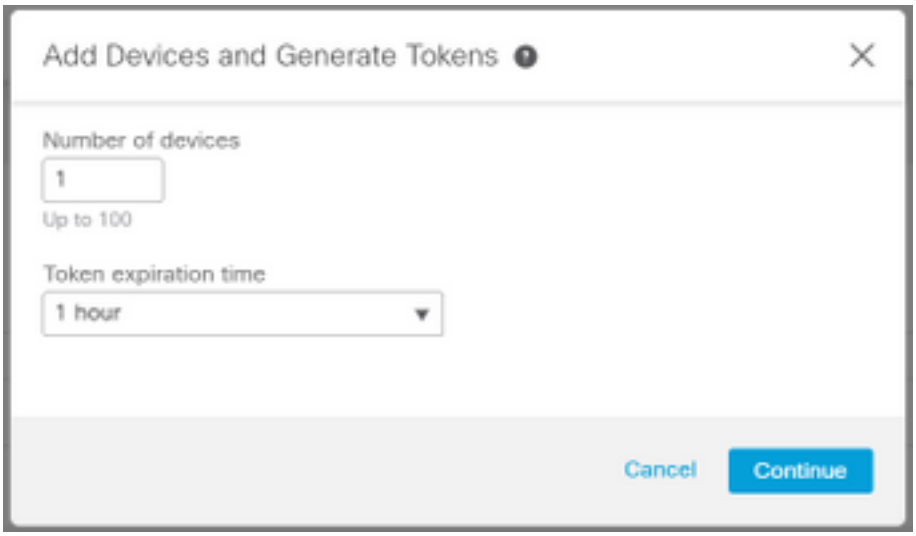
注册设备

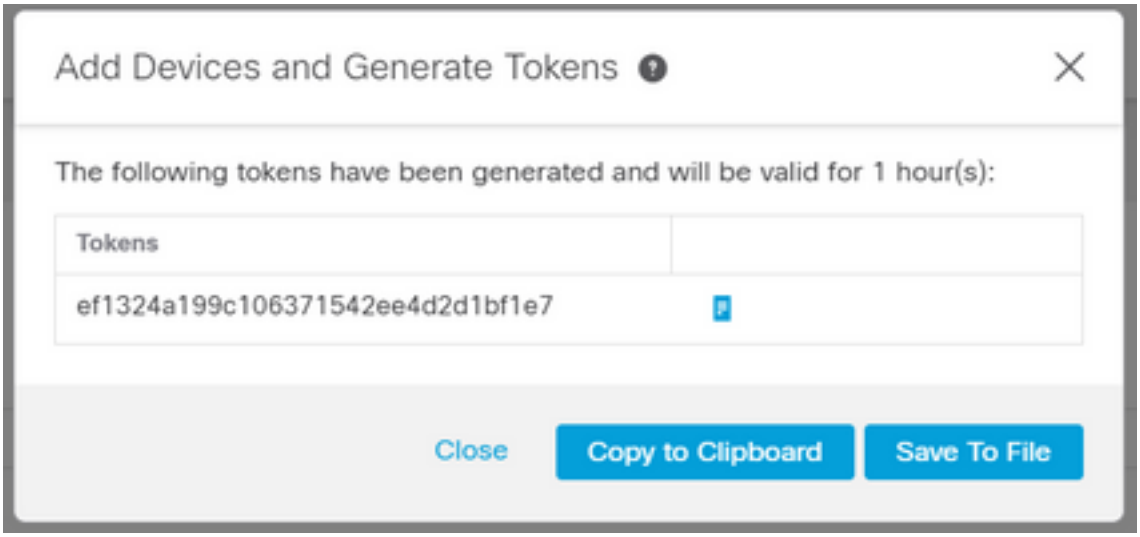
步骤1.从安全服务交换(SSE)门户获取注册令牌，以在安全服务交换门户注册设备。

SSE门户链接为https://admin.sse.itd.cisco.com/app/devices。

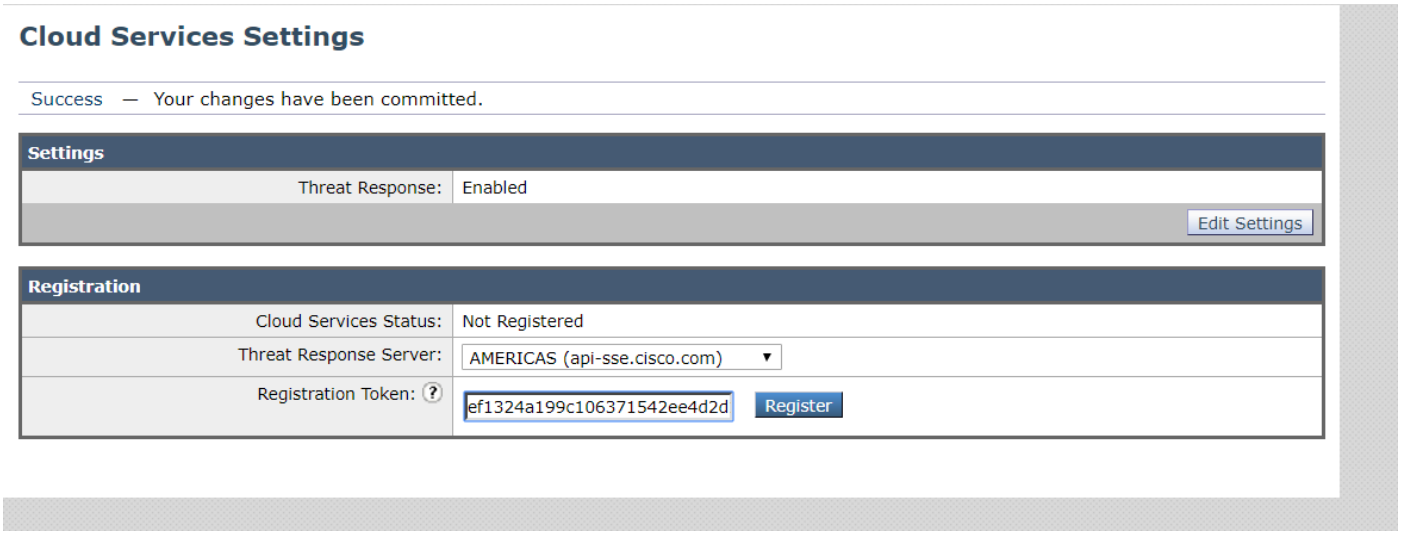
注意：使用CTR帐户凭证登录SSE门户。





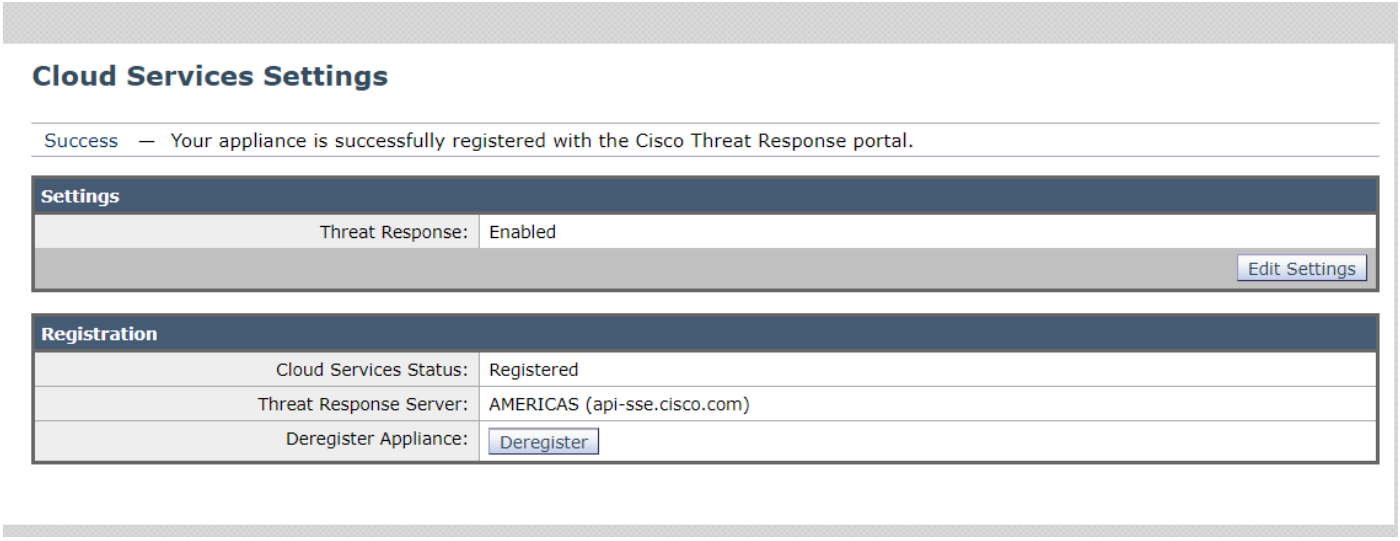


步骤2.输入从WSA中的安全服务交换门户获取的注册令牌，然后**单击**注册，如图所示。

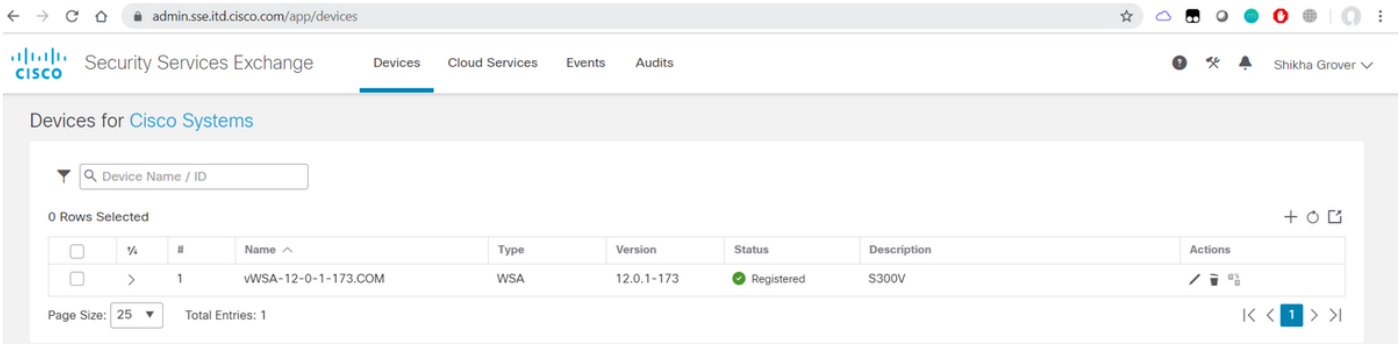


步骤3.几秒钟后，您将看到注册成功。

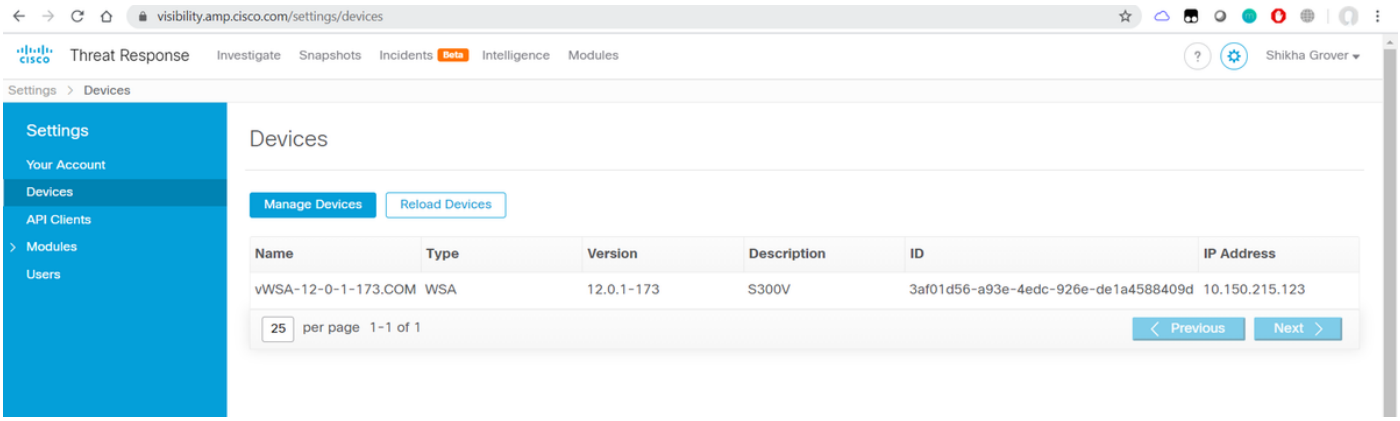
警告：确保生成的令牌在到期之前已使用。



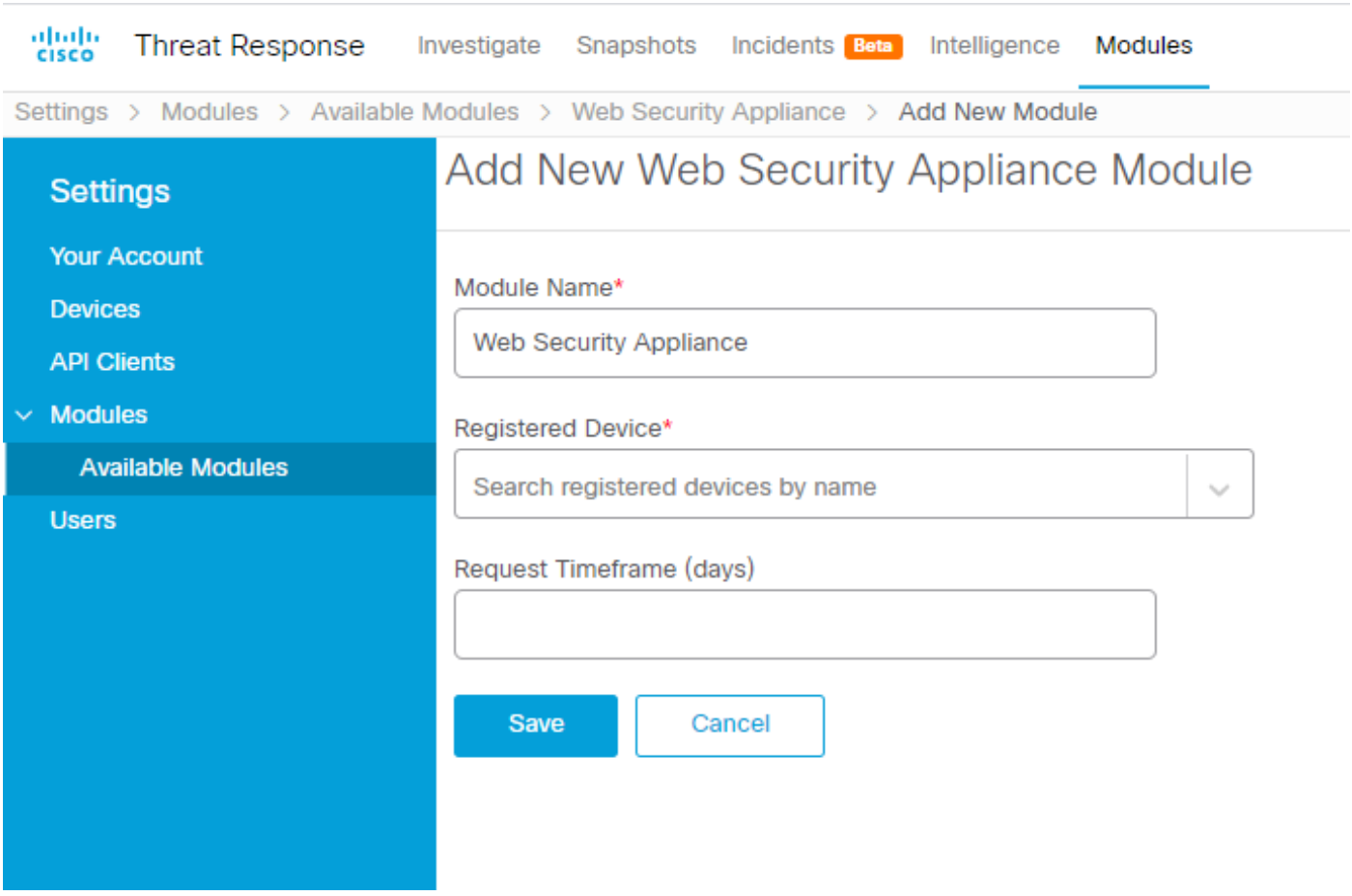
步骤4.在SSE门户上，您可以看到设备状态。



步骤5.在CTR门户上显示注册的设备。



您可以将此设备关联到模块，导航至**Modules > Add New Module > Web Security Appliance**，如图所示。



设备现已集成。您可以通过WSA的流量并在CTR门户上调查威胁。

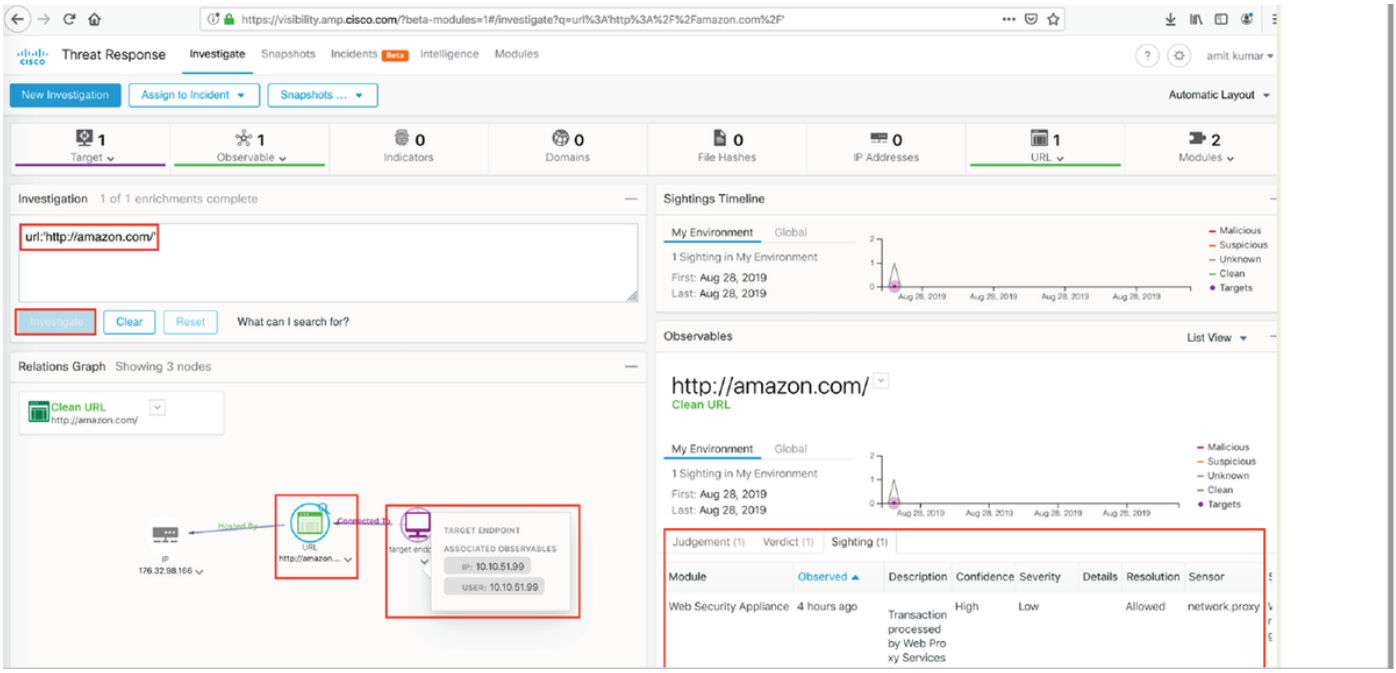
验证

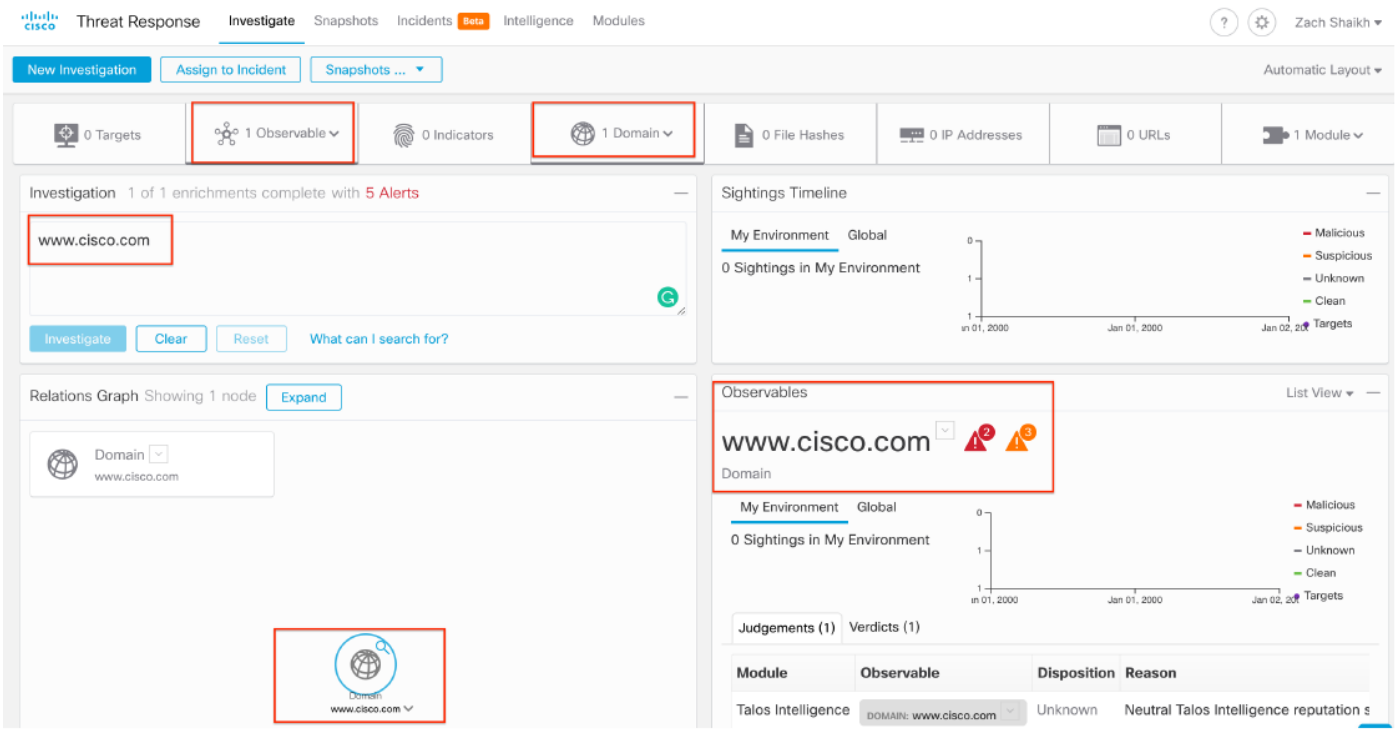
使用本部分可确认配置能否正常运行。

用于WSA模块的加密（查询WSA日志）及其支持的格式，用于从CTR门户运行查询：

- 域 — 域:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip:"172.217.26.164"
- 文件名- file_name:"test.txt"

使用中的加密示例：





如果我遗漏了应包含的内容，请随时通知我。 如果我遗漏了应包含的内容，请随时通知我。 如果我遗漏了应包含的内容，请随时通知我。 如果我遗漏了应包含的内容，请随时通知我。