WSAとCTRの統合

内容

概要

このドキュメントでは、Webセキュリティアプライアンス(WSA)とCisco Threat Response(CTR)ポータルを統合する手順について説明します。

著者：Shikha Grover、編集：Yeraldin Sanchez Cisco TACエンジニア

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WSAアクセス
- CTRポータルアクセス
- シスコセキュリティアカウント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Async Operating Systemバージョン12.x以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

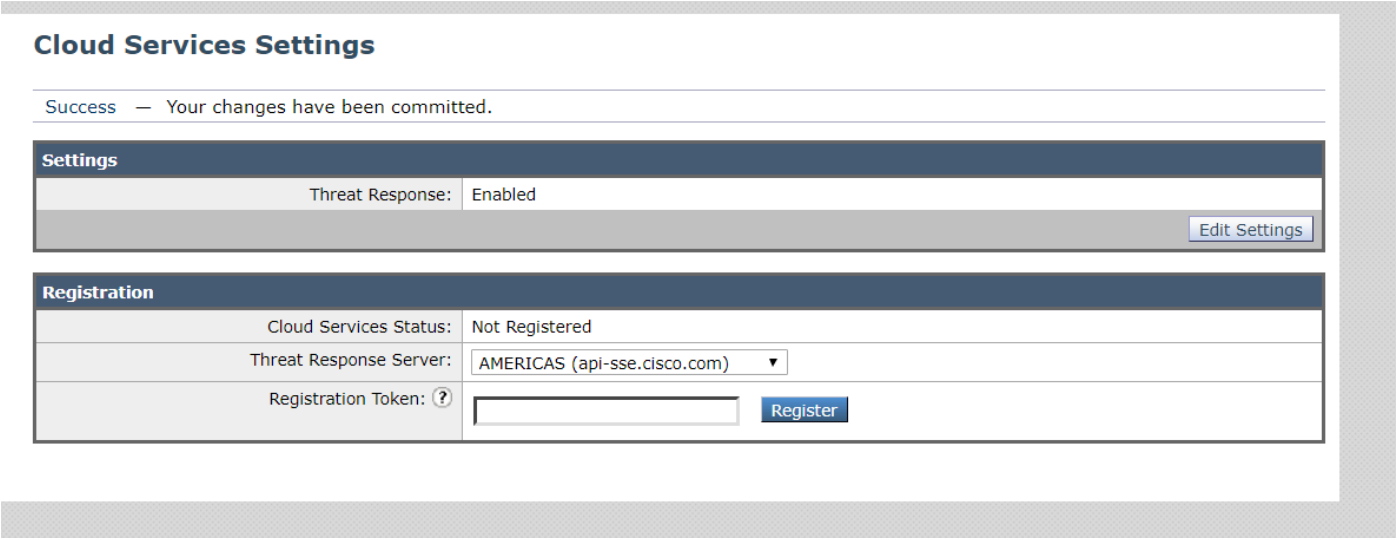
> **注意**：アジア太平洋地域、日本、中国のURL(https://visibility.apjc.amp.cisco.com/)を持つCTRにアクセスする場合、アプライアンスとの統合は現在サポートされていません。

ステップ1：図に示すように、CLIでREPORTINGCONFIGの下のCTROBSERVABLEを有効にし、変更を確定します。

```
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.
```

ステップ2: Security Service Exchange (SSE)クラウドポータルを設定し、**Network > Cloud Services Settings > Edit settingsに移動し、**Enable and **Submitをクリックします。**

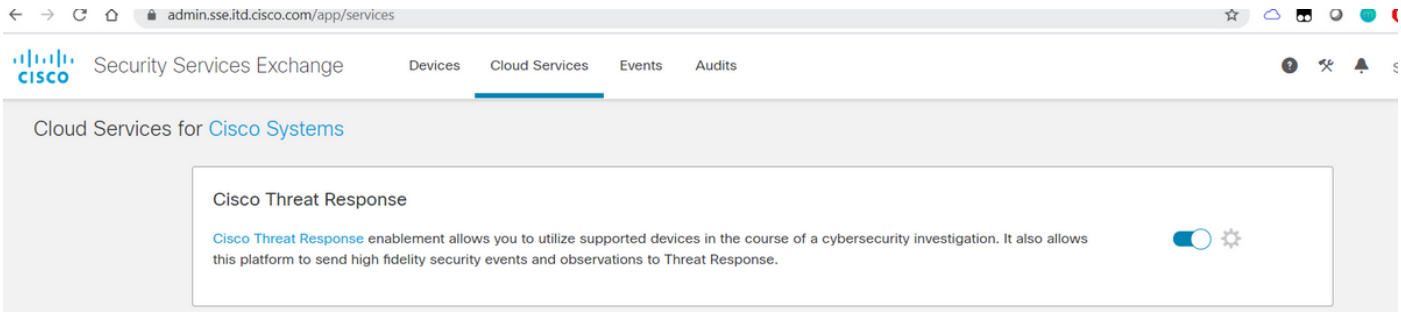
図に示すように、ロケーションに応じてクラウドを選択します。



ステップ3:Cisco Securityアカウントがない場合は、Cisco Threat Responseポータルで管理者アクセス権を持つユーザアカウントを作成できます。

新しいユーザアカウントを作成するには、Cisco Threat Responseポータルログインページに移動します。

ステップ4：図に示すように、SSEポータルのクラウドサービスでCisco Threat Responseを有効にします。



ステップ 5： WSAがポート443からSSEポータルに到達できることを確認します。

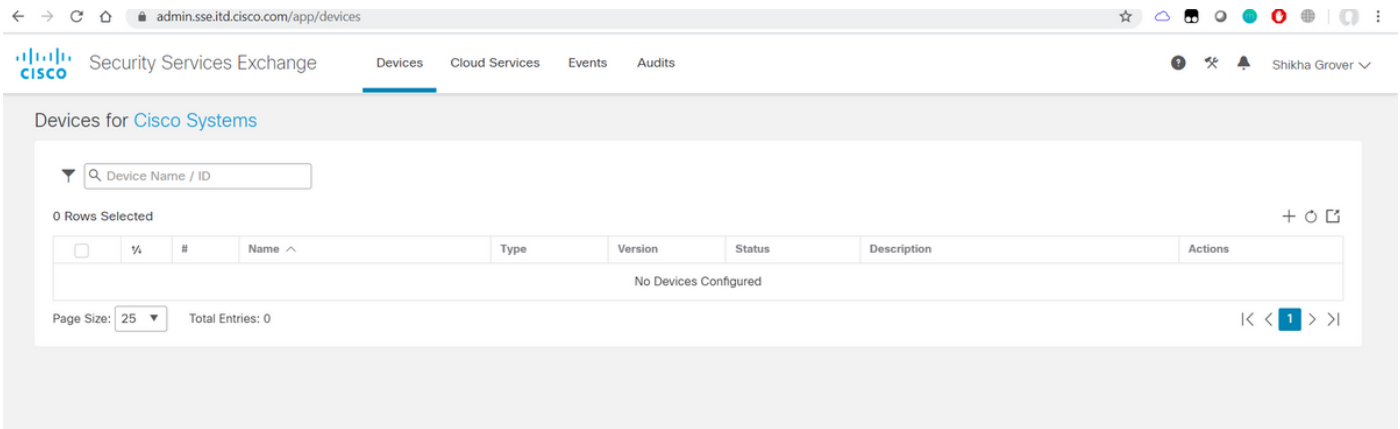
- api.eu.sse.itd.cisco.com（ヨーロッパ）
- api-sse.cisco.com（アメリカ）

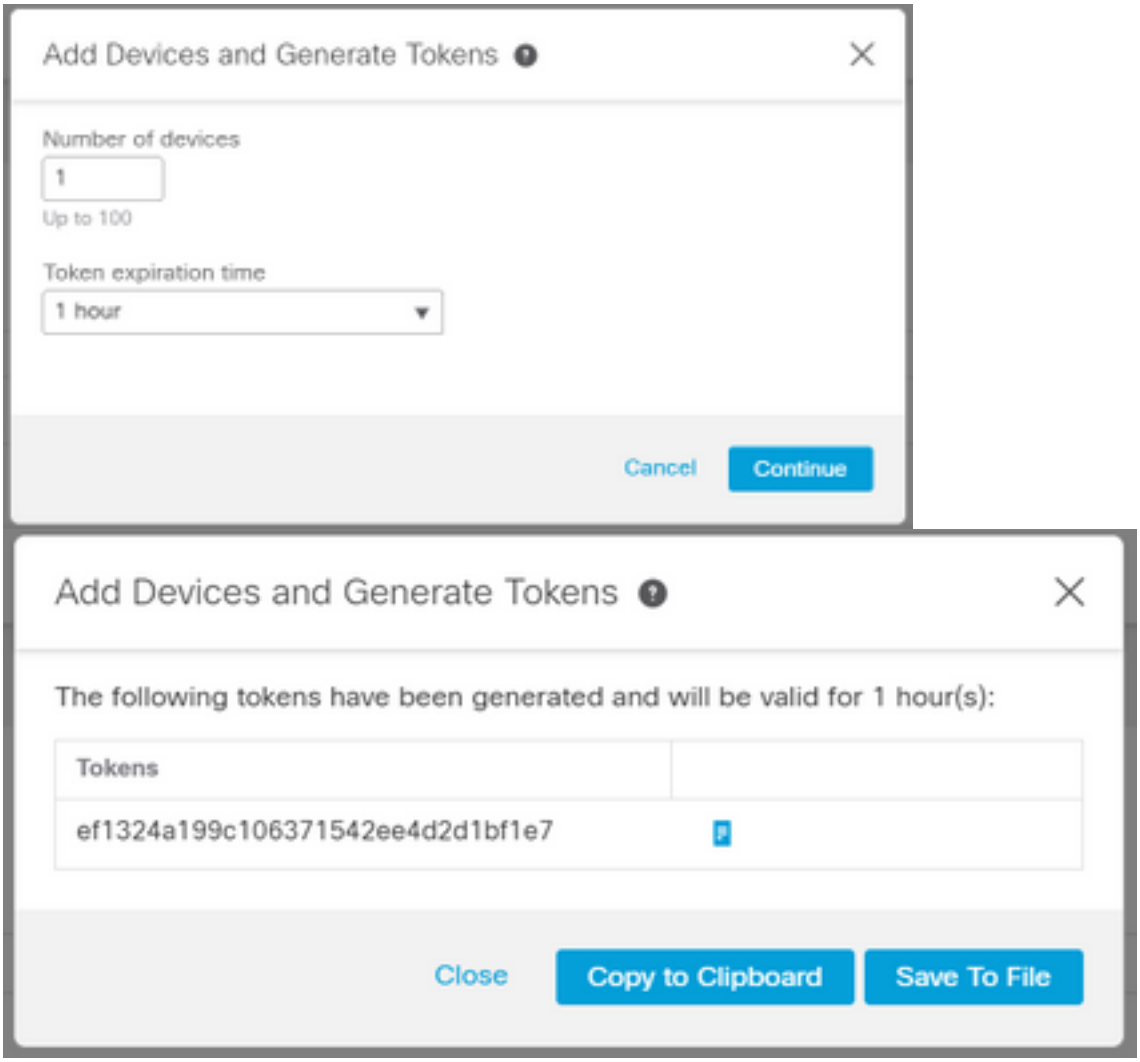
アプライアンスの登録

ステップ1：セキュリティサービス交換(SSE)ポータルから登録トークンを取得し、セキュリティサービス交換ポータルにアプライアンスを登録します。

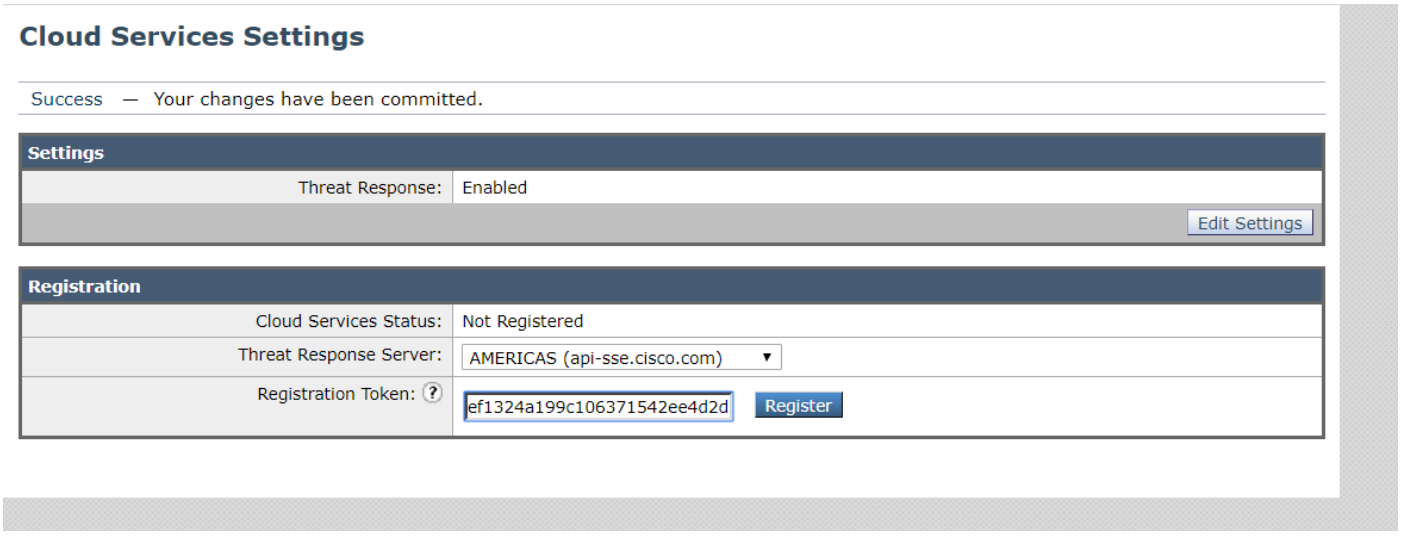
SSEポータルのリンクはhttps://admin.sse.itd.cisco.com/app/devicesです。

> **注：**CTRアカウントのクレデンシャルを使用してSSEポータルにログインします。



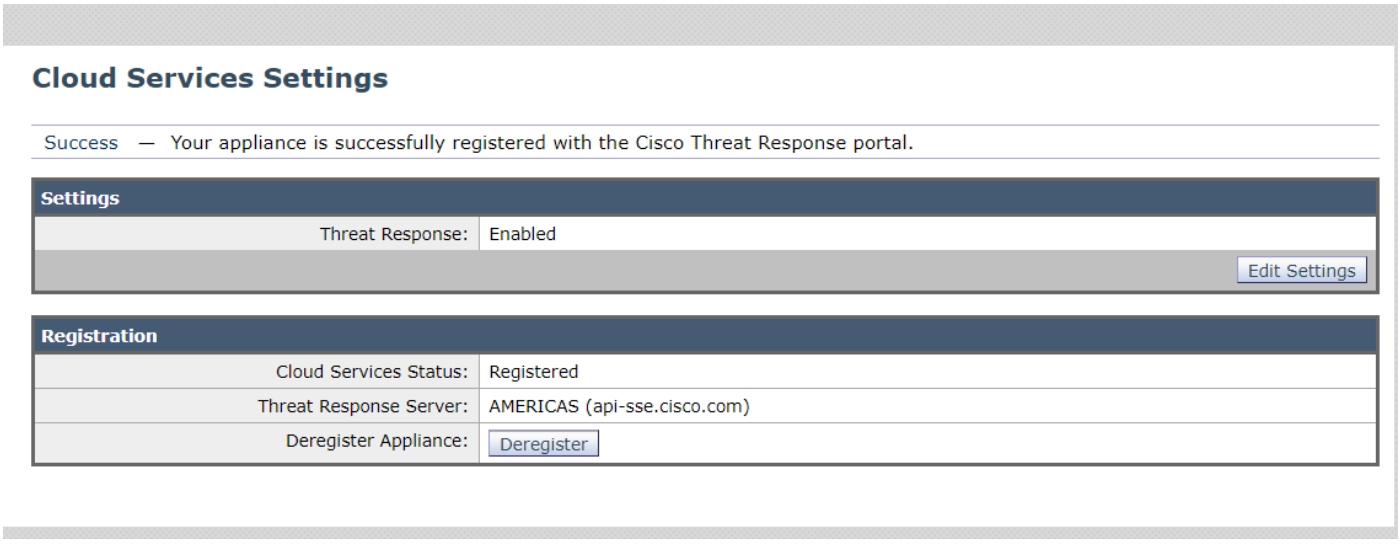


ステップ2:WSAのSecurity Services Exchangeポータルから取得した登録トークンを入力し、図に示すように[**Register**]をクリックします。

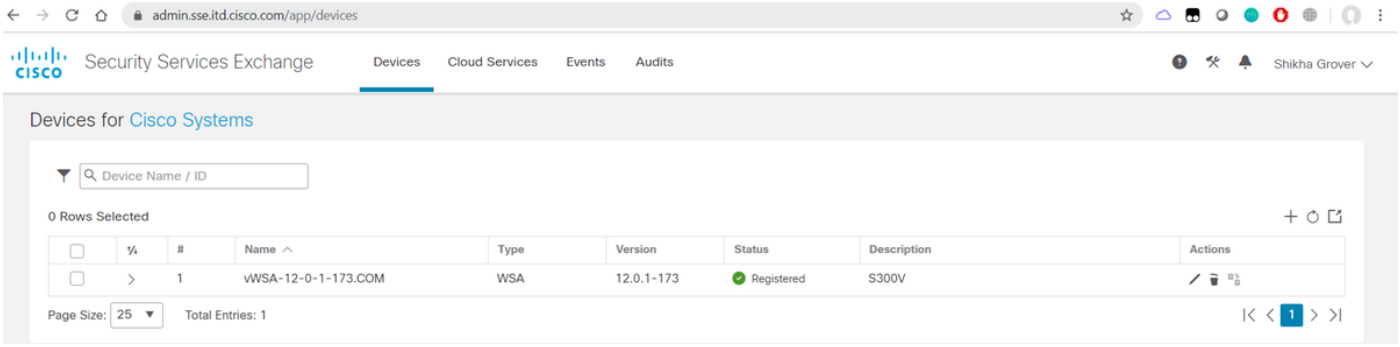


ステップ3:数秒後、登録が成功したことが表示されます。

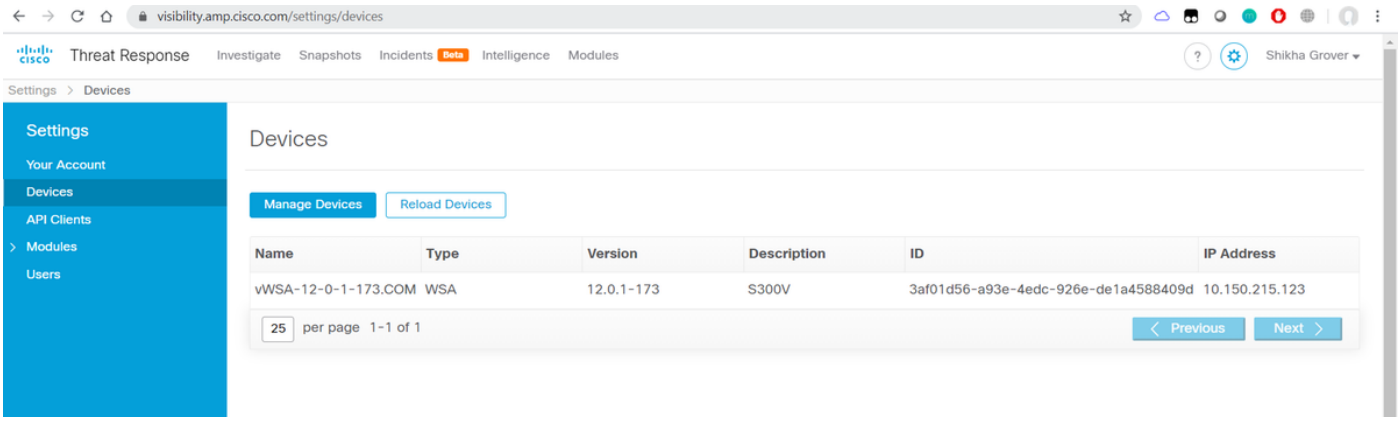
注意：生成されたトークンが期限切れになる前に使用されていることを確認します。



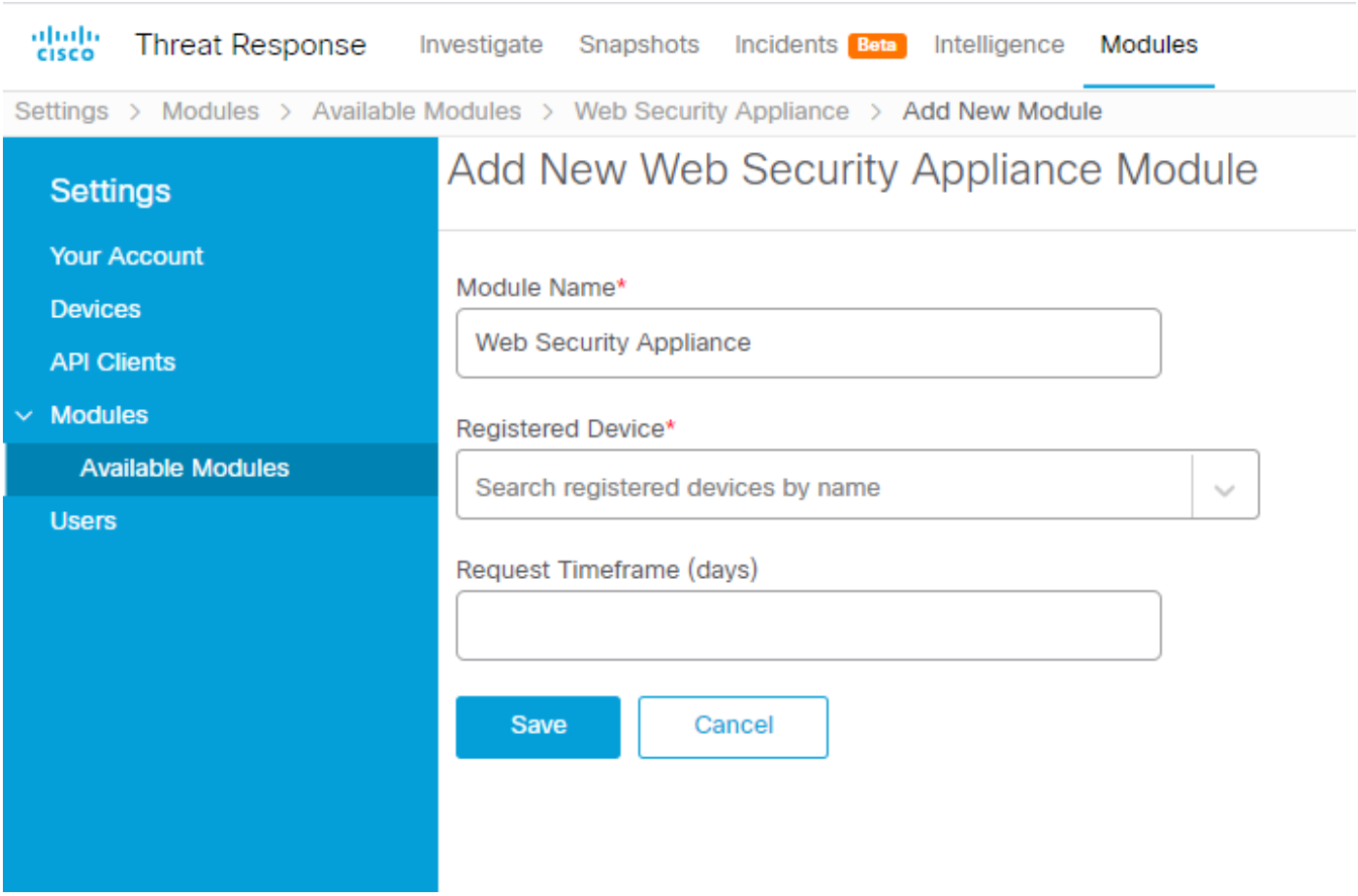
ステップ4:SSEポータルで、デバイスのステータスを確認できます。



ステップ5:CTRポータルに登録されたデバイスが表示されます。



このデバイスをモジュールに関連付け、図に示すように、**[Modules] > [Add New Module] > [Web Security Appliance]に移動**できます。



デバイスが統合されました。WSAからのトラフィックをパススルーし、CTRポータルの脅威を調査できます。

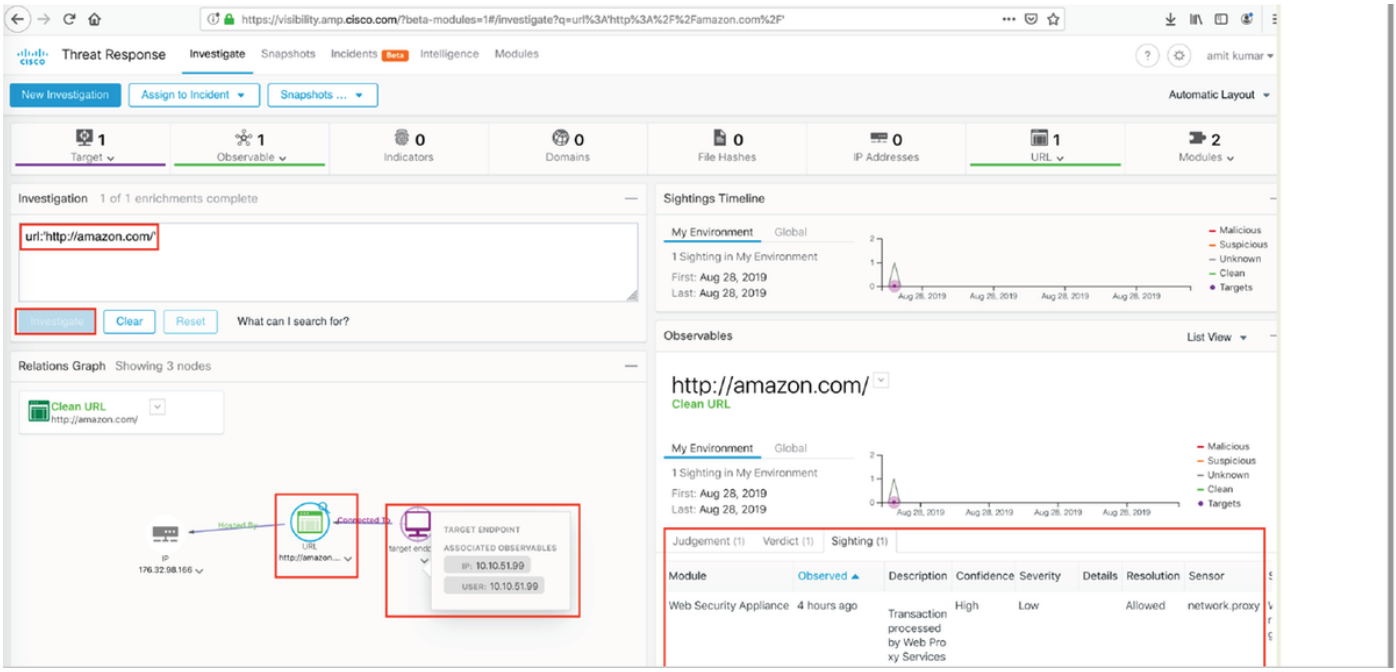
確認

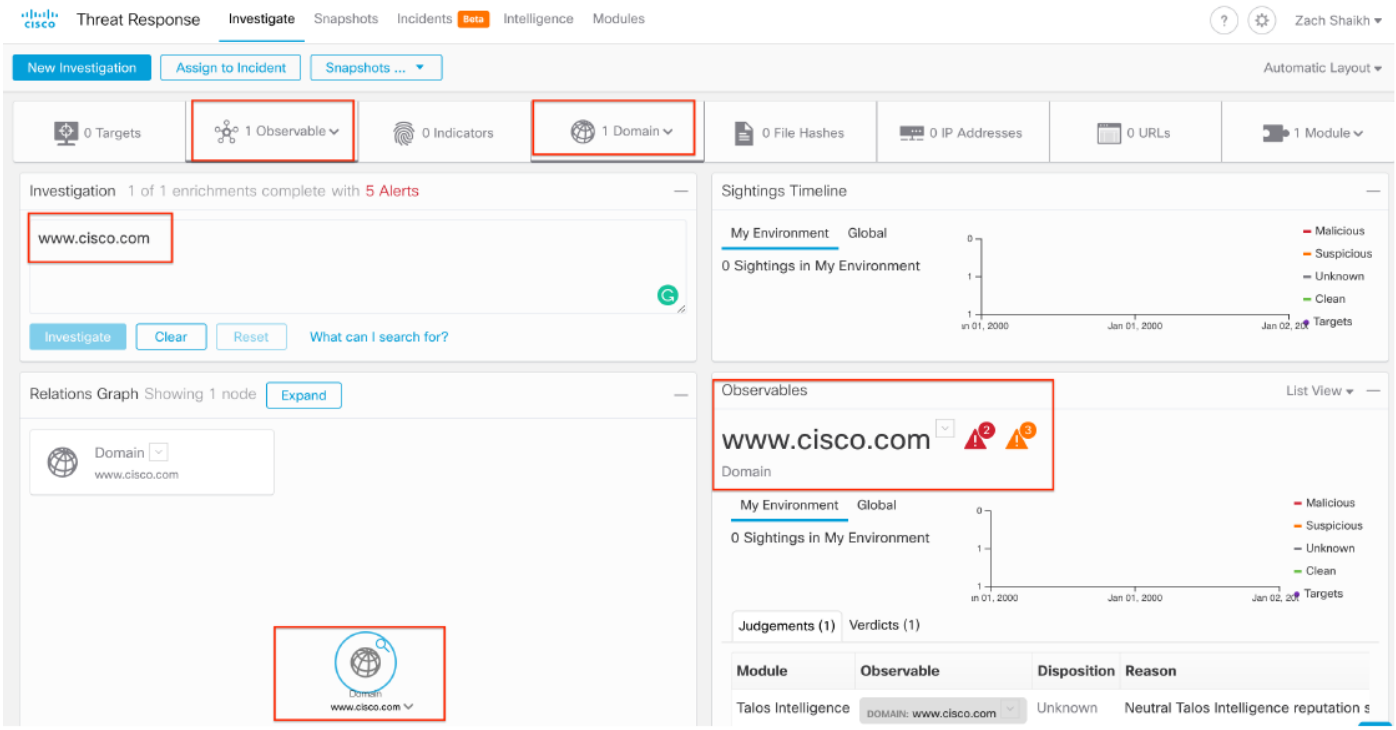
ここでは、設定が正常に機能しているかどうかを確認します。

WSAモジュールで使用可能な富化（WSAログの照会）、およびCTRポータルからクエリを実行するためのサポートされる形式：

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

例として使用される富化：





含めるべき何かを見逃した場合は、ご連絡ください。 含めるべき何かを見逃した場合は、ご連絡ください。 含めるべき何かを見逃した場合は、ご連絡ください。 含めるべき何かを見逃した場合は、ご連絡ください。