Cisco Secure Network Analytics

Alarm Configuration for Cisco XDR Guide 7.4.2

Table of Contents

Introduction

Overview

This guide provides instructions for promoting specific alarm data to Cisco XDR using a webhook through Response Management for Cisco Secure Network Analytics v7.4.2.

> When you upgrade to v7.5.1, make sure to disable this webhook configuration through Response Management before initiating a Cisco XDR integration.

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for configuring Secure Network Analytics products.

> Use this guide only if you have both Secure Network Analytics v7.4.2 *and* Cisco XDR Analytics (formerly Cisco Secure Cloud Analytics).

Requirements

The instructions in this guide require you to have access to Secure Network Analytics v7.4.2 and Cisco XDR Analytics. Having a Threat Feed License with Secure Network Analytics and being registered for Cisco XDR are also requirements.

Threat Feed License

Make sure you've set up your Threat Feed License because it's required to enable the *Bot Infected Host - Successful C&C Activity* alarm. For more information about the license, refer to the Smart Software Licensing Guide 7.4.2. For information about setting up the feed, refer to the "Threat Feed" section of the Cisco Secure Analytics System Configuration Guide 7.4.2.

For details about "Threat Feed" and related topics, click (**Help**) icon > **Help**.

Cisco XDR

Make sure you've registered for Cisco XDR before you begin configuring alarms in Secure Network Analytics to send to Cisco XDR. To confirm you've registered for Cisco XDR or for more information, contact your Cisco partner.

Cisco XDR is a cloud-based solution, designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. It reduces false positives and enhances threat detection, response, and forensic capabilities through clear prioritization of alerts and providing the shortest path from detection to response. For more information about Cisco XDR, go here.

Best Practices

Before you get started, review the requirements and instructions provided in this guide.

Additionally, be aware that while failover is supported, with the secondary Manager becoming active if needed, any other configuration with multiple Managers is not supported.

> Cisco XDR doesn't support multiple domains.

We suggest you follow the instructions in this order:

1. **Confirming Severity Level for the Alarms**
2. **Retrieving the AWS Root Certificate From Cisco XDR Analytics**
3. **Adding the AWS Root Certificate to the Trust Store**
4. **Retrieving the Service Key and Service Host from Cisco XDR Analytics**
5. **Setting Up a Webhook through Response Management**

1. Confirming Severity Level for the Alarms

The alarms are notifications of unusual network activity that meets or exceeds a defined set of criteria indicating unacceptable behavior on your network. Only the following three alarms generate data to send to Cisco XDR:

- Bot Infected Host - Successful C&C Activity
- Suspect Data Hoarding
- Suspect Data Loss

While these alarms typically default to a severity level of Major, make sure to confirm the severity level is either Critical or Major for each one. If an alarm doesn't have a severity of Critical or Major, it's data won't be sent to Cisco XDR.

The following table provides information about the Critical and Major alarm severity levels.

Alarm Severity	Alarm Definition
Critical	A Critical alarm is well-tuned, well-understood, and typically a low-volume alarm. The chance of a false positive is generally quite low. When indicated by a color, it is red.
Major	A Major alarm should be of interest to you. When you have tuned a Major alarm to the point that you believe it is a valuable source of intelligence, you can re-assign it to Critical. When indicated by a color, it is orange.

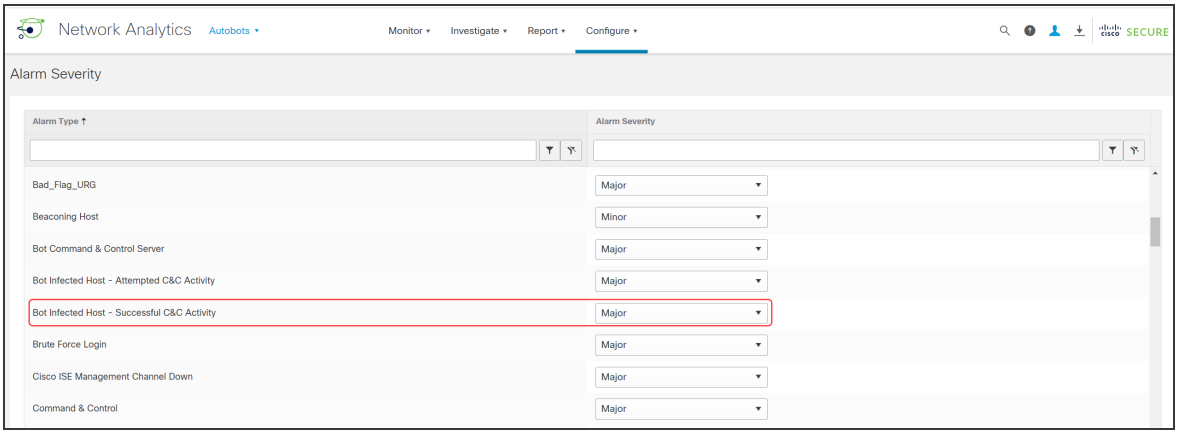
Make sure all three alarms have a **Critical** or **Major** severity level. If not, the data won't be shared with Cisco XDR.

Assign or Confirm the Alarm Severity for Each Alarm

To configure, or confirm, the alarm severity for each of the three alarms is Critical or Major, do the following:

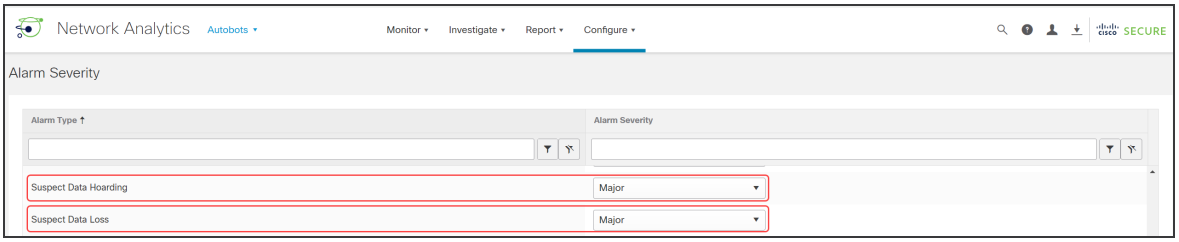
1. From the main menu, choose **Configure > DETECTION Alarm Severity**.
2. When the Alarm Severity page displays, locate the first alarm, **Bot Infected Host - Successful C&C Activity**.

> The Threat Feed License is required to enable the *Bot Infected Host - Successful C&C Activity* alarm. Refer to **Threat Feed License** for more information.



3. Select either **Critical** or **Major** for Alarm Severity.

4. Repeat Step 3 for each of the other two alarms.



5. Click **Save**.

Review Additional Information About the Alarms

The following table provides more details about these alarms.

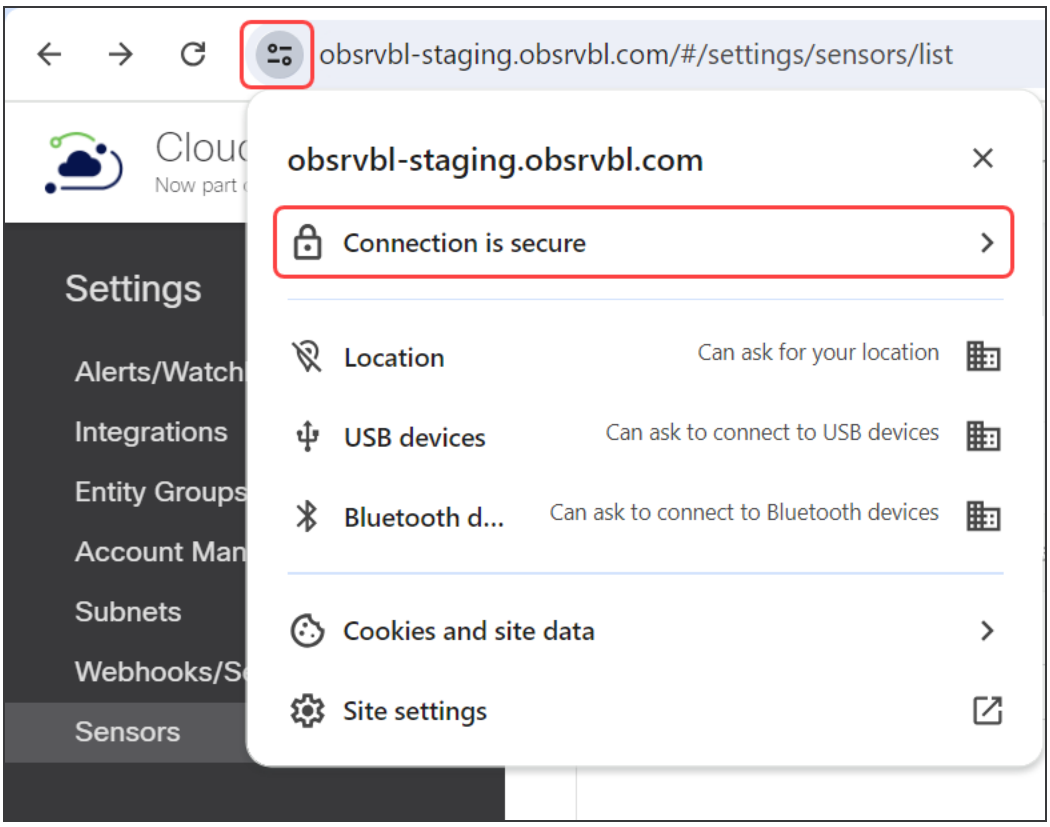
Secure Network Analytics			MITRE Tactics and Techniques			
Display Name	**Event ID**	**Event Description**	**MITRE Tactic**	**Tactic ID**	**MITRE Technique**	**Technique ID**
Bot Infected Host - Successful C&C Activity	42	The source host has successfully contacted a & server using a port identified in the Command-and-Control (C&C) server list. The communication is two-way, indicating the C&C server has responded. The inside host, as the initiator, accumulates Concern Index (CI) points. If the C&C server it contacts is also an inside host, then that C&C server accumulates Target Index (TI) points.	Command and Control (C&C)	TA0011	Application Layer Protocol	T1071
Suspect Data Hoarding	315	The source host has downloaded an unusual amount of data from one or more hosts.	Collection	TA0009	Data Staged	T107

Secure Network Analytics			MITRE Tactics and Techniques			
Display Name	**Event ID**	**Event Description**	**MITRE Tactic**	**Tactic ID**	**MITRE Technique**	**Technique ID**
Suspect Data Loss	40	This indicates that an inside host has uploaded an abnormal amount of data to outside hosts.	Exfiltration	TA0010	Exfiltration over C2 Channel	T1041

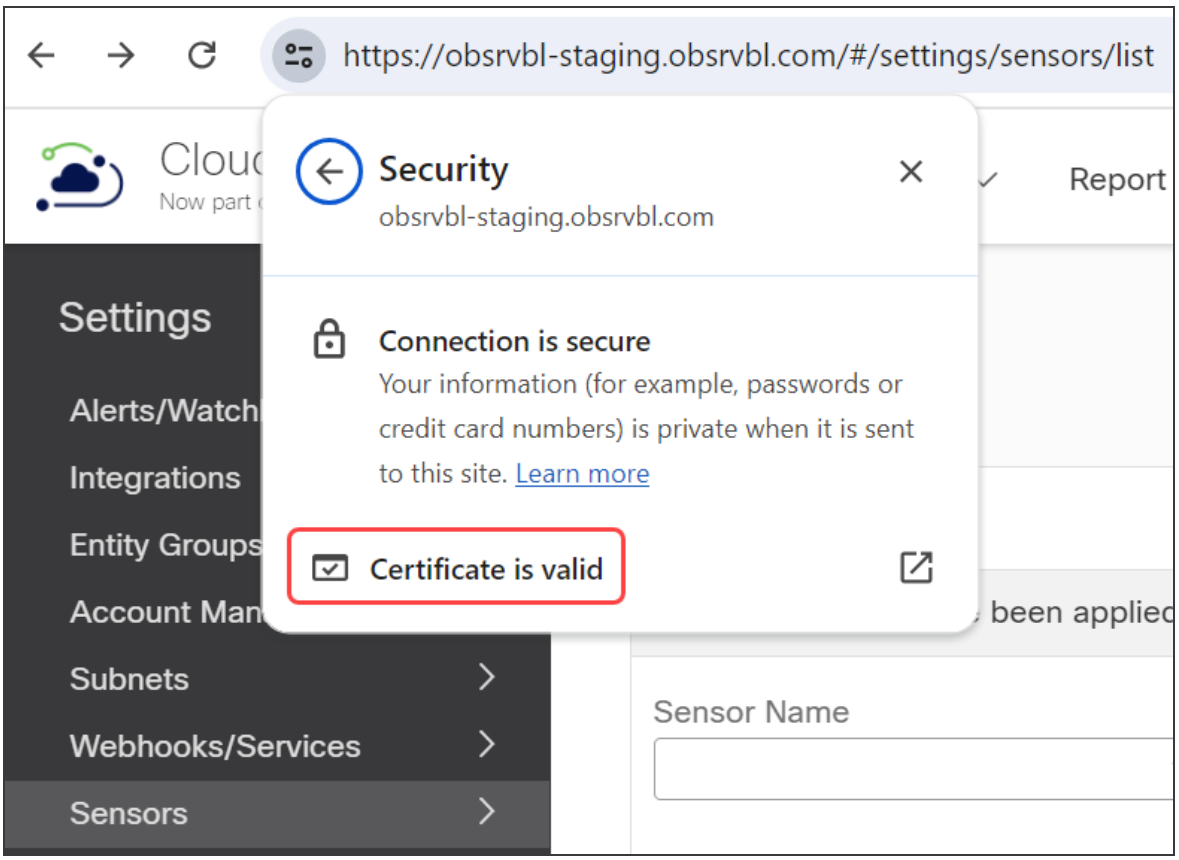
2. Retrieving the AWS Root Certificate From Cisco XDR Analytics

To import the AWS Root Certificate from Cisco XDR Analytics, do the following:

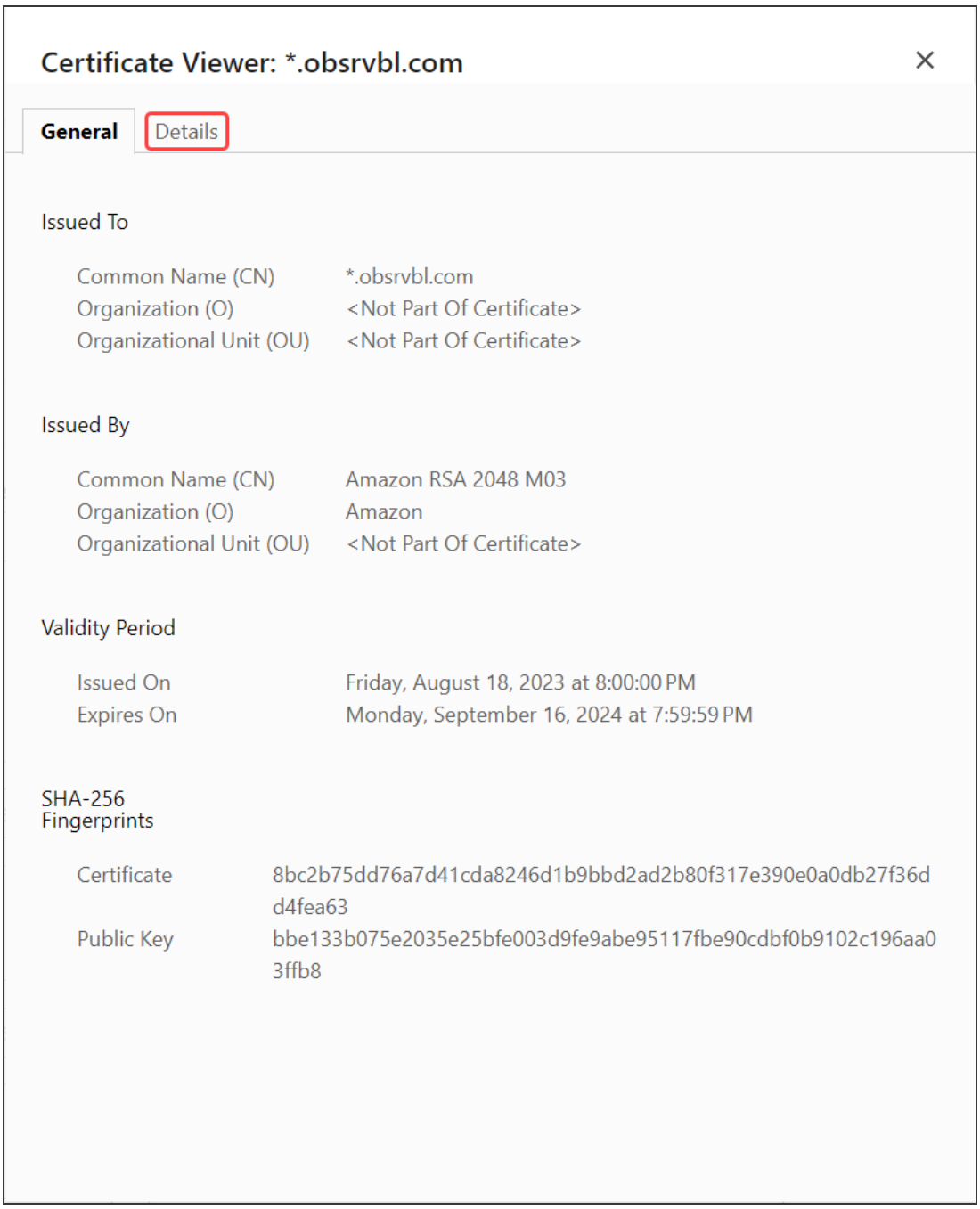
1. Log in to your Cisco XDR Analytics web portal.
2. Select **Settings > Sensors**.
3. When the Sensors page displays, right-click the **(View site information)** icon next to the URL in the browser bar at the top of the page to view the following dialog box:



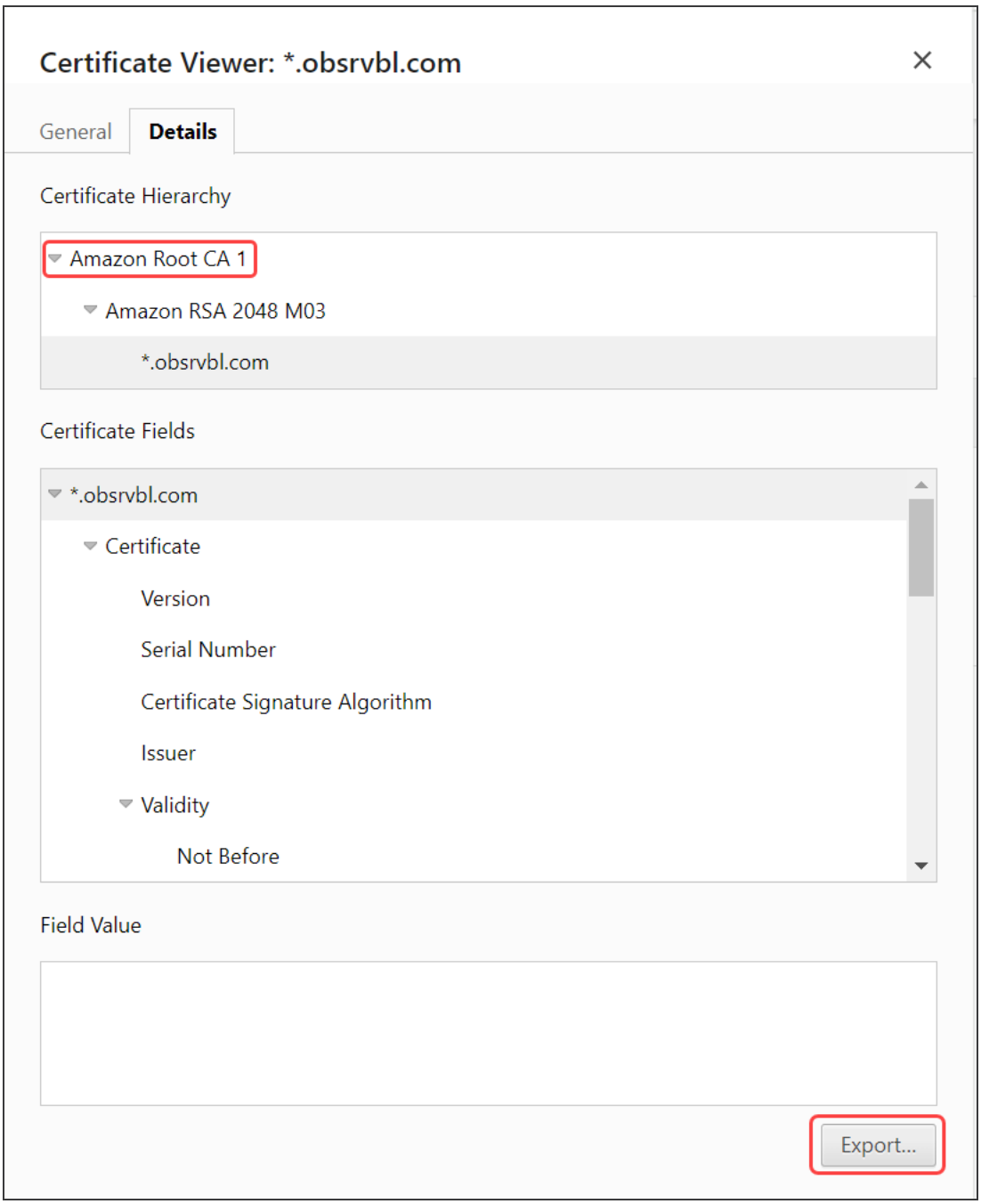
4. Select **Connection is secure** to see the following dialog box:



5. Select **Certificate is valid** to display the following dialog box:



6. Click the **Details** tab to see the following dialog box:

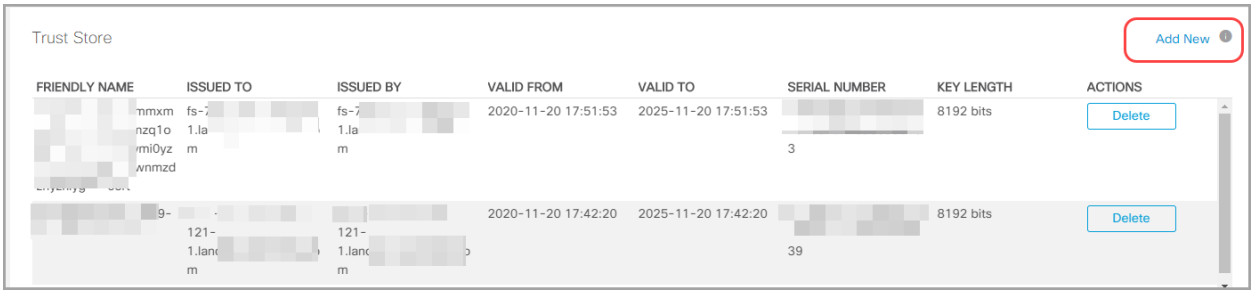


7. Make sure the AWS Root Certificate, **Amazon Root CA 1** in this example, is selected.
8. Click **Export** and save the file.

3. Adding the AWS Root Certificate to the Trust Store

To add the AWS Root Certificate to the Trust Store, do the following:

1. Log in to the primary Manager as admin.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. On the Inventory page, click the ••• (**Ellipsis**) icon next to **Actions** for the appliance.
4. Choose **Edit Appliance Configuration**.
5. On the **General** tab, locate the Trust Store section.
6. Click **Add New**.



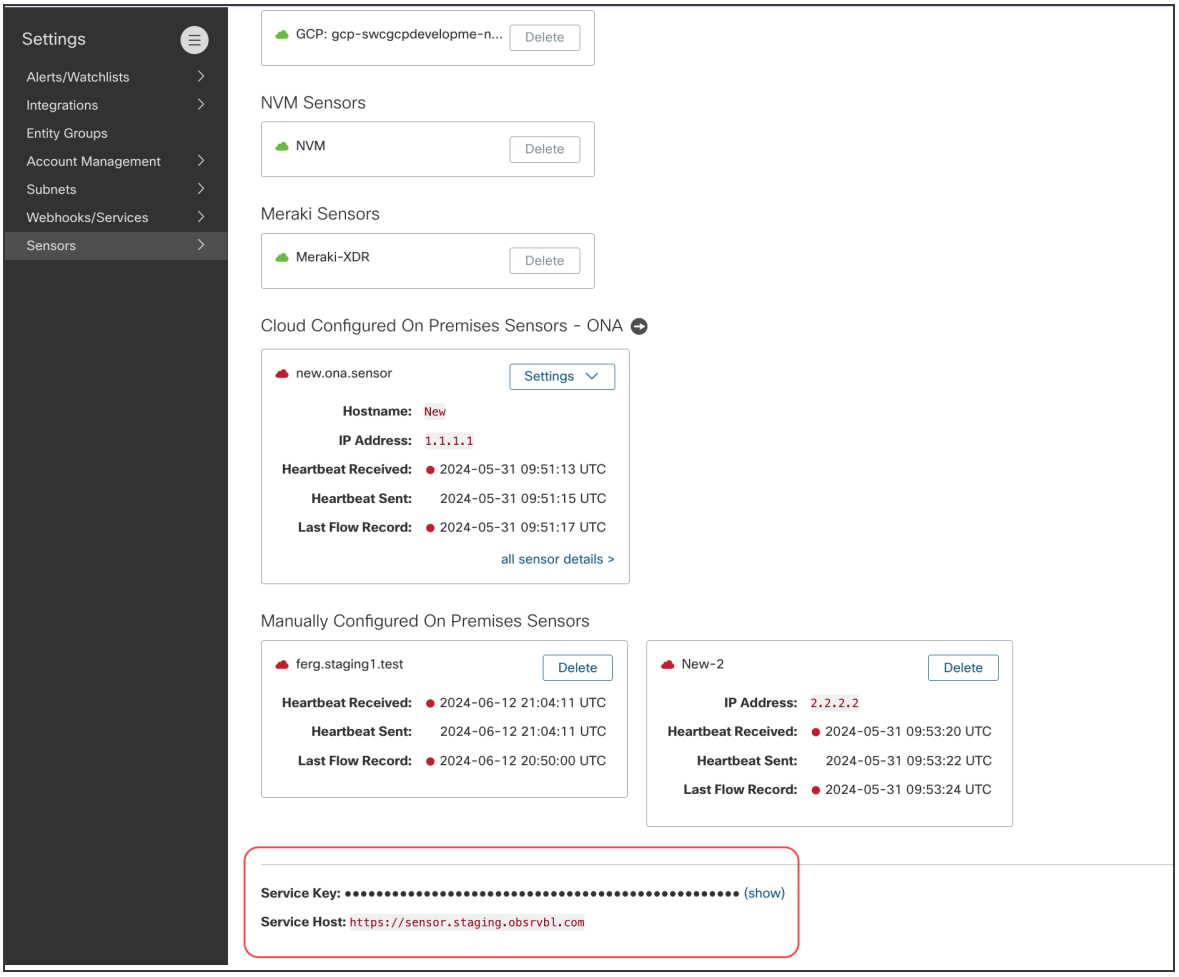
7. In the **Friendly Name** field, enter a name for the AWS root certificate.
8. Click **Choose File**. Select the AWS root certificate that you exported and saved in **2. Retrieving the AWS Root Certificate From Cisco XDR Analytics**.
9. Click **Add Certificate**. Confirm the AWS certificate is shown in the Trust Store list.
10. Repeat these steps for a secondary Manager, if applicable.

> For more information about adding certificates to the trust stores, refer to the SSL/TLS Certificates for Managed Appliances Guide.

4. Retrieving the Service Key and Service Host from Cisco XDR Analytics

To retrieve the Service Key and Service Host information from Cisco XDR Analytics, which are needed for **5. Setting Up a Webhook through Response Management** , do the following:

1. Log in to your Cisco XDR Analytics web portal.
2. Select **Settings > Sensors**.
3. When the Sensors page displays, scroll to the bottom to view the **Service Key** and **Service Host** fields.



4. Click **(show)** to view the Service Key.
5. Copy the Service Key and Service Host information to use in **5. Setting Up a Webhook through Response Management** .

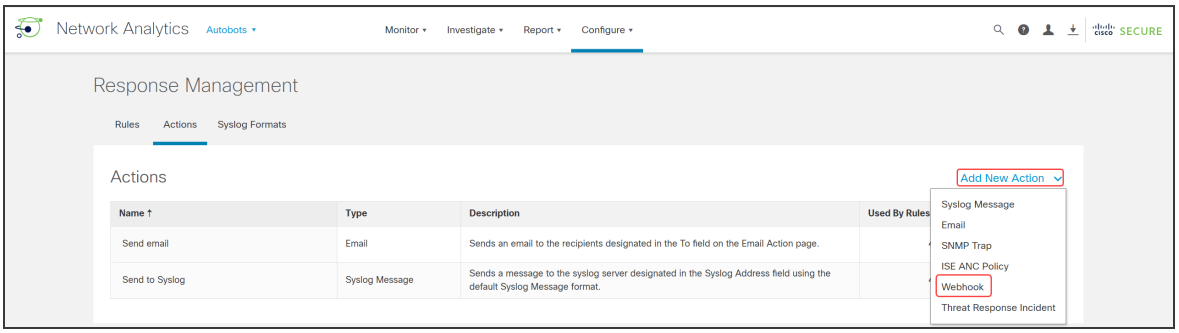
5. Setting Up a Webhook through Response Management

Start with **Create the Webhook Action** to create the new webhook action; then go to **Create the Rule for the Webhook Action** to assign the rule to the action you've created.

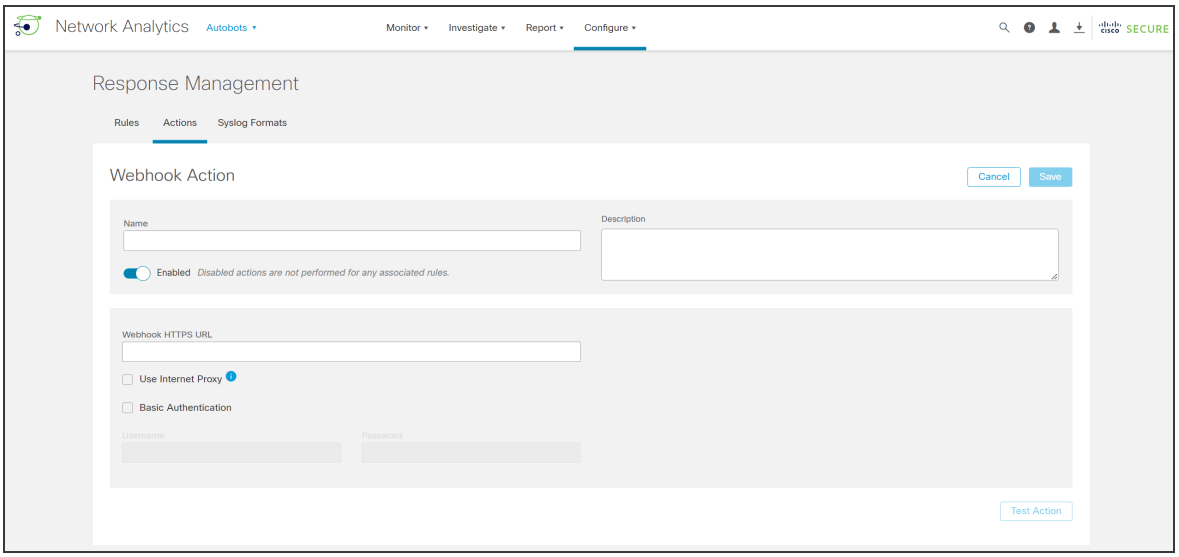
Create the Webhook Action

To create the webhook action, do the following.

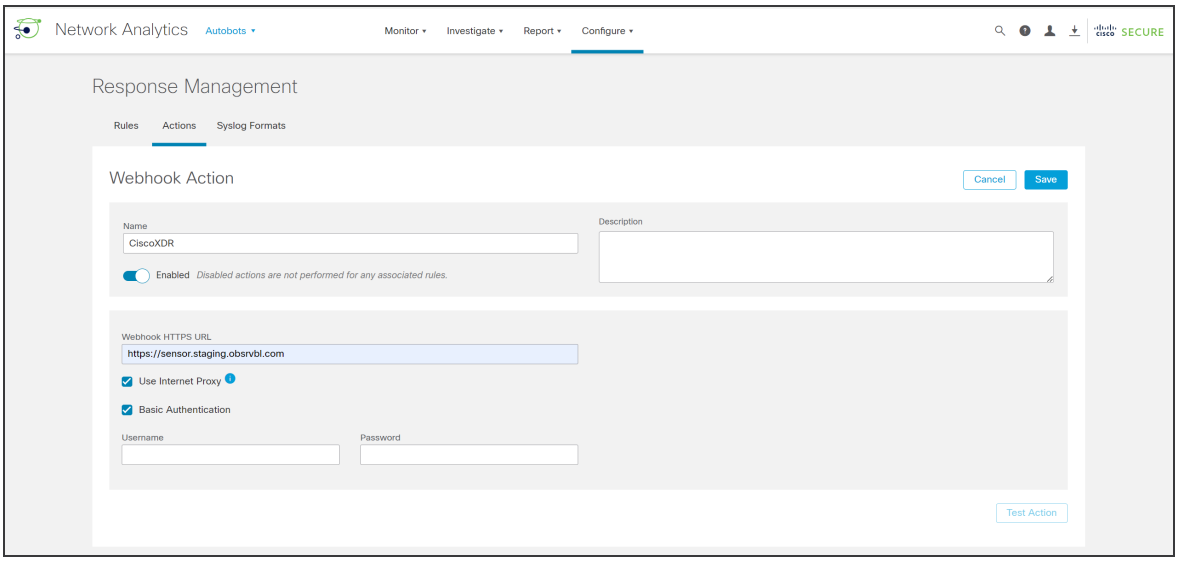
1. From the main menu, choose **Configure > DETECTION Response Management**.
2. When the Response Management page displays, click the **Actions** tab.
3. In the Actions area, select **Webhook** from the **Add New Action** menu.



4. When the Webhook Action dialog box displays, type a unique name in the **Name** field.



5. Paste the Service Host URL you copied from Cisco XDR Analytics into the **Webhook HTTPS URL** field.
6. Check the **Use Internet Proxy** check box if you have an Internet proxy in Central Management.
7. Check the **Basic Authentication** check box.



8. Type **service_key** into the **Username** field
9. Paste the Service Key value you copied from Cisco XDR Analytics into the **Password** field.
10. Confirm **Enabled** is toggled on.
    - When the action is enabled, the **Toggle** icon bar is blue.
    - When the action is disabled, the **Toggle** icon bar is gray.
13. Click **Test Action** to confirm the alarms are successfully sending to Cisco XDR, or **Edit** (to make changes), if needed.

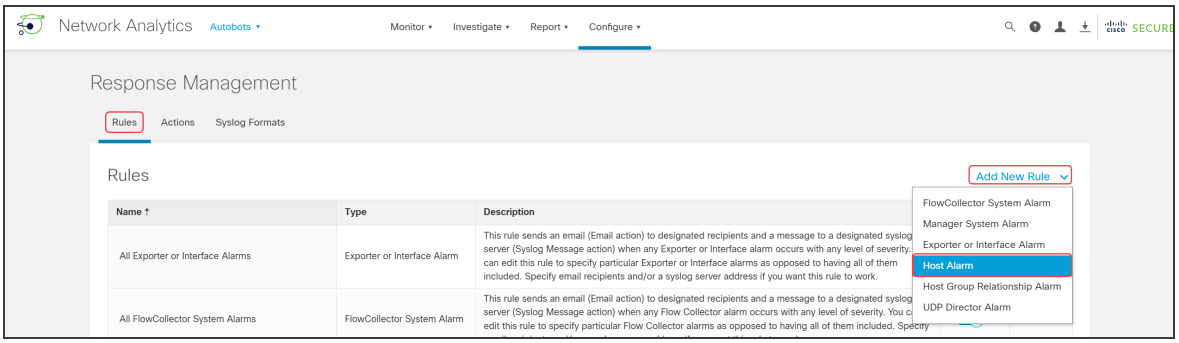
> To dismiss a preview, click **Edit** or anywhere in the **Body** area.

14. Click **Save**.

Create the Rule for the Webhook Action

Use the following instructions to create a new rule to assign the webhook action you created.

1. Click the **Rules** tab, then select **Webhook** from the **Add New Action** menu.
2. Select **Host Alarm**.



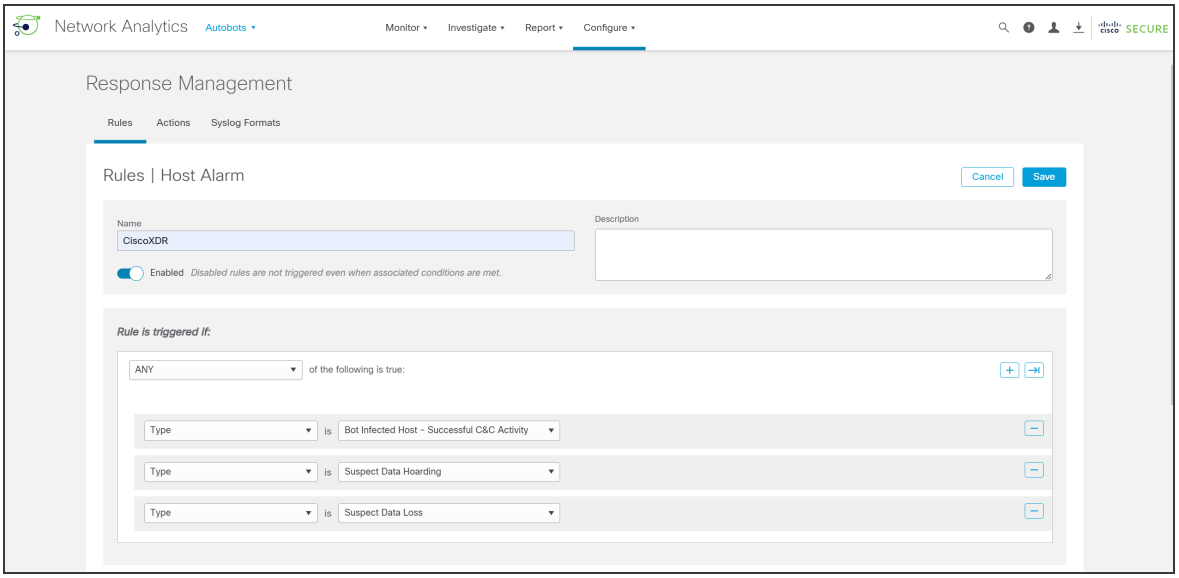
3. Locate the **Name** field in the **Rules | Host Alarm** area, then type the name; "CiscoXDR" for example. You may also want to add a description in the **Description** field.

> Make sure the **Enabled** button is toggled on.

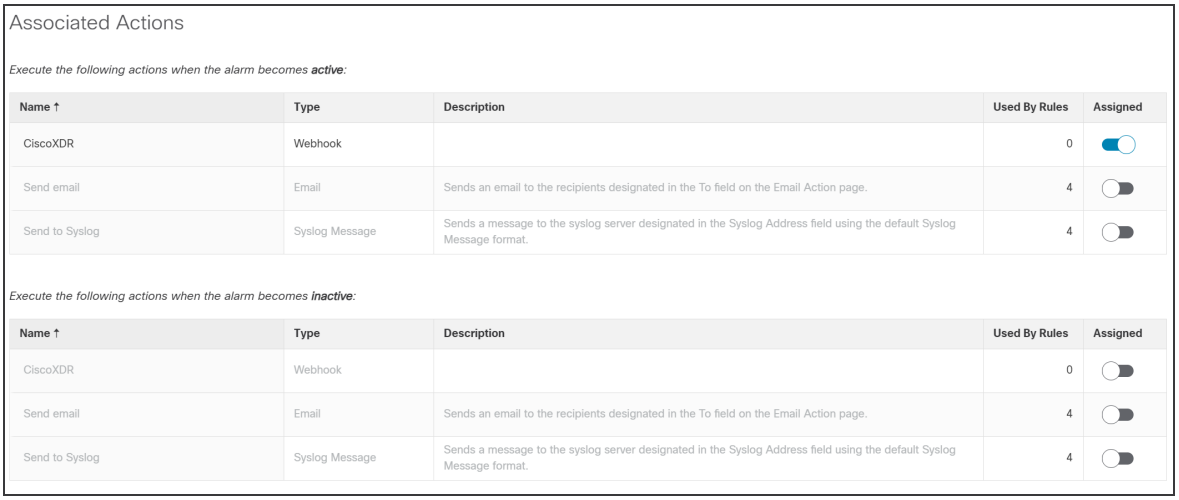
4. In the **Rule is triggered if:** area, select **ANY**.
5. Click the **+** (Plus) icon to add three selection options.
6. Select **Type** (where"Severity" initially displays).
7. Scroll through the list of types to select each of the three alarms:
    - Bot Infected Host - Successful C&C Activity
    - Suspect Data Hoarding
    - Suspect Data Loss

> If you click the **-** (Minus) icon, it removes a selection.

8. Make sure you've selected all three alarms, then click **Save**.



9. Locate the **Associated Actions** area, then toggle on (blue) the Assigned column for the webhook action you just created in the **active** table.



> Make sure the **inactive** table remains toggled off (gray) because Cisco XDR won't require this data.

10. Click **Save**.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	July 25, 2024	Initial version.

Copyright Information