Cisco Stealthwatch

Cisco Threat Response Integration Guide 7.1.2



Table of Contents

Introduction	4
Cisco Threat Response Regional Clouds	4
Guidelines and Limitations for Choosing a Regional Cloud	5
Contacting Support	5
Stealthwatch Data and Threat Response	6
About Sending Stealthwatch Alarms to Cisco Threat Response	6
About Stealthwatch Enrichment Data for Threat Response	6
About the Cisco Threat Intel Model	7
About Translating Stealthwatch Alarms to CTIM Objects	7
About Translating Stealthwatch Security Events to CTIM Objects	9
Cisco Cloud Accounts	10
Required Account for Cisco Threat Response Access	10
Create an Account to Access Cisco Threat Response	10
Manage Access To Your Organization's Cisco Security Account	11
Configuring Stealthwatch and Cisco Threat Response Integration	12
Configuring Cisco Threat Response Integration	12
Prerequisites	12
Procedure	12
Additional Information	16
Register your SMC in the Cisco Cloud	16
Procedure	16
Configuring Stealthwatch Integration Module in Cisco Threat Response	19
Prerequisites	19
Procedure	19
Access Security Services Exchange	20
Before you begin	20
Procedure	20

Known Issues and Limitations		2
------------------------------	--	---

Introduction

Cisco Threat Response (CTR) is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.

This integration allows you to use Cisco Threat Response Pivot menu, Cisco Threat Response Casebook in your SMC appliance UI, send Stealthwatch Alarms to Cisco Threat Response and allows CTR to retrieve information about security events from your Stealthwatch deployment during the investigation process.

For more information about Cisco Threat Response, see <u>https://www.-</u> <u>cisco.com/c/en/us/products/security/threat-response.html</u>. For videos about the use and benefits of the application on YouTube, see <u>http://cs.co/CTRvideos</u>.

Region	Link	Supported Stealthwatch Integ- rations
North America	https://visibility.amp.cisco.com	 Threat Response Pivot Menu Threat Response Casebook Sending Stealthwatch Alarms to CTR as Incidents Enrichment with Stealth- watch Security Events
Europe	https://visibility.eu.amp.cisco.com	 Threat Response Pivot Menu Threat Response Casebook Sending Stealthwatch Alarms to CTR as Incidents Enrichment with Stealth- watch Security Events
Asia (APJC)	https://visibility.apjc.amp.cisco.com	 Threat Response Pivot Menu

Cisco Threat Response Regional Clouds

Region	Link	Supported Stealthwatch Integ- rations
		 Threat Response Casebook Sending Stealthwatch Alarms to CTR as Incidents

Guidelines and Limitations for Choosing a Regional Cloud

- When possible, use the regional cloud nearest to your Stealthwatch deployment.
- Data in different clouds cannot be aggregated or merged.
- If you need to aggregate data from multiple regions, devices in all regions must send data to the same regional cloud.
- You can create an account on each regional cloud. Data on each cloud will be separate.

Contacting Support

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

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

Stealthwatch Data and Threat Response

About Sending Stealthwatch Alarms to Cisco Threat Response

When Cisco Threat Response Integration is configured, Stealthwatch will send active security alarms with Critical and Major severity to the Cisco Threat Response private intelligence store as Incidents with corresponding Sightings, Observables and Indicators objects created from the Alarm metadata.

This information will be available in the Incidents tab and during the investigation process as corresponding Sightings and Indicators derived from the Incident.

- Incidents created for Alarms derived from Relationship policy will not include IP addresses as observables as this information is not available in the Alarm.
- If you do not want Stealthwatch to send Alarms to Cisco Threat Response, do not select **Global Intelligence** and **Private Intelligence** scopes when creating the API Client in Cisco Threat Response.
 - Please contact <u>Technical Support</u> if you want to change the minimal severity of the alarms to be sent to Cisco Threat Response.

About Stealthwatch Enrichment Data for Threat Response

Once your SMC is registered with the Cisco Security Services Exchange and the Stealthwatch module is configured in Cisco Threat Response, you will be able to see the enrichment data from Stealthwatch in the Threat Response Investigation workflow.

For every valid IP address requested in the investigation, Stealthwatch will return security events associated with this IP in the form of corresponding Sightings and Indicator objects, with the following limitations and rules:

- Security Events from *all* configured domains.
- Security Events for the last 15 days.
- Top 10 Security Events by points.
- Security Events where the IP was a subject for source or destination.

 Please contact <u>Technical Support</u> if you want to change these settings, spe cifically if Enrichment requests from Stealthwatch Enterprise are failing on Cisco Threat Response with "Relay Module Timeout".

About the Cisco Threat Intel Model

Before sending to Cisco Threat Response, Stealthwatch alarms and security events are transformed to Cisco Threat Intel Model (CTIM) objects.

To read more about Cisco Threat Intel Model, refer to the <u>Cisco Threat Intel Model doc</u>umentation.

The key entities used in this translation are listed below:

- Incident Discrete instance of indicators affecting an organization, as well as information associated with incident response.
- Sighting A record of the appearance of a cyber observable at a given date and time.
- Observable A simple, atomic value which has a consistent identity and is stable enough to be attributed an intent or nature: domain names, IP addresses, file hashes, specific devices or users. Stealthwatch shares information only about observables of IP address type.
- Target The device, identity, or resource that a threat has targeted. Target is identified by one or more Observables.
- Indicator Describes a pattern of behavior or a set of conditions which indicate malicious behavior.

About Translating Stealthwatch Alarms to CTIM Objects

Every critical and major alarm is translated to an Incident, a Sighting, an Indicator object, and the relationships between them. The picture below shows the representation of Stealthwatch alarm in CTIM model (simplified):



When building a Sighting object for the Incident, Stealthwatch includes Observables with the following constraints:

- Alarms derived from the Relationship Policy Event will not have Observables in the Sighting object.
- Alarms that have Source as "Multiple Source" or Target as "Multiple Destinations" will not include corresponding Observables in the Sighting object.

When building a Target object for the Sighting, the following constraints apply:

- Target object is included only for Alarms generated from the following types of core events:
 - beaconing-host
 - bot-infected-host
 - bot-infected-host-controlled
 - brute-force-login
 - fake-app-detect
 - half-open-attack
 - host-lock-violation
 - icmp-received
 - max-flows-served
 - new-flows-served
 - packet-flood
 - ping
 - port-scan
 - addr-scan-talking-detect
 - \circ slow-connection-flood
 - ssh-rev-shell
 - suspect-long-flow
 - suspect-quiet-long-flow
 - suspect-udp-activity
 - syns-received
 - target-data-hoarding
 - touched
 - udp-received
 - watch-host-active
 - high-target-index
 - high-ddos-target-index
 - high-recon-index
 - attack-index

For more information about Stealthwatch Security Events, refer to <u>Stealthwatch Security Events and Alarm Categories</u>.

- Target object is not included if alarm target is "Multiple Destinations".
- Target object is not included if alarm target is an external IP address.

About Translating Stealthwatch Security Events to CTIM Objects

Upon an investigation request from Cisco Threat Response, Stealthwatch returns Security Events associated with an IP address.

Every Security Event is translated to the CTIM model Sighting and Indicator objects, with the relationships, as shown on the picture below:



When translating Stealthwatch Security Events to a CTIM object, the following constraints and rules apply:

• Target objects are not included in the Sighting objects for Security Events

Cisco Cloud Accounts

Required Account for Cisco Threat Response Access

In order to use Cisco Threat Response and associated tools, you must have one of the following accounts on the regional cloud you will use:

- Cisco Security Account
- AMP for Endpoints account
- Cisco Threat Grid account

Create an Account to Access Cisco Threat Response

If you or your organization already has an account on the regional cloud you will use, use the existing account. Do not create a new account.

To create an account on a regional cloud, complete the following steps:

- Determine which Cisco Threat Response cloud to use: Refer to the <u>supported</u> <u>functionality and guidelines and limitations in Cisco Threat Response Regional</u> <u>Clouds</u> section.
- 2. If you do not already have an account on the regional cloud you will use, ask your management if your organization already has a Cisco Security Account (CSA) set up in that cloud.
- 3. If anyone else in your organization already has a Cisco Security Account in that region:
 - Have the administrator of that account add an account for you using the <u>Manage Access To Your Organization's Cisco Security Account</u> instructions.
- 4. Otherwise, create a new Cisco Security Account for your organization (You will be its administrator):
 - a. In your browser, go to your chosen regional cloud.
 - b. For links, refer to the Cisco Threat Response Regional Clouds section.
 - c. Click the link to create an account.
 - d. Look for an email message to complete the registration.
- 5. On the Cisco Security Dashboard, launch Threat Response. On first log in you'll be asked to review and agree to the cloud subscription agreement. Once you accept the agreement, click **Launch**.

i) To add users in your organization, click on **Users** at the top of the page.

- 6. If it's your first use of Cisco Threat Response, you'll be asked to connect your Stealthwatch device. To do this:
 - a. Under Connect a Device such as SMA Email or NGFW, click Connect.
 - b. Select **Register Device**. The Cisco Security Services Exchange portal will open in a new window. To register your SMC, refer to the <u>Register your SMC</u> in Cisco Cloud section. Start on step 2.
 - c. Once registration is complete, in the Cisco Security Services Exchange portal, click **Confirm Device is Connected**.
- 7. Continue to the <u>Configuring your Stealthwatch and Cisco Threat Response Integ</u>ration section.

Manage Access To Your Organization's Cisco Security Account

If you are a Cisco Security Account owner or administrator, you can grant additional users access to your organization's Cisco Security Account and manage existing users, including resending the account activation email.

To manage users, complete the following steps:

- 1. In a browser window, go to your regional Cisco Security Account:
 - North America: https://castle.amp.cisco.com/my/users
 - Europe: https://castle.eu.amp.cisco.com/my/users
- 2. Click Users.
- 3. Add or edit user access. If you select Account Administrator, the user will have permissions to grant and manage user access.

Configuring Stealthwatch and Cisco Threat Response Integration

Configuring Cisco Threat Response Integration

Configuring the CTR Integration in Stealthwatch will enable:

- Cisco Threat Response Pivot menu in Stealthwatch UI.
- Cisco Threat Response Casebook in Stealthwatch UI.
- Sending Stealthwatch Alarms to Cisco Threat Response.

Prerequisites

- SMC v7.1.2 or later
- You have an account to access CTR (see <u>Required Account for Cisco Threat</u> <u>Response Access</u>).
- Your SMC must be able to connect outbound to the Cisco clouds:
 - North America clouds:
 - api-sse.cisco.com, port 443
 - visibility.amp.cisco.com, port 443
 - EU clouds:
 - api.eu.sse.itd.cisco.com, port 443
 - visibility.eu.amp.cisco.com, port 443
- Your Stealthwatch deployment is generating security events and Alarms as expected.

Procedure

To configure the CTR Integration, complete the following steps:

- 1. Go to your regional Cisco Threat Response cloud:
 - North America cloud: <u>https://visibility.amp.cisco.com</u>
 - Europe cloud: <u>https://visibility.eu.amp.cisco.com</u>
- 2. Sign in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
- 3. Go to **Settings > API Clients**.
- 4. Click Add API Credentials.

← → C (a) visibility.amp.cisco.cc	*	s 📿 🛕 🛈 🕞 🔕 🗄 🖻 Other Bookmarks			
cisco Threat Response Investig	gate Snapshots Incidents Beta Intelligen	ce Modules		(1	?)
Settings	API Clients 📟				
Your Account	API Clients allow you to integrate and automa	te Cisco Threat Respo	nse by calling the collection of APIs it is built upon.		
Devices	Add API Credentials How do API Clients	s work?			
API Clients	Client	ID	Description		Actions
Integration Modules					🔻
Users					💌
					💌
					💌

5. In the opened dialog fill in the name and description for the API Client and select all scopes then click **Add New Client**.

	Add New Client
Client Name *	
smc-ctr-client	
Scopes* · Select None	
🗹 Casebook	Access and modify your casebooks.
Enrich	Query your configured modules for threat intelligence - Read Only
Inspect	Extract Observables and data from text - Read Only
🗹 Global Intelligence	Access AMP Global Intelligence - Read Only
🗹 Private Intelligence	Access AMP Private Intelligence
Response	List and execute response actions using configured modules.
Description	
Add description	

If you do not want Stealthwatch to send Alarms to Cisco Threat Response, do not select **Global Intelligence** and **Private Intelligence** scopes.

6. The system will create a Client ID and Client Password for you.

	Ac	d New Clier	nt
The Client Pa	ssword cannot l	pe recovered, once	you close this window.
Client ID · Co	by to Clipboard		
Client Passwo	rd · Copy to Clipt	oard	
			Close

i) The Client Password cannot be recovered once you close this window.

- 7. Log in to your SMC as Master Admin or Configuration manager.
- 8. From the navigation menu, click the Global Settings icon and select **Threat Response Configuration**.



9. In the Threat Response Configuration section, click Add New Configuration.

Cisco Threat Response Integration Configuration		
Threat Response Configuration	No Cisco Threat Response information available. Click Add New Configuration to begin.	Add New Configuration
Device Registration	No Device Registration Information available. Click New Device Registration to begin.	New Device Registration

10. In the opened form, select the regional cloud used to create the API Client and paste the Client ID and Client Password from Step 6. Then click **Save**.



- 11. System will validate and store the API credentials.
- 12. Verify that your SMC has the Threat Response Pivot Menu and Casebook available.
 - For Threat Response Pivot Menu:
 - Open any page in the SMC that contains a relevant IP address.
 - Click the ellipsis (\bigcirc) beside the applicable IP address.
 - In the pop-up menu that appears, click the arrow next to Cisco Threat Response. A secondary pop-up menu appears with menu content.

Target Host Groups		Target		Alarm	Policy	Event Alarms			
Catch	All	10. 		Watch Port Active	Inside Hosts				
Catch	View Flows Edi Top Reports External Lookup		lit > >	Watch Port Active	Inside Hosts				
Catch	Show Effe Cisco Thr	ective Policy eat Response [>	Watch Port Active	Inside Hosts				
			1	0.					
	Subject IP: 10.			IP Address					
	from: 10/0	07 12:18 PM	Copy to Clipboard						
	to: 10/07	12:23 PM	Add to New Case						
			Search for this IP						
			Stealthwatch Enterprise - Fusion Test						
			Host Report						
			S	tealthwatch Enter _l Host Report	orise-Sigma S	tudio			
			Та	alos Intelligence					
				Search for this IP					
			U	mbrella-Protection	1				
			Т	hreat Response					
				Investigate this IP A	Address				

- For Threat Response Casebook:
 - Navigate to any page in your SMC. Notice a Threat Response Casebook

Icon (\blacksquare) in the right bottom corner of the page.

• Click on the icon to expand the widget.

	Exploitation	DDoS Source	DDoS Target	Data	Hoarding	Exfiltration Policy Violation Costs Casebook	Anomaly 2 🗔 🖒 ? 🗙
	0	U	0		0	Find case CURRENT CASE Case October 7, 2019 12:25 PM	10/07/2019
Alarm	ns by Type			- 2	Today	0 Observables No description ALL CASES	
21	26					Case October 7, 2019 12:25 PM 0 Observables No description	10/07/2019 Investigate - Delete
20 11	5					Case October 4, 2019 11:33 AM 0 Observables No description	10/04/2019
1	54	4	8	4		Casebook October 1, 2019 3:29 PM 0 Observables No description	10/01/2019
	0 10/1 10/2	1 10/3 10/4 • Watch Port Active	0 10/5 10/6 1 Data Exfitration	0/7		Case September 30, 2019 10:44 AM 4 IP Addresses Network Scan Attack Case	09/30/2019
	Policy Violation	1	Deselect All Selec	t All		Relationship Alarm Investigation 2 IP Addresses No description	09/30/2019

- 13. Verify your Stealthwatch alarm in CTR:
 - a. Wait until Stealthwatch detects Critical or Major Security Alarm or generate a test security alarm.
 - b. Log in to your regional Cisco Threat Response cloud.
 - c. Navigate to Incidents tab from Threat Response menu.
 - d. Your Alarm should be available in the list.

Additional Information

For additional information about the integration, refer to the following links:

- <u>About Cisco Threat Response Pivot menu</u>
- About Cisco Threat Response Casebook

You have to log in to Cisco Threat Response to view the Pivot menu and Casebook help.

About Sending Stealthwatch Alarms to Cisco Threat Response

Register your SMC in the Cisco Cloud

Registering your SMC in Cisco Security Exchange Cloud will allow Threat Response to retrieve enrichment data such as Security Events from your SMC to be included in the investigation workflows.

For more details, refer to the <u>About Stealthwatch Enrichment Data for Threat</u> Response section.

Procedure

To register your SMC in Cisco Secured Exchange Cloud, complete the following steps:

- 1. Go to your regional Cisco Threat Response cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
- 2. Navigate to **Module > Devices** and click **Manage Devices**. The Cisco Security Services Exchange portal opens.

threat Response Inves	tigate Snapshots	Incidents Beta	Intelligence	Modules	
Devices Manage Devices Reload Device	S				
Name		Туре			Version
fmc65.ciscothreatresponse.local		Cisco Firepov	wer Managem	ent Center for VMWare 300	6.5.0
fdm65.ciscothreatresponse.local		Cisco Firepov	wer Threat De	fense for VMWare	6.5.0-5
ftd65.ciscothreatresponse.local		Cisco Firepov	wer Threat De	fense for VMWare	6.5.0
fmc64.ciscothreatresponse.local		Cisco Firepov	wer Managem	ent Center for VMWare	6.4.0
ftd64.ciscothreatresponse.local		Cisco Firepov	wer Threat De	fense for VMWare	6.4.0
fdm64.ciscothreatresponse.local		Cisco Firepov	wer Threat De	fense for VMWare	6.4.0-102
sma2.teamnorthwind.ca.iphmx.com		SMA			13.0.0-087

- 3. In your Cisco Security Services Exchange portal, enable **Cisco Threat Response** in Cloud Services Menu.
- 4. Click the **Add Devices and Generate Tokens plus icon** located on the right of the page, above the table with your devices.

ciso	s S	ecurity Se	ervices Ex	change Dashboard Devices	Cloud Services	Events			• *	~	
Devices for Cisco - Integration											
▼ Q. Device Name / ID O Rows Selected											
		%		Name <	Туре	Version	Status	Description	Actions		
		>	1	7-x-smc-SLIC	SWE	7.1.2	Registered	Stealthwatch Management Console	/ 🖬 🖷		
		>	2	SMC30	SWE	7.1.2	Registered	Stealthwatch Management Console	/ 🖬 🗈		
		>	3	Secure Event Connector - ctr-dev-sec.ciscot	Secure Event Con	e15c616b39a3da	Registered	Secure Event Connector listening on TCP: 10125, UDP: 10	/ 🖬 😘		
		>	4	cssp-nam-prod-77	CSSP	1.0	Registered	Cisco Security Services Proxy	/ 🖬 🗅		
		>	5	fdm64.ciscothreatresponse.local	Cisco Firepower T	6.4.0-102	Registered	Standalone fdm64	/ 🗑 📑		

5. In the opened dialog, click **Continue** and let system generate a token for your device.

Number of devices			
1			
Up to 100			
Token expiration time			
1 hour	•		

6. Copy the generated token into the memory buffer or save the generated token into the file.



- 7. Log in to your SMC as Master Admin or Configuration manager.
- 8. From the navigation menu, click the Global Settings icon and select **Threat Response Configuration**.

Q 🖸	Desktop Client				
	Global Settings Central Management				
	Packet Analyzer Configura				
olation	UDP Director Configuration				
	External Lookup Configura				
	User Management				
	Threat Response Configur				
	Select Language				

9. In the Device Registration section, click **New Device Registration**.

Cisco Threat Response Integration Configuration		
Threat Response Configuration ()	No Cisco Threat Response information available. Click Add New Configuration to begin.	Add New Configuration
Device Registration	No Device Registration information available. Click New Device Registration to begin.	New Device Registration

 In the opened dialog, select the Cloud Region that matches your Cisco Threat Response regional cloud and insert the Security Services Exchange token generated and saved in step 5. Click **Register**.

Device Registration	
CLOUD REGION:	
North America (US) V	
DEVOS TORISE *	
Liter Device Token No token? Get it from: https://admin.sse.ikd.cisco.com	
	Cancel Register

- 11. The device will be registered in Cisco Security Services Exchange and the status will show as **Enrolled**.
- 12. Verify the status of the device in the Cisco Security Services Exchange portal. The status of the device should show as **Registered**.

Configuring Stealthwatch Integration Module in Cisco Threat Response

For Threat Response to retrieve enrichment data from Stealthwatch the integration module must be configured.

Prerequisites

- Your SMC is registered in the Cisco Security Services Exchange cloud.
- Cisco Threat Response is enabled in Cisco Security Services Exchange portal Cloud Services.

Refer to the <u>Register your SMC in the Cisco Cloud</u> section for more details.

Procedure

To configure the Stealthwatch module in Cisco Threat Response, complete the following steps:

- 1. Go to your regional Cisco Threat Response cloud and log in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.
- 2. Click **Modules** in the navigation pane and then click **Add New Module** in the *Your Configurations* area on the *Modules* page.

Alternatively, you can expand **Modules** in the navigation pane and click **Available Modules**.

- 3. On the *Available Modules* page, click **Add New Module** in the Stealthwatch Enterprise module pane.
- 4. In the opened dialog:
 - a. Name your module.
 - b. In the Registered Device drop down, locate your SMC.
 - c. Click Save.
- 5. Verify that Cisco Threat Response can retrieve enrichment data from your SMC. To do this:
 - a. Review your SMC Security Dashboards and notice an IP that generates security events.
 - b. Enter this IP into the Investigation search panel in Cisco Threat Response.
 - c. The graph should show you other hosts involved in Security Events with the requested host.
 - d. The Sightings will represent the security events associated with the requested host.

Access Security Services Exchange

Before you begin

• In your browser, disable pop-up blocking.

Procedure

- 1. In a browser window, go to your regional Cisco Threat Response cloud:
 - North America cloud: <u>https://visibility.amp.cisco.com</u>
 - Europe cloud: https://visibility.eu.amp.cisco.com
- 2. Sign in using the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account. Your account credentials are specific to the regional cloud you sign in to.

3. Navigate to Security Services Exchange: Click **Settings > Devices > Manage Devices**. The Security Services Exchange will open in a new browser window.

Known Issues and Limitations

- Failover is not supported for the CTR integration in v7.1.2. The configuration needs to be repeated for the secondary SMC for the integration to work.
- Backup and Restore is not supported for Device Registration in the Cisco Security Services Exchange Cloud portal. The Device Registration panel in the Cisco Threat Response configuration on your SMC shows the actual status of the device registration in the cloud. Therefore, restoring configuration from the backup for the device registration is not available. If deleted after the backup, the registration will have to be re-done again after restore.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <u>https://www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)