

# Integrations

- pxGrid, on page 1
- FMC, on page 2
- FTD, on page 3
- SecureX, on page 4

# pxGrid

From this page, you can configure ISE pxGrid Cisco Cyber Vision integration.

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems.

uluilu cisco		<u>⊬</u> 8 ×
Ø	& Network Organizat	Platform Exchange Grid
Ð	. Sensors ~	Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless
Ħ	糸 Users ~	integration between multivendor identity, network, security and asset management systems. Filling and submitting the fields below activates the sharing of endpoint assets discovered by this system with a Cisco
¢		Identity Services Engine (ISE) pxGrid controller. This information can then be leveraged by upstream security systems to monitor security, detect threats, and set network policy. Learn more here.
۹	¢ API ∽	
\$	₽ License	Carter Cartificate Authority
	糸 LDAP Settings	© You must download the CA Center to upload it in ISE.
	⊘ Snort	≟ Download certificate
	Risk score	ISE Server
	< Integrations	© No connection has been set up Register a new node Client certificate
	— pxGrid	Node Name:
	- CTR	Name of the pxGrid Node to be created on ISE pxGrid Server
	— FMC	Host Name: Host Na

For more information about how to perform this integration, refer to the manual "Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid".

# FMC

FMC administration page permits to configure a link between Cisco Cyber Vision with your Firepower Management Center. This connection will permit to send regularly (every 10 seconds) the components discovered by Cisco Cyber Vision. Every 10 seconds a list of new discovered components will be sent with the following properties in Cisco Cyber Vision:

- Name
- Id
- Ip
- Mac
- And if they are available:
  - hw\_version
  - model-ref
  - serial\_number
  - fw\_version
  - tags

The configuration of this connection consists of adding the IP address of FMC, then importing a certificate in Cisco Cyber Vision.

uluulu cisco			<u>⊬</u> ⊗ ·
Ø		Firepower Management Center	
Ē	& API	Connect Cisco Cyber Vision with your Firepower Management Center.	
Ħ	₽ License	IP Address:	
¢	A≳ LDAP	上 Import FMC certificate (pkcs12)	
۹	@ PxGrid	Cancel Save	
¢	© SNORT		
	< Integrations		
	— CTR		
	— FMC		
	- FTD		
	H Extensions		

In FMC, to download the necessary certificate, please navigate to "System" then to "Integration" and open the "Host Input Client" tab. In the tab create a new Client with the button "Create Client". Add the Cisco Cyber Vision Center IP address as host name, then download the pkcs12 certificate.

Then, in FMC, menu "Policies", "Application Detectors" add a new Product Map with the button "Create Product Map Set". Please create the new product Map with the exact name and case as presented below:

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
Access Cont	rol 🔻 Ne	twork Discover	у Ар	plication De	tectors	Correlation	Actions 🔻
Third-Part	y Product	Maps					
Product Ma	р						
CyberVision Integration	<u>n</u> vith Cisco Cyl	ber Vision					

#### Third-Party Vulnerability Maps

No vulnerability mapping sets currently defined.

The created hosts could be consulted in FMC, menu "Analysis", tab "Hosts - Network Map":

Overview A	nalysis	Policies	Devices	Objec	ts AM	IP Intelligence			
Context Explore	r Conr	nections 🔻	Intrusion	ns 🔻	Files 🔻	Hosts > Network Map	Users 🔻	Correlation <b>v</b>	Advar
Hosts N	etwork D	evices	Mobile De	evices	Indic	Network Map	pplicati	on Protocols	Vulnei
						Hosts			
Rilter by IP a	nd MAC add	lresses		×		Indications of Compromise			
			Unique ho	osts: 46		Applications			
						Application Details			
Hosts [IPv4] (3	31)			- 8		Servers			
<u>         192</u> (22)				- 6		Host Attributes			
<u>216</u> (2)				- 6		Discovery Events			
				i		Vulnerabilities			
				- 8		Third-Party Vulnerabilities			
+ <u>255</u> (1)				i	· `				
Hoete [IDv6] (	15)								
<u>fe80</u> (7)				- 6					
Hosts [MAC] (0	))								

# FTD

FTD administration page permits to connect Cisco Cyber Vision with your Firepower Threat Defense. It will allow to automatically kill anomalies detected by monitor mode and snort events. The corresponding session found in FTD will be killed.

Every 10 seconds Cisco Cyber Vision will browse the new monitor and SNORT events and send the corresponding action to the firewall. To enable that functionality, the user needs to add the following parameters in the FTD administration page:

• Ip address of the firewall

- Login: admin login, an ssh connection will be established between the center and the firewall
- Password: corresponding password
- Hostname: is the name of the device, by default "firepower"

Two option are available: kill session from monitor difference detection events and kill session from snort events.

.ılı.ılı. cısco		
Ø		Firepower Threat Defense
P	b <sup>¢</sup> API	Connect Cisco Cyber Vision with your Firepower Threat Defense. It will allows us to automatically kill anomalies detected by monitor mode and
Ħ	₽ License	snort events
¢	条 LDAP	IP Address:
۹	PxGrid	Login:
۵	Ø SNORT	Password:
	< Integrations	Hostname:
	— CTR	
	- FMC	Kill session from monitor difference detection events :
	— FTD	Kill session from snort events:
	器 Extensions	Cancel Save

# SecureX

Cisco SecureX is an online platform that centralizes security events from different Cisco software equipments through an API. For example, events like Cisco Cyber Vision events or firewall events can be sent to Cisco SecureX and correlated to be presented through different dashboards.

SecureX integration enables three features in Cisco Cyber Vision:

- without SecureX SSO login, the button Investigate in SecureX Threat Response will appear in components' technical sheet.
- with SecureX SSO login, the button Report to SecureX will appear in some events of the event calendar page. This button is used to push the events to SecureX.
- with SecureX SSO login, a SecureX ribbon with several features can be activated in Cisco Cyber Vision.

This section describes how to configure SecureX in Cisco Cyber Vision and the different features authorized.

### SecureX configuration

### Before you begin

The Cisco SecureX configuration in Cisco Cyber Vision requests:

An Admin access to Cisco Cyber Vision.

I

- A Cisco Cyber Vision Center with internet access.
- A SecureX account with an admin role.

ø <sup>ø</sup> API الم	· · · ·	SecureX
E Ucens		
自 泉 Extern	al Authen 🗡	SecureX is a cloud-native, built-in platform that connects our Cisco Secure portfolio and your infrastructure. It allows you to radically reduce du time and human-powered tasks.
© ⊙ Snort		
Q 🙆 Risk so	ore	Configuration
<ul> <li>Integra</li> </ul>	tions ^	If you activate this option users will be able to login (with SecureX SSO) and benefit from SecureX integration's features: Investigate button from Cyber Vision technical sheet of devices/components Create incidents from the events page (for xxx event only)
— pxGri		Activate SecureX Ribbon and benefit from the associated features
— FMC		Region
- FTD		v v
- Secur		North America
BB Extens	ons	Asia Pacific Japan China
⊡ Cente	certificate	
		7
The button <b>Enable</b>	SecureX	appears.
	Region	

**Step 3** Click **Enable SecureX** to enable the link.

Once the link enabled, the button turns red to disable SecureX.

Region		
Europe	$\vee$	
	Disabl	le SecureX

By completing the steps above, you are now able to use the button **Investigate in SecureX Threat Response** that will appear in the components' technical sheet. To install and use the SecureX ribbon and the Report to SecureX button, complete the steps herebelow.

**Step 4** Navigate to the user menu on the top right corner of the GUI and click **My Settings**.

A new SecureX menu appears on the right.

		G Home ▼		<u>~</u> 8
	_			Signed in as <b>admin</b>
/ setting	S			My Settings
is page you can (	edit your personal information (fir	st name, last name), account settings, and change your passwo	rd.	Logout
<b>q</b> General		Pa Language	E SecureX	
Email:	admin@sentryo.net	English (US)	Before activating the S Secure X site.	SecureX ribbon, please log in the
Role:	Admin	Deutsch	SecureX SSO	
Firstname:	admin			
Lastname :	admin	Español (España)		
		Français		
		●日本語		
		C Türkçe		

### **Step 5** Click the **SecureX SSO** button.

A popup appears with an authentication code.

GRANT APPLICATION ACCESS
fy the code provided here matches the code displayed via the nk and please accept it to authorize CyberVision on SecureX
5F5185BC

A page opens in the browser to grant Cisco Cyber Vision access to SecureX.



- Step 6 Click Authorize Cyber Vision.
- **Step 7** A Client Access Granted popup appears.



Step 8In Cisco Cyber Vision > My Settings, the SecureX menu indicates that Cisco Cyber Vision is connected to SecureX.A toggle button to enable the SecureX ribbon and a button to logout of SecureX are displayed.

E SecureX
(i) You are now connected to SecureX. You can activate the ribbon
Ribbon Status:
Logout of SecureX

**Step 9** Use the **Ribbon status** toggle button to enable the SecureX ribbon.

Click Save settings.

### Step 10

E SecureX
() You are now connected to SecureX. You can activate the ribbon
Ribbon Status:
Logout of SecureX

A message indicating that the SecureX ribbon is enabled appears.

L



## SecureX ribbon

Once configured and activated, the SecureX ribbon will appear at the bottom of the Cisco Cyber Vision GUI of the Explore menu.

The SecureX ribbon in the Device List view:

uluilu cisco					Ø Explore	🗸 / All data 🔻 / Device list	•		~	8~
ø	Criteria Selectali Rejectali Default 🔷 Last 2 years (Jan 27, 2020 10:50:57 AM – Jan 26, 2022 10:50:57 AM) 🖉 Refresh									
ß		۹	9 De	vices and 15 othe	r components	Q New data			Export t	to CSV
Ħ	RISK SCORE	~							< 1 2 > 20/p	page ∨
¢	副 NETWORKS	~	0	Device 💠 👻	Group	First activity $\  \                                $	Last activity	IP T	MAC T	Risk so
o ه	<ul> <li>Devices without tags</li> <li>Ø Device - Level 0-1</li> </ul>			Dell 192.168.105.70		Jan 26, 2022 10:49:56 AM	Jan 26, 2022 10:49:56 AM	192.168.105.70	00:11:43:6c:f8:89 (+ 1 other)	^
Ŭ	<ul> <li>Ø Device - Level 2</li> <li>Ø Device - Level 3-4</li> </ul>			Yokogawa 192.168.1.124	-	Jan 26, 2022 10:49:56 AM	Jan 26, 2022 10:49:56 AM	192.168.1.124	00:00:64:8c:6a:2c	
	A Network analysis     Software		0	10.99.99.182		Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	10.99.99.182	00:2a:e3:cc:a2:2e	
	► ♀ System			10.99.99.8		Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	10.99.99.8	00:2a:e3:cc:a2:2e	
	≁ ACTIVITY TAGS	^		172.23.33.1	-	Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	172.23.33.1	00:2a:e3:cc:a2:2e	
	Activities without tags  Control system behavior  GIT behavior			Vmware 172.23.33.10		Jan 26, 2022 10:49:48 AM	Jan 26, 2022 10:49:48 AM	172.23.33.10	00:0c:29:9e:89:5f	~
	Vetwork analysis	~	۲							>
>	<				×	<b>Ⅲ                                    </b>			< 1 2 > 20/p	page ∨

The Cisco SecureX Getting Started Guide explains how to use the SecureX ribbon.

For example, to find observables and investigate them in SecureX Threat Response, click the **Find Observables** icon like below:

	Dell 192.168.105.70	-	Jan 26, 2022 10:49:56 AM	Jan 26, 2022 10:49:56	5 AM 192
	Yokogawa 192.168.1.124	✓ Observables on Page	27.	All 0 + 0 🗭 0 👁	27 🛈 2
	10.99.99.182	<ul> <li>I0 IP Addresses</li> <li>192.168.1.124</li> </ul>			0.9
	10.99.99.8	□ 172.23.33.1 ✓			
	172.23.33.1	<ul><li>192.168.41.23</li><li>192.168.41.21</li></ul>			'2
	Vmware 172.23.33.10	<ul> <li>192.168.105.70</li> <li>10.99.99.182</li> <li>192.168.41.22</li> </ul>			v <sup>'2</sup>
<		Add 27 Observ	ables to Case Investigat	te in Threat Response	
		×	₩ 수 = द + :		

## SecureX event integration

Once SecureX has been configured in Cisco Cyber Vision, a **Report to SecureX** button appears on some events of the event calendar page. Using this button will push the event to SecureX and create an incident.

The SecureX button appears on three categories of event:

- Anomaly Detection
- Control Systems Events
- Signature Based Detection

The Report to SecureX button on a Control Systems Events:

cisco						
Ø	Today		category Control Systems Events	severity veryhigh	Day	Neek
B			Q Search an event			
	5	6:2d:ec:17 to 5069-L310ER/4	A   (\$ 5069-L310ER/A)   IP:192.168.41.22	MAC:5c:88:16:be:5a:6d		~
		15:40:38 Control Systems Events ( d:ec:17 to 5069-L310ER/A (4	Online command has been detected from	ROCKWELLVLAN41 IP:192.168.4 MAC:5c:88:16:be:5a:6d	41.10   MAC:00:50:56:2	~
¢		15:40:38 Control Systems Events 3	Stop CPU command has been detected from	ROCKWELLVLAN41   IP : 192.16	8.41.10   MAC:00:50:5	^
Q		5007 E010E00		10000000000000000000000		
-		source des	Flow	Component source	Component destination	
0			Source port: 61688 Destination port: 44818	Name:ROCKWELLVLAN41 MAC:00:50:56:2d:ec:17 IP:192.168.41.10	Device: <b>©</b> 5069-L310ER/A Name: 5069-L310ER/A MAC: 5c: 88:16: be: 5a: 6d	
		ROCKWELLVLAN41 5069	9-L310E R/A	Tags : 🧳 Engineering Station 🗳 Windows	IP:192.168.41.22	
					lags:  Controller  Rockwell Automation	
					9 vulnerabilities detected	
					REPORT TO SECURE പ്രിന	x
		15:40:48 Control Systems Events ( d:ec:17 to and 1756-L81E/B   (\$ 0	Online command has been detected from COMMON   1756-L81E/B (Port1-Link01))   I	ROCKWELLVLAN41 IP:192.168.4 P:192.168.41.21   MAC:08:61:95:d	41.10   MAC:00:50:56:2 12:11:38	~
		15:40:48 Control Systems Events diec:17 to 1756-L81E/B (@ 0	Offline command has been detected from COMMON   1756-L81E/B (Port1-Link01))   I	ROCKWELLVLAN41 IP:192.168. P:192.168.41.21   MAC:08:61:95:d	41.10   MAC:00:50:56:2  2:11:38	~
	4:00 PM					

## SecureX component button

Once SecureX has been configured in Cisco Cyber Vision, the button **Investigate in Cisco Threat Response** appears on the components' technical sheet. The component's IP and MAC addresses will be investigated in SecureX Threat Response if you use this button.

Componen	t			
	5069-L310ER/A	R	First activity	Tags
Rockwell Automation	<ul> <li>5069-L310ER/A</li> <li>IP: 192.168.41.22</li> <li>MAC: 5c:88:16:be:5a:6d</li> </ul>	_	Jan 20, 2022 10:49:22 AM	🔗 Controller,
		R	Last activity Jan 31, 2022 3:40:46 PM	Rockwell Automation
				Activity tags
	🖉 Edit			🗬 Start CPU, 🗬 Stop CPU,
Investigate in Cisco Threat Response				🗬 Broadcast, 🗬 Low Volume,
				- ARP

## **External resources for SecureX integration**

Herebelow is the list of all URLs called by the Cisco Cyber Vision Center in case you need to authorize them, for example in a firewall.

### Center:

- private.intel.eu.amp.cisco.com
- private.intel.apjc.amp.cisco.com
- private.intel.amp.cisco.com
- intel.amp.cisco.com
- visibility.eu.amp.cisco.com
- visibility.apjc.amp.cisco.com
- visibility.amp.cisco.com

#### Web client:

- securex.apjc.security.cisco.com
- securex.us.security.cisco.com

I