

DEPLOYMENT GUIDE

IntSights External Threat Protection Suite User Guide

Integrate a Fortinet FortiSIEM On-premises Device



Integrate a Fortinet FortiSIEM On-premises Device

Configure a Fortinet FortiSIEM on-premises device to pull indicators of compromise (IOCs) from the IntSights ETP Suite. You must first add the device to the ETP Suite and then configure the device itself to pull IOCs from the ETP Suite.

Before you begin, ensure:

- You have the credentials to access the IntSights virtual appliance web interface
- You have the credentials to access the FortiSIEM device
- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Orchestration and TIP modules.

Add a FortiSIEM Device

You can add a Fortinet FortiSIEM device to the IntSights virtual appliance.

To add a FortiSIEM device:

- 1. From an internet browser, navigate to https://<virtual appliance IP address>.
- 2. Log in to the virtual appliance using the web access username and password created.
- 3. From the **Devices** page, click **Devices** (Pull).
- 4. Click Add new device.
- 5. In the Devices (Pull) screen, set up the new device:
- a. Type a user-defined, unique device name (for example, CBR External).
- b. Select the FortiSIEM device type.

c. Click Create.

Devices (Push) Devices	(Pull) Active Directory
Devices (Pull)	Q Search
Name	
Splunk Enterprise Secu	CREATE
Туре	
On Blue Coat Proxy	FirePower
Palo Alto Networks 7.1 and above	
Splunk Enterprise Security (CSV)	ght REST
Splunk Enterprise Security (TAXII)	
Panorama 7.1 and above	hk Enterprise Security (TAXII)
FortiSIEM	
McAfee ESM	on Black Response
ArcSight ESM	Cont Denny
ArcSight REST	LOAT Proxy
LogRhythm SIEM	rama 7.1 and above
Cisco FirePower	

6. Verify that the new device is displayed in the ETP Suite platform:

a. Log in to the IntSights ETP Suite at dashboard.intsights.com.

b. From the main menu, select **Automation > Integrations**. If this window is already open, refresh it by selecting **Automation > Integrations** from the menu. The new device is displayed in the **On-Premises tab**.

On-Premise Cloud	T	Fortisiem FortisiEM Last successful sync was on: Nov 18, 19 12:17	Device IDC Limit 300000	\$
Devices	21	IOC Groups		
Q, Search		Test		0 -
ArcSight	•	Test_2		0 -
AresightREST				
Fortisiem				

Configure a FortiSIEM Device to Pull IOCs

After a device has been added to the IntSights virtual appliance, you must enable it to pull IOCs from the ETP Suite.

Before you begin, ensure:

- You have the device login credentials
- The device has been integrated in the IntSights virtual appliance (if necessary) and the ETP Suite
- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Automation (Orchestration) and TIP modules
- An IOC group for this device exists in the IntSights ETP Suite Creating IOC groups is described fully in the "Create IOC group" section of the IntSights External Threat Protection Suite User Guide. Due to device limitations, IOC groups can consist of only one type of IOC. To support more than one type (domains, IP addresses, etc.), create multiple IOC groups.

To pull IOCs into FortiSIEM, you must set up a separate FortiSIEM resource group for each IntSights IOC group. The process of creating different forms of FortiSIEM groups is very similar and is described together. The small differences are noted in the description.

To configure a FortiSIEM device to pull IOCs:

- 1. From the ETP Suite, copy the IOC group URL:
- a. From the ETP Suite, select **Automation > Integrations**.
- b. From the On-Premise device list, select the FortiSIEM device.
- c. Click the link icon to the far right of an IOC group (label 1).

for For Las	tisiem tiSIEM it successful sync was on: Sep 25, 19 15:34		Device IOC Limit 300000	\$
IOC Group	15			
ip_iocs				0 -
url_iocs	i			0 -
domair	n_iocs			0 -
hash_i	IOC Group URL	×		0 -
	Make sure to edit the URL and include the IP add your IntSights virtual appliance.	dress of		
	http://[APPLIANCE_IP]:8080/fortisiem_ip_iocs	٥		
	2			
	С	lose		

- d. From the **IOC Group URL** dialog box, copy the URL (label 2). The diagram shows the URL for the IP address group. The URL is unique for each IOC group.
- e. To ensure that the IOC group contains values, hover over the IOC group line, then click the information icon.

INTEGRATIONS On-Premise Cloud		Fortisiem FortiSIEM Last successful sync was	on: Oct 03, 19 15:44	Device IOC Limit	\$	
Devices	22	IOC Groups				
Q Search		a A bbb				
		aa			0 -	
Fortisiem	IOC List					×
	Q, Search					
	IOC		Туре	Severity	Last Seen	
	http://apk.plus/products	s_dudi-apk/	URLs	Low	Oct 3, 2019	
	http://maildomaindisabl	led1.com/kusgdfh	URLs	Low	Oct 3, 2019	
	thisisatestforsocialmedi	a.com/blababla	URLs	Low	Oct 3, 2019	
	http://disabledasset1.co	m/hgdf	URLs	Low	Oct 3, 2019	
			< 1-10 >			

If the IOC list is not populated, stop and then try again.

- 2. Log in to the FortiSIEM management console.
- 3. From the main menu, click **Resource**.

Forti	SIEM		2 DASHBO	DARD		CASE	СМОВ	📑 TASK	o Admin	
0.0000	Overview	III List	🗠 Risk	C 11	minute 👻					≡ Select Rows ▼

The task The task description will continue with the Malware Domains resource group, to match the IntSights domains IOC group. The same steps are used for the other resource groups.

4. In the Resources menu, click Malware Domains (label 1). The list of currently defined malware domains groups is displayed.

Devices - IntSights X	Integration	ns - Automation - Int. X	5 FortiSIEM		× +				- c) ×
↔ ♂ @ 0) 🔒 https://	192.168.0.167/phoenb	/html/resource				⊠ ☆		∭\ (□)	: ≡
🕂 FortiSIEM	60 🖿	A # 8		os				0	A 🕮	8 O
• 🔶 🛛 o	Resourc	es > Malware Dor	nains							
Reports		Edit Voloto	More + Q	Search			C 🔳	К <	1/20 999	> н
Rules										
Networks	Active	Domain Name	IP		Country	Description			Date Fou	ad
a market star	2	100032351.hol.es								î
Watch Lists	8	100033212k.hol.es								
Protocols		1000-00-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0								
Event Types	1. S	1000rupaiya.com								
, and the	S	1006565215.hol.es								
 Malware Domains 	R	101 homeschool.com	n							
Malware IPs	R	101wsxzsa1.club								
Mabware URLs	-									
h Halana Barana	R	1102350s. hol. es								
 Manware Processes 	8	19tv. top								
 Country Groups 	R	2-bit.net.ru								
Mabware Hash	8	2nv-acc.online								

- 5. Click + (label 2) to create a new group.
- 6. In the **Create New Malware Domain Group** dialog, type a name and a description (optional), then click **Save**. In our example, the resource was named IntSights1_Domains.
- Expand the Manage Domains section and select the new resource (label 1 IntSights1_Domains), then click More > Update (label 2).



8. In the Update Malware Domain dialog, select Update via API, then click the URL edit icon.

Devices - IntSights	X 💿 Integrations - Automation - Int X 🔀 FortiSIEM X +	- 🗆 ×
(←) → C ^a	① 🔒 https://192.168.0.167/phoenix/html/resource 🗵 🏠	II\ ① ③ ≡
FortiSIEM	an in ≜ m ≅ in ≕ cc	0 A B & ¢
	Update Malware Domain O Import from a CSV file @ Update via API URL: Not defined Cose Close	X 0/0 Date Found
ThreatStream Domain IntSights1_Domains		

The dialog box expands to display additional parameters.

) Import from a CSV fi	le				
Update via API					
URL:	http://192.168.0.252:8080/fortisiem_domain_iocs				
User Name:					
Password:					
Plugin Class:	com.accelops.service.threatfeed.impl.ThreatFeedWithMap	pingPolicyService			
Field Separator:	,				
Data Format:	● CSV ○ Custom ○ STIX-TAXII				
Date Update:	● Full ○ Incremental				
Data Mapping:					
	Domain Name	~	1	• •	•

9. Enter the details for the resource group, as described in the table for the specific resource group type. (This is the only step where creating resource groups differs.)

Update	Malware	Domain	Values
opaato	mannaro	Donnann	10100

Field in update dialog	Enter this
URL	 Paste URL from the domains IOC group in the ETP Suite Integrations page. Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance. Ensure that the port matches the port in use.
User Name	Leave blank
Password	Leave blank
Plug-in Class	Leave as-is
Field Separator	Type a comma (this is the default)
Data Format	CSV
Date Update	Select Full
Data Mapping	Select Domain Name and Position = 1

Field in update dialog	Enter this
URL	 Paste URL from the IP address IOC group in the ETP Suite Integrations page. Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance. Ensure that the port matches the port in use.
User Name	Leave blank
Password	Leave blank
Plug-in Class	Leave as-is
Field Separator	Type a dash (this is the default)
Data Format	CSV
Date Update	Select Full
Data Mapping	Select Low IP and Position = 1

Update Malware IP Values

Update Malware URL Values

Field in update dialog	Enter this
URL	 Paste URL from the URLs IOC group in the ETP Suite Integrations page. Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance. Ensure that the port matches the port in use.
User Name	Leave blank
Password	Leave blank
Plug-in Class	Leave as-is
Field Separator	Type a comma (this is the default)
Data Format	CSV
Date Update	Select Full
Data Mapping	Select URL and Position = 1

Field in update dialog	Enter this
URL	 Paste URL from the Hashes IOC group in the ETP Suite Integrations page. Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance. Ensure that the port matches the port in use.
User Name	Leave blank
Password	Leave blank
Plug-in Class	Leave as-is
Field Separator	Type a comma (this is the default)
Data Format	CSV
Date Update	Select Full
Data Mapping	 Select Botnet Name and Position = 1 Select Algorithm and Position = 2 Select HashCode and Position = 3

Update Malware Hashes Values

10. Click Save.

11. In the **Update Malware Domain** dialog, click the Schedule + icon. The dialog box expands to display additional parameters.

Update Malware Domain	×
○ Import from a CSV file ● Update via API	
Time Range	
Start Time: 18:00:00 Local V Etc/UTC V	
Recurrence Pattern	
Once O Hourly O Daily O Weekly O Monthly Start From: 09/25/2019	
Save Cancel	

12. Set a schedule and recurrence pattern for when FortiSIEM should pull the IOCs, then click Save.

13. Click Close.

14. To verify that IOCs are uploaded to FortiSIEM, go to the resource you created and verify that IOCs are populated in the table. For example:

😹 FortiSIEM	AN DASHBOARD IN ANALYTICS & NCIDENT IN CASE IN CADE IN RESOURCE INTASK. CC ADMIN	0 A 88 A 0	
	Resources > Malware Domains > IntSights1_Domains		
Reports	New Edit Delete More + Q Search Last updated at Oct 6, 2019 12:08:00 PM	S 🖩 🕴 🕯 1/23 \cdots 🕨 H	
Rules			
Networks	Active Domain Name IP Country Description	Date Found	
Watch Lists	😸 (18:002255: hot.es)		
Protocols	W 110012119.800.65		
Event Types	B 180 upshys.com		
▼ Alabrare Domains	G 13(0)(0215,100-15		
MalwareDomainc.bt	G 131homeschool.com		
Zeus Domains	S 111vszzs1.dub		
SANS Domains			
ThreatStream Domain	S 19tk.ttp		
Hall-1-TXVII Maharas Domain	S 2-bit.net.ru		
Partitional tables of bounds	S 2nv-acc.online		
Fortiveard Matware Pomain	Gr 25-Sauthfahures.gq		
ThreatConnect Malware Domain	8 3statheemoga		
Ungrouped	43ed922ac7.000webhostapp.com		
intslights Domain Group 1	🐼 Astablestick. Ir		
IntSights Malware Dornains	Störthereun.in		
IntSights1_Domains	🗭 Stw.ru		
Mahrare Ps	☑ 63sectach.com		
Maheare URLs	🗑 99waccawl0.dub		
Aialware Processes			
Country Groups	C alygiais.com.my		
 Mahrare Hash 	R a5718370.000webhostase.com		
2.20	Semnary Auto espand	A ¥	



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet^{*}, FortiGate^{*}, FortiGate^{*}, FortiCare^{*} and FortiQuard^{*}, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and fortinet disclaims all waranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinets General Counsel, with a purchaser that expressly warants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.