

DEPLOYMENT GUIDE

IntSights External Threat Protection Suite User Guide

Integrate a Fortinet FortiManager On-premises Device



Integrate a Fortinet FortiManager On-premises Device

Configure a Fortinet FortiManager on-premises device. IOCs are pushed from the IntSights ETP Suite to the device.

When IOCs are pushed to this device, only new IOCs that were discovered since the last push (the delta) are sent.

To receive IOCs, you use the IntSights virtual appliance web interface to integrate the device with the ETP Suite, and then use the ETP Suite to configure an IOC group whose IOCs will be pushed to the device. IOC groups for FortiManager devices can consist of the following types of IOCs: domains, URLs, and IP addresses.

Before you begin, ensure:

- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Orchestration and TIP modules.
- You have the credentials to access the IntSights virtual appliance web interface.
- You have the administrative credentials to access the device management console.
- All managed FortiGate firewalls are configured with the inspection engine in "Proxy" mode. "Flow" mode is not supported for this integration due to limitations in FortiGate Firewall.
- You know whether you want to push IOCs to the FortiManager Root ADOM or the Global Database ADOM.

Integrate a Fortinet FortiManager Device

Use the IntSights virtual appliance to integrate the device with the ETP Suite.

To integrate a FortiManager device:

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

Devices (Pu	ish) De	evices (Pull) Activ	/e Directory
Devices (P	ush) Co No	nnection: 1 o connection: 0	Q Search
+ Forti	iDemo	User	
Fort	tiManager 🗸 🗸	Password	
Type	k Point R77.30	Workspace Mode	
Fortil	Manager	2	CREATE
QRad Splur Web	sort Exchange Online ' Jar nk Standalone sense AP-WEB 8.3	Zscaler Internet Access URL/IP	×
Zscal	ler Internet Access	https://admin.zscalerbeta	

c. Type values for $\ensuremath{\textbf{User}}$ and $\ensuremath{\textbf{Password}}.$

These should be the same values used to access the FortiManager web management console.

- d. Type the URL or IP address of the FortiManager machine.
- e. Select the FortiManager Workspace Mode:
 - 1. To push IOCs to the root ADOM, do not select Workspace Mode (default).
 - 2. To push IOCs to the Global Database ADOM, select Workspace Mode.
- f. You can test the connection by clicking Test connection.
- g. Click Create.
- h. Review and approve messages.

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

- a. Log in to the IntSights ETP Suite at ${\it dashboard.intsights.com}.$
- 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**.

The following figure shows a newly added device in the ETP Suite **Automation > Integrations** window:

INTEGRATIONS On-Premises Cloud		FortiDemo FortiManager Last successful sync was on: Apr 28, 20 12:56	Device IOC Limit 30000	÷
Devices Q Search	2			
FortiDemo	•			

Configure an IOC Group to Push IOCs to the Device

Once the FortiManager device has been added and is synching with the IntSights virtual appliance, it is ready to receive IOCs that are pushed from the ETP Suite. IOCs are pushed by creating an IOC group for this device in the ETP Suite.

Creating IOC groups is described briefly <u>here</u>, and is described fully in the "Automating Internal Remediation" section of the *IntSights External Threat Protection Suite User Guide*.

When creating IOC groups, you can choose whether the matched IOCs should be monitored or blocked in the FortiManager device. This choice is transmitted to the device, together with the IOC identification.

IOC groups for FortiManager devices can consist of the following types of IOCs: domains, URLs, and IP addresses.

Verify That IOCs Are Being Pushed to the Device

You can verify that IOCs are being pushed to the FortiManager device.

To verify IOCs:

- 1. From the ETP Suite, select Automation > Integrations.
- 2. Select the device.
- 3. On an IOC group of the device, click the Information icon:

FortiDemo	Device IOC Limit		
Last successful sync was on: Apr 28, 20 12:56	30000	¢	
C Groups			
Forti_IOCs			

The IOCs in the group are displayed:

			×
Туре	Severity	Last Seen	
Domains	Low	Apr 28, 2020	
Domains	Low	Apr 28, 2020	
Domains	Low	Apr 28, 2020	
Domains	Low	Apr 28, 2020	
Domains	Low	Apr 28, 2020	
Domains	Low	Apr 28, 2020	
	Type Domains Domains Domains Domains Domains Domains	Type Severity Domains Low Domains Low	Type Severity Last Seen Domains Low Apr 28, 2020 Domains Low Apr 28, 2020

In the FortiManager management console, select Policy & Objects > Object Configurations > Security Profiles > Web Filter.

IntSights IOCs are displayed in the User-Defined section under the following name format (in lower case):

<DeviceName_IOCGroupName> for example, fortidemo_forti_iocs



Ensure that you are in the correct ADOM.

Double-click the IOCs listing to see the IOCs:

Edit Web	Filter Profile					
Name	e fortidemo_forti_iocs					
Comn	nent					0/255
L LO	g all search keyword:	5				
Static	URL Filter					
Ble	ock Invalid URLs					
VF	RL Filter					
+ 4	Add 🗹 Edit 🛗 D	Delete				
	URL	Туре	Action	Referrer Host	Status	
	marinabay.trave	wildcard	monitor		enable	
	marinabay.eu/*	wildcard	monitor		enable	
	nba.com.bbrevie	wildcard	monitor		enable	
	xn80ad0a.xn	wildcard	monitor		enable	
	xnb1aet.xnp	wildcard	monitor		enable	
	xnb1ae5a.xn	wildcard	monitor		enable	

Note that the "monitor" action was passed from the ETP Suite.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, FortiCare* and FortiGuard*, 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 atlained 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 Tortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet Seneral Counsel, with a purchaser that expressly warrants that the identified product will perform accerding 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 darity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. 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.

October 29, 2021 5:10 PM Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 7:DG-FortiManager-102021:DG-F