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

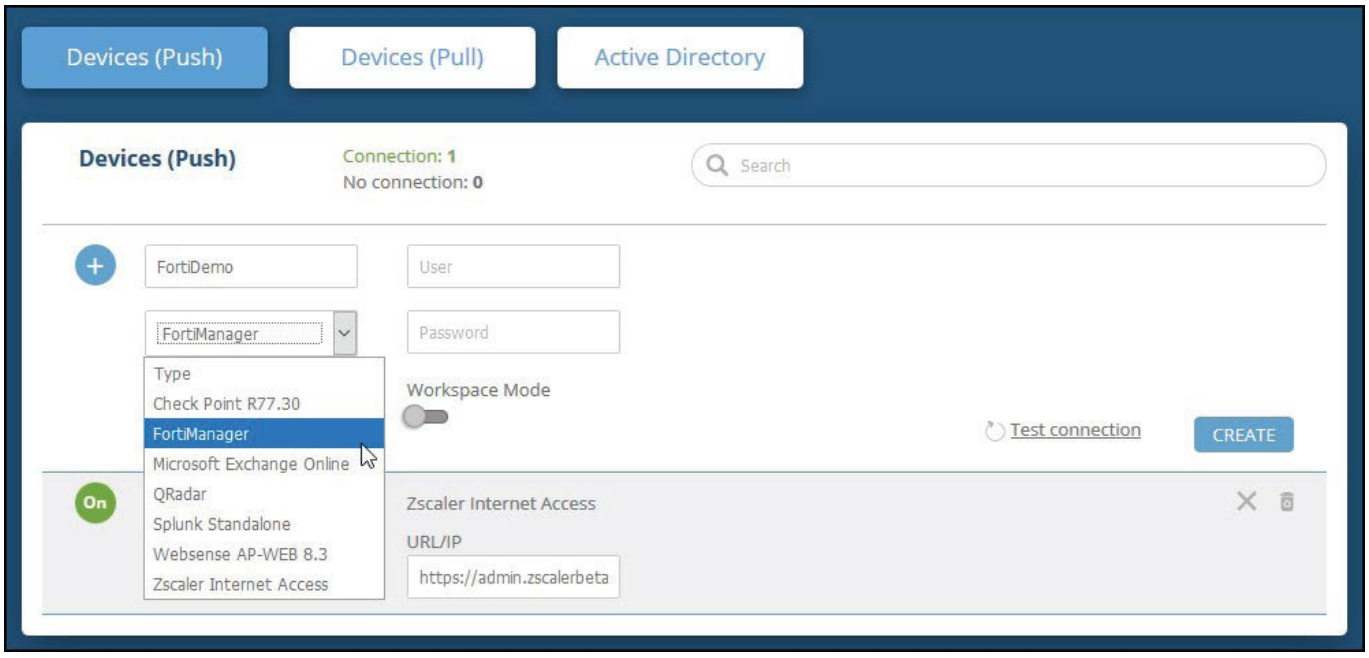
Use the IntSights virtual appliance to integrate the device with the ETP Suite.

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.



c. Type values for **User** and **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.

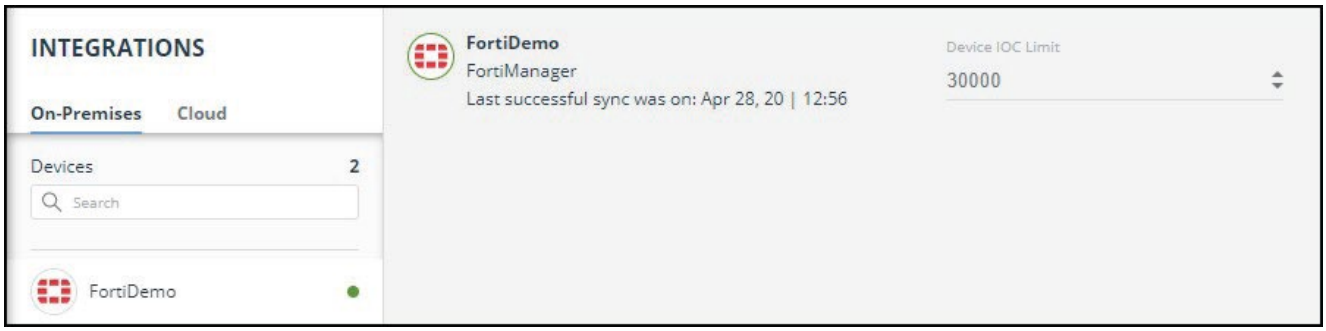
h. Review and approve messages.

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

a. Log in to the IntSights ETP Suite at **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:



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 here, 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.

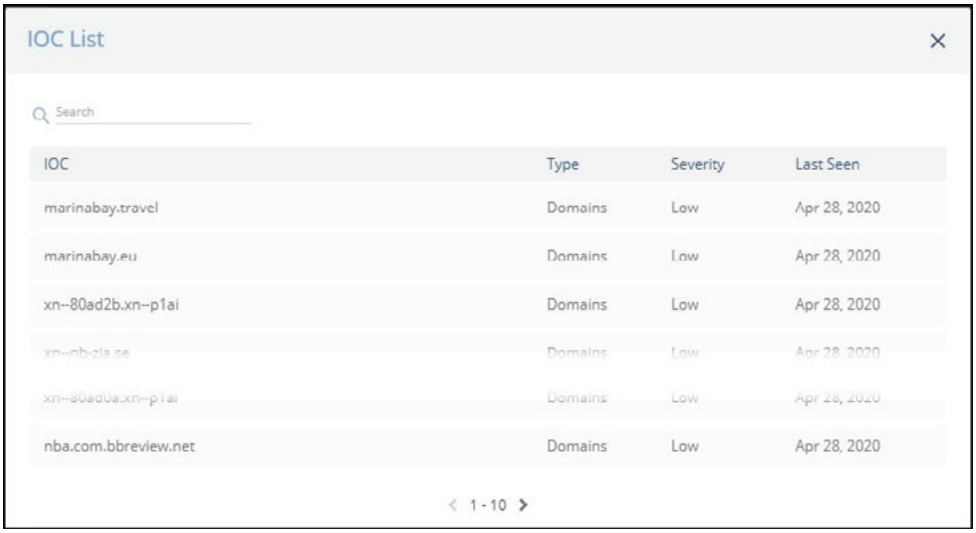
Verify That IOCs Are Being Pushed to the Device

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:

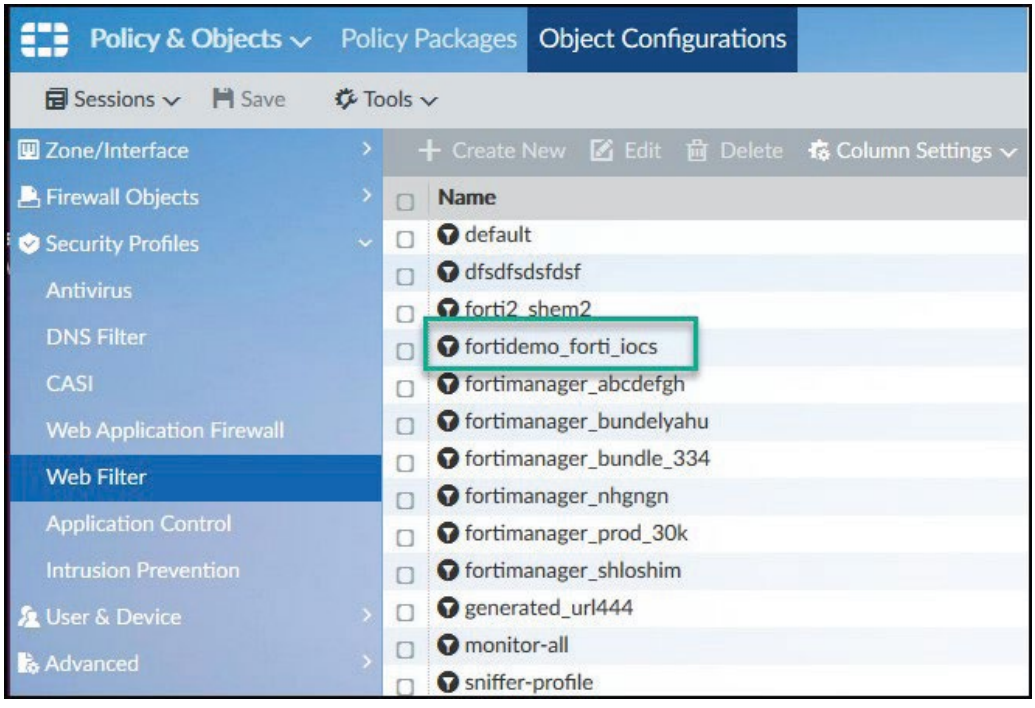
The IOCs in the group are displayed:



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

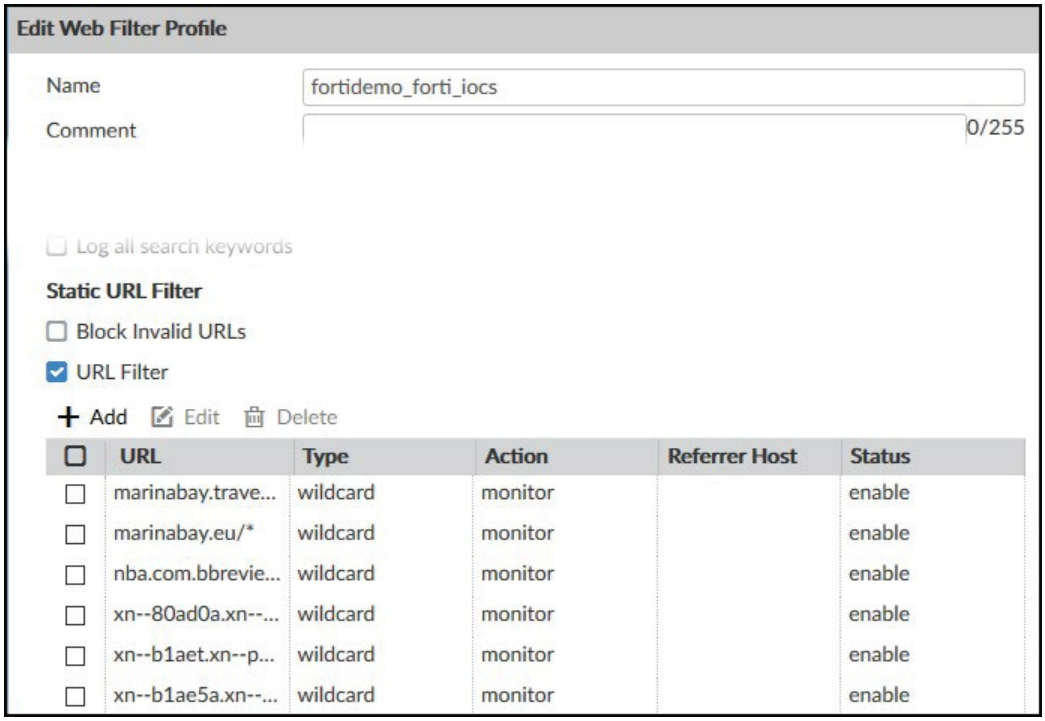
IntSights IOCs are displayed in the **User-Defined** section under the following name format (in lower case):

<DeviceName_IOCGroupName> for example, **fortidemo_forti_iocs**



Ensure that you are in the correct ADOM.

Double-click the IOCs listing to see the IOCs:



Note that the “monitor” action was passed from the ETP Suite.

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-FortiManager-102021

697784-A-0-EN-A