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:

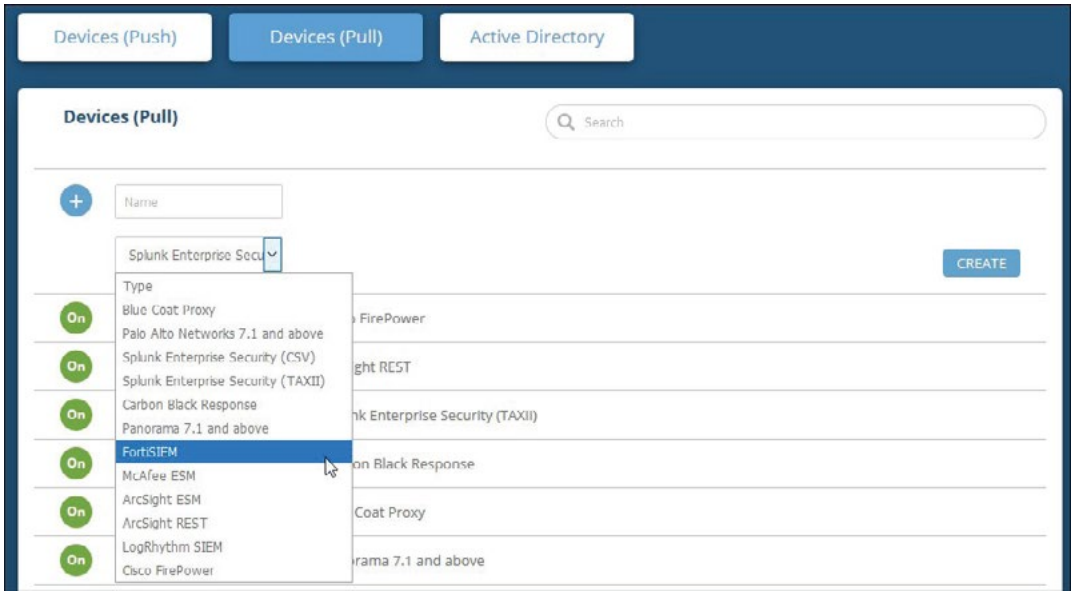
- You have the credentials to access the IntSights virtual appliance web interface
- You have the credentials to access the FortiSIEM device
- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Orchestration and TIP modules.

## 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**.




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**.


## 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.

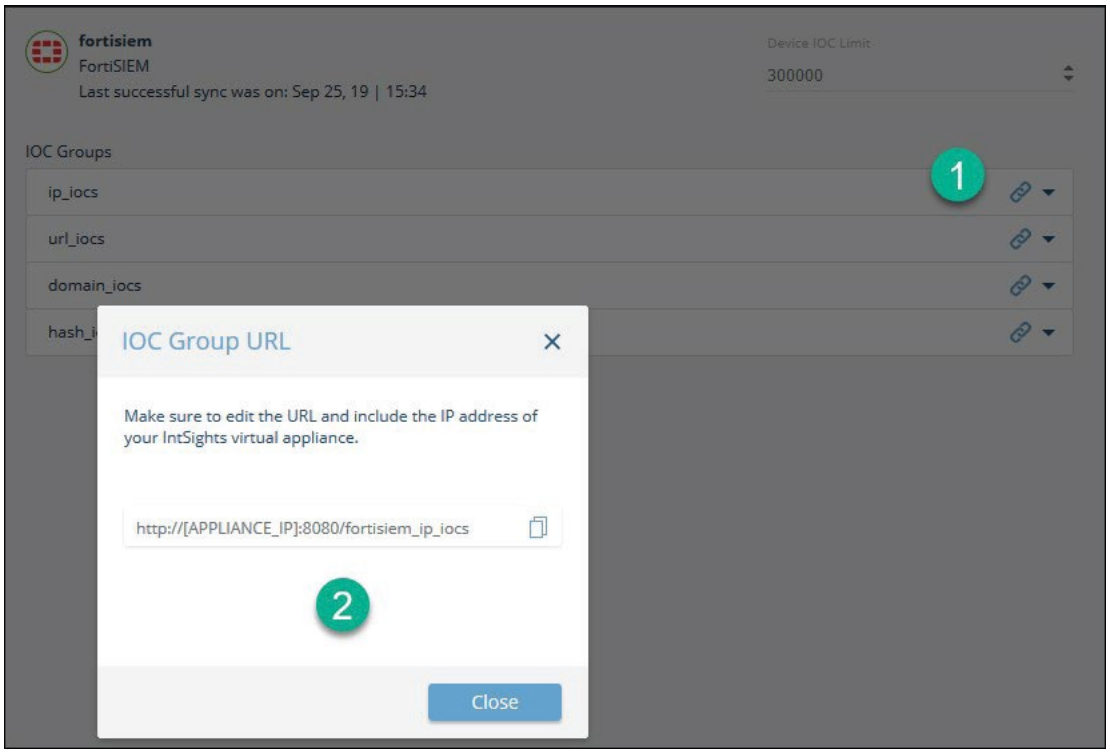
**To configure a FortiSIEM device to pull IOCs:**

1. From the ETP Suite, copy the IOC group URL:

a. From the ETP Suite, select **Automation > Integrations**.

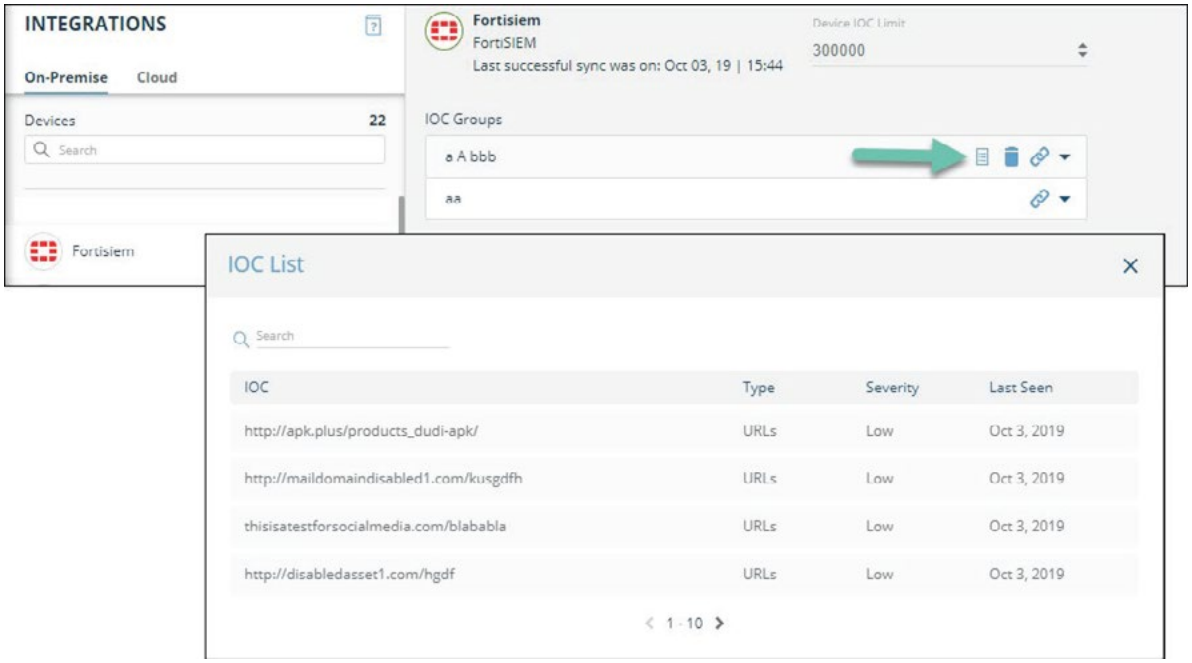
b. From the On-Premise device list, select the **FortiSIEM** device.

c. Click the link icon to the far right of an IOC group (label 1).



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.

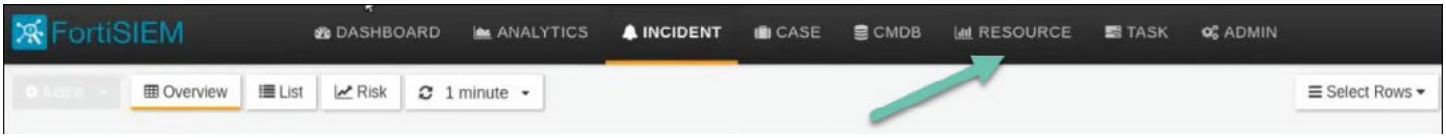
e. To ensure that the IOC group contains values, hover over the IOC group line, then click the information icon.




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

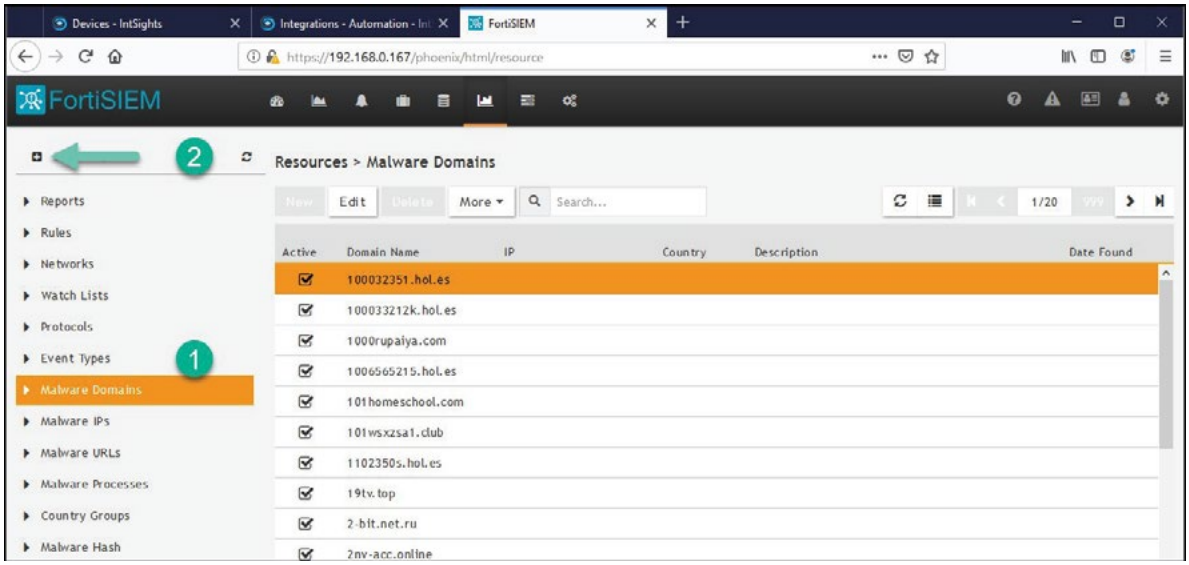
2. Log in to the FortiSIEM management console.

3. From the main menu, click **Resource**.

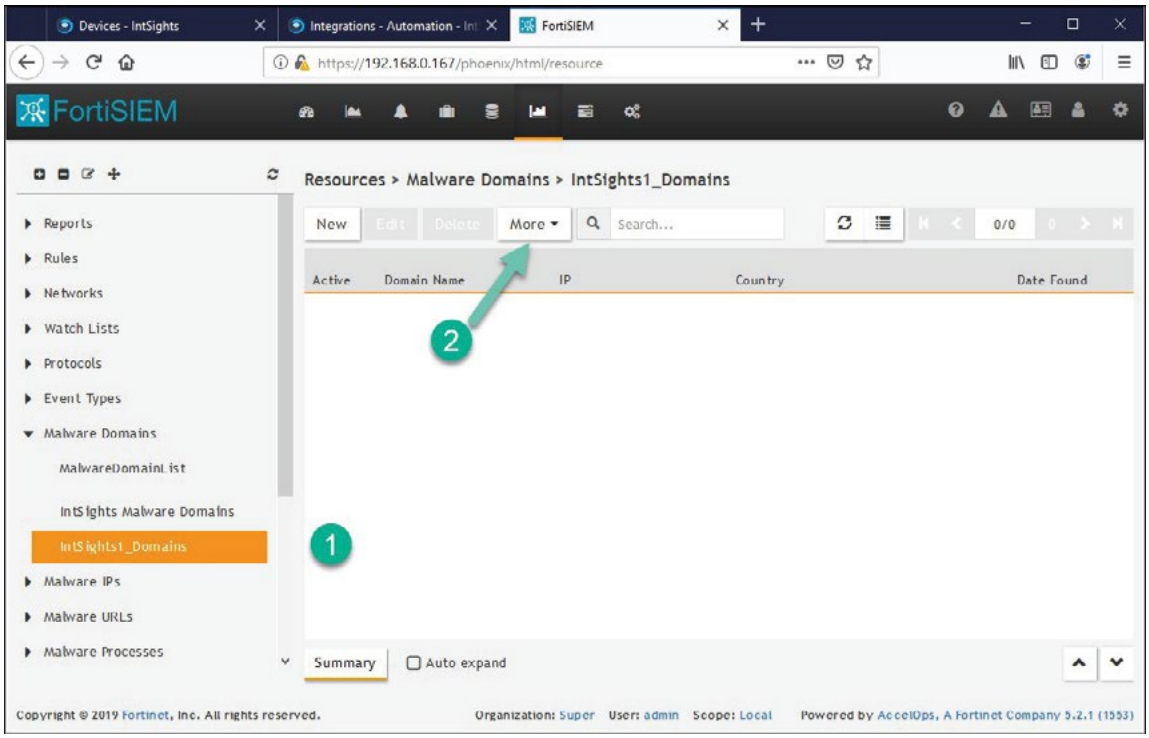



The task The task description will continue with the Malware Domains resource group, to match the IntSights domains IOC group. The same steps are used for the other resource groups.

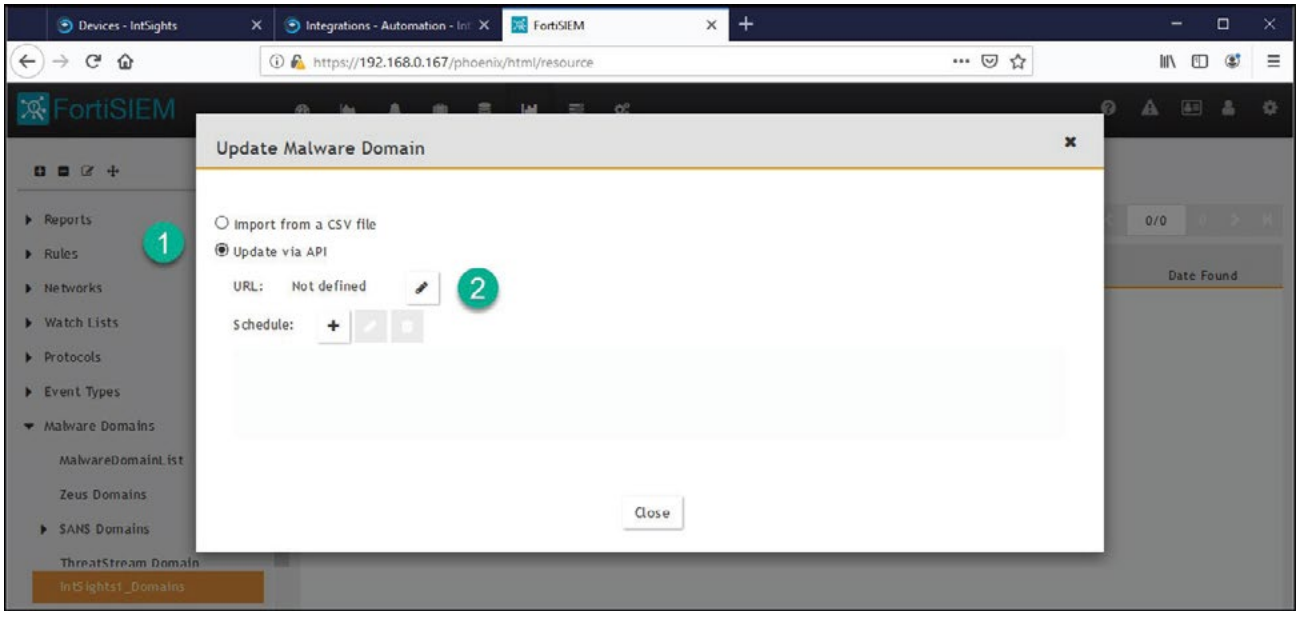
4. In the **Resources** menu, click **Malware Domains** (label 1). The list of currently defined malware domains groups is displayed.



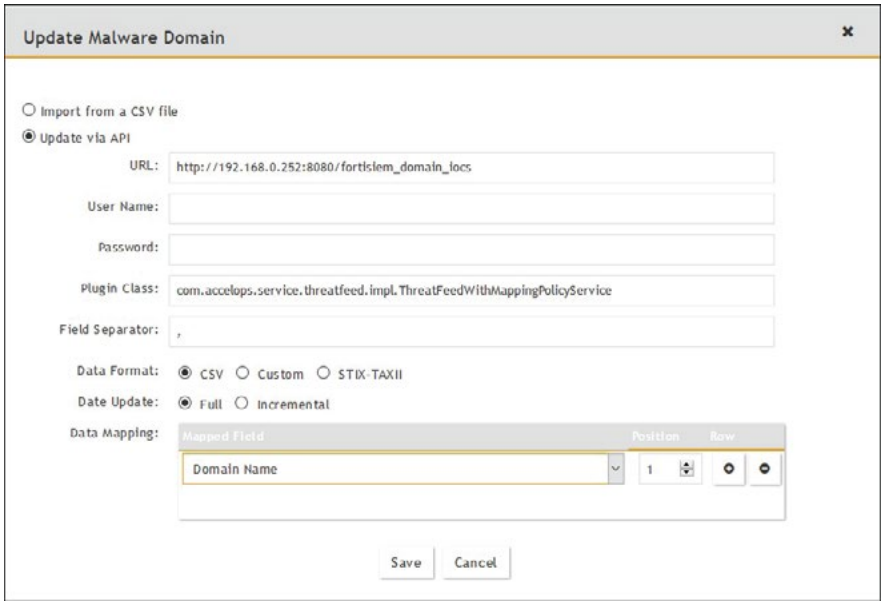
5. Click + (label 2) to create a new group.
6. In the **Create New Malware Domain Group** dialog, type a name and a description (optional), then click **Save**. In our example, the resource was named IntSights1_Domains.
7. Expand the **Manage Domains** section and select the new resource (label 1 IntSights1_Domains),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




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



The dialog box expands to display additional parameters.




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

| Field in update dialog | Enter this |
|---|---|
| URL | Paste URL from the domains IOC group in the ETP Suite Integrations page.<br>■ Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance.<br>■ 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 |

Update Malware IP Values

| Field in update dialog | Enter this |
|---|---|
| URL | Paste URL from the IP address IOC group in the ETP Suite Integrations page.<br>■ Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance.<br>■ 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 |

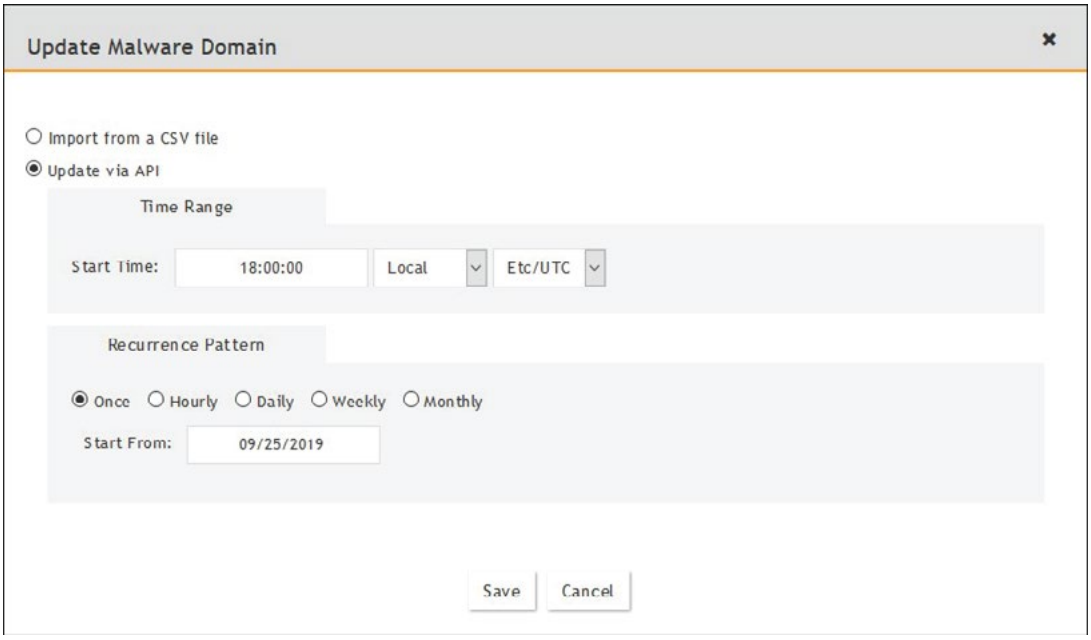
Update Malware URL Values

| Field in update dialog | Enter this |
|---|---|
| URL | Paste URL from the URLs IOC group in the ETP Suite Integrations page.<br>■ Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance.<br>■ 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 |

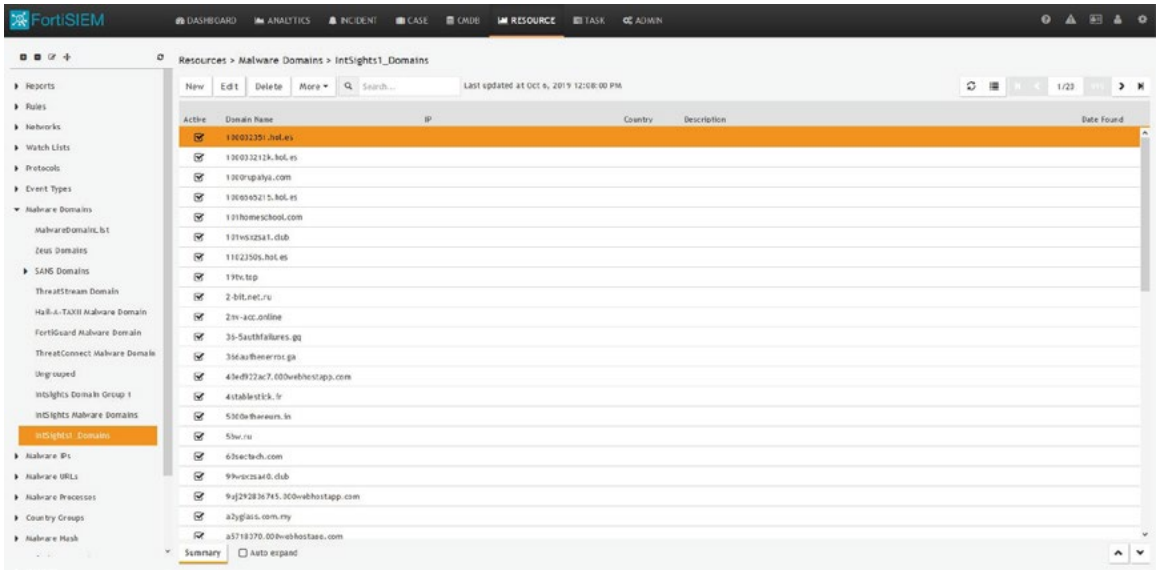
Update Malware Hashes Values

| Field in update dialog | Enter this |
|---|---|
| URL | Paste URL from the Hashes IOC group in the ETP Suite Integrations page.<br>■ Replace [APPLIANCE_IP] with the IP address of your IntSights virtual appliance.<br>■ 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<br>■ Select Algorithm and Position = 2<br>■ Select HashCode and Position = 3 |

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



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:








October 29, 2021 4:20 PM
Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 7:DG-FortiSIEM-102021:DG-FortiSIEM-102021
697784-A-0-EN-B