HOWTO – Integrate External CMDB via CSV

Contents

CMDB via CSV Overview

FortiSIEM has a feature that allows you to upload a CSV file to a specific location and map its contents to the CMDB using the GUI.

The limitation of this functionality is that your file needs a comma (from **Comma** Separated Values) as a separator and will not process any other delimiter. If the CMDB CSV you wish to import has a different separator, you need to convert it to a comma. Use your favourite method to find and replace and be careful with fields that use commas, you'll have to change them too, prior to replacing the wrong delimiter.

Example original CSV file headers from Nozomi:

name;level;appliance_hosts;ip;mac_address;mac_address_level;mac_vendor;os;roles;vendor;vendor:info;firmware_version;firmware_version:info;os_or_firmware;serial_number;serial_number:info;product_name;product_name:info;type;type:info;protocols;nodes;custom_fields

This will not work, we need to replace ";" with ","

Example original CSV data from Nozomi:

192.168.94.1;2;sg.labnozomi.com;192.168.94.1;00:50:56:c0:00:01;00:50:56:c0:00:01, unconfirmed;VMware, Inc.;;other;;source, passive;;source, passive;;;source, passive;;source, passive;-;source, passive;dropbox-lsp, igmp, mdns, netbios-ns;192.168.94.1;

Again, we need to replace ";" with "," but notice in yellow that we have the columns that will cause issues, because they use "," to separate multiple values. We need to make sure these are changed to something different than a comma (i.e replace "," with " and", otherwise FortiSIEM will not process the file correctly because the number of headers don't match the number of columns.

You can troubleshoot issues with CMDB CSV imports by looking at the /opt/phoenix/log/server.log file.

If there is a mismatch in columns you will see an error message such as this:

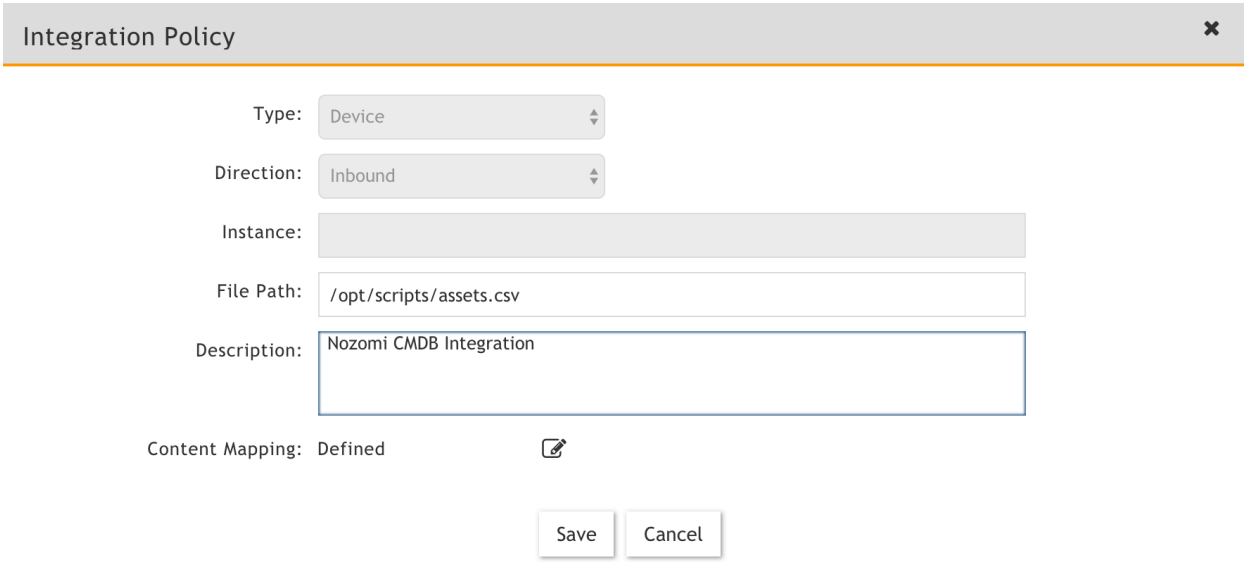
[#|2019-02-26T16:55:26.737+0000|WARNING|glassfish3.1.2|com.ph.phoenix.commons.Utils|_ThreadID=250;_ThreadName=Thread-2;|Column number not match in line 163|#]

Copy your CSV to a location on the Supervisor

1. Create a directory, i.e /opt/scripts/
2. Make sure admin is set as user and group
    a. chown -R admin:admin /opt/scripts/
3. Copy your csv to the directory
    a. scp assets.csv admin@super.ip:/opt/scripts/.

Create a CMDB Inbound Integration

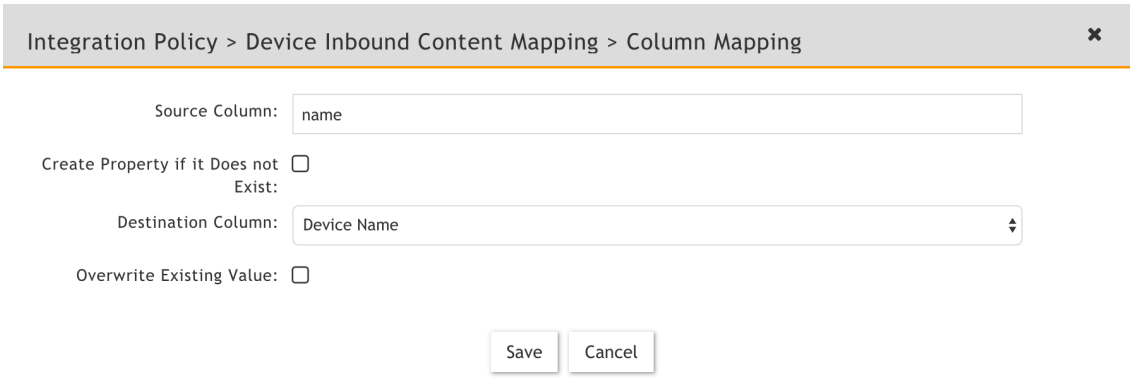
1. Go to Admin > Settings > General > Integration and Click New
2. Set Type: Device and Direction: Inbound
3. Enter the File Path to the CSV file. This example uses Nozomi assets.csv file. We will put this file in this path /opt/scripts/assets.csv on the Supervisor.



4. Click on Content Mapping
   The file we have has these columns, interesting ones in **bold**:

   name,*level*,*appliance_hosts*,***ip***,***mac_address***,*mac_address_level*,***mac_vendor***,***os***,***roles***,*vendor*,*vendor:info*,*firmware_version*,*firmware_version:info*,***os_or_firmware***,***serial_number***,*serial_number:info*,***product_name***,*product_name:info*,***type***,*type:info*,***protocols***,*nodes*,*custom_fields*

   Create the following mappings:



Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: ip

Create Property if it Does not Exist: ☐

Destination Column: Device IP

Overwrite Existing Value: ☐

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: mac_vendor

Create Property if it Does not Exist: ☐

Destination Column: Device Type Vendor

Overwrite Existing Value: ☐

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: os

Create Property if it Does not Exist: ☐

Destination Column: Device OS Edition

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: firmware_version

Create Property if it Does not Exist: ☐

Destination Column: Device Version

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: type

Create Property if it Does not Exist: ☐

Destination Column: Device Type Model

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: product_name

Create Property if it Does not Exist: ☐

Destination Column: Device Hardware Model

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: protocols

Create Property if it Does not Exist: ☑

Destination Property: protocols

Property Type: STRING

Property Display Name: Communication Protocols

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: mac_address

Create Property if it Does not Exist: ☐

Destination Column: Property Device MAC Address

Overwrite Existing Value: ☑

Save Cancel

Integration Policy > Device Inbound Content Mapping > Column Mapping

Source Column: roles

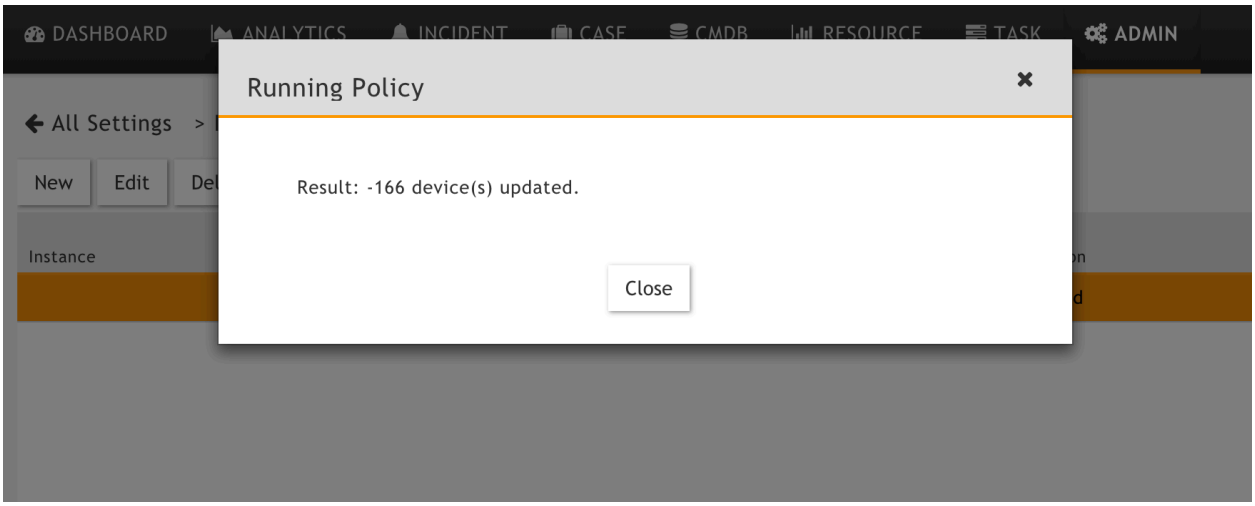
Create Property if it Does not Exist: ☐

Destination Column: Property Device Roles

Overwrite Existing Value: ☑

Save Cancel

5. Run the integration policy:



6. Then we can go to the CMDB and see our devices: