



# HOWTO – Integrate External CMDB via CSV

# Contents

CMDB via CSV Overview	. 2
Copy your CSV to a location on the Supervisor	. 3
Create a CMDB Inbound Integration	. 3





### 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\_ve rsion;firmware\_version:info;os\_or\_firmware;serial\_number;serial\_number:info;product\_name;product\_name:info;typ e;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;<mark>00:50:56:c0:00:01, unconfirmed</mark>;VMware, Inc.;;other;;<mark>source, passive</mark>;;<mark>source, passive</mark>;;<mark>source, passive</mark>;;source, passive;-source, passive;dropbox-lsp, igmp, <mark>mdns, netbios-ns</mark>;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=Th read-2;|Column number not match in line 163|#]

# F



### Copy your CSV to a location on the Supervisor

- 1. Create a directory, i.e /opt/scripts/
- Make sure admin is set as user and group

   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.

Integration Policy			×
Туре:	Device	\$	
Direction:	Inbound	¥	
Instance:			
File Path:	/opt/scripts/assets.csv		
Description:	Nozomi CMDB Integration	n	
Content Mapping:	Defined		
		Save Cancel	

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,fir mware\_version,firmware\_version:info,os\_or\_firmware,serial\_number,serial\_number:info,product\_name,pr oduct\_name:info,type,type:info,protocols,nodes,custom\_fields

Create the following mappings:

Integration Policy > Device Inbound Content Mapping > Column Mapping						
Source Column:	name					
Create Property if it Does not Exist:						
Destination Column:	Device Name					
Overwrite Existing Value:						
	Save Cancel					



INET.		
Integration Policy > Dev	ice 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 > Dev	ice 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 > Dev	ice Inbound Content Mapping > Column Mapping	×
Source Column:	20	
Create Property if it Does not Exist:	0	
Destination Column:	Device OS Edition	\$
Overwrite Existing Value:		
	Save Cancel	
Integration Policy > Dev	ice Inbound Content Mapping > Column Mapping	×
Source Column:	firmware_version	
Create Property if it Does not Exist:		
Destination Column:	Device Version	\$
Overwrite Existing Value:	ſ €	
	Save Cancel	
Integration Policy > Dev	ice Inbound Content Mapping > Column Mapping	×
Source Column:	type	
Create Property if it Does not Exist:		
Destination Column:	Device Type Model	\$
Overwrite Existing Value:	<b>⊻</b>	
	Save Cancel	



TINET				
Integration Policy > Devi	ce Inbound Content Mapping > Column Mapping		×	
Source Column:	product_name			
Create Property if it Does not ( Exist:				
Destination Column:	Device Hardware Model	\$		
Overwrite Existing Value: (	<b></b> ∠			
	Save Cancel			
Integration Policy > Devi	ce Inbound Content Mapping > Column Mapping	1	×	
Source Column:	protocols			
Create Property if it Does not Exist:	€			
Destination Property:	protocols			
Property Type:	STRING	\$		
Property Display Name:	Communication Protocols			
Overwrite Existing Value:	ſ			
	Save Cancel			
Integration Policy > Devi	ce 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:	⊡ S			
	Save Cancel			
Integration Policy > Dev	ice Inbound Content Mapping > Column Mappin	g	×	
Source Column:	roles			
Create Property if it Does not Fxist	0			
Destination Column:	Property Device Roles	\$		
Overwrite Existing Value:	ſ €			
	Save Cancel			



5. Run the integration policy:

🙆 DASHBOARD 📗	🖿 ANALYTICS 🌲 INCIDENT 💼 CASE 😂 CMDB 🔤 RESOURCE 🧮 TASK	📽 ADMIN
	Running Policy 🗙	
← All Settings > T New Edit Del	Result: -166 device(s) updated.	
Instance	Close	on d

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

😿 FortiSIEM	89 DASHBOARD		A INCIDENT	💼 CASE	🛢 СМДВ	Lull RESOURCE	📰 TASK	¢\$ ADMIN				•	<b>A</b>	â.	4 ¢
C + C	-			<b>O</b> Routers	<b>0</b> Firewalls	<b>O</b> Windows	<b>O</b> Unix	<b>O</b> ESX	<b>O</b> AWS	<b>O</b> Azure					
<ul> <li>Applications</li> </ul>	CMDB > Devic	es		0											
Users	New Edit	Delete Orgs v	nthout collector 🔻	Q Search						Action •		M <	7/7		
Business Services	Name	IP	▼ Туре				Status A	Agent Policy	Agent Status	Monitor Status	Event Status	Location		Vers	ion
CMDB Reports	acme-plc-00	172.16.1.175	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.150	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.155	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.146	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.151	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.154	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.148	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.177	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	acme-plc-00	172.16.1.156	POWER MEASUREM	ENT LTD. PLC			Pending							2	.90
	Summary Pr	roperties Monit	or Software 🕶	Hardware 🔻	Configurat	ion Relations	nips 🕑	Auto expand	,						<b>^                                    </b>
		Name: acme-plc-	00191	Acces	s IP: 172.16.1	.151	_								-
	Device Type: POWER MEASUREMENT Version:							Statistics							_
	Model: Modicon M340 BMX P34							Created:	Feb 28 2019, 02	2:22:59 L	ast Discovered	d:			
	Member of 1 Group							Last Updated:	Feb 28 2019, 02	2:22:59	Interface:	s: 1			
	Group #1: /Network Segment/Net-172.16.1.0/24							Components:	0	3	Running App	s: 0 s: 0			
			-					Patches:	0		Storage	e: 0			
								Active:	false		Schedule	e:			
								Status:							