Release Notes for FireMon Asset Manager 4.9.0

FireMon is pleased to provide this overview of the new features and enhancements made for this Asset Manager 4.9 release, which is recommended for all users. Any additional maintenance releases (4.9.0.x) will be added to this topic.

FireMon Asset Manager Edition 4.9	
The upgrade file is now available in FireMon User Center > Downloads. The supported upgrade path to Command Center 4.9 is from the 4.8 and 4.7 versions.	For the upgrade procedure, see Upgrading Asset Manager.

We recommend that you upgrade your Scouts whenever you upgrade your Command Center. However, Scouts 4.7x and 4.8x are compatible with the 4.9 version of the Command Center.

For customers upgrading from 4.7, previous branding customizations will be reapplied after the upgrade to FireMon Asset Manager 4.9.

For customers upgrading from 4.5 or 4.6, previous branding customizations will not be reapplied after the upgrade to FireMon Asset Manager 4.9. Contact support@firemon.com for instructions on how to rebrand after upgrading.

FireMon Support knows customers deploying an OVA using *ovftool* may receive a warning message (*Warning: No supported manifest ...).* This message can be ignored, and its reason will be corrected in a 4.9 fix release or the 4.10 release.

Database Schema

The **4.9 database schema** shows a visual representation of the database.

CLI Commands

The Asset Manager CLI is a powerful hierarchical menu-driven interface that provides virtually all administrative functionality in the browser interface. To administer your system using the command-line interface, see System Administration via CLI.

Security Updates & STIG

4.9 resolves Common Vulnerabilities & Exposures (CVEs) and incorporates a variety of security-related (and non-security-related) enhancements. See Security Advisories 4.9 for a list of CVEs resolved in this release.

Release Highlights

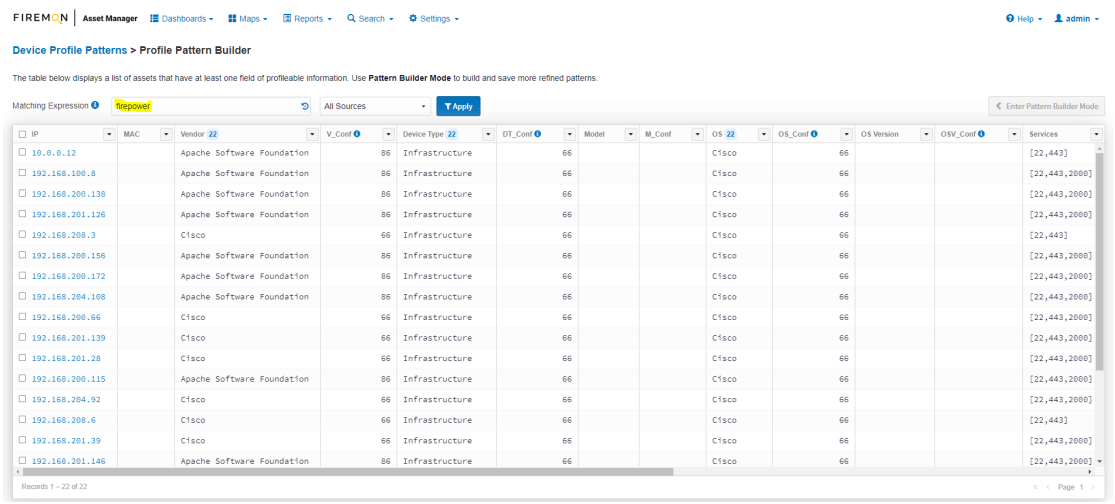
Profile Pattern Builder

Profile Pattern Builder is our brand-new user interface that empowers field engineers and administrators by providing a UI-based environment in which to build upon Asset Manager's vast profile pattern library. With a user-driven search function, you can quickly search all assets for meaningful, profileable attribute matches and create a new custom profile on the fly.

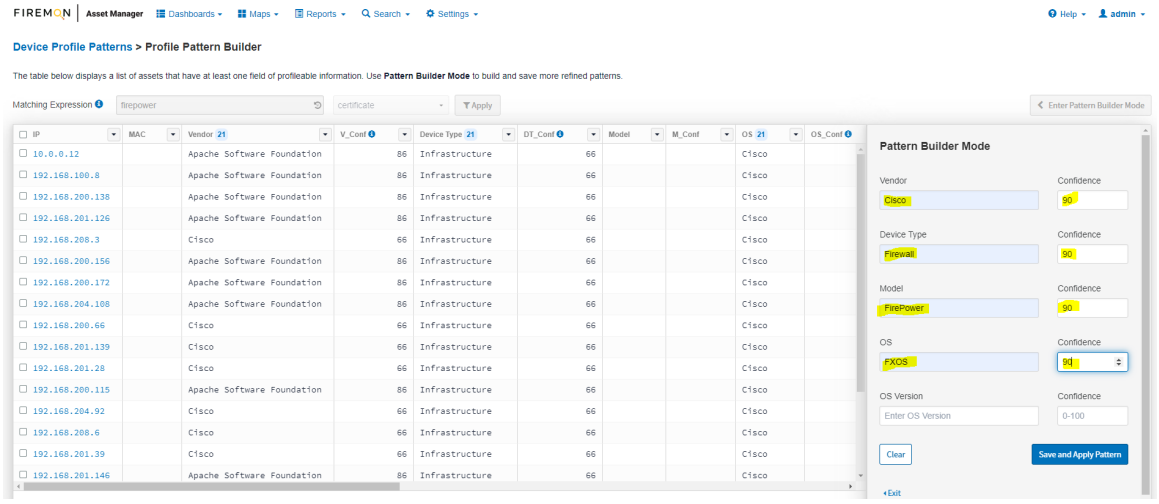
Previously, a manual method was used; you had to create a custom query to identify matching assets, write and test a regex expression, and then manually update an XML template and import that .xml file into the system.

The manual method will remain available for anyone who wishes to still use it.

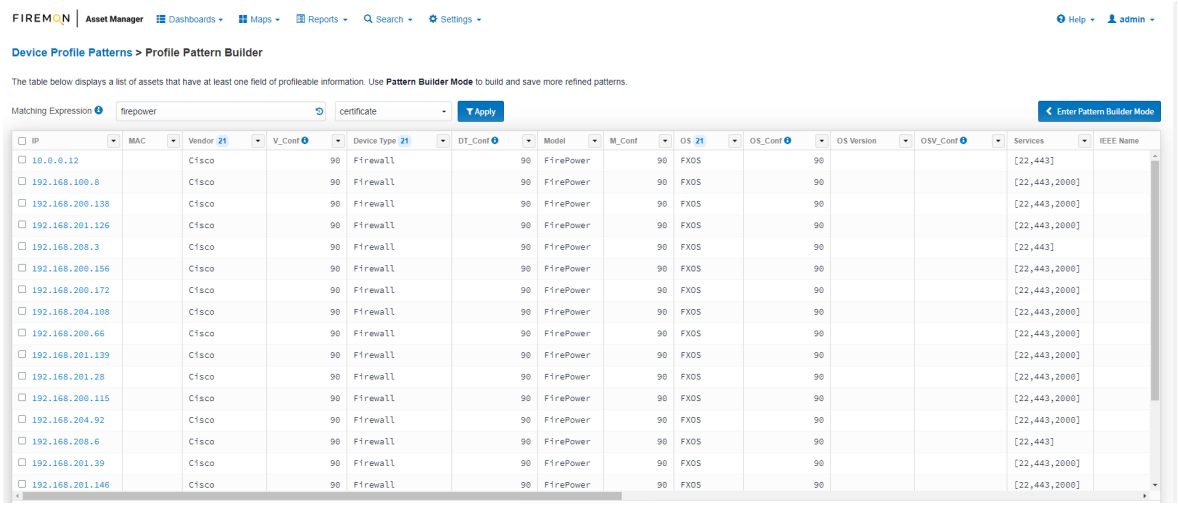
Example of using Profile Pattern Builder



Profile Pattern Builder Step 1: Enter a Matching Expression



Profile Pattern Builder Step 2: Enter the pattern data

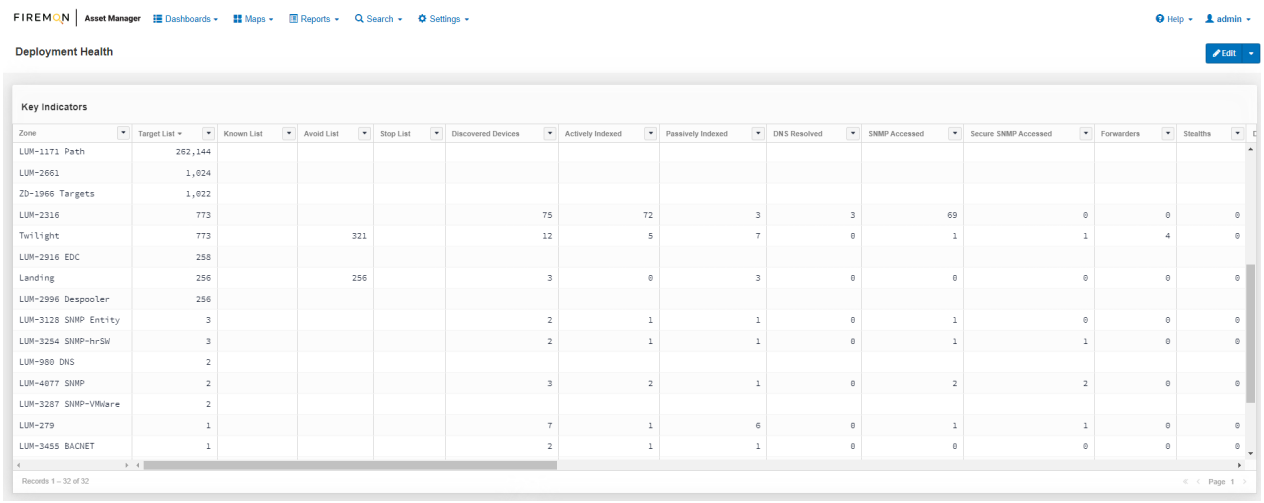


Profile Pattern Builder Step 3: New pattern output

Deployment Health Dashboard

The new Deployment Health Dashboard is a visual tool created for customers to aid in their deployment process and to ensure their success with Asset Manager. Whether you are standing up a new Command Center or checking the general health of a long-standing deployment this feature provides all of the critical benchmarks needed to ensure your deployment will yield maximum results. We now provide **Key Indicators by Zone**, can be used to detail the size (in IPs) of your crucial configuration lists (Target, Known, Avoid and Stop). Other counts such as actively vs passively discovered assets, DNS resolved assets, forwarders and stealths, assets with open and closed ports and individual profiling data-source responsiveness (cifs, certs, http banners). These counts give you a very fast and very informative look into your overall deployment and the general effectiveness of your current configuration/visibility.

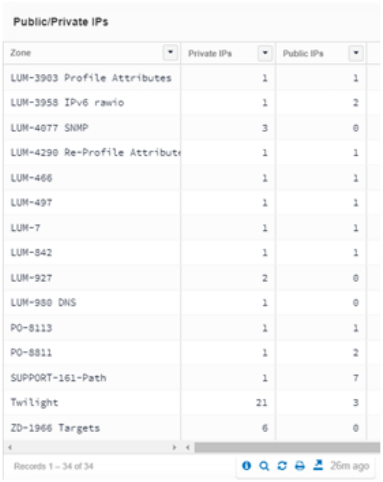
Examples of the Deployment Health dashboard



Zone	Target List	Known List	Avoid List	Stop List	Discovered Devices	Actively Indexed	Passively Indexed	DNS Resolved	SNMP Accessed	Secure SNMP Accessed	Forwarders	Stealths
LUM-1171 Path	262,144											
LUM-2661	1,024											
ZD-1966 Targets	1,022											
LUM-2316	773				75	72	3	3	69	0	0	0
Twilight	773		321		12	5	7	0	1	1	4	0
LUM-2916 EDC	258											
Landing	256		256		3	0	3	0	0	0	0	0
LUM-2996 Despooler	256											
LUM-3128 SNMP Entity	3				2	1	1	0	1	0	0	0
LUM-3254 SNMP-hrSW	3				2	1	1	0	1	1	0	0
LUM-980 DNS	2											
LUM-4077 SNMP	2				3	2	1	0	2	2	0	0
LUM-3287 SNMP-VMWare	2											
LUM-279	1				7	1	6	0	1	1	0	0
LUM-3455 BACNET	1				2	1	1	0	0	0	0	0

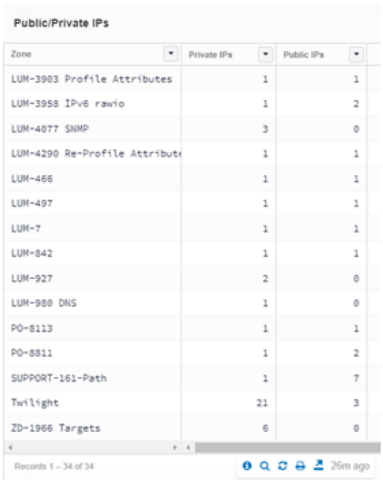
Records 1 – 32 of 32 Page 1

The Deployment Health Dashboard of Key Indicators



Zone	Private IPs	Public IPs
LUM-3903 Profile Attributes	1	1
LUM-3958 IPv6 rawio	1	2
LUM-4077 SNMP	3	0
LUM-4290 Re-Profile Attribute	1	1
LUM-466	1	1
LUM-497	1	1
LUM-7	1	1
LUM-842	1	1
LUM-927	2	0
LUM-980 DNS	1	0
PO-8113	1	1
PO-8811	1	2
SUPPORT-161-Path	1	7
Twilight	21	3
ZD-1966 Targets	6	0

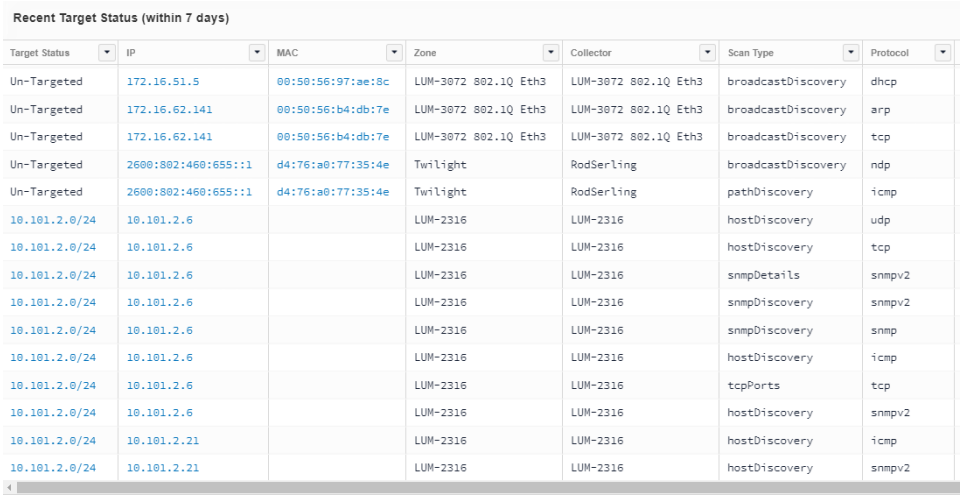
Records 1 – 34 of 34 26m ago



Zone	Private IPs	Public IPs
LUM-3903 Profile Attributes	1	1
LUM-3958 IPv6 rawio	1	2
LUM-4077 SNMP	3	0
LUM-4290 Re-Profile Attribute	1	1
LUM-466	1	1
LUM-497	1	1
LUM-7	1	1
LUM-842	1	1
LUM-927	2	0
LUM-980 DNS	1	0
PO-8113	1	1
PO-8811	1	2
SUPPORT-161-Path	1	7
Twilight	21	3
ZD-1966 Targets	6	0

Records 1 – 34 of 34 26m ago

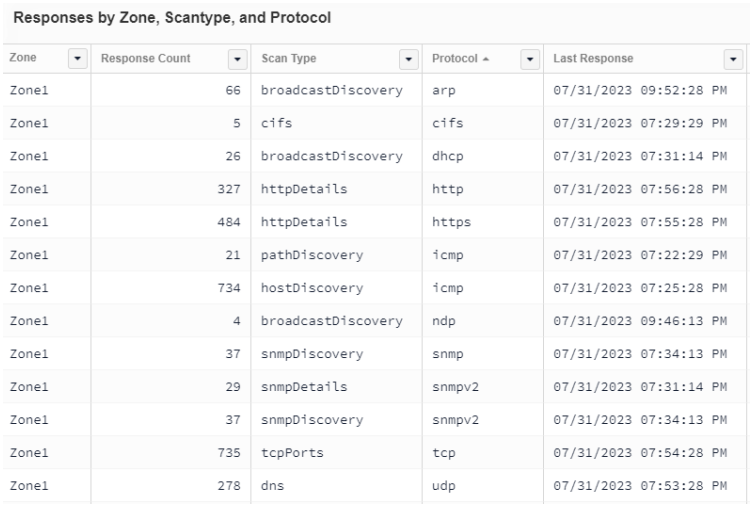
The Deployment Health Dashboard provides a breakdown of your private vs. public IP counts per zone as well as your SNMP credential utilization across zones.



Recent Target Status (within 7 days)

Target Status	IP	MAC	Zone	Collector	Scan Type	Protocol
Un-Targeted	172.16.51.5	00:50:56:97:ae:8c	LUM-3072 802.1Q Eth3	LUM-3072 802.1Q Eth3	broadcastDiscovery	dhcp
Un-Targeted	172.16.62.141	00:50:56:b4:db:7e	LUM-3072 802.1Q Eth3	LUM-3072 802.1Q Eth3	broadcastDiscovery	arp
Un-Targeted	172.16.62.141	00:50:56:b4:db:7e	LUM-3072 802.1Q Eth3	LUM-3072 802.1Q Eth3	broadcastDiscovery	tcp
Un-Targeted	2600:802:460:655::1	d4:76:a0:77:35:4e	Twilight	RodSerling	broadcastDiscovery	ndp
Un-Targeted	2600:802:460:655::1	d4:76:a0:77:35:4e	Twilight	RodSerling	pathDiscovery	icmp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	hostDiscovery	udp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	hostDiscovery	tcp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	snmpDetails	snmpv2
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	snmpDiscovery	snmpv2
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	snmpDiscovery	snmp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	hostDiscovery	icmp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	tcpPorts	tcp
10.101.2.0/24	10.101.2.6		LUM-2316	LUM-2316	hostDiscovery	snmpv2
10.101.2.0/24	10.101.2.21		LUM-2316	LUM-2316	hostDiscovery	icmp
10.101.2.0/24	10.101.2.21		LUM-2316	LUM-2316	hostDiscovery	snmpv2

You can review the most recent **Target Status** with collector, scantype and protocol in a single searchable table widget to determine how and why any asset was discovered (relative to targeting).



Responses by Zone, Scantype, and Protocol

Zone	Response Count	Scan Type	Protocol	Last Response
Zone1	66	broadcastDiscovery	arp	07/31/2023 09:52:28 PM
Zone1	5	cifs	cifs	07/31/2023 07:29:29 PM
Zone1	26	broadcastDiscovery	dhcp	07/31/2023 07:31:14 PM
Zone1	327	httpDetails	http	07/31/2023 07:56:28 PM
Zone1	484	httpDetails	https	07/31/2023 07:55:28 PM
Zone1	21	pathDiscovery	icmp	07/31/2023 07:22:29 PM
Zone1	734	hostDiscovery	icmp	07/31/2023 07:25:28 PM
Zone1	4	broadcastDiscovery	ndp	07/31/2023 09:46:13 PM
Zone1	37	snmpDiscovery	snmp	07/31/2023 07:34:13 PM
Zone1	29	snmpDetails	snmpv2	07/31/2023 07:31:14 PM
Zone1	37	snmpDiscovery	snmpv2	07/31/2023 07:34:13 PM
Zone1	735	tcpPorts	tcp	07/31/2023 07:54:28 PM
Zone1	278	dns	udp	07/31/2023 07:53:28 PM

The **Responses by Zone, Scantype and Protocol** table gives you counts of your discovery responses across the deployment.

Change Log

Improvements

Key	Summary
LUM-4306	Uptick openssh to 9.3p2 or later
LUM-4287	Analyze ZoneData.getDevices.idlist for performance under many attributes
LUM-4285	Scout disconnect from Command Center due to issues with httpd24-httpd service failing
LUM-4271	Feature Request: CLI command System reinit display the existing network values
LUM-4256	Security | Uptick python3
LUM-4252	Replace McAfee logo with Trellix logo in our UI
LUM-4241	Disallow console logins while system is starting up
LUM-4235	Refinements of gracefully preventing user from logging in to CLI until system is completely ready to accept logins

LUM-4227	Right justify numeric types in grid widgets
LUM-4224	Render commas in widgets for the applicable integers
LUM-4223	Support column pinning in table widgets
LUM-4222	Uptick Bouncy Castle in lumeta-api
LUM-4221	Add support for hyper-v and azure to platform in sysObjectId
LUM-4207	Devicify Tenable.sc integration devices
LUM-4201	Add API call to list / show / set timezone
LUM-4200	Clean up integrations configuration code for zones
LUM-4199	Warehouse: Improvements and fixes to CSV uploads
LUM-4191	Devicify Tripwire Integration Devices
LUM-4189	Tripwire | CLI | Add server and credential options
LUM-4178	Change to sshd_config to pass Azure certification
LUM-4177	Uptick 3rd-party libraries
LUM-4176	Update rpms based on Nessus and R7 scans for 4.9
LUM-4172	Create "deployment health" dashboard that shows fundamental discovery statistics
LUM-4166	Fix rogue "Lumeta" in enterprise SNMP response
LUM-4147	Warehouse: Support Elasticsearch as an external data source
LUM-4132	Create "set collector uuid" API call
LUM-4131	Write script to ingest log bundle with spool files
LUM-4100	Tripwire | GUI | Replace Logo to new Fortra color theme
LUM-4094	FireMon | API | Server Error 500 when Risk Analyzer is not configured on SIP
LUM-4077	Uptick Bouncy Castle in discovery
LUM-4067	Uptick JRE to Temurin 17 latest
LUM-4044	OpenSSL vulnerabilities
LUM-3702	Feature Request: Profiling Improvement Zebra Technologies
LUM-3426	Add timezone's to event.* tables

Resolved Issues

Key	Summary
LUM-4317	Integrations | CLI | Invalid values for purge and test commands hook to Infoblox
LUM-4308	API savedQuery is failing with no error to the user
LUM-4277	Warehouse saved queries, widgets and dashboards have some differences between upgrade and netboot.
LUM-4274	CLI authentication pki ssh install will not accept username with period
LUM-4269	Patterns | Cannot import an exported pattern file
LUM-4263	Path doesn't handle responses from 0.0.0.0 well
LUM-4262	Patterns | Retain Pattern Database after a System Config Import
LUM-4259	Patterns imported even if the user presses Escape when asked whether to Overwrite Existing Patterns
LUM-4253	Patterns | Overwrite does not work deleting all existing patterns and Success popup window does not show occassionally
LUM-4236	When login is disabled, GUI displays error
LUM-4228	Queries | Editor | Saving the widget fails after the first save

LUM-4226	error on shutting down scan agent
LUM-4203	Support Tools | Import Systems | System Config import may fail when containing custom patterns
LUM-4195	Cannot export 'Port Density' query
LUM-4185	CLI - for tenable SC integration setting api key authentication is not working
LUM-4164	Warning message about no zones is not completely visible on Zones page
LUM-4144	cloud scanner with Target Discovered Devices enabled is not targeting devices
LUM-4133	Integrations | API | Seeing "unable to find valid certification path to requested target" when enabling integration
LUM-4119	Security | Uptick nss
LUM-4045	UI | "No zone" Warning toast message is empty
LUM-3994	Dashboards | Delete widget doesn't delete the widget, but displays success message

4.9.0.1

Change Log

Improvements

Key	Summary
LUM-4371	Corrected upgrade files being flagged as malware

Resolved Issues

Key	Summary
LUM-4385	Upgrade - when FIPS is enabled 4.9.0.1 upgrade is getting errors
LUM-4346	GUI table widgets show "No Data Available" before showing data

4.9.0.2

Change Log

Improvements

Key	Summary
LUM-4402	Need Tenable.sc to ingest 'all devices' managed by Tenable

Resolved Issues

Key	Summary
LUM-4394	Archived Collector appearing in Integrations Dashboard to add IP to a collector
LUM-3981	Infoblox | API | Bulk post fails with "Unknown argument/field: 'mac'" response