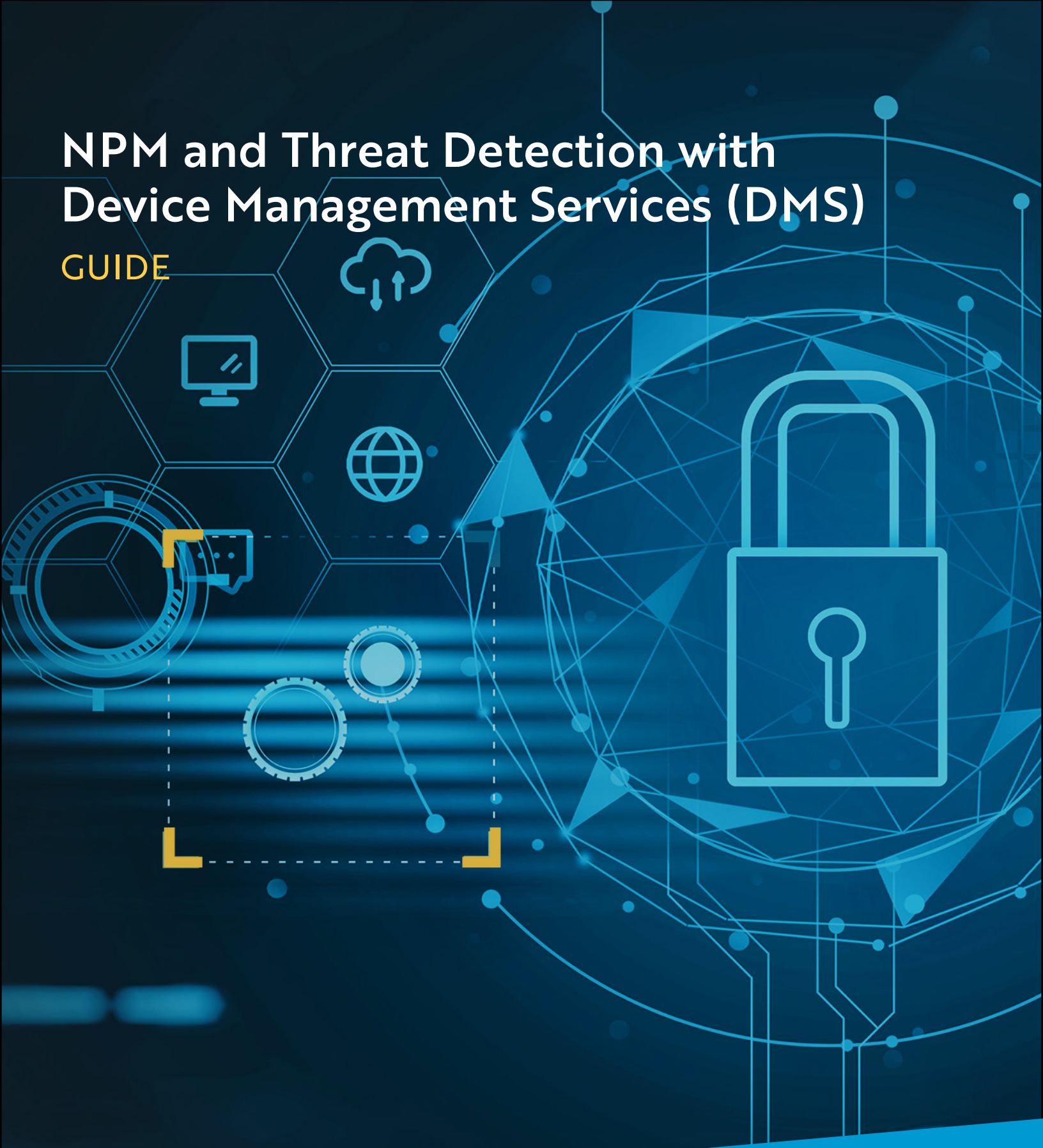


# NPM and Threat Detection with Device Management Services (DMS)

GUIDE

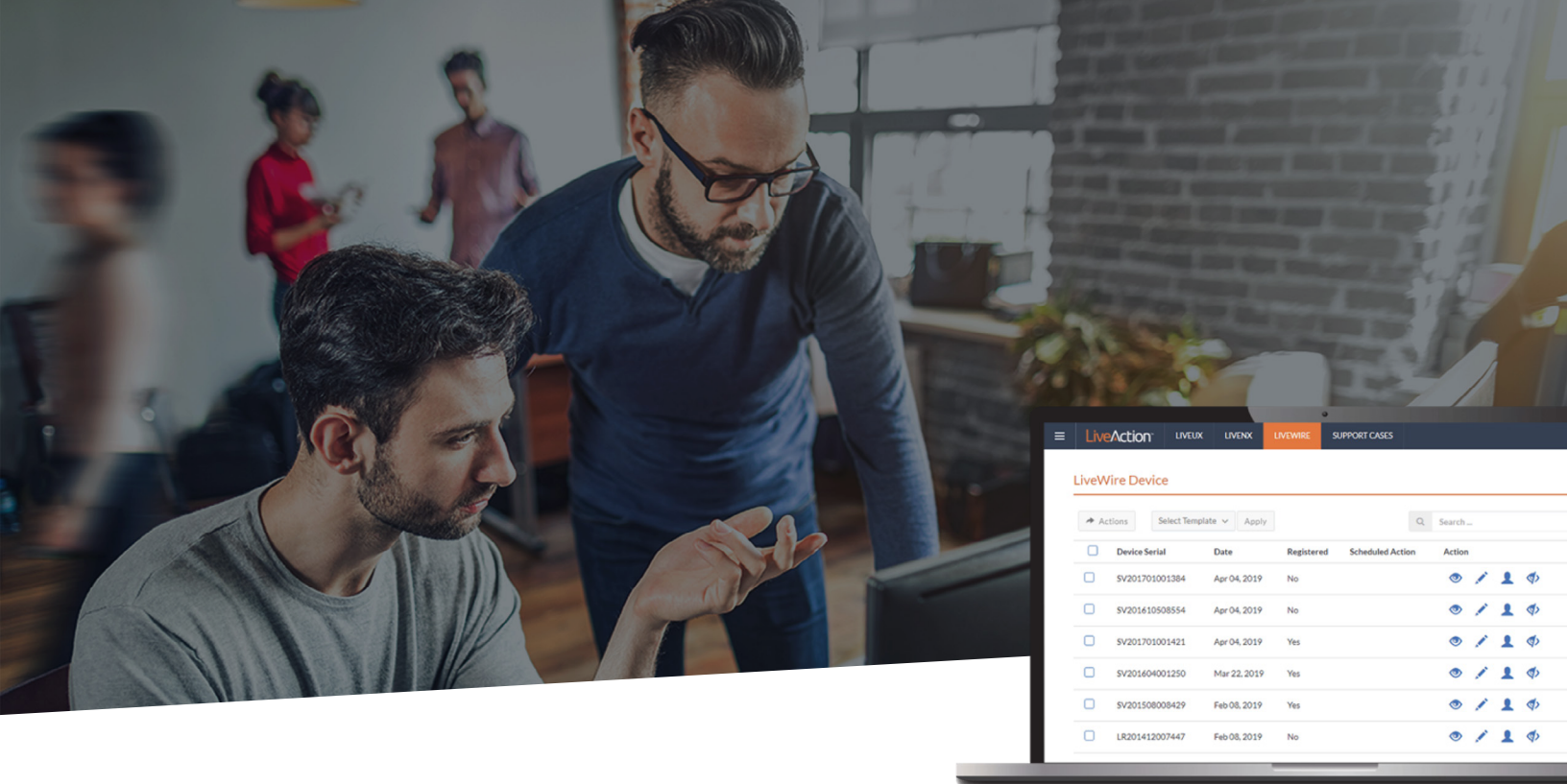


LiveAction®

# Table of Contents

---

<b>03</b>	What is DMS?
<b>03</b>	What Products Include DMS?
<b>03</b>	What Problem Does a DMS Solve?
<b>04</b>	Technical Details of the DMS Portal
<b>05</b>	DMS Communications
<b>06</b>	DMS Registration
<b>06</b>	Invite
<b>06</b>	DMS Automatic Activation
<b>06</b>	DMS Functions
<b>08</b>	What do ThreatEye & LiveWire do?
<b>08</b>	ThreatEye
<b>09</b>	LiveWire
<b>10</b>	About LiveAction



Caption: DMS Portal

## What is DMS?

Device Management Services is a SaaS offering that pulls data from multiple devices into one console and allows global changes to be made to network devices.

The LiveAction Device Management Service (DMS) is a SaaS offering that allows LiveWire devices to be managed and monitored at scale and in bulk from a single dashboard.

### What Products Include DMS?

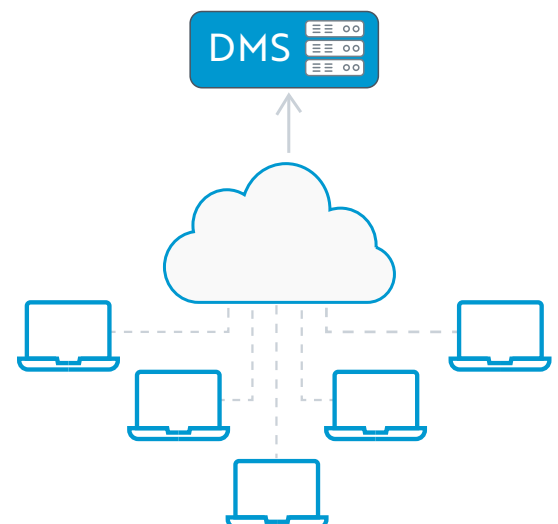
LiveWire and ThreatEye use network probes that enable the DMS portal.

These probes are devices or programs placed on key nodes in a network to collect and monitor data and to extend network visibility to remote sites.

### What Problem Does a DMS Solve?

There are many hardware and software appliances distributed throughout any given enterprise-level network. While the benefits of having packet-level visibility into the whole network are clear, the many hardware and software appliances distributed throughout a network can be difficult to manage on a large scale. A DMS SaaS solves that problem.

LiveAction provides a centralized DMS portal to manage and make global changes to all LiveWire and ThreatEye Devices on a network.

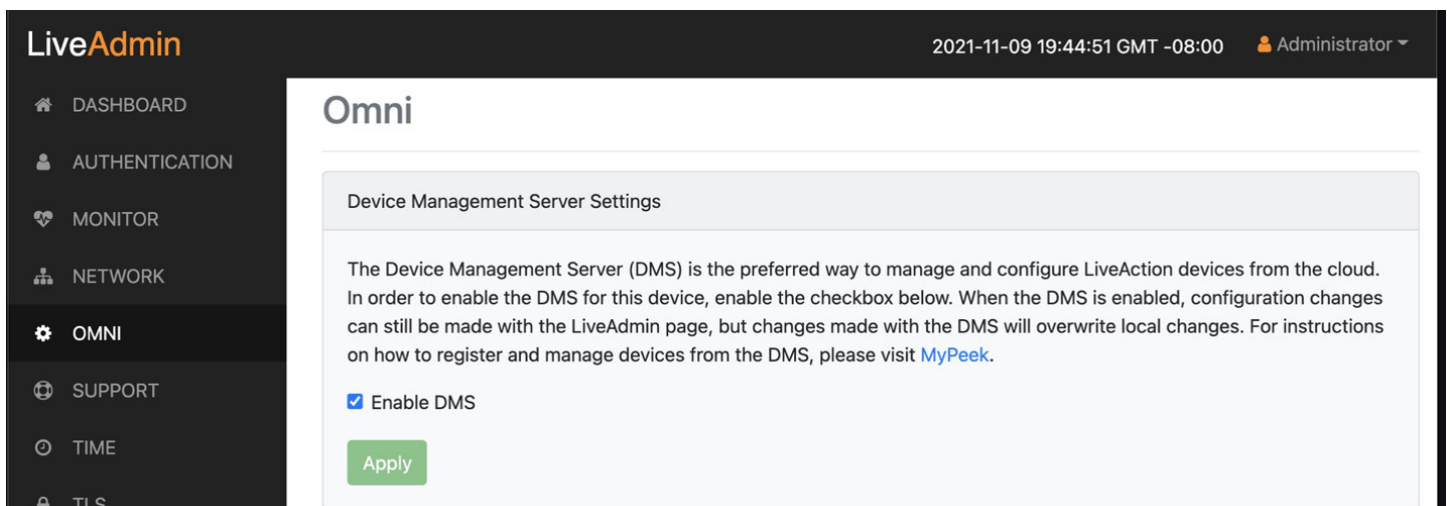


# Technical Details of the DMS Portal

The DMS Portal is hosted on AWS as a part of a larger service known as [cloudkeys.liveaction.com](https://cloudkeys.liveaction.com)

The DMS Portal consists of the following software components:

- ▶ web server - nginx
- ▶ REST - API
- ▶ authentication server - okta
- ▶ database - mongo
- ▶ user interface - react



The DMS Agent with LiveWire and ThreatEye is the liaison between the DMS Portal and the device. The DMS Agent running on the network probe, implemented as a service in the communicates using a REST-API to share data between the device and the DMS portal.

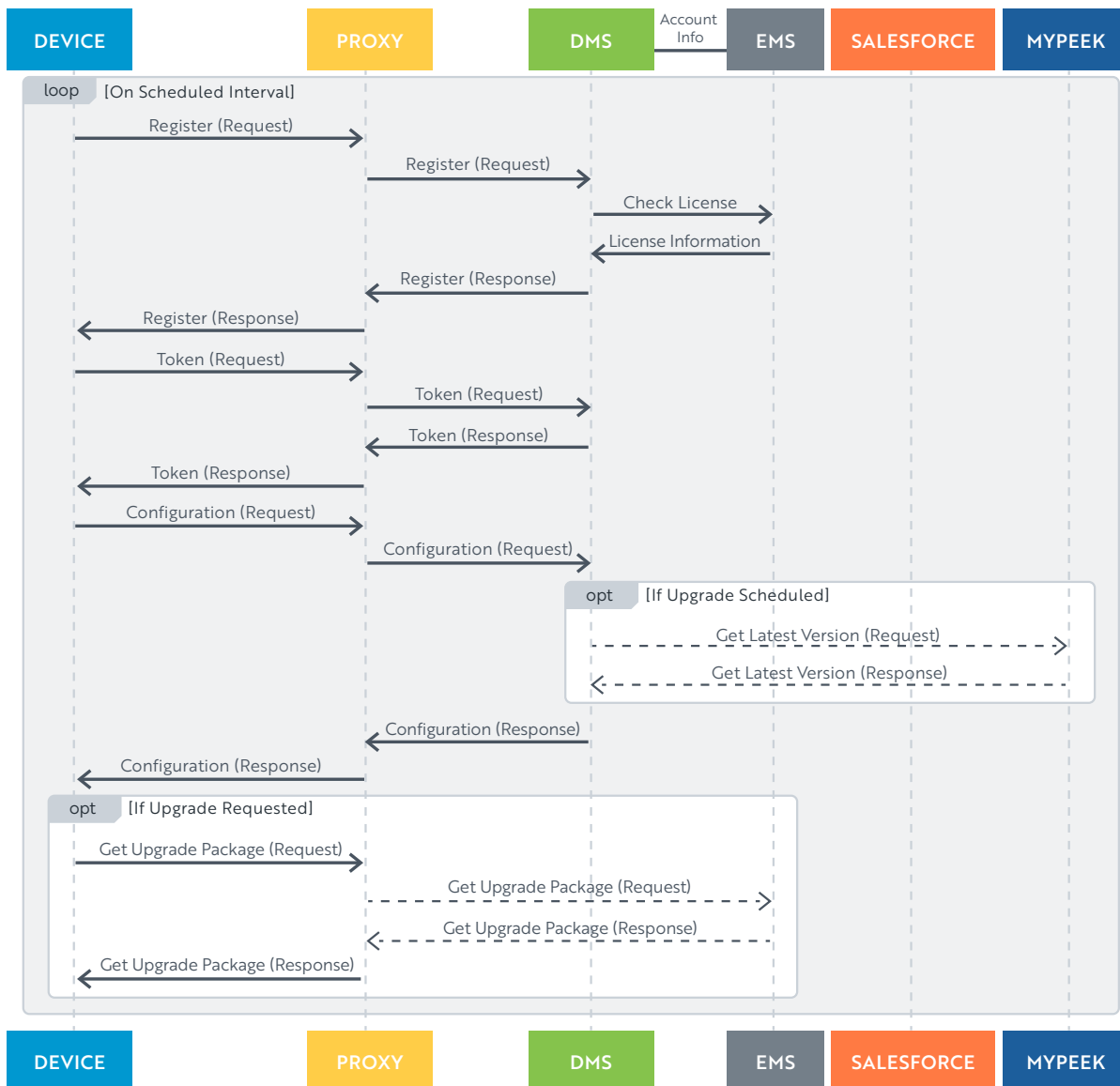
The DMS Service is an option in LiveAdmin that is enabled by default.





## DMS Communications

The diagram below illustrates how the communication flow between the device, the DMS, and other cloud based services that the DMS uses.



Both sides of the DMS communicate through a REST-API. Within the DMS on the LiveAction side, the DMS service communicates with the device through the LiveAction REST-API. Our DMS supports proxy services and zero-touch configuration.

All Communications between the ThreatEye and LiveWire devices and the DMS Portal are initiated by the device. This is more secure, and practical, since most enterprise networks allow connections to be done from the inside out, but not from the outside in. This means that all LiveWire configuration made by the user through the DMS Portal are queued up, and made only when the LiveWire connects outbound to the DMS Portal. This happens when the device connects to the DMS Portal, which occurs at 10-minute intervals. For more detailed specifications of the DMS API, please [contact LiveAction](#).

## DMS Registration

When a LiveWire or ThreatEye is first connected to the network, it will reach out to the DMS Portal and register itself through zero-touch configuration. The DMS Portal will use the serial number to match the device to the entry in the database.

## Invite

When a customer purchases LiveWire or ThreatEye for the first time, a DMS account is created for them, the LiveWire or ThreatEye is added to the account, and the customer is sent an invite via email to login to their new DMS Portal Account. This takes them to a login on a cloudkeys page. You will not receive a second registration email if you purchase additional DMS supported products.

## DMS Automatic Activation

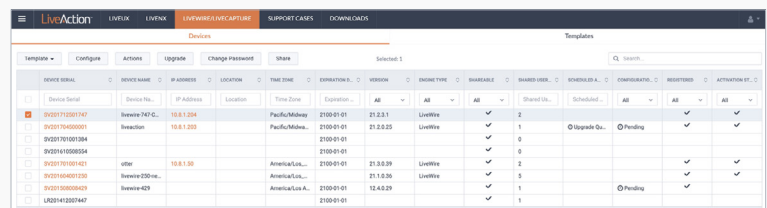
During the registration process, the DMS Portal will also send the serial number and locking code to the EMS to activate the device and get a product key. The result of the activation is a license file that is installed onto the device. With the license installed, the user will be able to go right to work on creating a capture, and using their LiveWire.

## DMS Functions

The DMS Portal provides the following functions to the user for managing and configuring LiveWire devices:

### DEVICE LIST

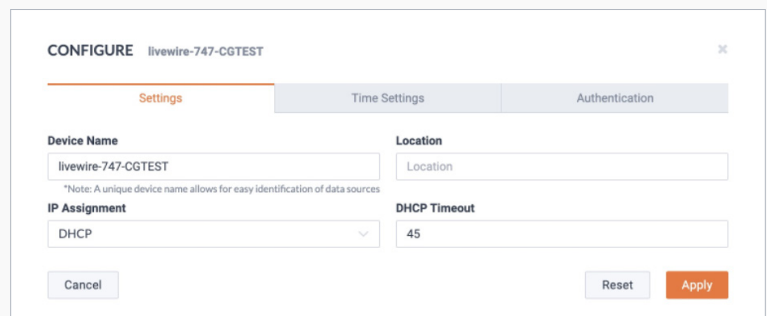
The main UI for the DMS is a list of the devices that the customer has purchased. The list has a header row, followed by a row for each device.



Device Serial	Device Name	IP Address	Location	Time Zone	Connection S.	Version	Device Type	Shareable	Shared User	Scheduled	Upgrade Status	Activation Status
SV031712001747	Brewey 747-CG...	10.0.1.204	Pacific/Mob...	2100-01-01	21.2.3.1	LiveWire	✓	2			✓	✓
SV031710000001	Brewey 747-CG...	10.0.1.205	Pacific/Mob...	2100-01-01	21.2.2.25	LiveWire	✓	1			✓	✓
SV031701001304				2100-01-01			✓	0			✓	✓
SV031610008554				2100-01-01			✓	0			✓	✓
SV031701001421	other	10.0.1.30	America/Los...	2100-01-01	21.3.2.29	LiveWire	✓	2			✓	✓
SV031600001150	Brewey 750me...		America/Los...	21-1-2-26		LiveWire	✓	5			✓	✓
SV03150000420	Brewey 403		America/Los...	2100-01-01	12.4.2.29		✓	1			✓	✓
LR031413307447				2100-01-01			✓	1			✓	✓

### CONFIGURE BUTTON

The Configure Button is used to configure the devices that are currently selected. If multiple devices are selected, certain configuration options are greyed out, like the Device Name.



**CONFIGURE livewire-747-CGTEST**

**Settings** | Time Settings | Authentication

**Device Name**  
livewire-747-CGTEST

**Location**  
Location

\*Note: A unique device name allows for easy identification of data sources

**IP Assignment**  
DHCP

**DHCP Timeout**  
45

Cancel | Reset | Apply

## DMS Functions

### UPGRADE BUTTON

The Upgrade button is enabled when one or more of the devices are selected. The Upgrade Button allows the user to upgrade the selected devices remotely through the DMS. The DMS upgrade is the latest shipping version. There is no capability to downgrade to a previously released version.

**UPGRADE SETTINGS** livewire-747-CGTEST

☐ Disable ☒ Enable

**Date and Time**

11/09/2021 02 : 32 PM

Cancel Apply

### ACTIONS BUTTON

The Actions button allows the user to perform the following actions against the currently selected devices: Power Off, Reboot, Factory Reset.

**ACTIONS** SV201712501747

**Actions**

Note: Once LiveWire is powered off, you need to manually press the button to power it back.

☒ None ☐ Power Off ☐ Reboot ☐ Factory Reset

Cancel Apply

### SHARE BUTTON

The Share Button allows the user to share the devices with others who manage and configure them. Hitting the Share button will bring up a popup modal dialog with a list of shared users, and a field to add new users.

**MANAGE USERS** SV201712501747

**Add User**

**First Name**

First Name

**Last Name**

Last Name

**Email**

Email

### TEMPLATES BUTTON

The Templates button allows the user to apply pre-defined configurations to the selected devices.

Template Configure Actions Upgrade

Search

upgrade

	DEVICE NAME	IP ADDRESS
<input checked="" type="checkbox"/>	SV201712501747	livewire-747-C... 10.8.1
<input type="checkbox"/>	SV201704500001	liveaction 10.8.1

# What do ThreatEye & LiveWire do?

## ThreatEye

[ThreatEye](#) NV's probe extracts a rich metadata set of more than 150 packet dynamic features to support threat and anomaly detection, response, hunting, forensics, and compliance validation reporting. ThreatEye NV's software components scale to ingest network data directly from physical or virtual network taps at wire-speeds up to 40Gbps. All ThreatEye products include a DMS console.

Minimum Requirements: ThreatEye NV hardware recommendations are based on standard internet traffic composition per bandwidth. Therefore, the network traffic mix may affect performance.

BANDWIDTH	SPECIFICATIONS	
1 Gbps	4x Processor Cores CentOS 7 or other Docker compatible Linux OS 16GB memory	4GB storage 2x 1G network interfaces (One for management, one for monitoring)
10-20 Gbps	48x Processor Cores CentOS 7 or other Docker compatible Linux OS 64GB memory	128GB storage Recommended Intel X710 2x10G (SFP+) network interface card and 1x1G for management
40 Gbps	48x Processor Cores CentOS 7 or other Docker compatible Linux OS 96GB memory	128GB storage Napatech SmartNIC 4x10G (SFP+) network interface card, and 1x1G for management



# What do ThreatEye & LiveWire do?

## LiveWire

[LiveWire](#) enables packet capture from virtually anywhere in the network extending network tracking to remote sites, branches, Cloud, WAN edge, LAN, and data centers.

LiveWire can be deployed as a hardware device or as a virtual product. LiveWire appliances are connected to the network with span ports or network packet brokers that capture north-south traffic. LiveWire Virtual captures north-south and east-west traffic. All LiveWire products include a DMS console.

Our diagram below includes the specifications for LiveWire products:

FEATURES	LIVEWIRE EDGE	LIVEWIRE CORE	LIVEWIRE POWERCORE*	LIVEWIRE VIRTUAL
Use Case	Small Office / Remote Office	Large Branch / WAN Edge	Data Center	All
LiveFlow Export	Up to 400 Mbps	Up to 6 Gbps	Up to 17 Gbps	Depends on Hardware
Forensic Capture (CTD)	Up to 850 Mbps	Up to 4 Gbps	Up to 40 Gbps**	Depends on hardware
Memory	16 GB	32 GB	192 GB	Minimum 8 GB
Storage Capacity	1 TB SSD	16 TB	64 TB or 128 TB	User Configurable
Dimensions/Weight	7 x 1.7 x 5.7 in, 2.64 lbs	1 U, 39 lbs	2 U, 73 lbs	N/A
Omnipeek for Windows	Yes, 1 license	Yes, 1 license	Yes, 1 license	No
VoIP, Video and UC Analysis	Yes	Yes	Yes	Yes

\* Supports 10Gbps and 100Gbps ; \*\* Using 2 external storage systems



# LiveAction®

© Copyright 2022 - LiveAction. All Rights Reserved.  
960 San Antonio Rd, Suite 200, Palo Alto, CA 94303  
+1 (888) 881-1116

## About LiveAction

LiveAction provides a DMS software platform for easy scalability, management and visibility into network probes. Questions about DMS-supported products and how DMS can improve your network management? [Reach out to us.](#)