LiveAction®

LiveWire Virtual

User Guide

LiveAction, Inc.
901 Campisi Way, Ste. 222
Campbell, CA 95008, USA
+1 (888) 881-1116
https://www.liveaction.com

20230330-LWVU_231a

Contents

CHAPTER 1

Introduction

In this chapter:

About LiveWire Virtual

Congratulations on your purchase of LiveWire Virtual™! LiveWire Virtual is a virtual version of the LiveWire hardware network appliance. LiveWire Virtual uniquely combines flow-based reporting using deep packet inspection (DPI) with high-speed, packet capture and storage. LiveWire Virtual is designed to work with both LiveAction's LiveNX and ThreatEye. Because LiveWire Virtual starts with packet data, it is able to provide a unique, and extended, set of flow-based monitoring data called LiveFlow. LiveFlow is extended IPFIX data and is exported to LiveNX and ThreatEye. See Chapter 3, *Sending Telemetry to LiveNX and ThreatEye* for the additional tasks you must perform in order to export LiveFlow data from LiveWire Virtual to LiveNX and ThreatEye. Please also refer to the LiveNX and ThreatEye documentation for more information on using the LiveFlow data exported to LiveNX and ThreatEye.

The Capture Engine software on LiveWire Virtual works in conjunction with Omnipeek, a separate software program required for the monitoring and analysis of the packets captured remotely by LiveWire Virtual. For detailed instructions on how to view and analyze remote captures from within the Omnipeek console, please see the *Omnipeek User Guide* or Omnipeek online help. For more information on the Capture Engine software, please see Chapter 4, *Capture Engines*.

What's included

Your standard LiveWire Virtual package includes:

- LiveWire Virtual packet capture and analysis software
- Omnipeek
- *LiveWire Virtual User Guide* (this guide)

Deploying LiveWire Virtual on VMware ESXi

Requirements

- VMware ESXI 5.5 or later
- vSphere client to deploy LiveWire Virtual OVA

OVA Deployment

1. Log into the ESXi/ESX host or vCenter Server using the vSphere Client.
2. Select any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host.
3. Right-click the inventory object and select **Deploy OVF Template**...
4. Select **Local file** option and then click **Choose Files**.
5. Select the *LiveWire Virtual OVA* file, and click **Open**, and then click **Next**.
6. Specify a unique name and location for the virtual machine, and then click **Next**.
7. Select a compute resource where to run the deployed OVA, and then click **Next**.
8. Review the template details, and then click **Next**.
9. For storage configuration select *Thick Provision Lazy Zeroed*, and then click **Next**.
10. Map the OVF destination networks with each of their respective source networks, and then click **Next**.
11. Review the **Ready to complete** dialog, and click **Finish**. A new task for creating LiveWire Virtual appears in the *Recent Tasks* pane. After the task is complete, the new virtual machine is created on the select resource, and now appears as an inventory object in VMware vSphere web client.

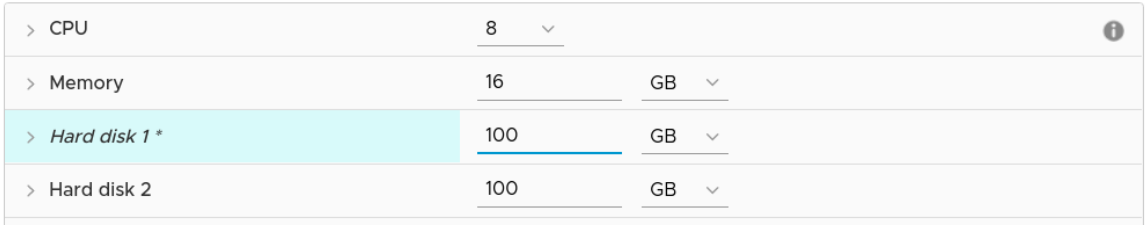
OVA Disk Configuration

By default LiveWire Virtual is configured with a single OS disk (*Hard disk 1*), and a single capture storage disk (*Hard disk 2*). Both of these hard disks can be extended to increase the amount of log storage and capture storage. Capture storage can also be increased by adding additional hard disk devices to LiveWire Virtual.

Note For ESXI 5.5 and later the largest sized disk is 62TB. The maximum number of disks per VM is 60 (requires 4 additional controllers).

Expanding OS storage:

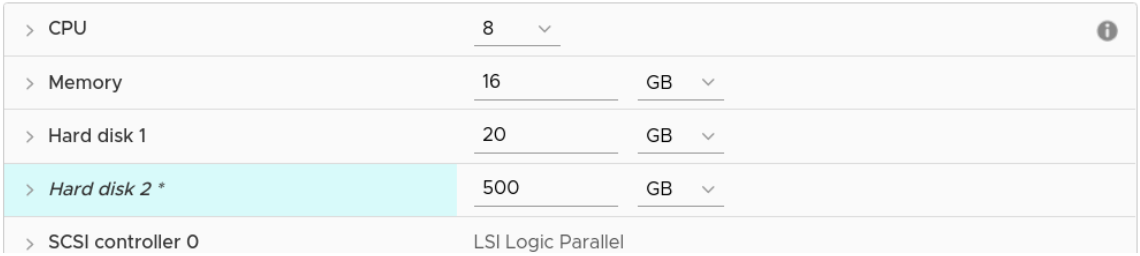
1. Select your LiveWire Virtual in the *Virtual Machines* inventory list.
2. From the **Actions** drop-down list, select **Edit Settings**.



3. Expand the *Hard disk 1* size to the new desired size.
4. Click **OK**.
5. From the **Actions** drop-down list, select **Power**, and then select **Restart Guest OS**. On reboot, LiveWire Virtual automatically resizes the capture partition to the new size.

Expanding capture storage disk(s):

1. Select your LiveWire Virtual in the Virtual Machines inventory list.
2. From the Actions drop-down list, select Edit Settings.
3. Expand the Hard disk N size to the new desired size.

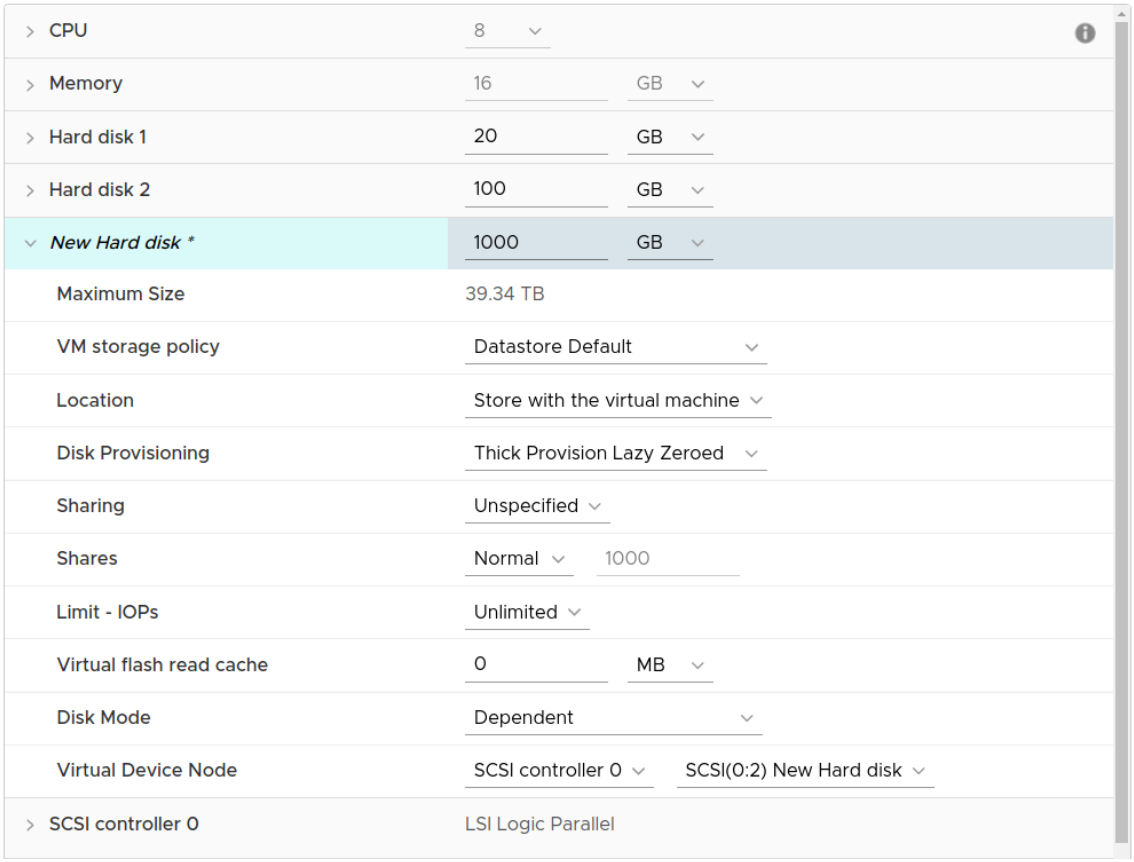


4. Click **OK**.
5. From the **Actions** drop-down list, select **Power**, and then select **Restart Guest OS**. On reboot, LiveWire Virtual automatically resizes the capture partition to the new size.

Adding capture storage disk(s):

1. Select your LiveWire Virtual in the Virtual Machines inventory list.
2. From the **Actions** drop-down list, select **Edit Settings**.
3. Click **Add New Device** and then click **Hard Disk**.
4. Enter the desired size of the New Hard disk

5. Expand the *New Hard disk* settings and select *Thick Provision Lazy Zeroed*.



6. Click **OK**.
7. From the **Actions** drop-down list, select **Power**, and then select **Restart Guest OS**. On reboot, LiveWire Virtual automatically resizes the capture storage to the new size.

Monitoring Traffic

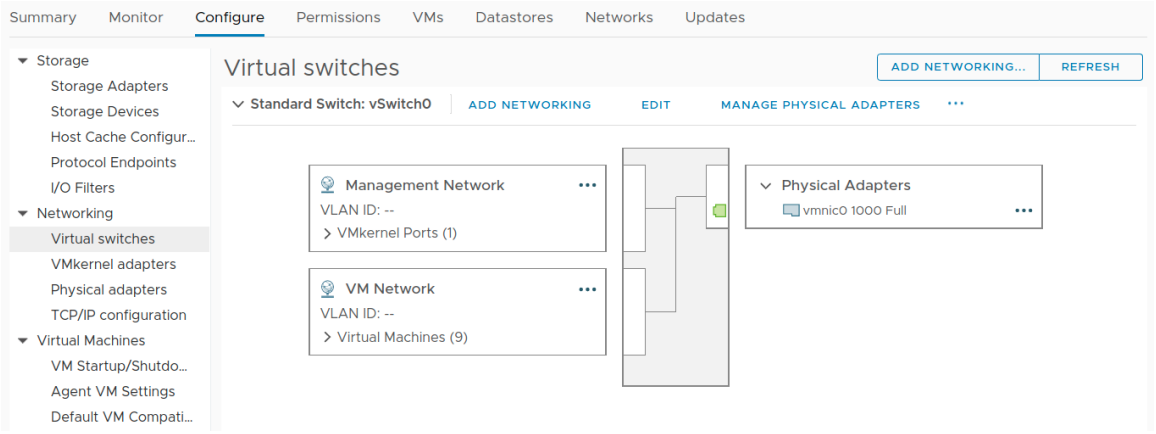
The following provide a 'Best Practices' for monitoring traffic in a VMware environment with LiveWire Virtual.

Monitoring VM Traffic (Standard Switch)

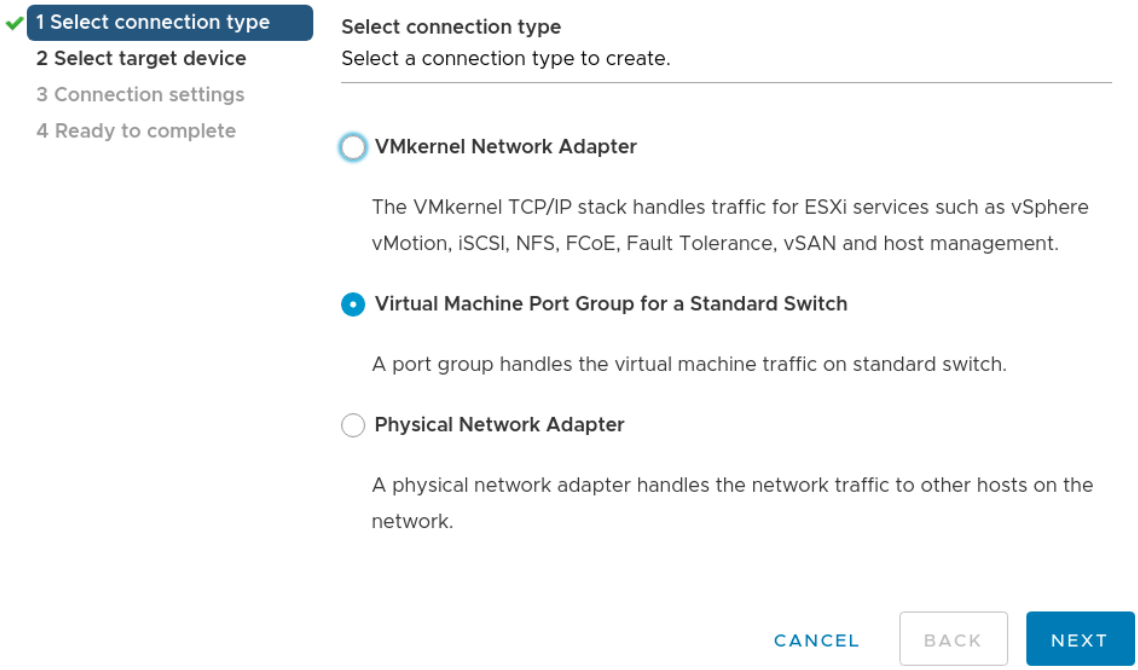
The following instructions will allow you to monitor all VM traffic going across a standard virtual switch. To do so, requires the creation of a new port group on the standard switch to be monitored. By creating the monitoring port group, we will be able to capture all traffic traversing the switch while not affecting the existing infrastructure.

Note To perform these actions you will need permissions to create port groups on existing vSwitches.

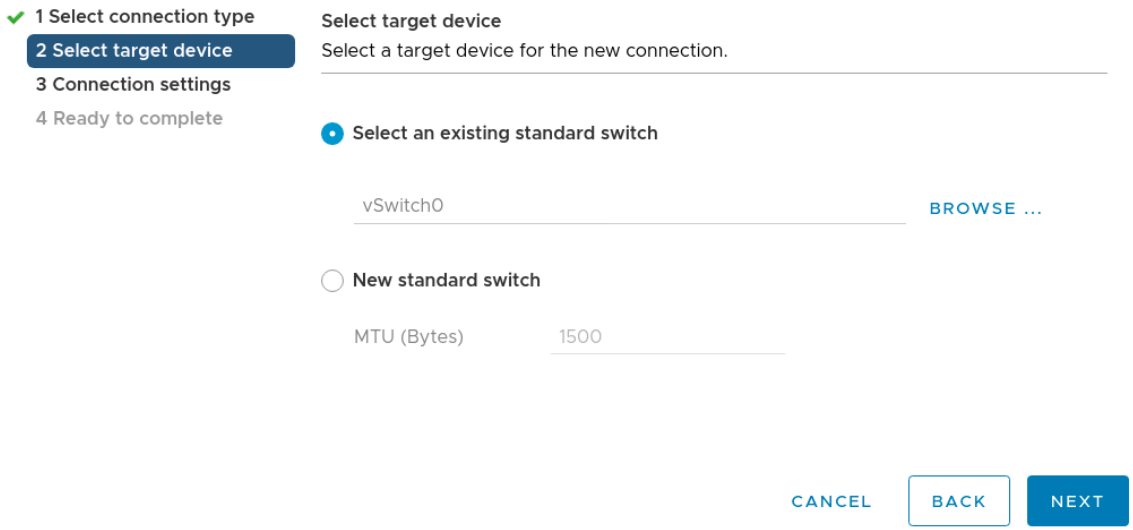
1. Log into the ESXi/ESX host or vCenter Server using the vSphere Client.
2. In the vSphere Client, navigate to the host.
3. On the *Configure* tab, expand Networking and select *Virtual Switches*.



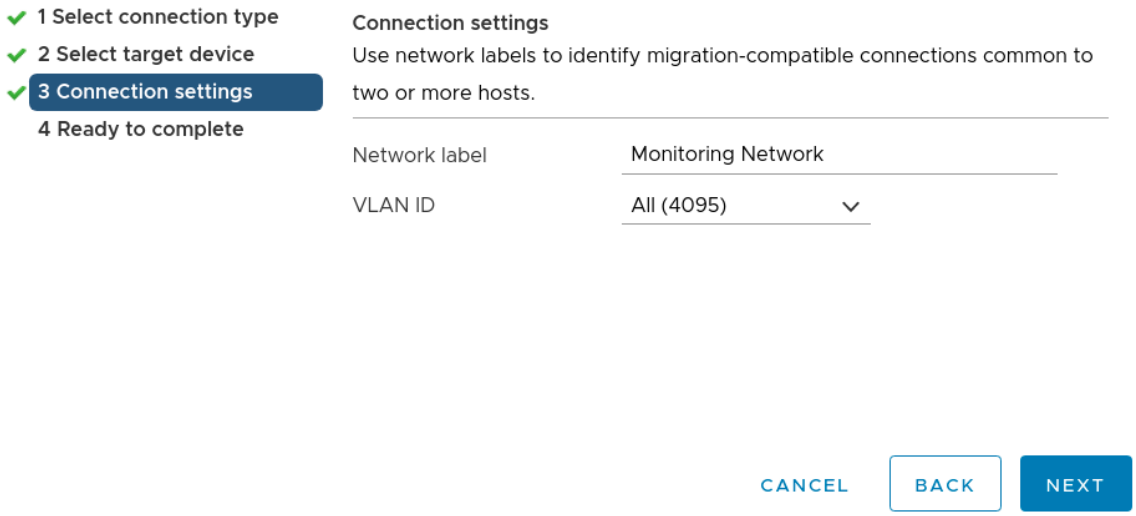
4. Click **Add Networking**.
5. In *Select connection type*, select *Virtual Machine Port Group for a Standard Switch* and click **Next**.



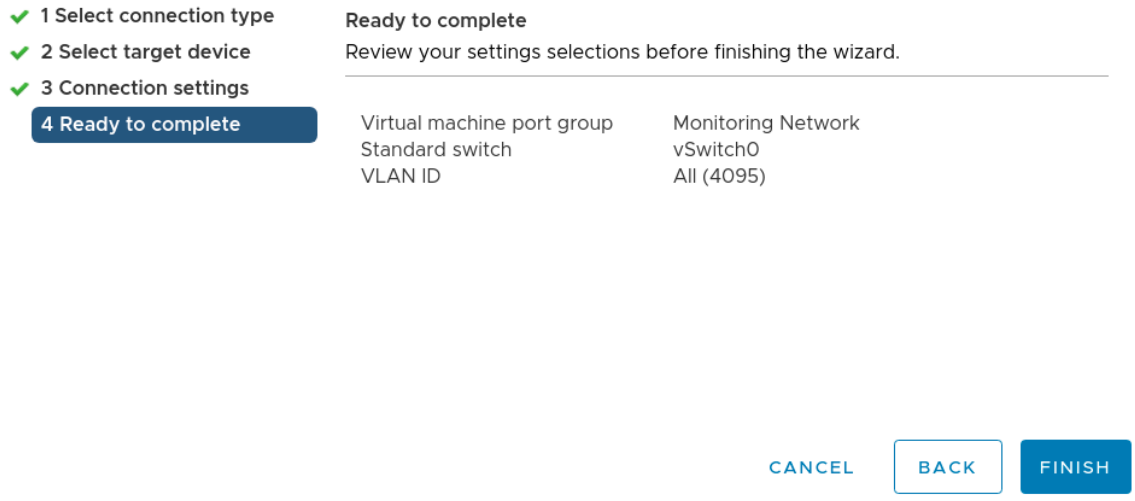
6. In *Select target device*, click **Browse...** and select an existing standard switch you wish to monitor.



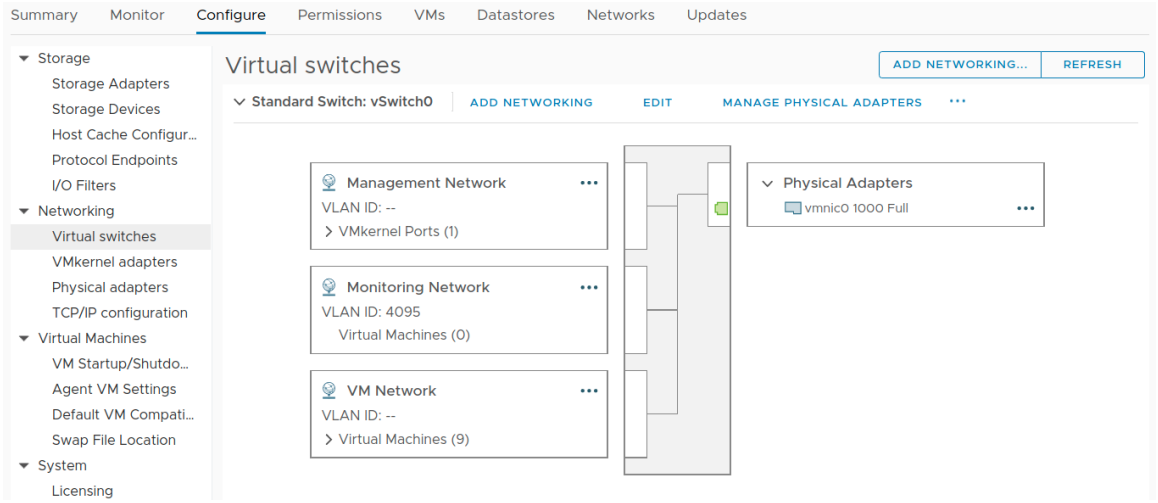
7. On the **Connection settings** dialog, enter a unique *Network label* for the new port group. Select the *VLAN ID* drop-down and choose *All (4095)*, and then click **Next**.



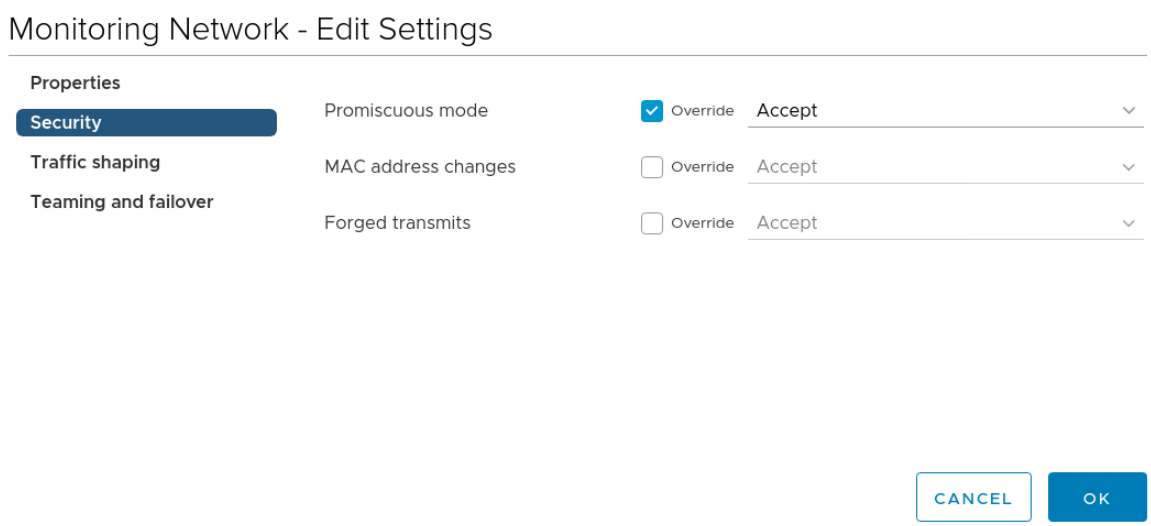
8. Review the port group settings in the *Ready to complete* page, and click **Finish**.



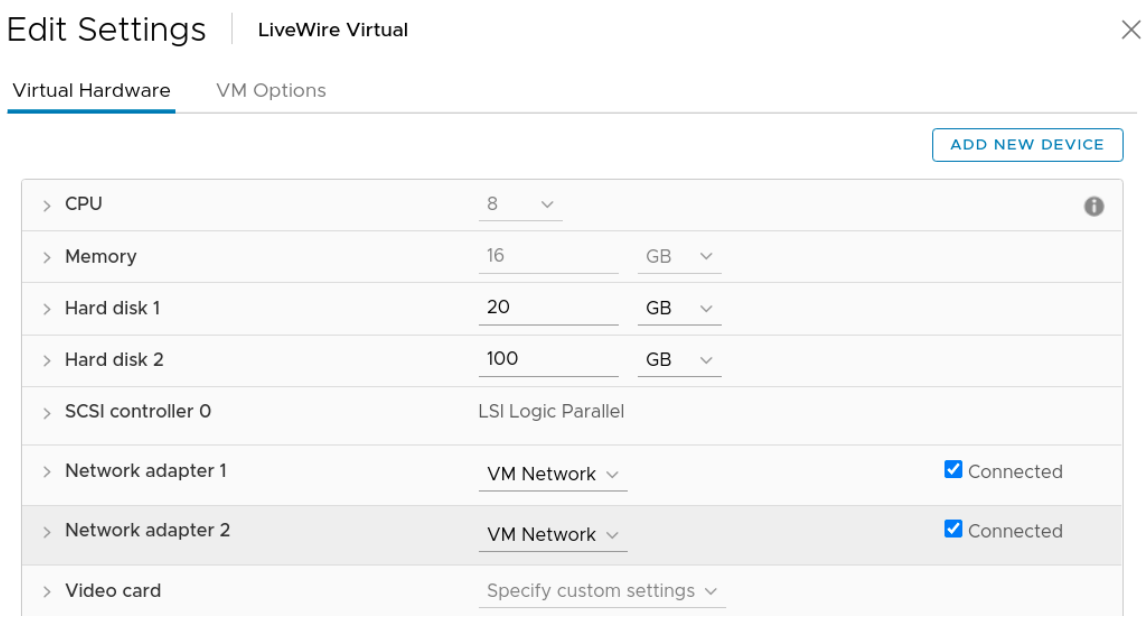
9. Once complete the new port group should appear in the topology diagram of the switch.



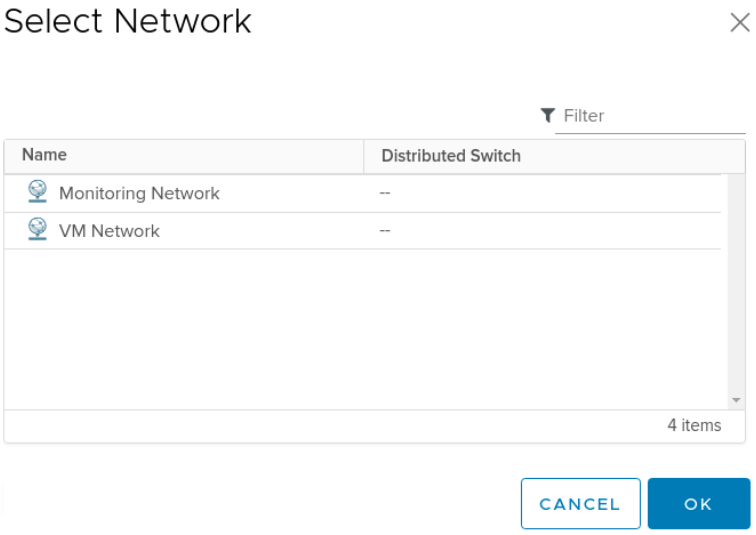
10. In the topology diagram of the switch, click the name of the port group.
11. Next to the *Monitoring Network*, click the horizontal … (elipsis) icon and select **Edit settings**.
12. Select the *Security* page.
13. Override the switch settings for **Promiscuous mode** and select **Accept**.



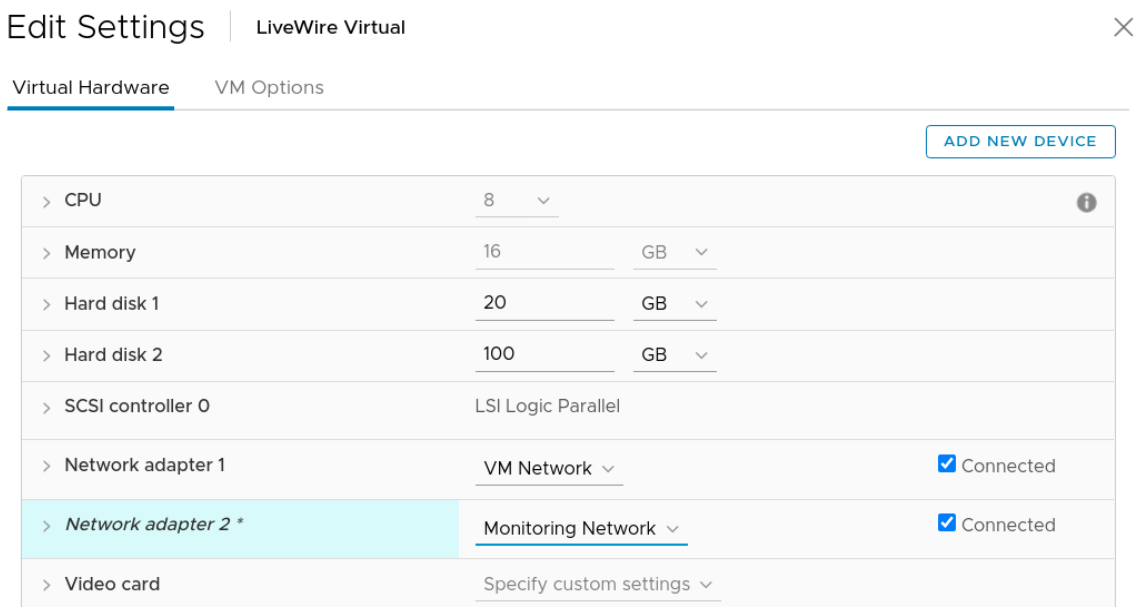
14. Click **OK**.
15. Click **Virtual Machines** in the VMware Host Client inventory.
16. Right-click a LiveWire Virtual machine in the list and select Edit settings from the pop-up menu.
17. Click the *Virtual Hardware* tab and select **Network adapter 2** from the hardware list.



18. In the network connection panel, **Browse...** and select **Monitoring Network** and then click **OK**.



19. Verify the *Monitoring Network* appears as the selected network for Network adapter 2 and click **OK**.



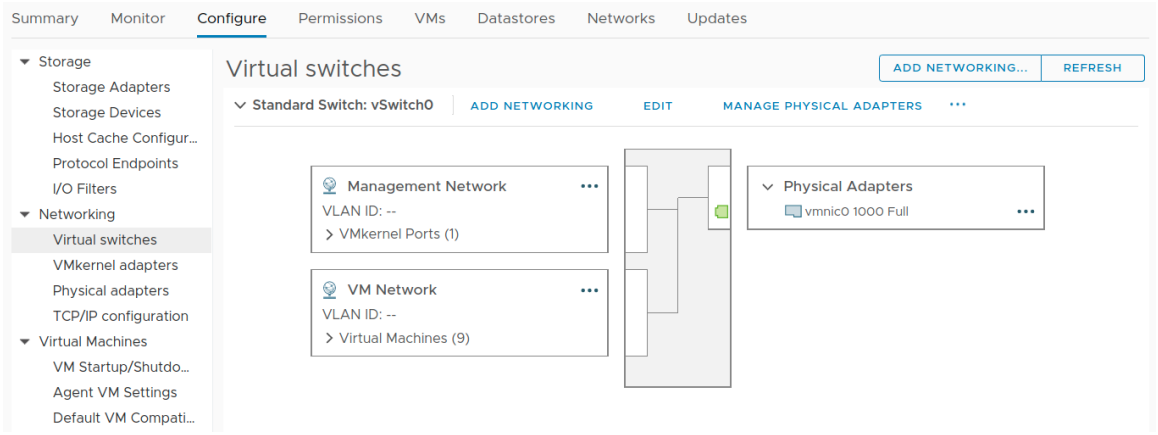
20. Restart the LiveWire Virtual.

Monitoring External Traffic

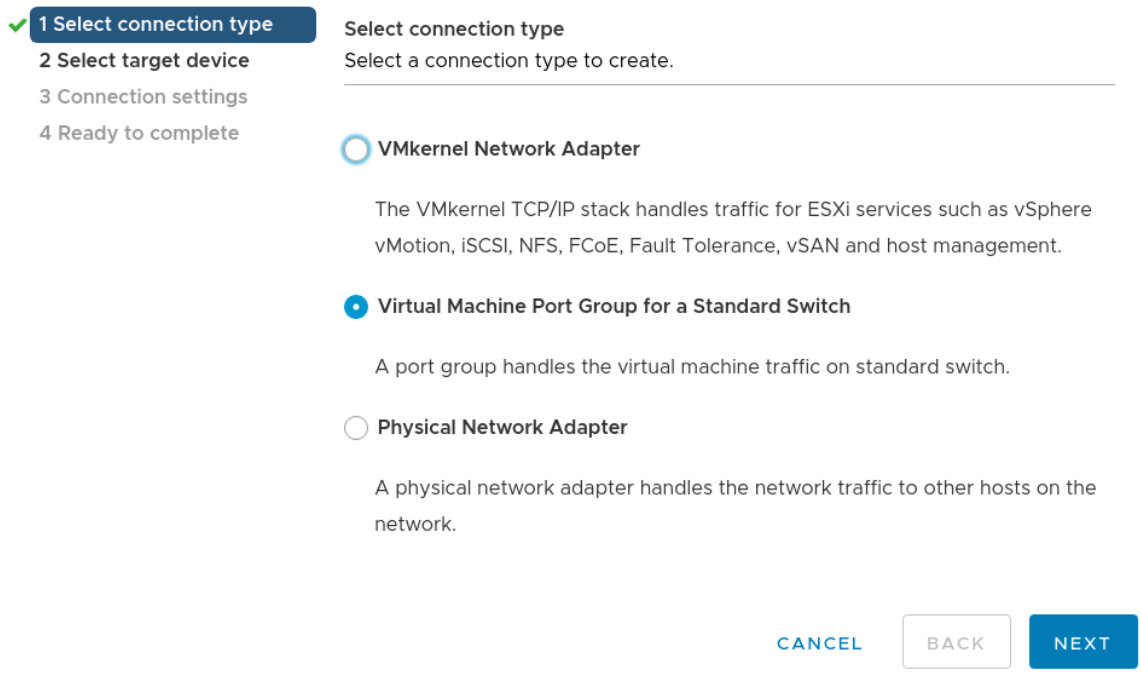
The following instructions will allow you to monitor spanned traffic into your LiveWire Virtual. This requires the creation of a new standard switch and port group.

> **Note** To perform these actions you will need permissions to create a standard switch and port group for monitoring.

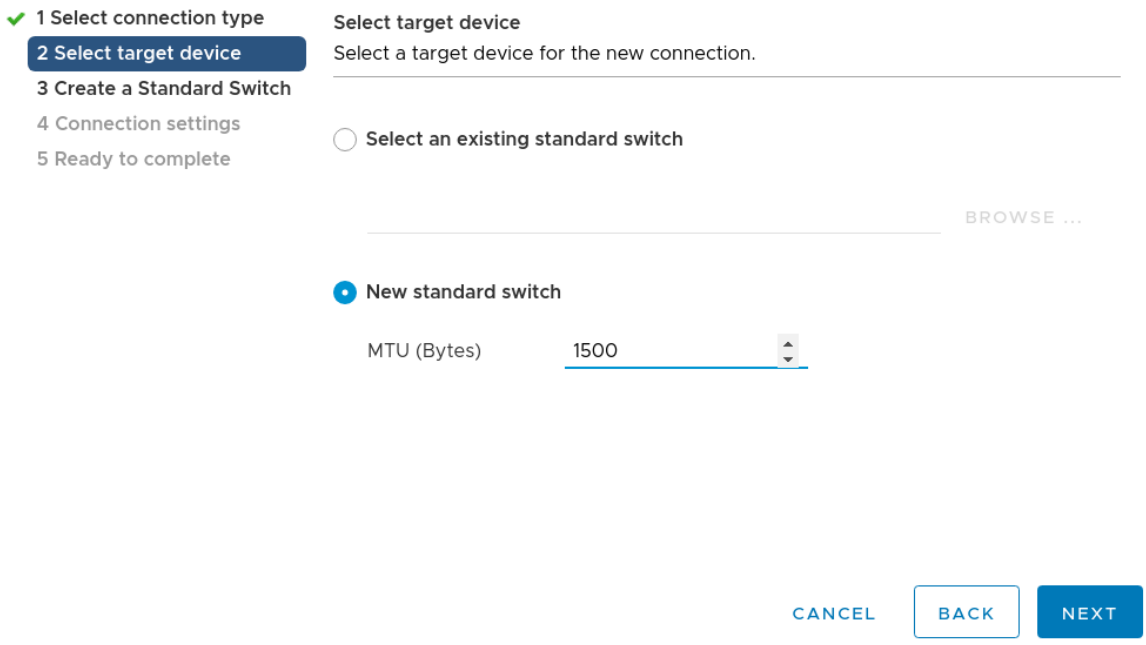
1. Log into the ESXi/ESX host or vCenter Server using the vSphere Client.
2. In the vSphere Client, navigate to the host.
3. On the *Configure* tab, expand **Networking** and select **Virtual Switches**.



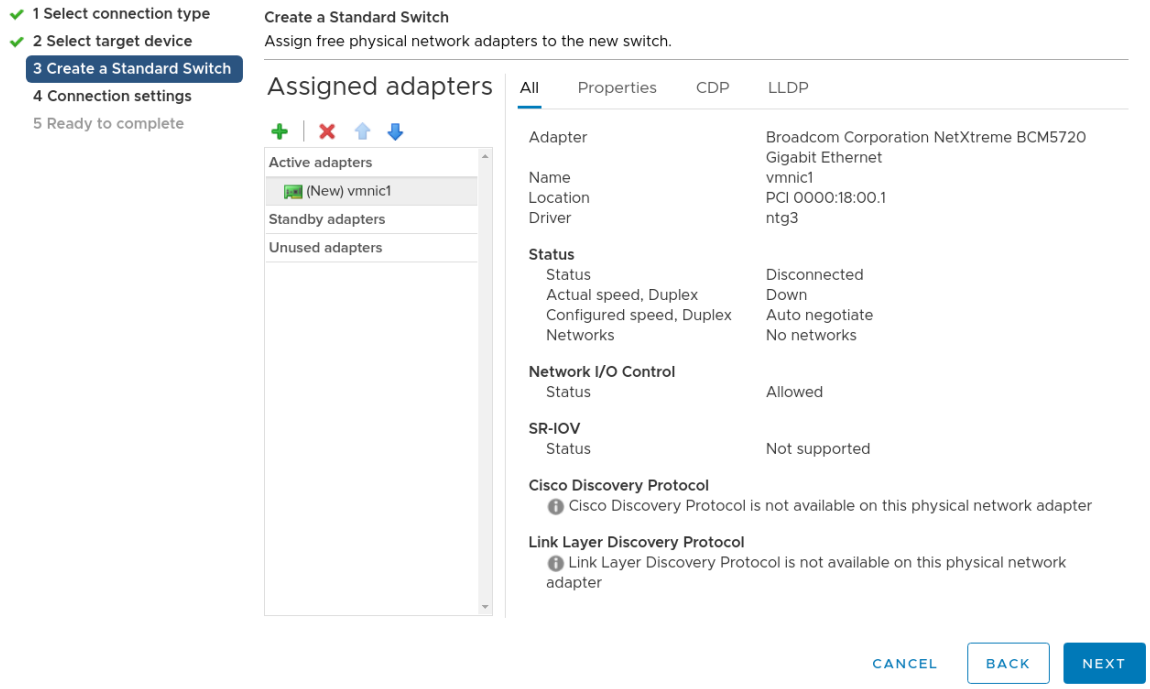
4. Click **Add networking**.
5. In *Select connection type*, select *Virtual Machine Port Group for a Standard Switch* and click **Next**.



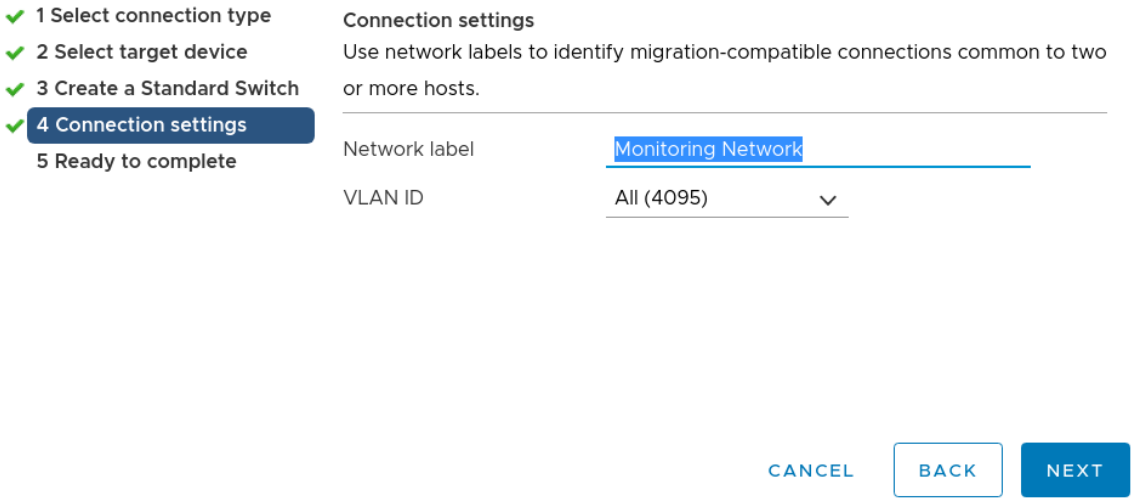
6. Select *New standard switch* and click **Next**.



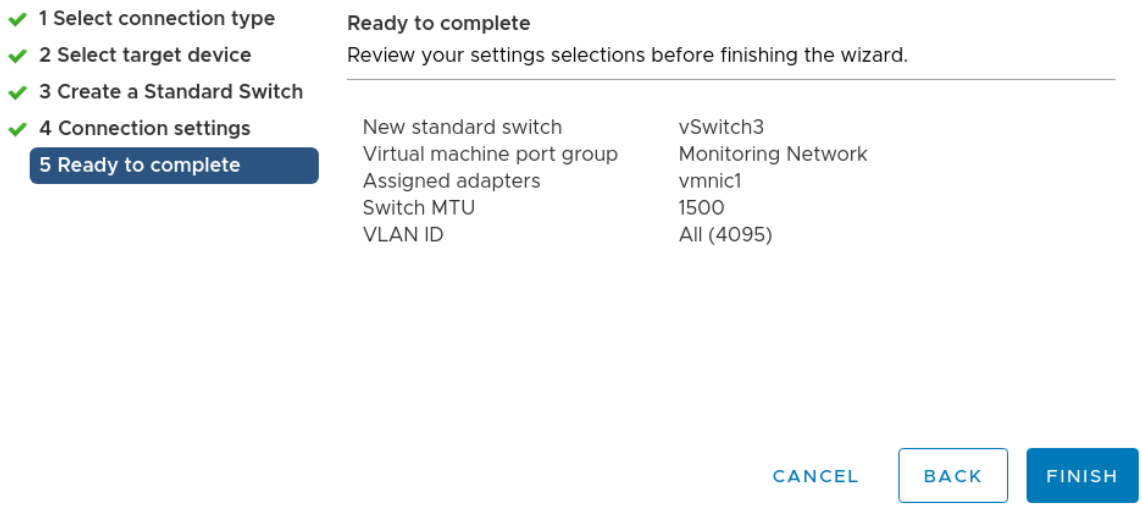
7. Add physical network adapters to the new standard switch. Under *Assigned adapters*, click **Add** adapters.
8. Select one or more physical network adapters from the list and click **OK**. Click **Next**.



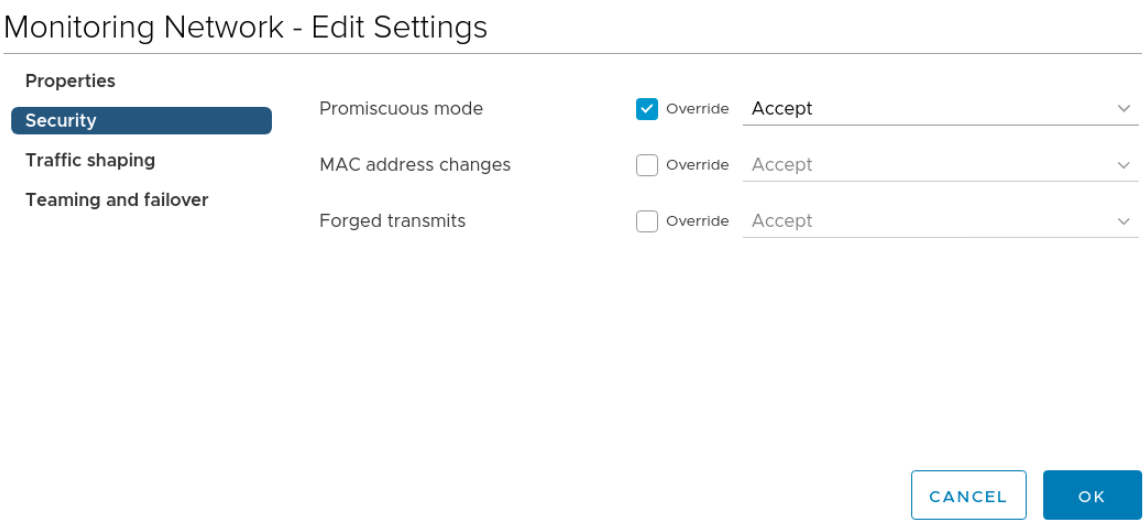
9. On the *Connection settings* dialog, enter a unique *Network label* for the new port group. Select the VLAN ID drop-down choose *All (4095)*, and then click **Next**.



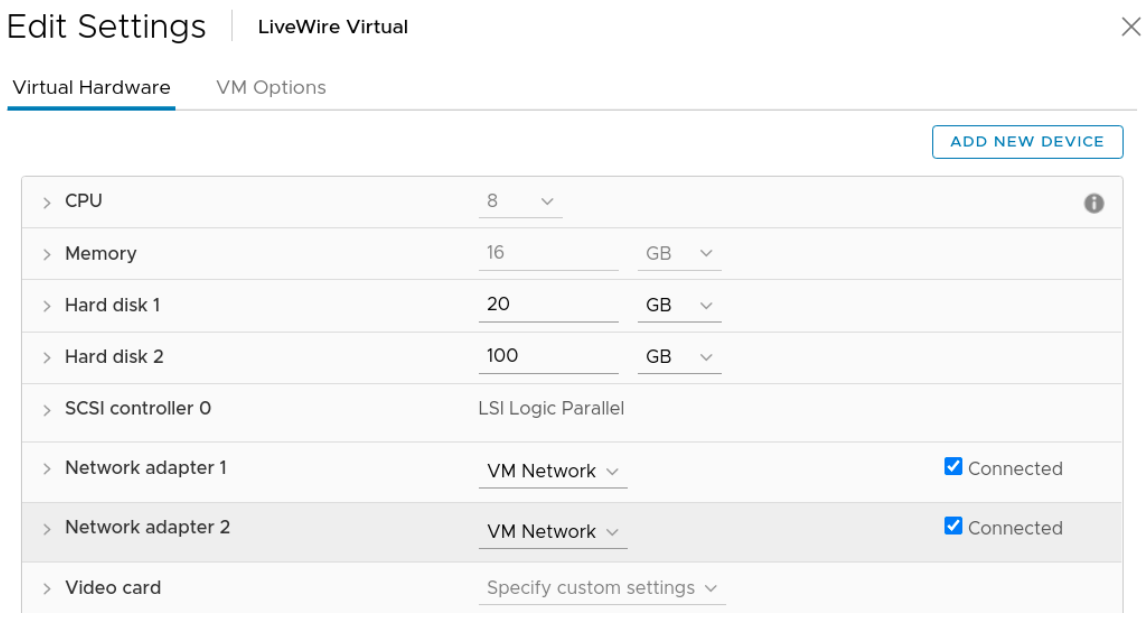
10. Review the port group settings in the *Ready to complete* page, and click **Finish**.



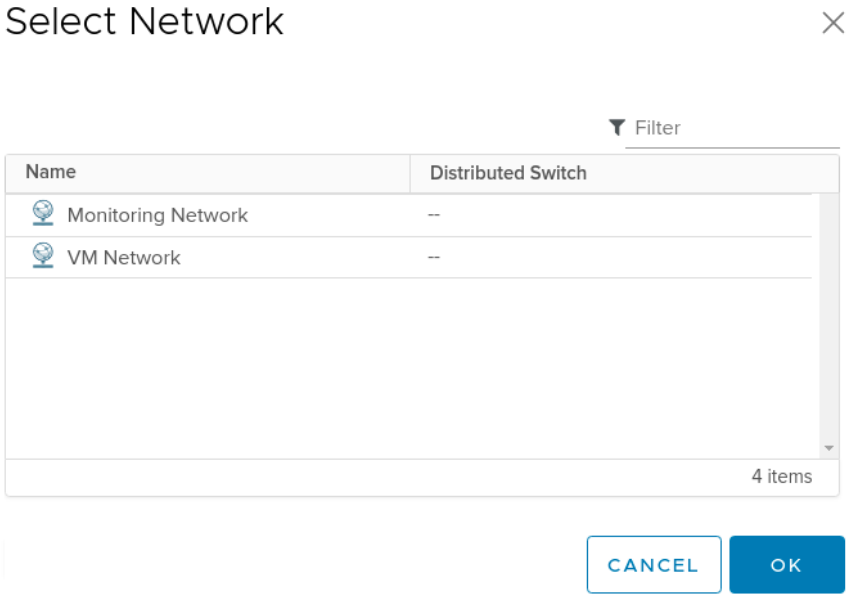
11. Once complete the new port group should appear in the topology diagram of the switch.
12. In the topology diagram of the new switch, click the name of the port group.
13. Next to the *Monitoring Network*, click the horizontal … (elipsis) icon and select *Edit settings*.
14. Select the *Security page*.
15. Override the switch settings for Promiscuous mode and select *Accept*.



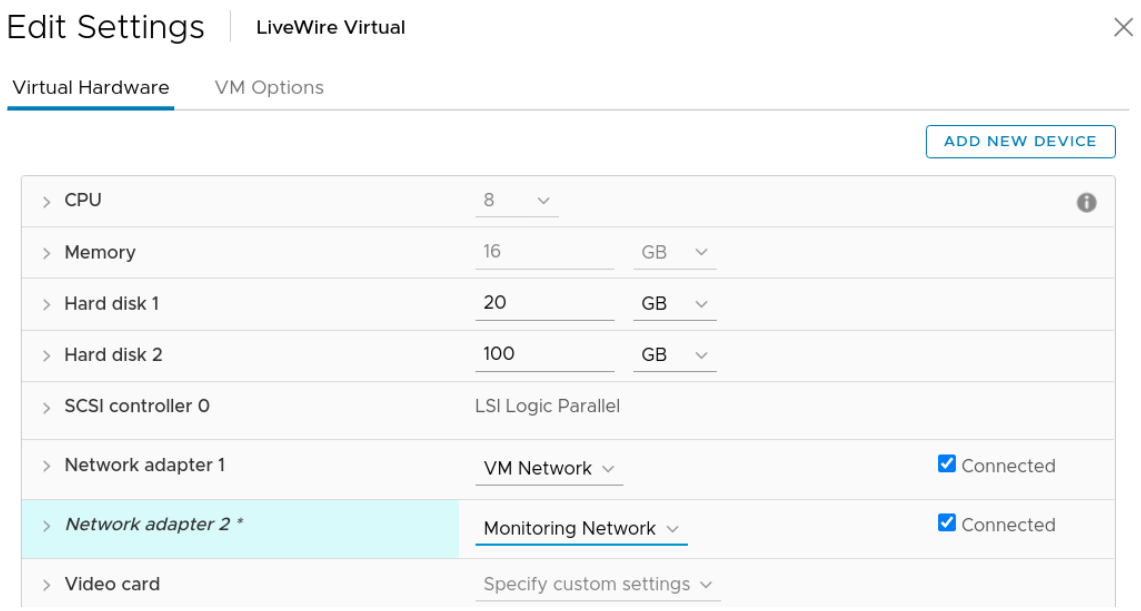
16. Click **OK**.
17. Click **Virtual Machines** in the VMware Host Client inventory.
18. Right-click a LiveWire Virtual machine in the list and select *Edit settings* from the pop-up menu.
19. Click the *Virtual Hardware* tab and select *Network adapter 2* from the hardware list.



20. In the network connection panel, *Browse*... and select *Monitoring Network* and then click **OK**.



21. Verify the *Monitoring Network* appears as the selected network for *Network adapter 2* and click **OK**.



22. Restart LiveWire Virtual.

Deploying LiveWire Virtual on KVM

To deploy an instance of LiveWire Virtual on KVM (QEMU emulator version 2.5.0 is supported), you can do so directly using the *virt-install* command from the command line or from the Virtual Machine Manager interface.

Minimum virtual computing requirements

The minimum virtual computing requirements to deploy LiveWire Virtual on KVM are:

Specification	Requirement
Memory	8 GB RAM
Virtual CPU (vCPU)	4 vCPU (x86_64)
Virtual Storage for Guest Hard disk 1: Hard disk 2:	(Minimum of 120 GB) 20 GB 100 GB
Virtual Network Interfaces	2 vNIC using virtio: • Management Port • Capture Port

Virt-install deployment from the command line

To deploy a LiveWire Virtual instance from the command line:

1. Download the *LivePCA_Virtual_KVM_*.tar.gz* package from LiveAction to the desired KVM host machine.
2. Determine the image store location. The recommended location for RedHat and Ubuntu is */var/lib/libvirt/images*. In this guide, the following path is used: */var/lib/libvirt/images/livepca*.

   sudo mkdir -p /var/lib/libvirt/images/livepca

3. Extract the two raw disk images from *LivePCA_Virtual_KVM_*.tar.gz* and archive to your desired image store location.

   sudo tar xvzf LivePCA_Virtual_KVM_*.tar.gz -C /var/lib/libvirt/images/livepca

4. Define the LiveWire Virtual machine using ***virt-install***. If you used a different image store location than mentioned earlier, please update both '--disk' entries with the correct path. The first 'network' entry is for the management, so we recommend configuring 'bridge' networking. The second 'network' entry is the capture network.

   sudo virt-install \
   --import \
   --name livepca \
   --description "LiveWire Virtual" \
   --virt-type kvm \
   --cpu host --vcpus 8 \
   --ram 16384 \
   --os-type linux --os-variant ubuntu18.04 \
   --network bridge=br0,model=virtio \
   --network network=default,model=virtio \
   --disk /var/lib/libvirt/images/livepca/disk1.img,device=disk,format=raw,bus=virtio,cache=none \
   --disk /var/lib/libvirt/images/livepca/disk2.img,device=disk,format=raw,bus=virtio,cache=none \
   --graphics vnc --noautoconsole

5. Your LiveWire Virtual image should have successfully installed and be up and running. To verify the current state of your LiveWire Virtual machine, execute the following command:

   sudo virsh list

6. To configure the LiveWire Virtual image to boot on start, execute the following command:

   sudo virsh autostart livepca

7. To determine the IP address of the running LiveWire Virtual image, execute the following command:

   sudo virsh domifaddr livepca

   Note You can also log in from the VM console and run *ifconfig eth0* to look up the IP address.

8. You can proceed to configuring Ethernet and NTP server settings for LiveWire Virtual. See *Configuring Ethernet settings by command script* on page 30 and *Configuring an NTP server* on page 31.

9. You can begin using LiveWire Virtual as a virtual appliance.

Virtual Machine Manager deployment

To deploy an LiveWire Virtual instance using the Virtual Machine Manager:

1. Download the *LivePCA_Virtual_KVM_*.tar.gz* package from LiveAction to the desired KVM host machine.

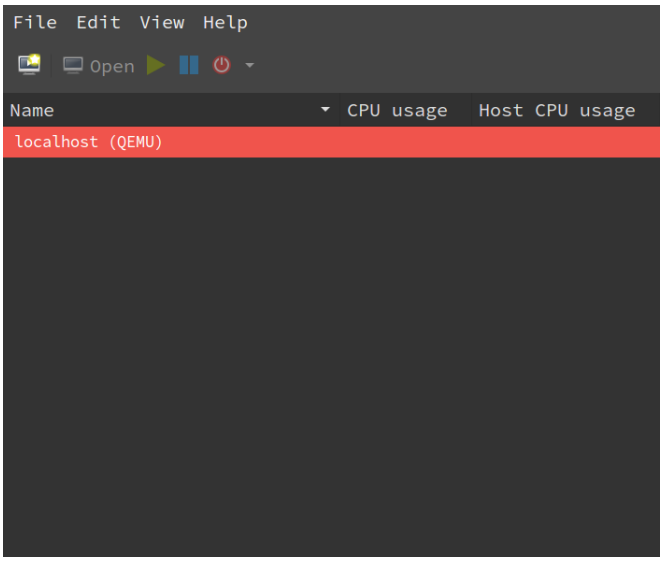
2. Determine the image store location. The recommended location for RedHat and Ubuntu is */var/lib/libvirt/images*. In this guide, the following path is used: */var/lib/libvirt/images/livepca*.

   sudo mkdir -p /var/lib/libvirt/images/livepca

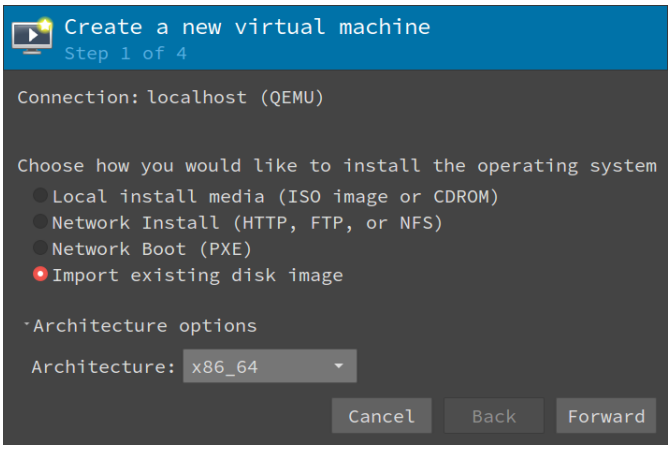
3. Extract the two raw disk images from *LivePCA_Virtual_KVM_*.tar.gz* and archive to your desired image store location.

   sudo tar xvzf LivePCA_Virtual_KVM_*.tar.gz -C /var/lib/libvirt/images/livepca

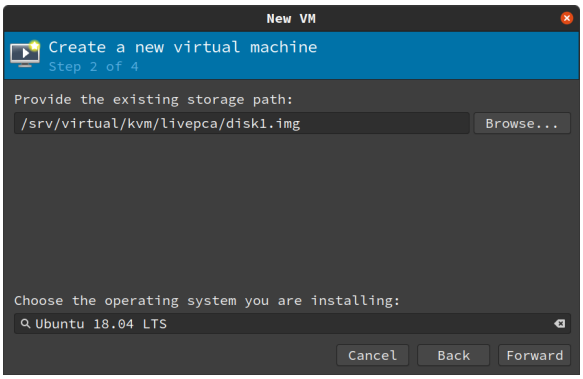
4. To open Virtual Machine Manager, click **Applications > System Tools > Virtual Machine Manager**.



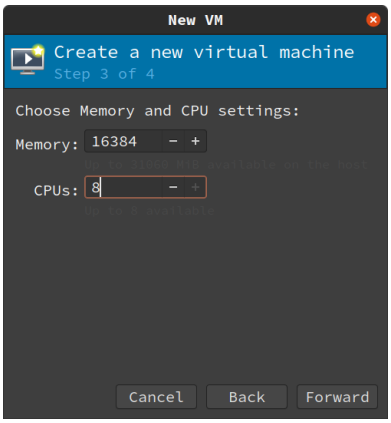
5. On the **File** menu, click **New Virtual Machine** to launch the *New VM* wizard.
6. Choose how to install the operating system and architecture options, and then click **Forward**:
   - Select *Import existing disk image*
   - *Architecture*: Select *x86_64*



7. Provide storage and OS details, and then click **Forward**:
   - *Provide the existing storage path*: Browse to the *disk1.img* file extracted above (for example, */var/lib/libvirt/images/omni-virtual/disk1.img*)
   - *OS type*: Select *Linux*
   - *Version*: Select *Ubuntu 18.04 LTS*



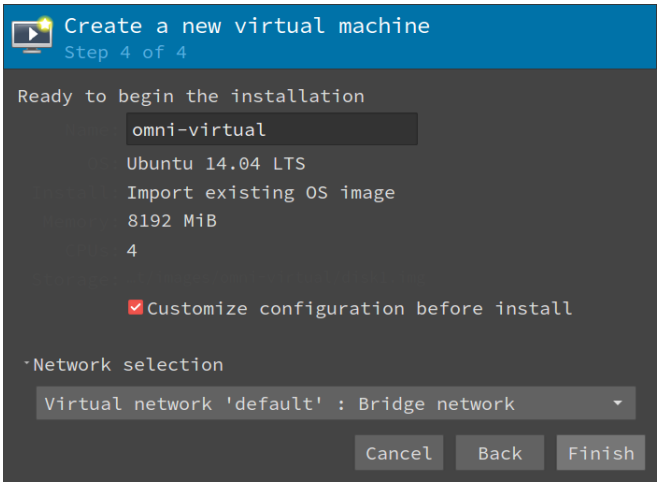
8. Choose Memory and CPU settings, and then click **Forward**:
   - *Memory (RAM)*: Select *16384* MiB
   - *CPUs*: Select *8*



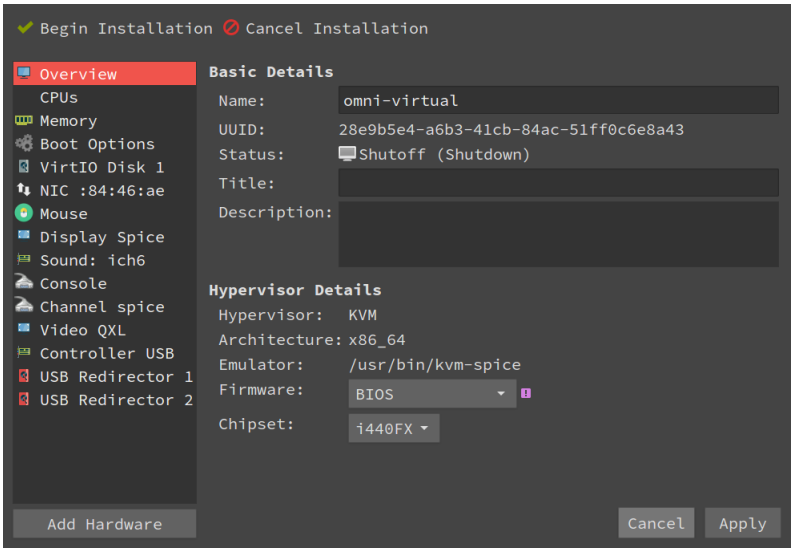
9. Assign a name to the VM, select the network selection, and then click **Finish**:
   - *Name*: Type a name for the virtual machine
   - *Customize configuration before install*: Select this check box.

Important! Make sure to select the *Customize configuration before install* check box.

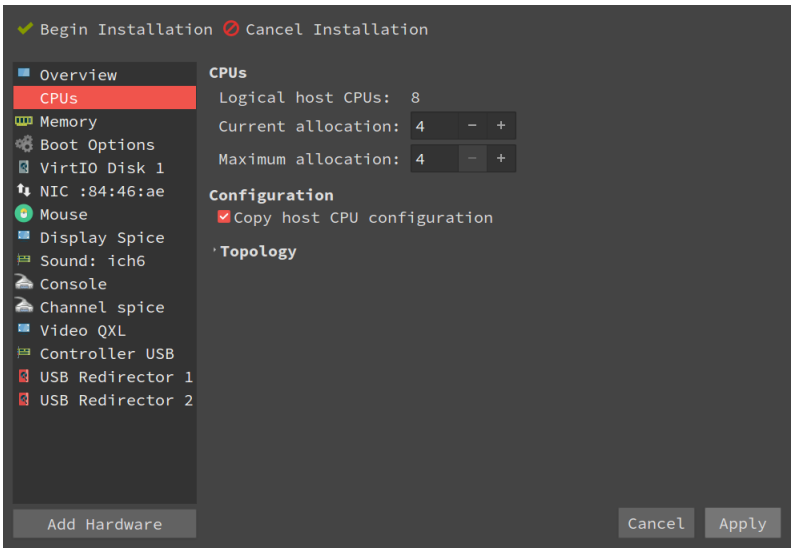
   - *Network selection*: Select *Bridge network* so that the management port can have its own assigned IP address.



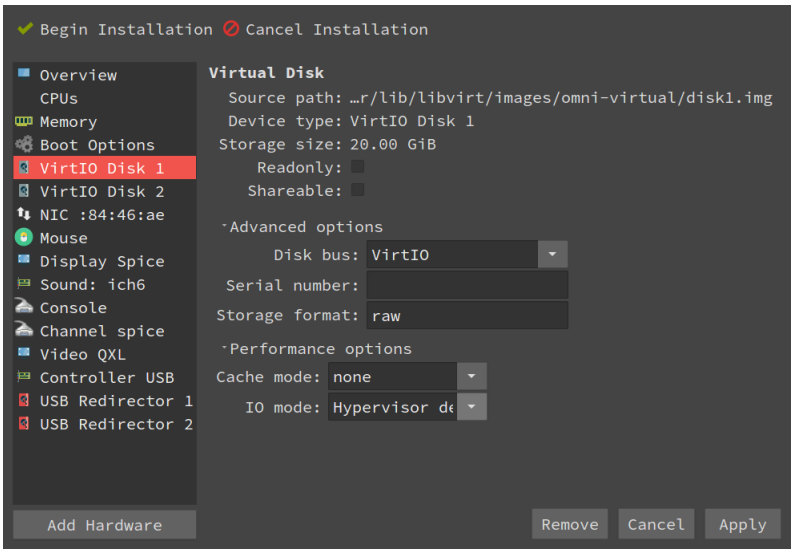
10. From the side menu, select **Overview**:
    - *Firmware*: Select *BIOS*.



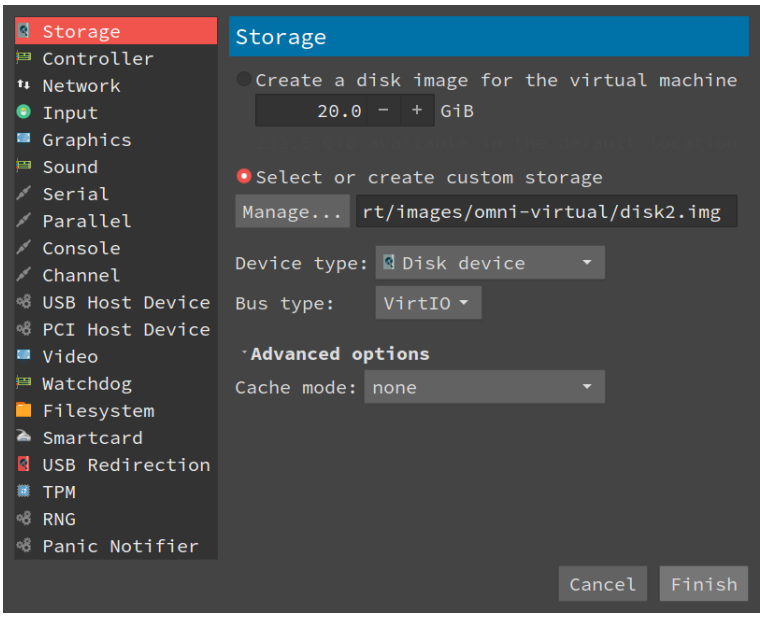
11. Click **Apply** to save the changes.
12. From the side menu, select **CPUs**:
    - Select *Copy host CPU configuration*.



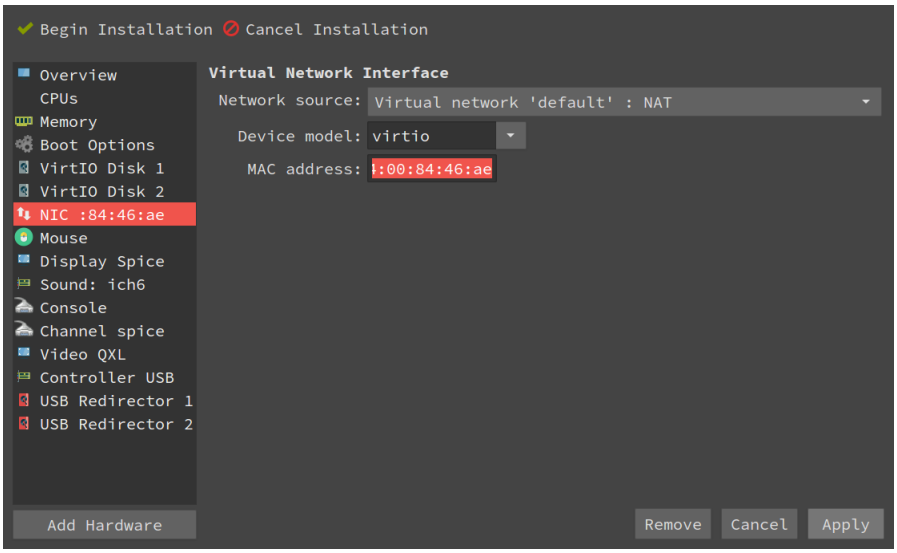
13. Click **Apply** to save the changes.
14. From the side menu, select **Disk 1**:
    - *Disk bus*: Select *VirtIO*.
    - *Cache mode*: Select *none*.



15. Click **Apply** to save the changes.
16. From the side menu, select **Add Hardware** and then select *Storage* in the **Add New Virtual Hardware** menu.
    - Select *Select or create custom storage* and click **Manage** to browse to the path of the *disk2.img* file extracted above (for example, */var/lib/libvirt/images/omni-virtual/disk2.img*)
    - *Device type*: Select *Disk device*.
    - *Bus type*: Select *VirtIO*.
    - *Advanced options*: Select *none* for cache mode.

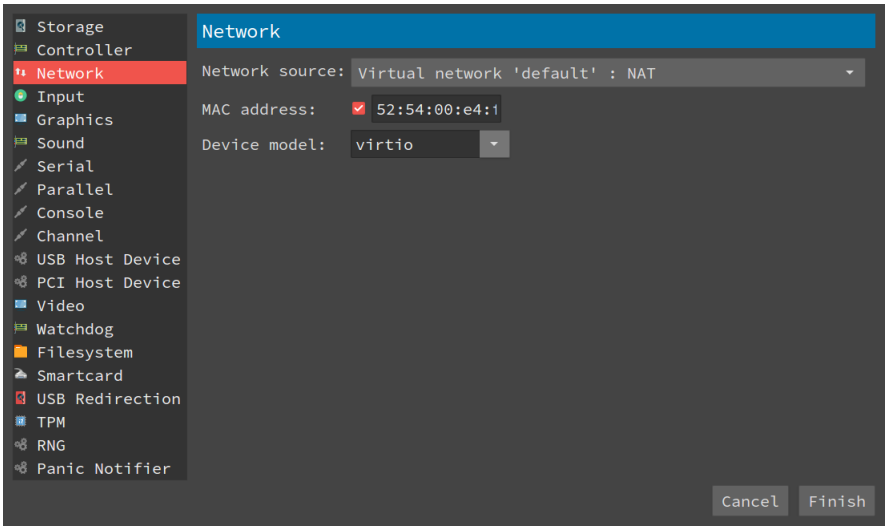


17. Click **Finish**.
18. From the side menu, select **NIC**:
    - *Network source*: Select your management port network source.
    - *Device model*: Select *VirtIO*.
19. Click **Apply** to save the changes.



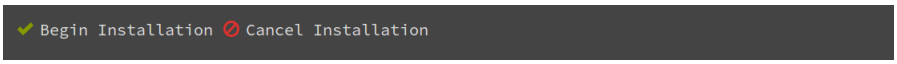
20. From the side menu, select **Add Hardware** and then select *Network* in the **Add New Virtual Hardware** menu.

- *Network source*: Select the primary network source from where you are capturing traffic.
- *Device model*: Select *VirtIO*.



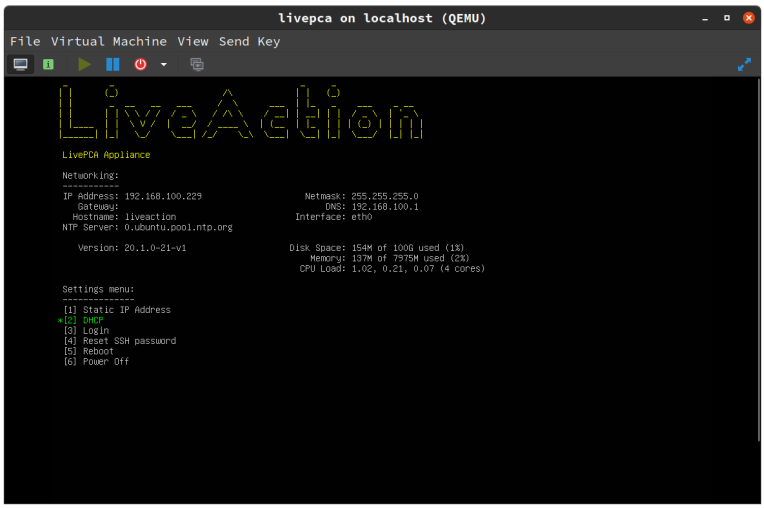
21. Click **Finish** to add the new capture interface.

22. Click **Begin installation** (upper left).



Virtual Machine Manager configures and automatically boots the LiveWire Virtual machine.

23. Log in from the console using the default credentials (*admin/admin*).



24. Use the following command to determine the management port's IP address:

    ifconfig eth0

25. You can proceed to configuring Ethernet and NTP server settings for the LiveWire Virtual machine. See *Configuring Ethernet settings by command script* on page 30 and *Configuring an NTP server* on page 31.

26. You can begin using LiveWire Virtual as a virtual appliance.

Deploying LiveWire Virtual on Hyper-V

Requirements

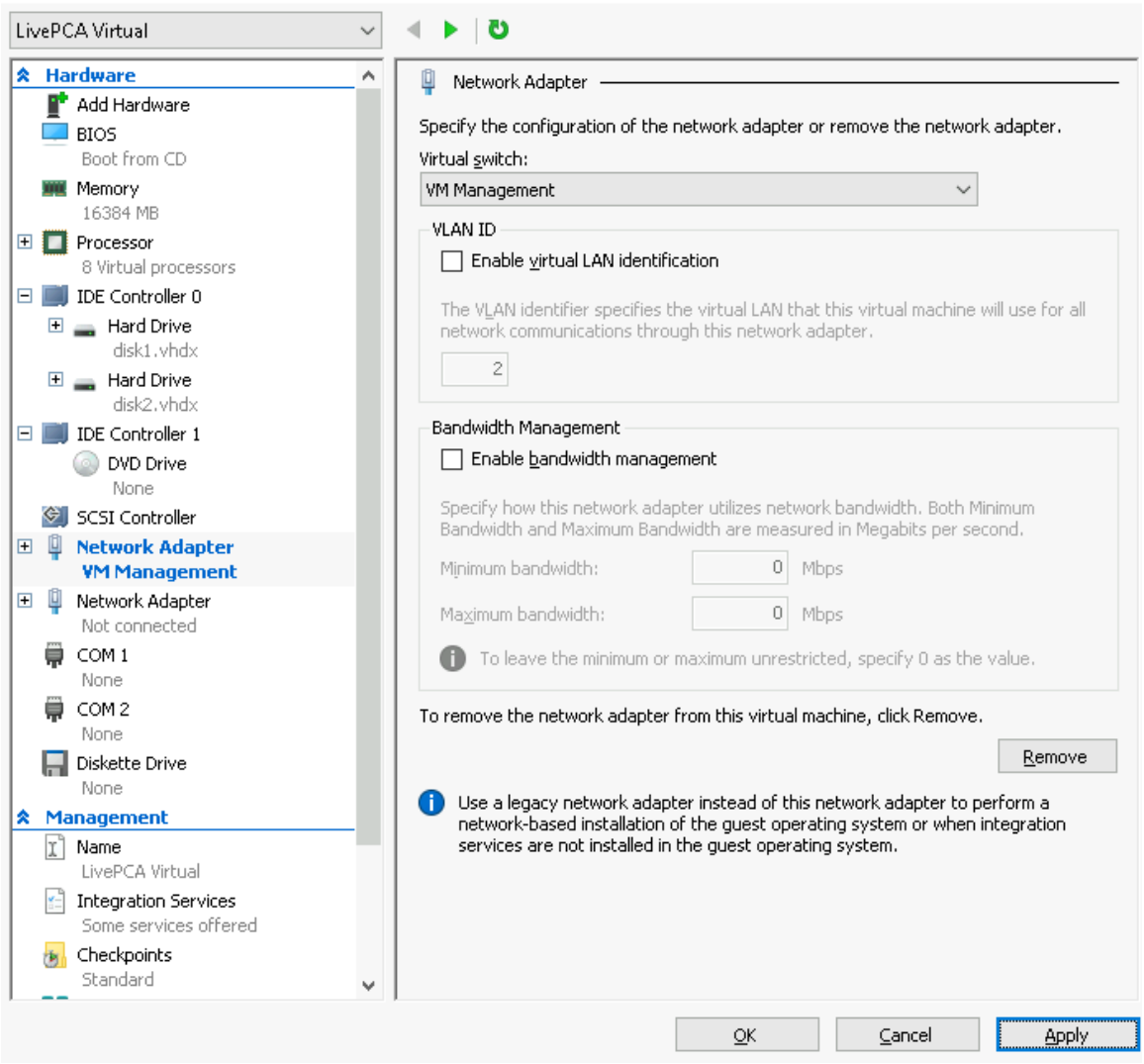
- A computer running Windows Server® 2012 R2 or later with the Hyper-V role installed.
- A user account that is a member of the local Hyper-V Administrators group, or the Administrators group.

LiveWire Virtual Deployment

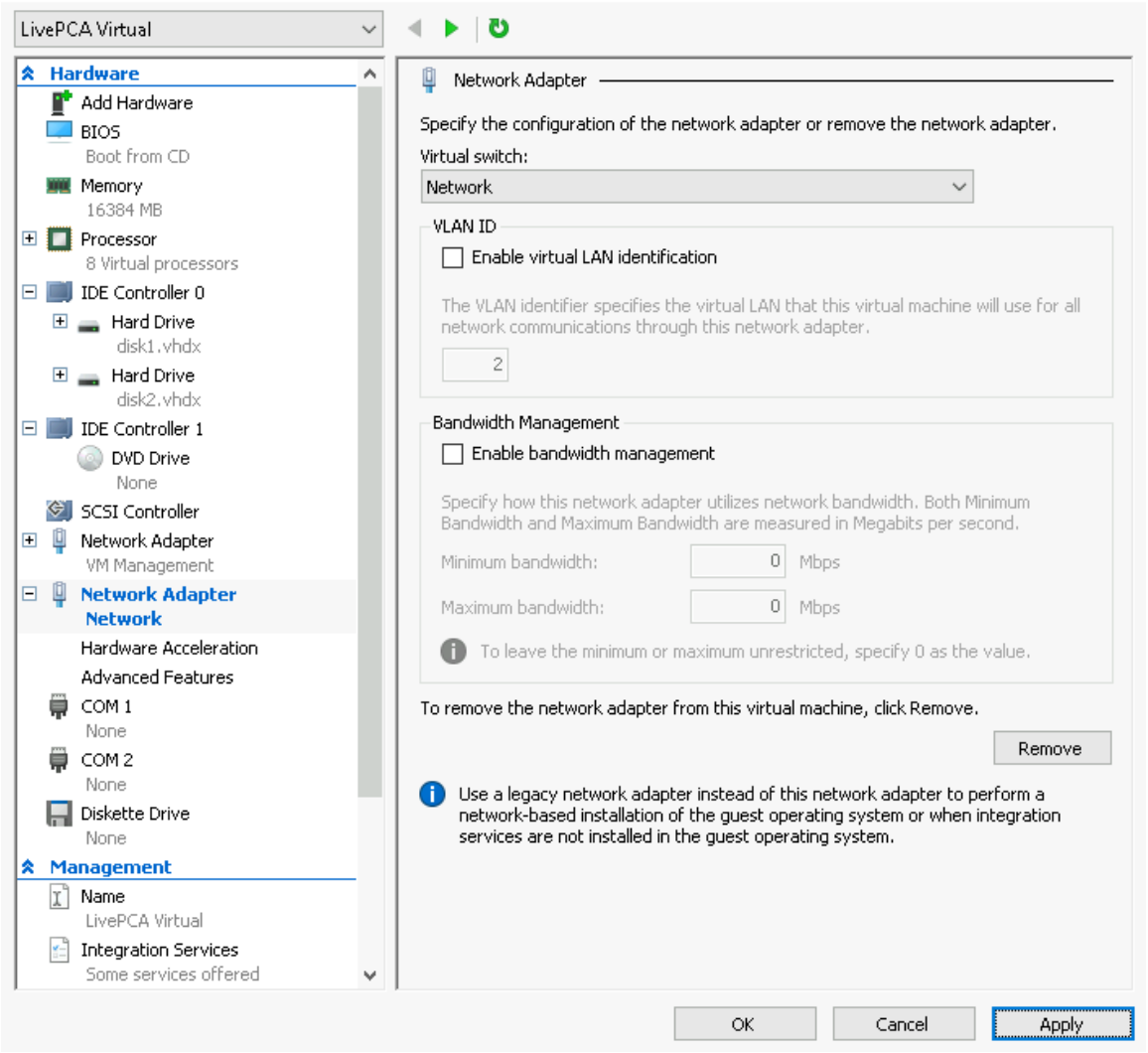
If you have not already done so, extract the contents of the LiveWire Virtual zip to your Hyper-V server.

1. Open Hyper-V Manager.
2. From the **Actions** menu in Hyper-V Manager, click **Import Virtual Machine**.
3. If the *Before You Begin* screen appears, click **Next**.
4. Browse to the folder that contains the extracted LiveWire Virtual files, and click **Next**.
5. Select the LiveWire Virtual machine to import, and click **Next**.
6. Choose *Copy the virtual machine* as the import type, and click **Next**.
7. On *Choose Folders for Virtual Machines Files*, specify new or existing folders to store the VM files and click **Next**.
8. On *Choose Folders to Store Virtual Hard Disks*, specify the folder to store the virtual hard disk files and click **Next**.
9. After verifying your choices in the Summary page, click **Finish**.
10. Wait several minutes for the import to complete.
11. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Settings...*

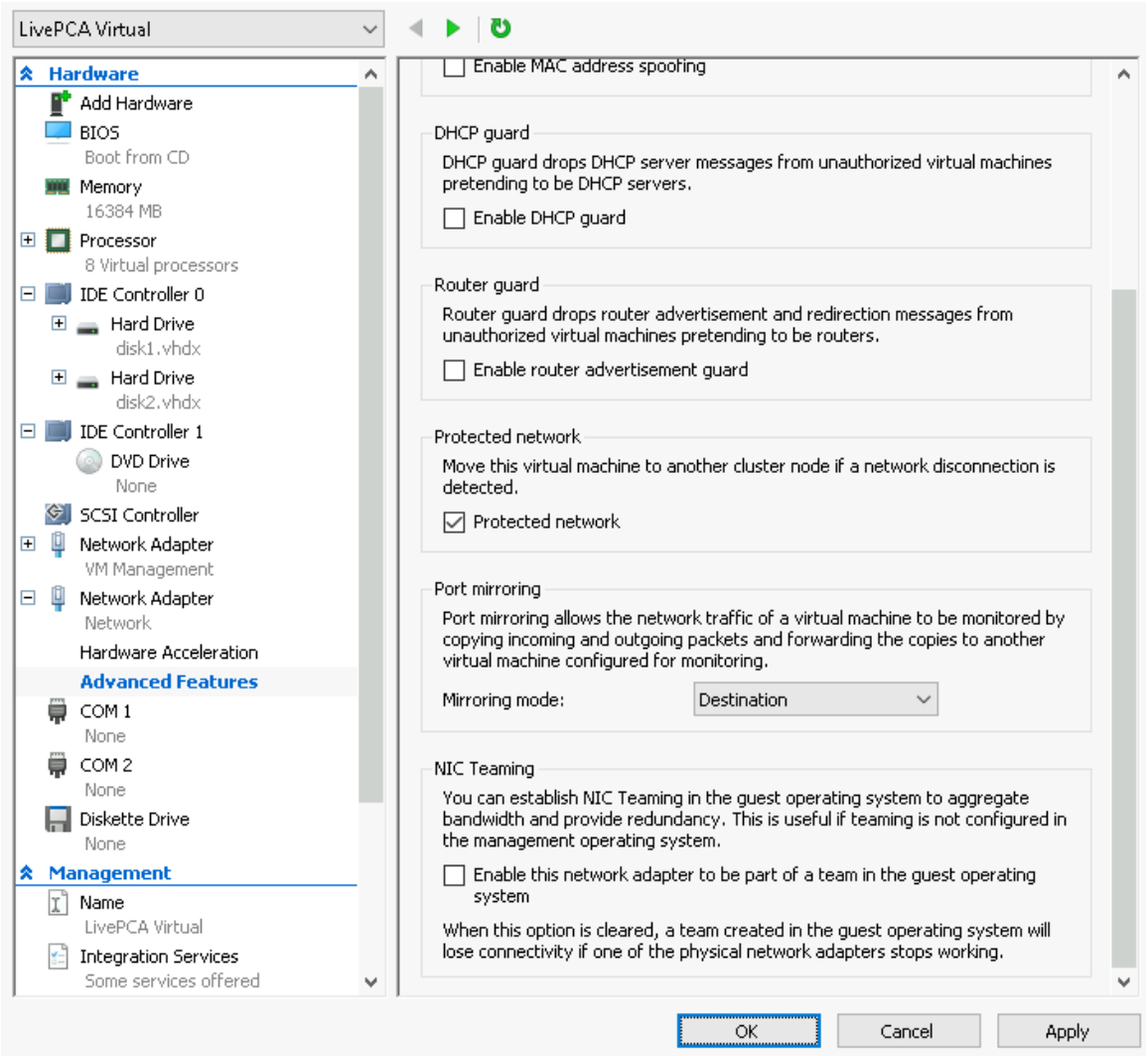
12. Select the first Network Adapter in the *Hardware* tree.



13. Specify the Virtual switch you wish to use for the *Management* connection, click **Apply**.
14. Select the second Network Adapter in the *Hardware* tree.
15. Specify the Virtual switch of the virtual machines you wish to monitor, click **Apply**.



16. Expand the selected Network Adapter and select *Advanced Features*.
17. In the Port mirroring section, select *Destination* as the mirroring mode, click **OK**.



18. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Connect*...
19. In the *Virtual Machine Connection* window, select *Action* > *Start*.

LiveWire Virtual Disk Configuration

By default LiveWire Virtual is configured with a single OS disk (Hard disk 1), and a single capture storage disk (Hard disk 2). Both of these hard disks can be extended to increase the amount of log storage and capture storage. Capture storage can also be increased by adding additional hard disk devices to LiveWire Virtual.

Note LiveWire VIrtual image must be shutdown to expand the existing disk

Expanding OS storage:

1. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Settings*...
2. Under *IDE Controller 0*, select *Hard Drive disk1.vhdx*.
3. Click **Edit** to start the *Edit Virtual Hard Disk Wizard*.
4. On the *Locate Virtual Hard Disk* page, click **Next**.
5. Select *Expand* to expand the capacity of the OS disk, click **Next**.

6. On the *Expand Virtual Disk* page, enter the new virtual hard disk size. The size is specified in gigabytes with a maximum size of 64TB for any virtual hard disk.
7. Click **Next**.
8. On the *Completing the Edit Virtual Hard Disk Wizard* page, click **Finish**.
9. Click **OK**.
10. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Connect...*
11. In the Virtual Machine Connection window, select *Action > Start*. On reboot, LiveWire Virtual automatically resizes the OS partition to the new size.

Expanding capture storage disk(s):

1. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Settings...*
2. Under *IDE Controller 0*, select *Hard Drive disk2.vhdx.*
3. Click **Edit** to start the *Edit Virtual Hard Disk Wizard*.
4. On the *Locate Virtual Hard Disk* page, click **Next**.
5. Select *Expand* to expand the capacity of the capture storage disk, click **Next**.
6. On the *Expand Virtual Disk* page, enter the new virtual hard disk size. The size is specified in gigabytes with a maximum size of 64TB for any virtual hard disk.
7. Click **Next**.
8. On the *Completing the Edit Virtual Hard Disk Wizard* page, click **Finish**.
9. Click **OK**.
10. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Connect...*
11. In the *Virtual Machine Connection* window, select *Action > Start*. On reboot, LiveWire Virtual automatically resizes the capture partition to the new size.

Adding capture storage disk(s):

1. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Settings...*
2. Click **SCSI Controller**. On the right pane, under *SCSI Controller*, click **Hard Drive**.
3. Click **Add**.
4. On the right pane, under *Hard Drive*, click **New**.
5. On the *Before You Begin* page, click **Next**.
6. On the *Choose Disk Format* page, choose *VHDX* and click **Next**.
7. On the *Specify Name and Location* page, type the name of the new virtual hard disk. If required, type the location of the virtual hard disk. Click **Next**.
8. On the *Configure Disk* page, type disk size and click **Next**.
9. On the *Completing the New Virtual Hard Disk Wizard* page, click **Finish**.
10. Click **OK**.
11. In Hyper-V Manager, right-click the LiveWire Virtual machine and select *Connect...*
12. In the *Virtual Machine Connection* window, select *Action > Start*. On reboot, LiveWire Virtual automatically resizes the capture partition to the new size.

Monitoring Traffic

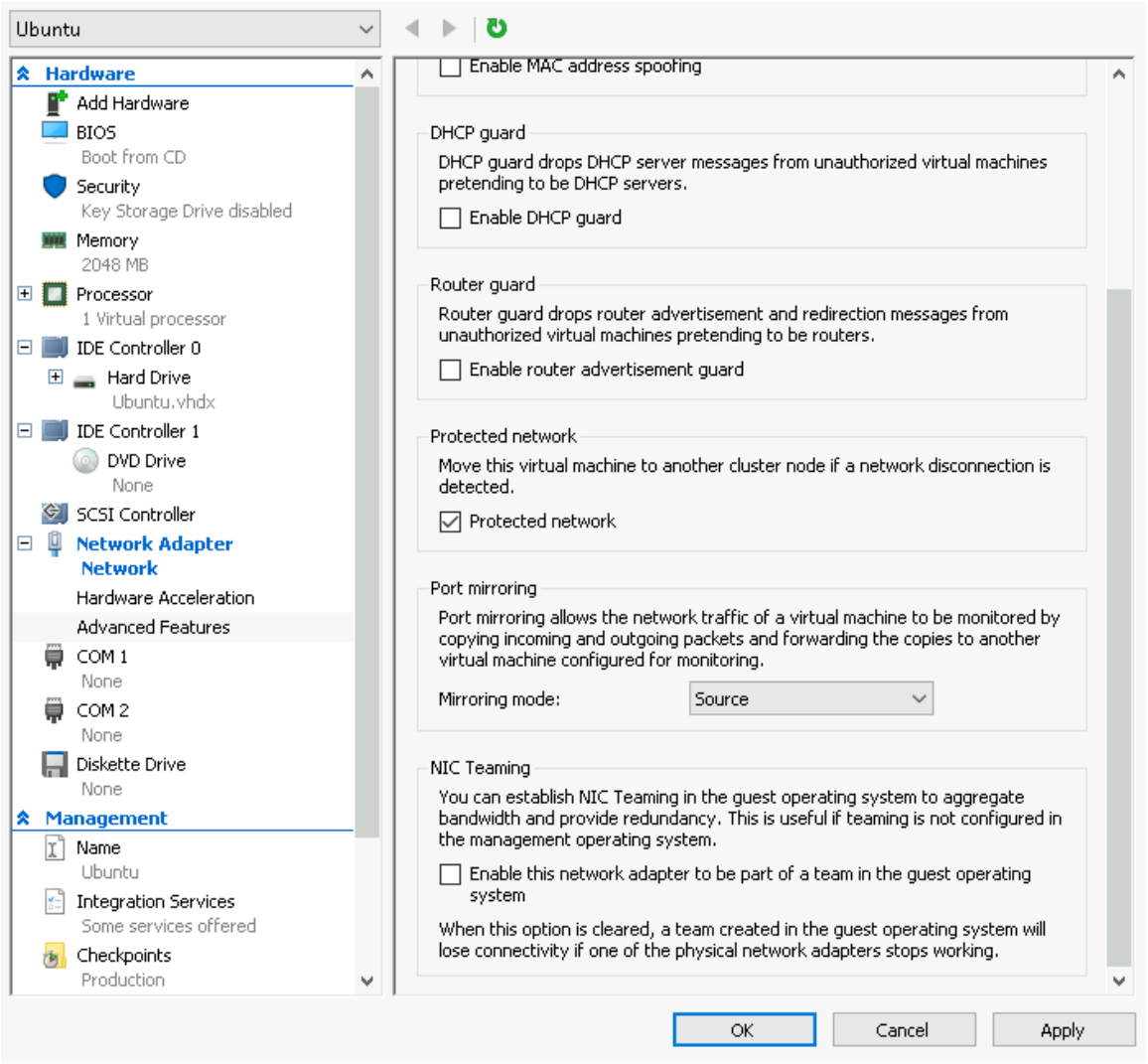
The following provide a 'Best Practices' for monitoring traffic in a Hyper-V environment with LiveWire Virtual.

Monitoring VM Traffic

The following instructions will allow you to monitor network traffic of VMs on the same host by selecting Port Mirroring mode in Hyper-V.

> **Note** LiveWire Virtual can only monitor virtual machines running on the same virtual switch.

1. Open Hyper-V Manager.
2. In Hyper-V Manager, right-click the source virtual machine and select *Settings*...
3. Expand the *Network Adapter* in the *Hardware* tree.
4. Select *Advanced Features*.
5. In the *Port mirroring* section, select *Source* as the mirroring mode, click **OK**.



6. Repeat these steps for all VM's you wish to monitor with LiveWire Virtual.

LiveWire Virtual Activation

Once LiveWire Virtual is installed, when you attempt to connect to it for the very first time, you must activate the product before it can be used. You can activate LiveWire Virtual either from logging directly into a web-based version of Omnipeek, or from the **Capture Engines Window** in Omnipeek.

Both an automatic and a manual method are available for activation. The automatic method is quick and useful if you have Internet access from the computer from where you are performing the activation. If Internet access is not available, the manual method is available; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

You will need to enter the following information to successfully activate LiveWire Virtual, so please have this information readily available:

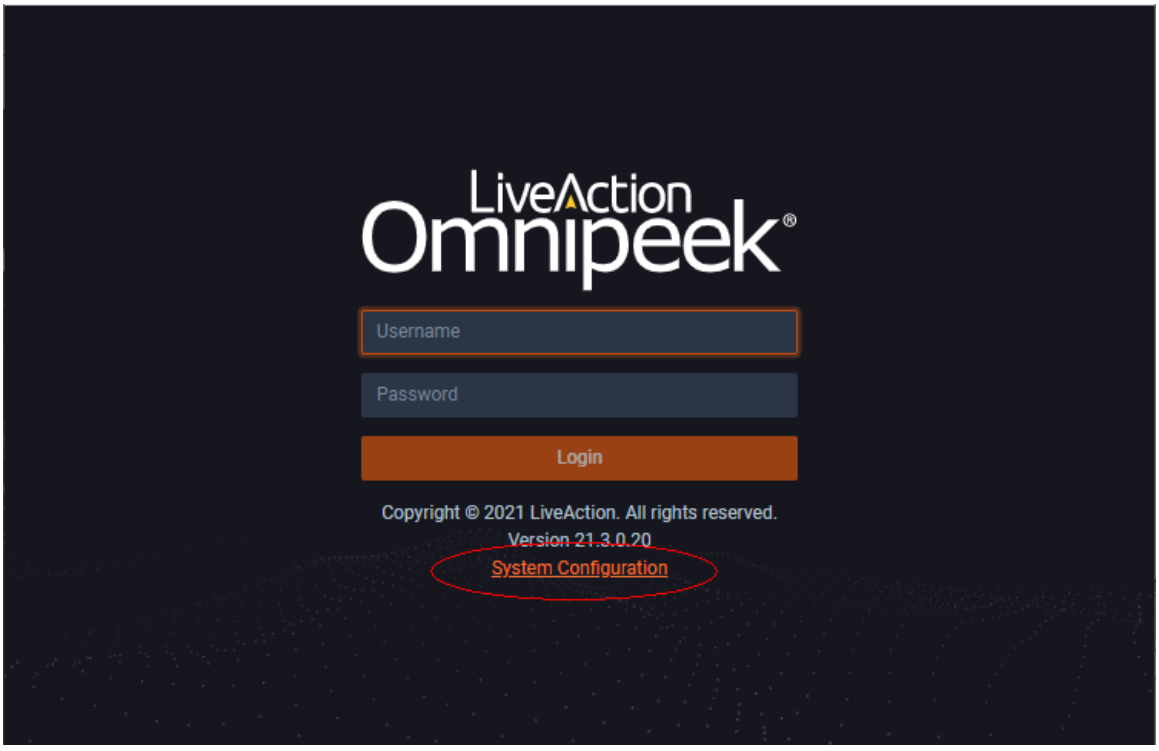
- IP address of LiveWire Virtual
- Product key
- User name
- Company name
- Email address
- Version number

Activation via Omnipeek Web

Note Activation via Omnipeek is not supported on an Internet Explorer web browser. Please use any web browser other than Internet Explorer to activate LiveWire Virtual via Omnipeek.

To activate LiveWire Virtual via Omnipeek:

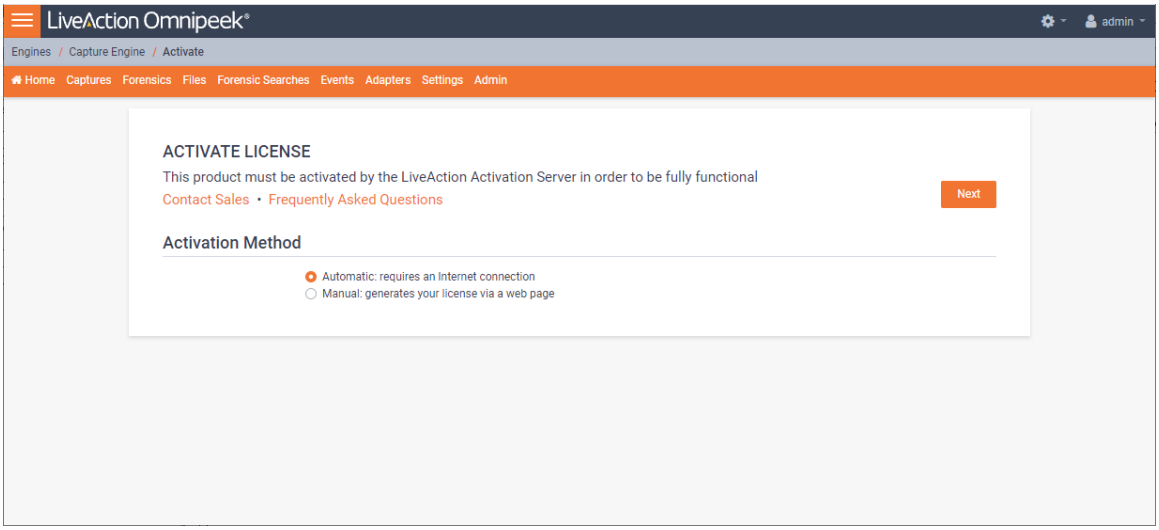
1. From your web browser, type the IP address of LiveWire Virtual into the URL field of the browser and press **Enter**. The Omnipeek login screen appears.



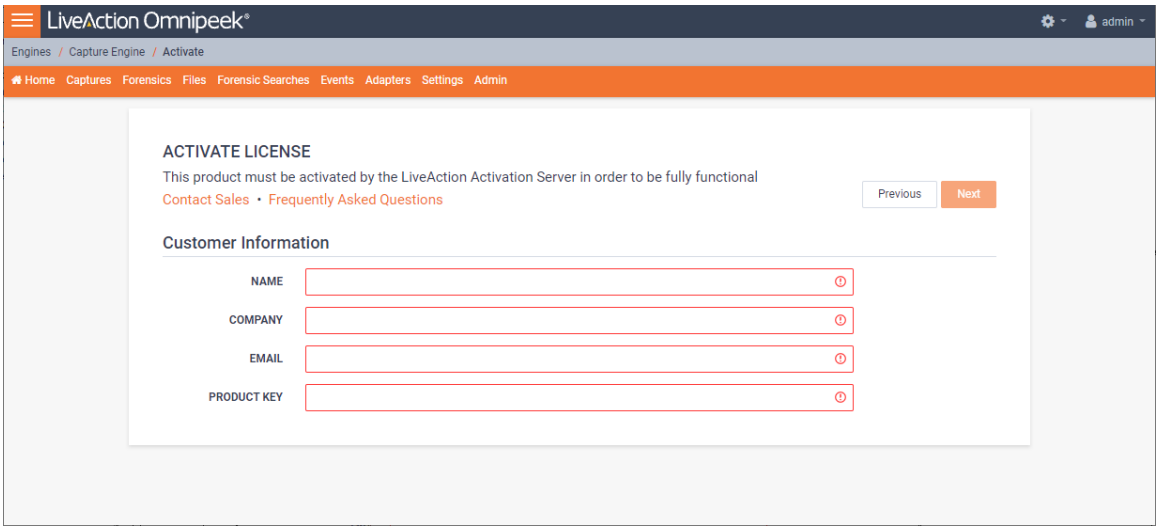
- *Username*: Type the username for LiveWire Virtual. The default is *admin*.
- *Password*: Type the password for LiveWire Virtual. The default is *admin*.

2. Type the *Username* and *Password* and click **Login**. The Omnipeek *Activation License* window appears.

Note You can also access the Omnipeek *Activation License* window by clicking *Update License* from the Capture Engine *Home* screen in Omnipeek.



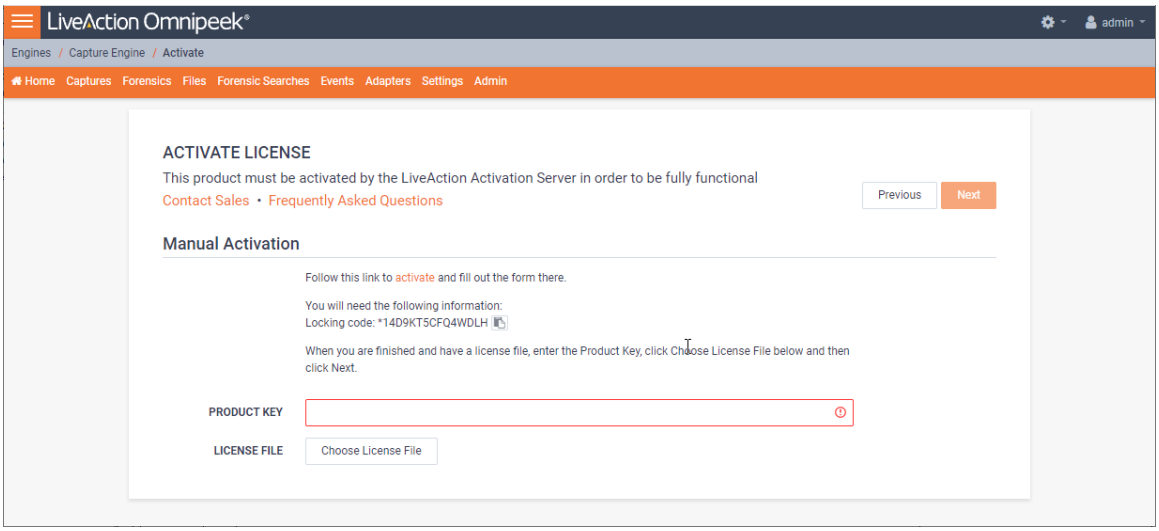
3. If your client has an active Internet connection, select *Automatic* and click **Next**. The **Customer Information** window appears. Continue with Step 4 below.



- *NAME:* Type the user name of the customer.
- *COMPANY:* Type the company name.
- *EMAIL:* Type the email address of the customer.
- *PRODUCT KEY:* Type the product key.

If your client does not have an active Internet connection, or you are prevented from accessing the Internet using personal firewalls, or there are other network restrictions that may block automatic activations, select *Manual* and click **Next.** The **Manual Activation** window appears. Skip to Step 5 below.

Note The manual activation method is available for instances described above; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

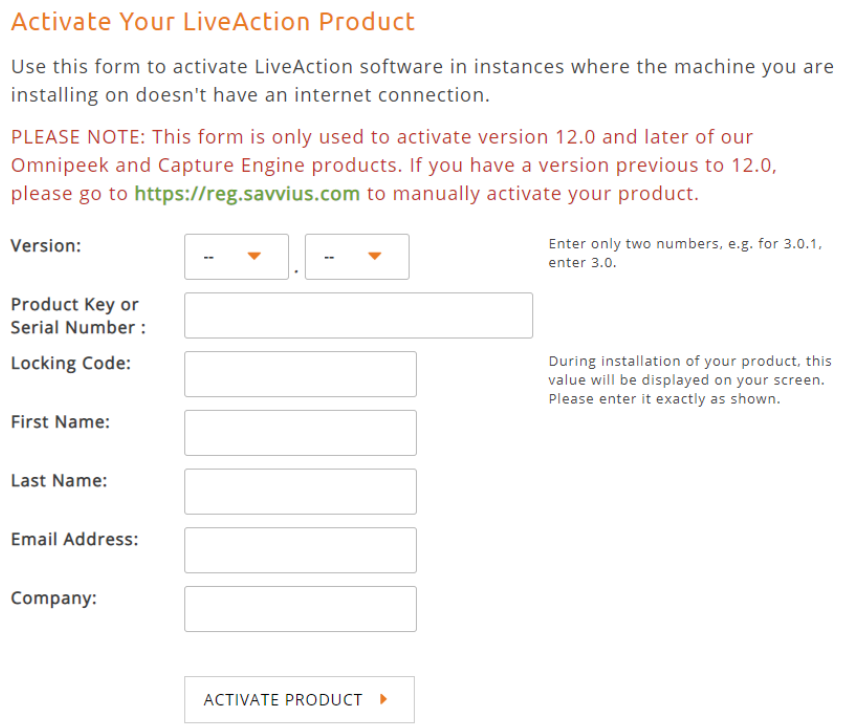


Note The ***Locking code*** displayed in the window above is required in Step 6 below. You can click the small icon next to the code to save it to the clipboard so you can paste it into the Locking Code field in Step 6 below.

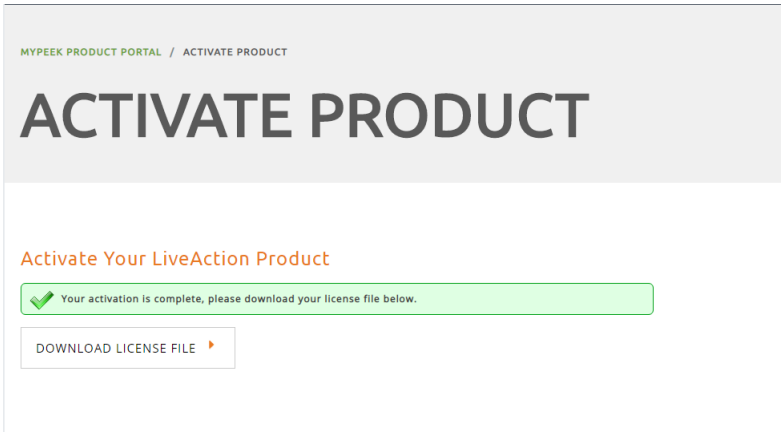
4. Complete the Customer Information window and click **Next**. LiveWire Virtual is now activated and you can begin using the product. The activation process is complete.

Note If the automatic activation does not complete successfully, go back and select the manual activation process. Personal firewalls or other network restrictions may block automatic activations.

5. Click the *activate* link (*https://mypeek.liveaction.com/activate_product.php*) in the window. A web browser page opens that allows you to activate your LiveAction product and to obtain and download a license file. The license file is required to complete the manual activation.



6. Complete the information on the activation page and click **ACTIVATE PRODUCT**. The following page appears once the activation is complete.



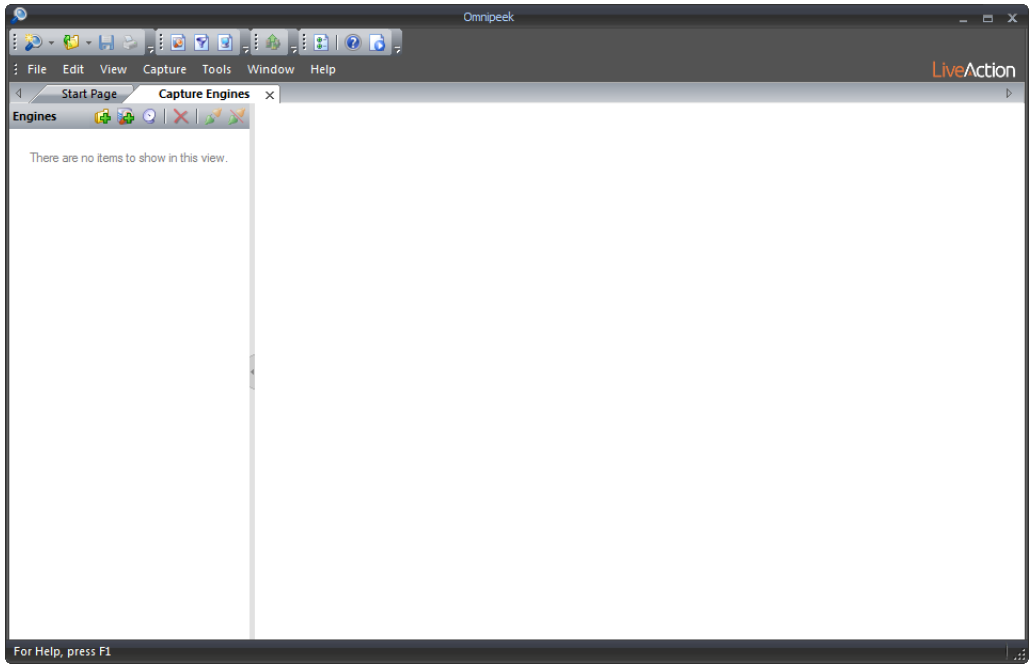
7. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in the following steps.
8. Return back to the to the **Manual Activation** window, and click **Choose License File**.
9. Navigate to the license file downloaded above and click **Open**.
10. Click **Next** in the **Manual Activation** window. LiveWire Virtual is now activated and you can begin using the product. The activation process is complete.

Activation via Omnipeek

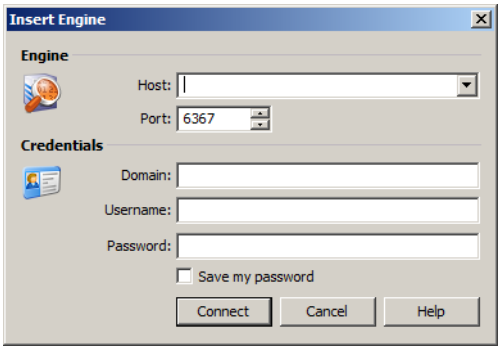
Note Activation of LiveWire Virtual via Omnipeek is supported on Omnipeek version 13.1 or higher.

To activate LiveWire Virtual via Omnipeek:

1. From the Omnipeek Start Page, click **View Capture Engines** to display the **Capture Engines** window.

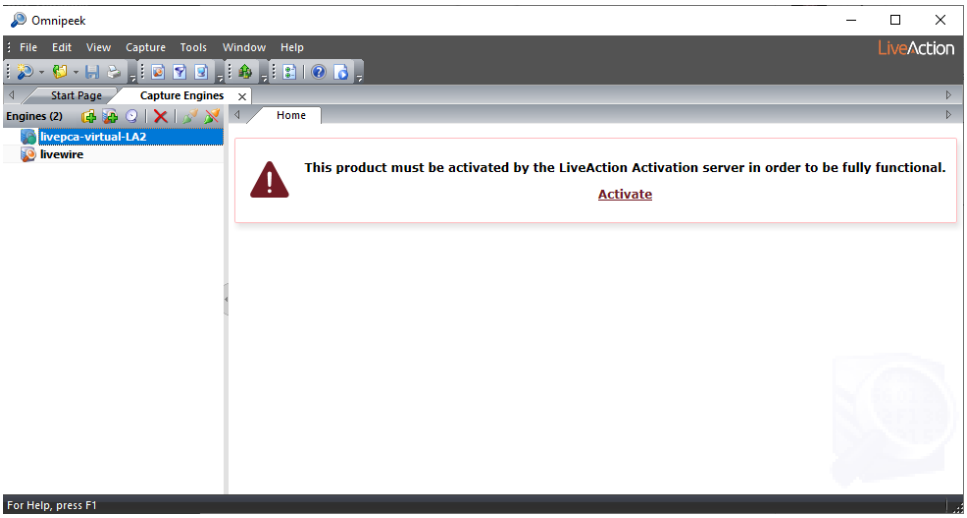


2. Click *Insert Engine* and complete the **Insert Engine** dialog.

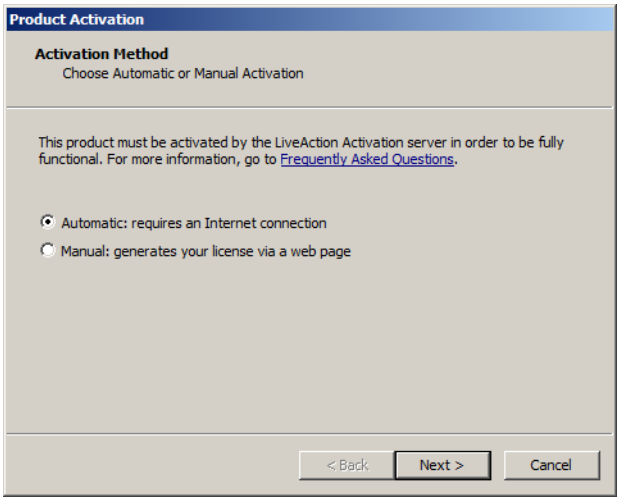


- *Host*: Enter the IP address of LiveWire Virtual.
- *Port*: Enter the TCP/IP port used for communications. Port 6367 is the default for LiveWire Virtual.
- *Domain*: Type the Domain for login to LiveWire Virtual. If LiveWire Virtual is not a member of any Domain, leave this field blank.
- *Username*: Type the username for LiveWire Virtual. The default is *admin*.
- *Password*: Type the password for LiveWire Virtual. The default is *admin*.
- *Save my password*: Select this option to remember your password to connect to LiveWire Virtual.

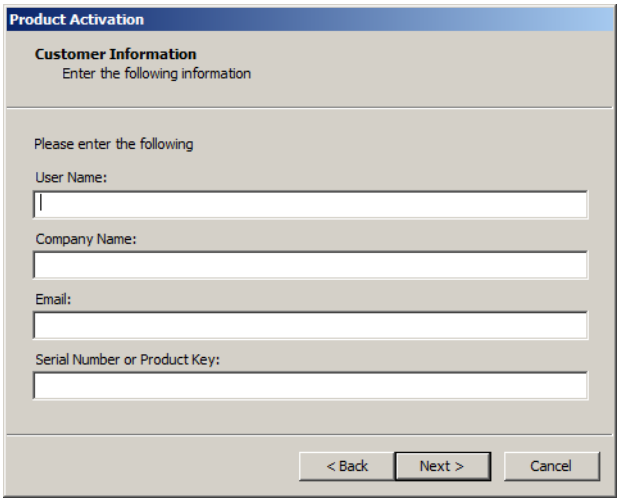
3. Click **Connect** to connect to LiveWire Virtual. If LiveWire Virtual has not yet been activated, the activation message appears in the **Capture Engines** window.



4. Click *Activate*. The **Activation Method** dialog appears.



5. If your client has an active Internet connection, select *Automatic* and click **Next**. Otherwise, select *Manual* and click **Next.** The **Customer Information** dialog appears.



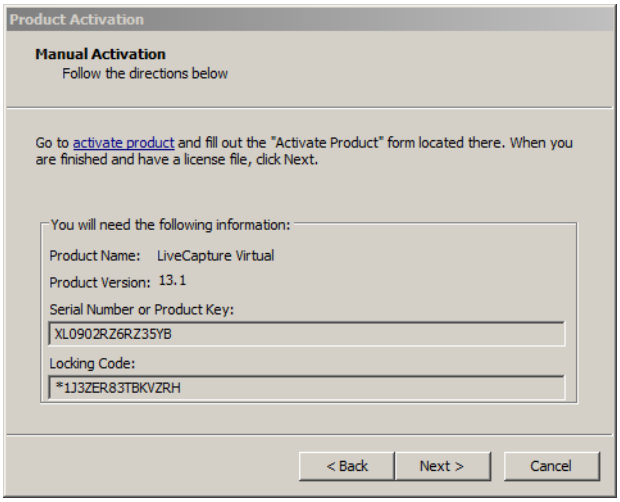
- *User Name*: Type the user name of the customer.
- *Company Name*: Type the company name.

- *Email*: Type the email address of the customer.
- *Serial Number or Product Key*: Type either the serial number or product key.

6. Complete the **Customer Information** dialog and click **Next**. If you selected the *Automatic* activation, LiveWire Virtual is now activated and you can begin using the product. The activation process is complete.

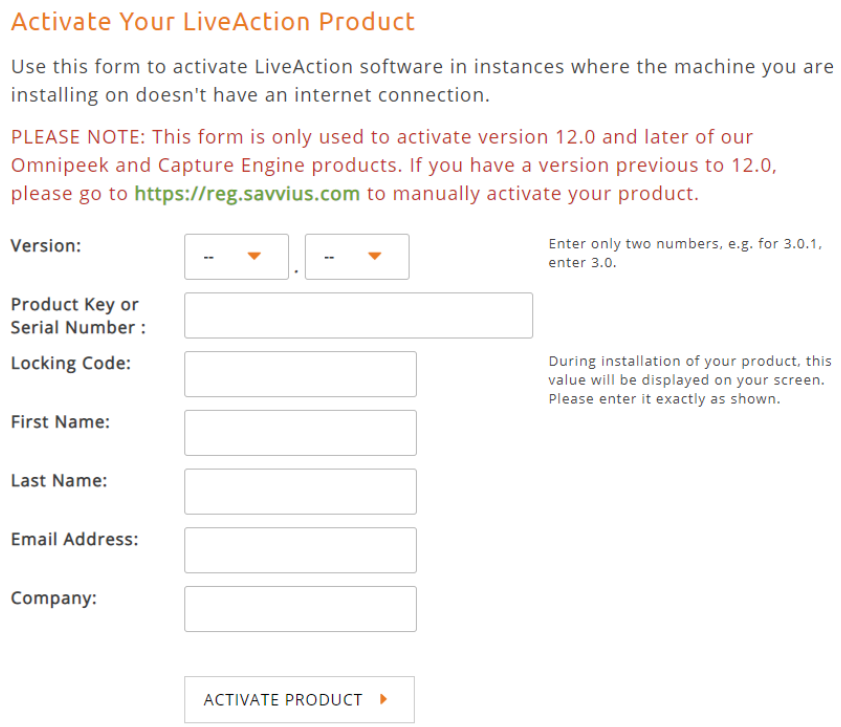
   If you selected the *Manual* activation, the **Manual Activation** dialog appears. You will need to continue with the remaining steps.

Note The manual activation method is available for instances when a computer does not have Internet access; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

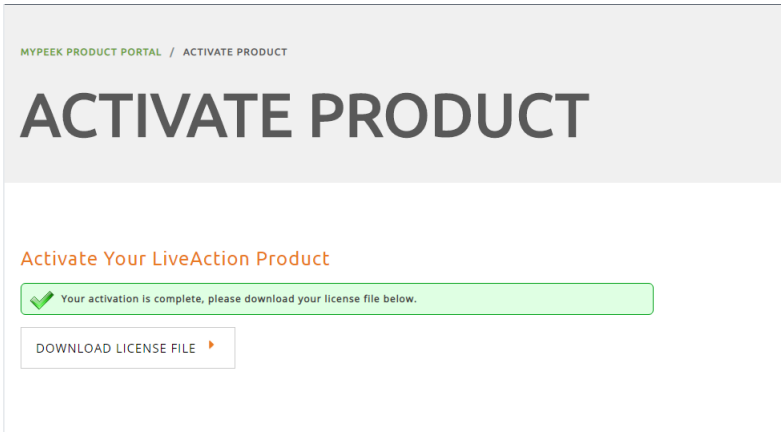


Note The *Product Key*, and also the *Locking Code* displayed in the **Manual Activation** dialog are required in the next step. You can cut and paste this information from the **Manual Activation** dialog when required in the next step.

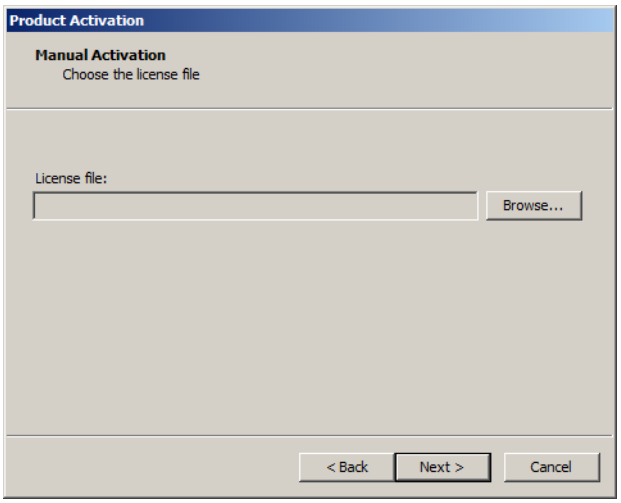
7. Click the *activate product* link (*https://mypeek.liveaction.com/activate_product.php*) in the dialog. A web browser page opens that allows you to activate your LiveAction product and to obtain and download a license file. The license file is required to complete the manual activation.



8. Complete the information on the activation page and click **ACTIVATE PRODUCT**. The following page appears once the activation is complete.



9. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in Step 11 below.
10. Return to the **Omnipeek Product Activation** dialog, and click **Next**. The **Manual Activation/Choose the license file** dialog appears.



11. Browse to the license file that was downloaded above and click **Next**. LiveWire Virtual is now activated and you can begin using the product. The activation process is complete.

Starting / shutting down LiveWire Virtual

To start LiveWire Virtual:

- Click **Power On** from the VMware or KVM console.

To shutdown LiveWire Virtual:

- SSH, or use a console connection to LiveWire Virtual and use the 'shutdown' command from the command prompt (*admin@livewire*):

  shutdown -h now

Contacting LiveAction support

Please contact LiveAction support at *https://www.liveaction.com/contact-us* if you have any questions about the installation and use of LiveWire Virtual.

CHAPTER 2

Configuring LiveWire Virtual

In this chapter:

Logging-in to LiveWire Virtual command line

You can log into the LiveWire Virtual command line by doing the following:

- Remotely, using remote SSH software such as *Putty*

The first time you log into LiveWire Virtual, use the following as your username and password:

username: *admin*

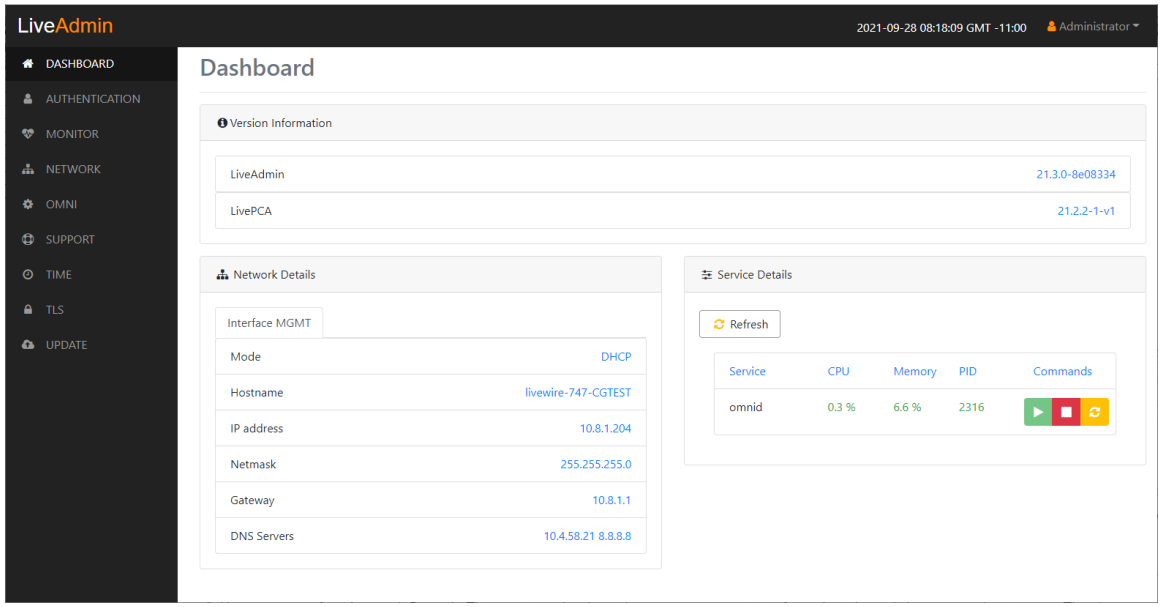
password: *admin*

After you have logged into LiveWire Virtual for the first time, you can then change your password and add users and privileges.

Note For security reasons, we strongly recommend changing the default password.

Using the LiveAdmin utility

The LiveAdmin utility on LiveWire Virtual lets you view and configure a variety of settings from the LiveAdmin views in the left-hand navigation pane of the utility. To learn more about each of the LiveAdmin views, go to the appropriate section below:



- *Dashboard*: The *Dashboard* view provides you with some very basic information about the system. See *Dashboard* on page 39.
- *Authentication*: The *Authentication* view lets you change the password for LiveWire Virtual. See *Authentication* on page 40.
- *Monitor*: The *Monitor* view displays the health of the overall system. See *Monitor* on page 41.
- *Network*: The *Network* view lets you configure the primary network interfaces network settings and the hostname of the system. See *Network* on page 41.
- *Omni*: The *Omni* view lets you enable the Device Management Server (DMS) for the appliance. See *Omni* on page 43.
- *Support*: The *Support* view let you download logs from the system that would be helpful in troubleshooting issues. See *Support* on page 45.
- *Time*: The *Time* view lets you configure the system's Timezone and NTP servers. See *Time* on page 46.

- *TLS*: The *TLS* view lets you change the self-signed certificates that LiveAdmin and Omnipeek use for HTTPS. See *TLS* on page 47.
- *Update*: The *Update* view lets you update the appliance using a software update package. See *Update* on page 48.
- *Administrator*: The *Administrator* context menu in the upper right lets you restart LiveWire Virtual, power off LiveWire Virtual or log out from the LiveAdmin utility. See *Restart and power off* on page 49.

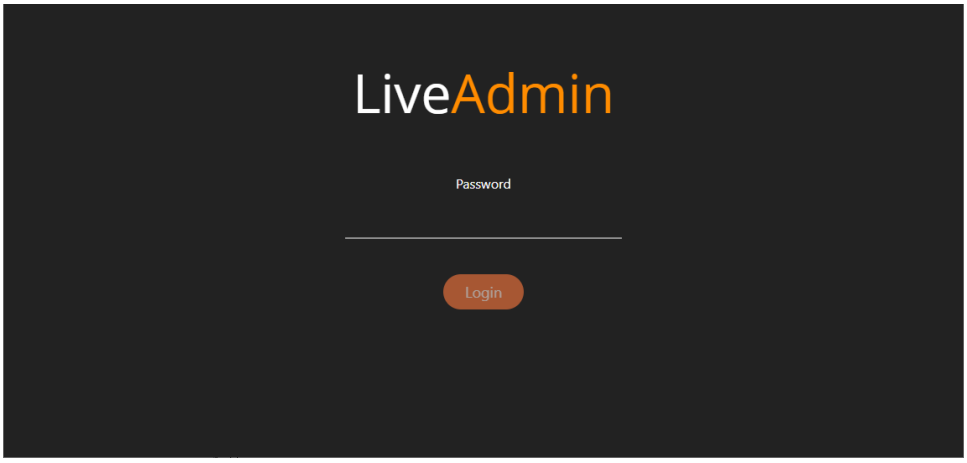
Important! LiveWire Virtual comes pre-configured to obtain its IP address via DHCP. The IP address is required to configure LiveWire Virtual, as described below. You can obtain the IP address by logging into the DMS as described in *Using DMS to manage and configure LiveAction appliances* on page 49.

Note If an IP address is not assigned to LiveWire Virtual by the DHCP server within two minutes of being connected to the network, LiveWire Virtual defaults to a static address of 192.168.1.21.

Login

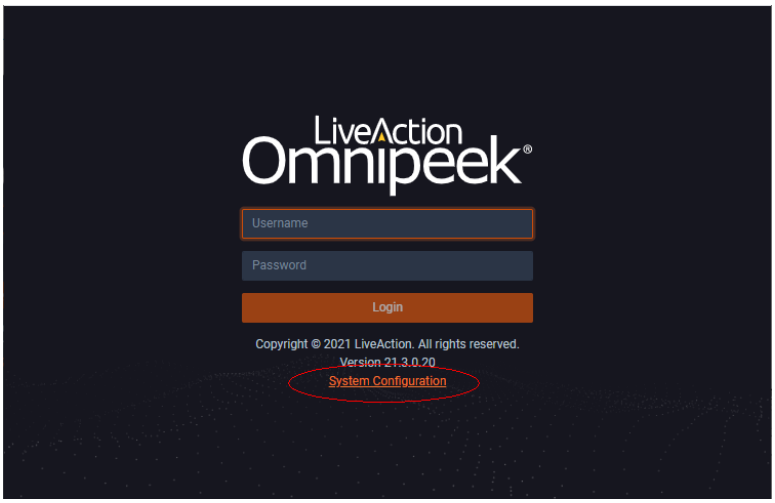
To log into the LiveAdmin utility:

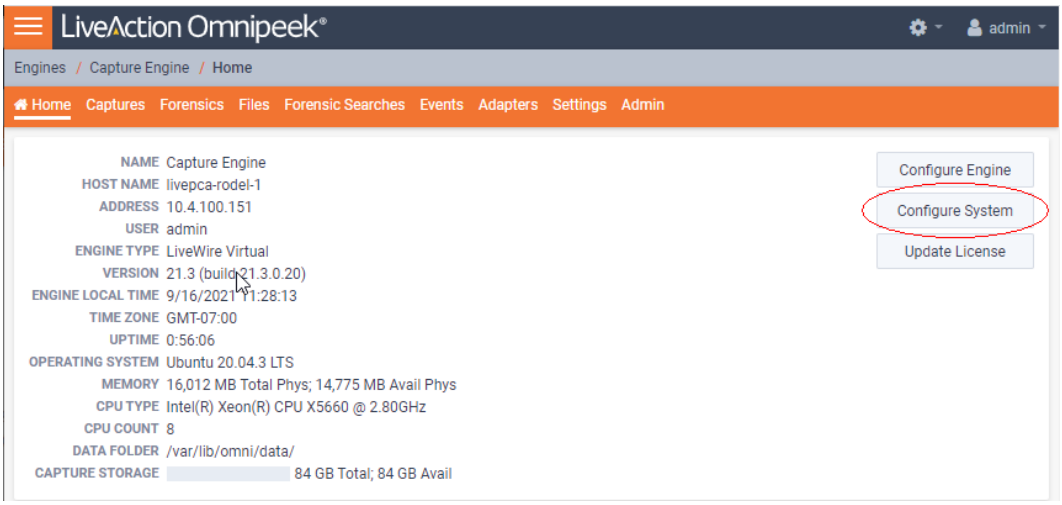
1. From a browser window on a computer connected to the same network as LiveWire Virtual, enter the IP address for LiveWire Virtual in the URL box as *<IP address>:8443* (e.g., 192.168.1.21:8443). The LiveAdmin Login screen appears.



2. Enter the default password 'admin' and click **Login**.

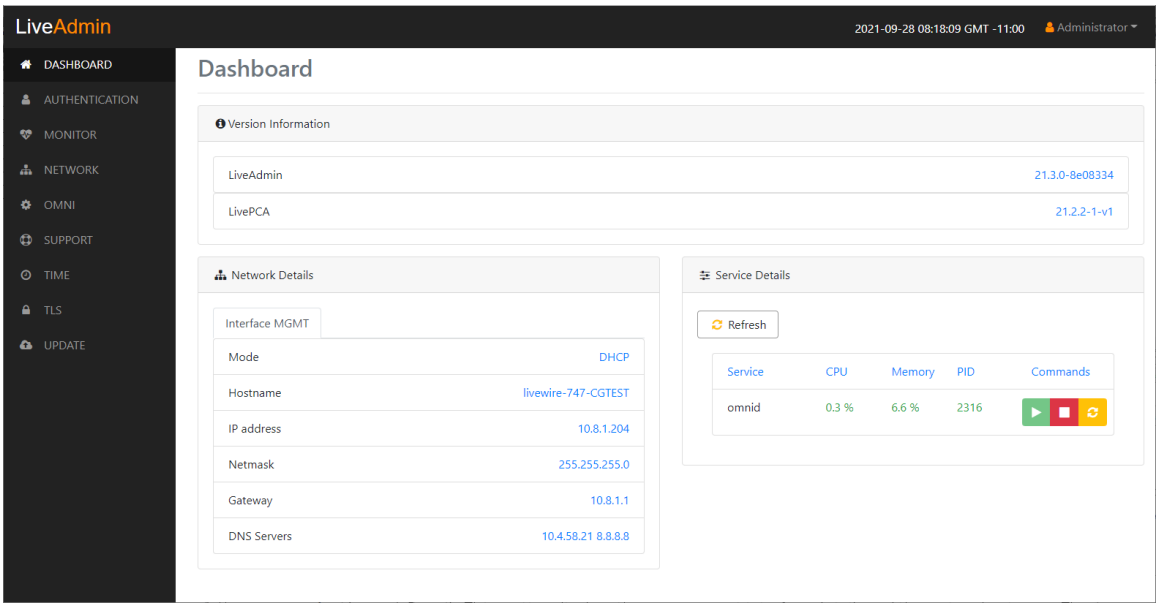
Note If you are using Omnipeek Web, you can also access the LiveAdmin Login screen by clicking *System Configuration* from either the Omnipeek Login screen, or by clicking *Configure System* from within Omnipeek itself.





Dashboard

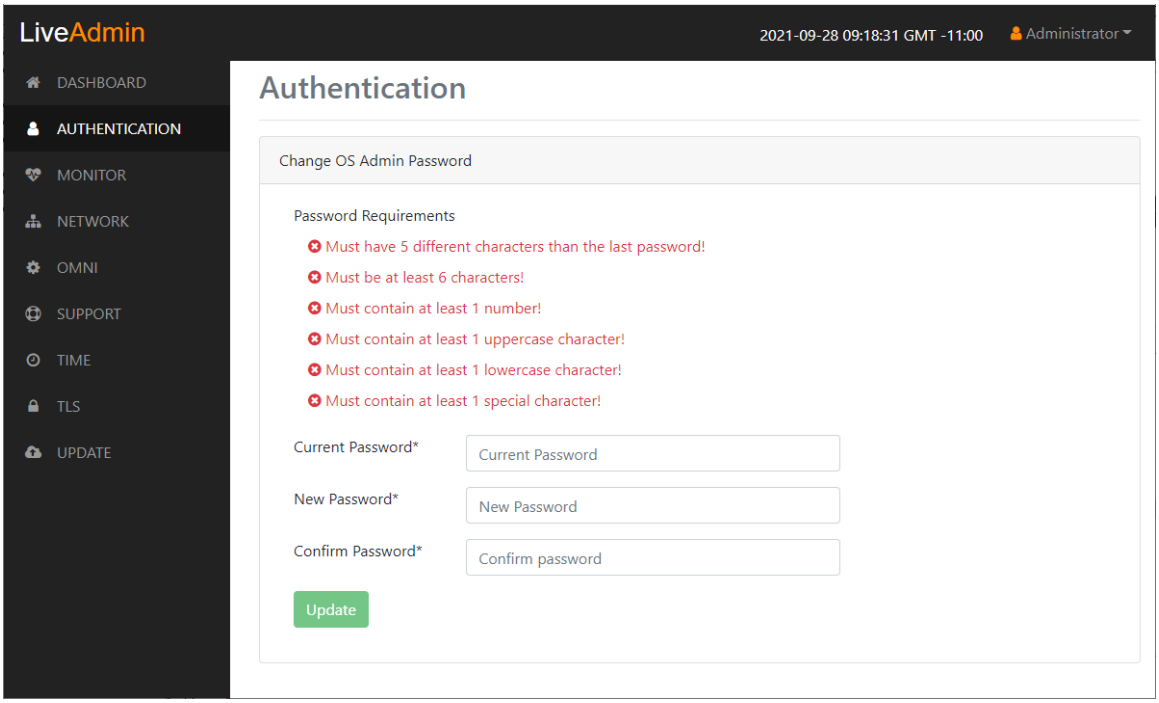
The Dashboard view provides you with some very basic information about the system.



- *Version Information*: This section displays the version numbers of the LiveAdmin utility and the software on the LiveAction appliance.
    - *LiveAdmin*: Displays the version number of the LiveAdmin utility
    - *LivePCA*: Displays the version number of the software installed on the LiveAction appliance.
- *Network Details*: This section displays the management interface details and the system hostname. The management interface is defined from the Network view in LiveAdmin. See *Network* on page 41.
- *Service Details*: This section lists a set of services you are able to monitor. This has currently been limited to the omnid process only, although additional services could easily be added:
    - *Refresh*: Click to update the view
    - *Service*: Displays the name of the service
    - *CPU*: Displays the amount of CPU the service is using
    - *Memory*: Displays the amount of memory the service is using
    - *PID*: Displays the Process ID of the service
    - *Commands*:
      Start - Click to start the service and can only be triggered if the service is stopped.
      Stop - Click to stop the service and can only be triggered if the service is running.
      Restart - Click to restart the service and can only be triggered if the service is running.

Authentication

The *Authentication* view lets you change the password for LiveWire Virtual.



- *Current Password*: Enter the current password for LiveWire Virtual. The default is *admin*.
- *New Password*: Enter the new password for LiveWire Virtual. The new password must meet the following requirements:
    - Must have 5 different characters than the last password.
    - Must be at least 6 characters.
    - Must contain at least 1 number

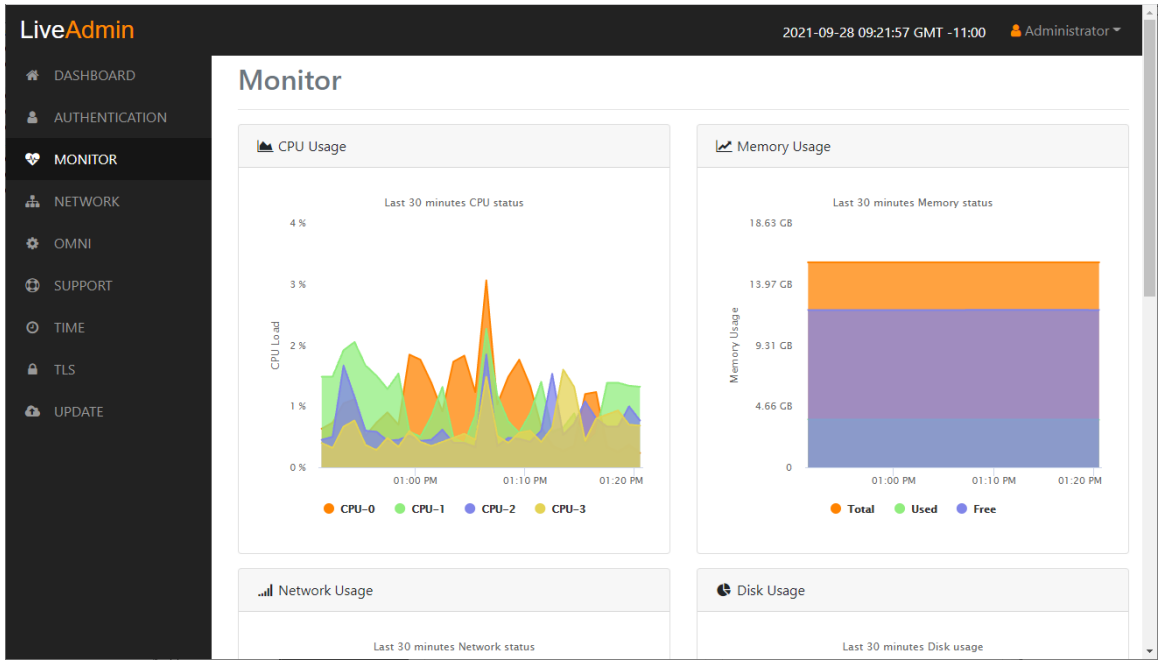
- Must contain at least 1 uppercase character.
- Must contain at least 1 lowercase character.
- Must contain at least 1 special character.

- *Confirm Password*: Enter the new password to confirm the password.
- *Update*: Click to change the password.

Note Make sure to note the *Password* that you configure.

Monitor

The Monitor view displays the health of the overall system. The view is broken up into four usage charts and one interface statistics table.

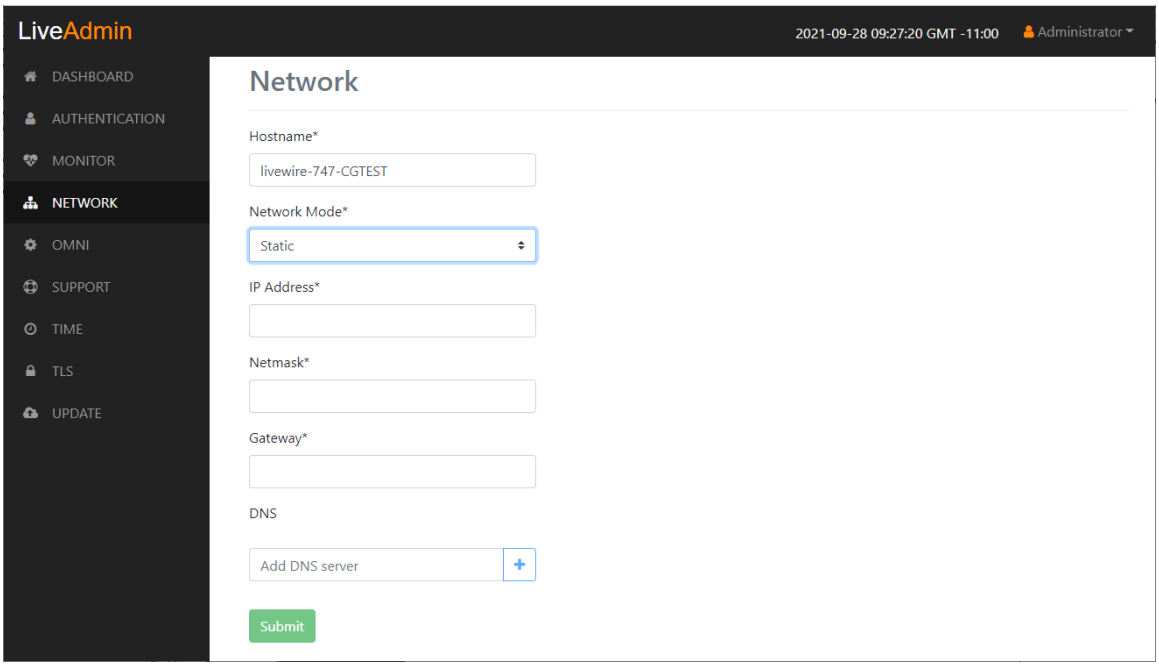


- *CPU Usage*: This chart displays the current usage of individual CPUs on the system. Click the CPU label in the legend to enable/disable its data displayed in the chart.
- *Memory Usage*: This chart displays the current amount of memory being consumed on the system. Click the *Total*, *Used*, or *Free* labels in the legend to enable/disable which data to display in the chart.
- *Network Usage*: This chart displays the current throughput of the network interfaces. Click the labels in the legend to enable/disable which data to display in the chart.
- *Disk Usage*: This chart displays the current amount of space being used by the Data and Metadata volumes. Click the *Total*, *Used*, or *Free* labels in the legend to enable/disable which data to display in the chart.
- *Interface Statistics*: This table displays the statistics of the primary management interface. To update the statistics click **Refresh**.

Network

The *Network* view lets you configure the primary network interface network settings and the hostname of the system. You can configure either DHCP or static network settings.

Note Changing the network settings will restart the omni service.



- *Hostname*: Enter a name for LiveWire Virtual. A unique device name allows for easy identification of data sources. The hostname can only contain alphanumeric characters and hyphens, and cannot be longer than 255 characters.
- *Network Mode*: This setting lets you to specify whether LiveWire Virtual uses a DHCP or static setting for its IP address. If *Static* is selected, then *IP Address*, *Netmask*, *Gateway*, and *DNS* settings can be configured for LiveWire Virtual. If *DHCP* is selected, then LiveWire Virtual is configured by a DHCP server.

Important! If DHCP is selected as the *IP Assignment*, and if the address should change on a new DHCP lease, then the user must look up the new IP address assigned to LiveWire Virtual. To help you look up the IP address, the MAC Address of LiveWire Virtual is displayed as the *Ethernet Address*.

- *IP Address*: This setting lets you specify the IP address that you are assigning to LiveWire Virtual.
- *Netmask*: A Netmask, combined with the IP address, defines the network associated with LiveWire Virtual.
- *Gateway*: Also known as 'Default Gateway.' When LiveWire Virtual does not have an IP route for the destination, the IP packet is sent to this address as it does not know how to direct it locally. Only a single default gateway can be defined.
- *DNS*: This is the domain name server. A Domain Name Server translates domain names (e.g., www.liveaction.com) into an IP address. To add a DNS server, enter the address of the server, and click the plus (**+**) icon. Multiple DNS name servers can be defined. You can also edit or delete any defined DNS servers.

Configure DHCP

To configure a DHCP IP address:

1. Enter a hostname in the *Hostname* field.
2. From the *Network Mode* list, select *DHCP*.

3. Click **Submit**.

Configure Static

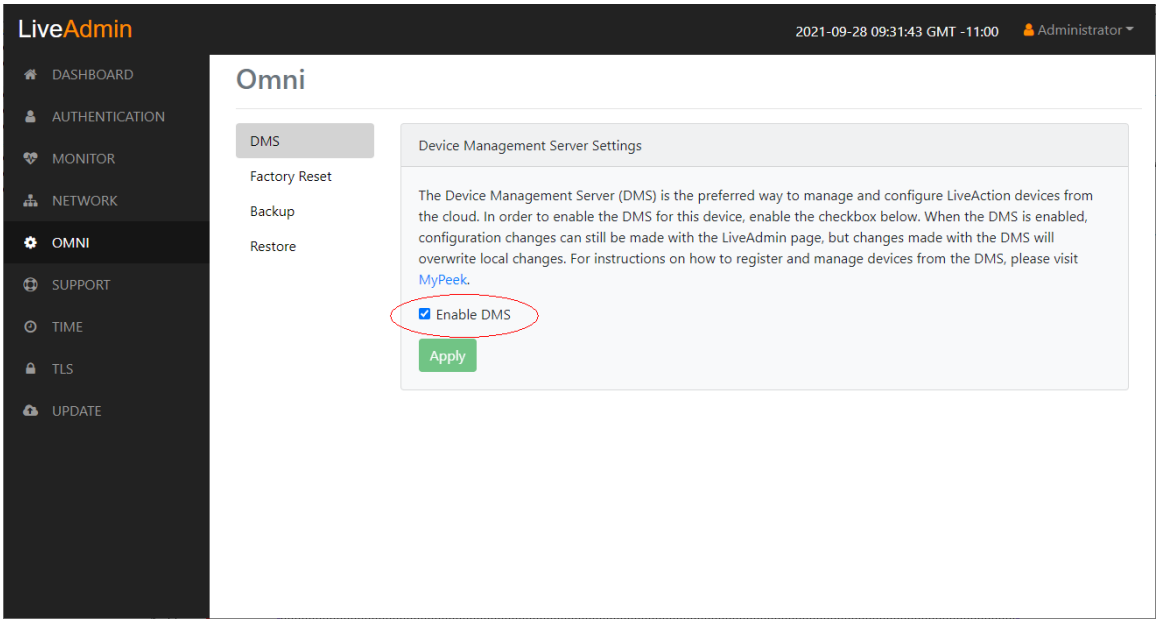
To configure a static IP address:

1. Enter a hostname in the Hostname field.
2. From the *Network Mode* list, select *Static*.
3. Enter a valid IP address in the *IP Address* field.
4. Enter a valid netmask in the *Netmask* field.
5. Enter a valid default gateway in the *Gateway* field.
6. (Optional) Enter a valid DNS server in the *Add DNS server* field and click the plus (**+**) button.
7. Click **Submit**.

> **Note** You will lose connection to LiveWire Virtual if you configured a new static address in *IP Address* above.

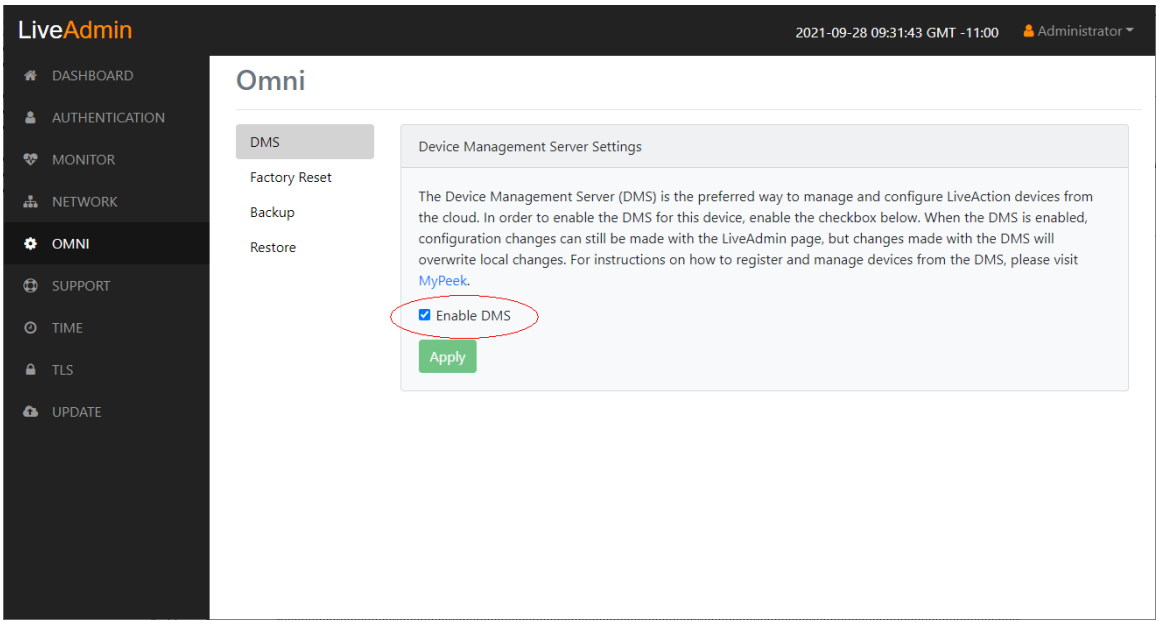
Omni

The *Omni* view lets you enable the Device Management Server (DMS) for the appliance, Backup, and Restore options.



DMS

The *DMS* (Device Management Server) is the preferred way to manage and configure LiveAction appliances from the cloud. In order to enable the DMS for LiveWire Virtual, enable the check box. When the DMS is enabled, configuration changes can still be made with the LiveAdmin utility, but changes made with the DMS will overwrite local changes. For instructions on how to register and manage devices from the DMS, please visit *MyPeek*.

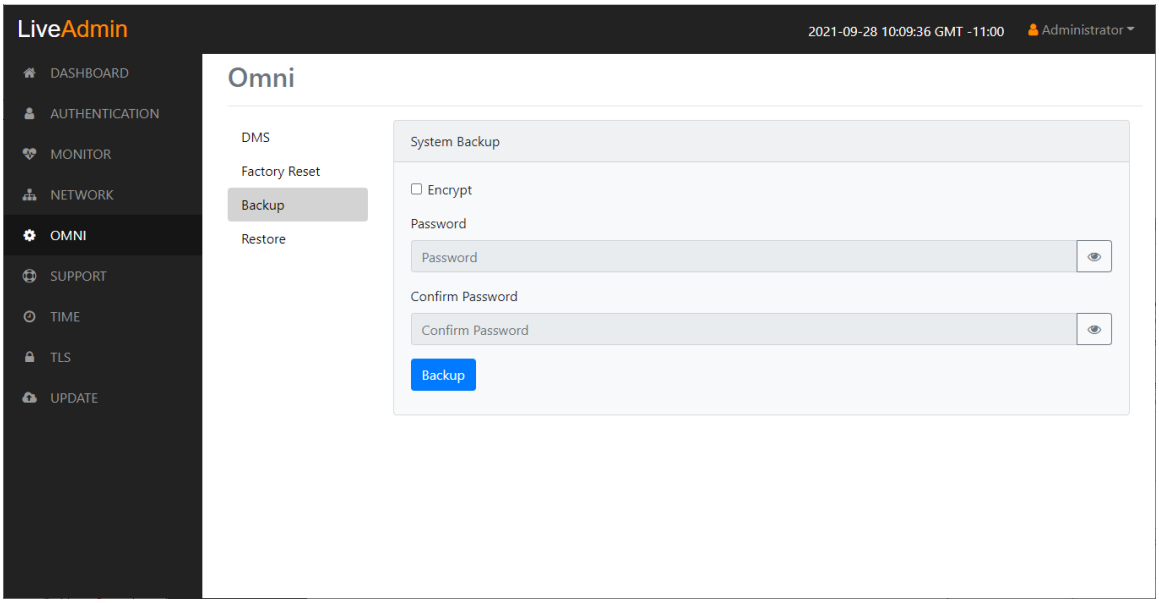


- *Enable DMS*: Select this check box to enable the DMS for LiveWire Virtual to manage and configure LiveWire Virtual from the cloud. See *Using DMS to manage and configure LiveAction appliances* on page 49.

Note When DMS is enabled, you can make local changes to LiveWire Virtual using the LiveAdmin utility; however, changes made with the DMS will overwrite any local changes made with the LiveAdmin utility.

Backup

Backup allows you to back up all the system data on LiveWire Virtual to a back up file that you can restore at a later time.

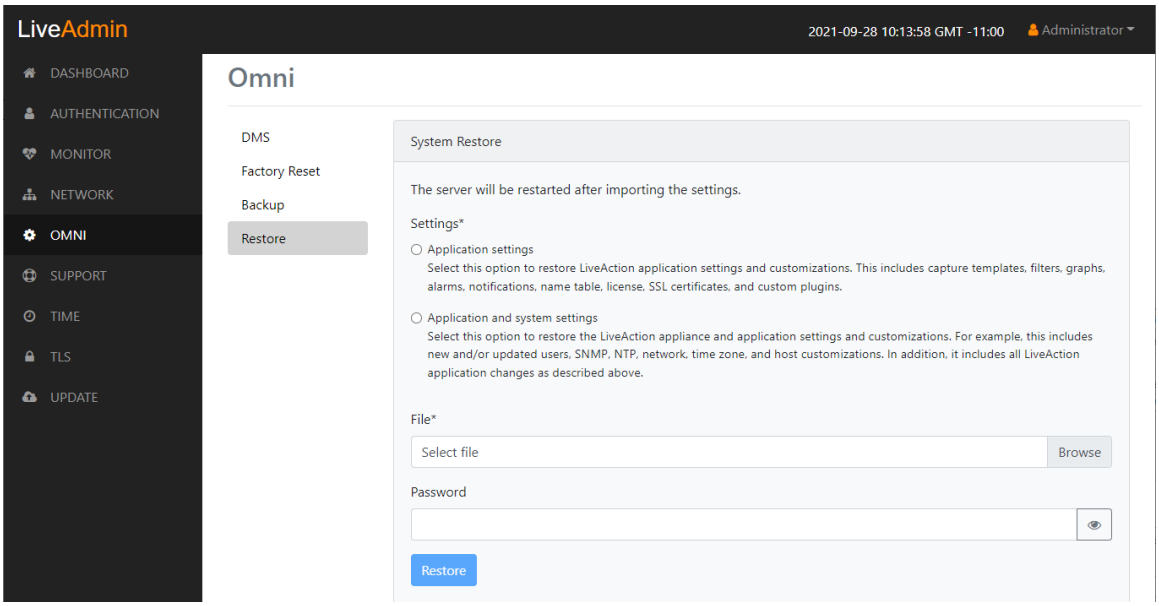


- *Encrypt*: Select this data to encrypt the system backup. You will need to enter a password that is required to restore the backup to LiveWire Virtual.
- *Password*: Type a password for the backup.

- *Confirm Password*: Type the password again to confirm the password.
- *Backup*: Click to start the backup.

Restore

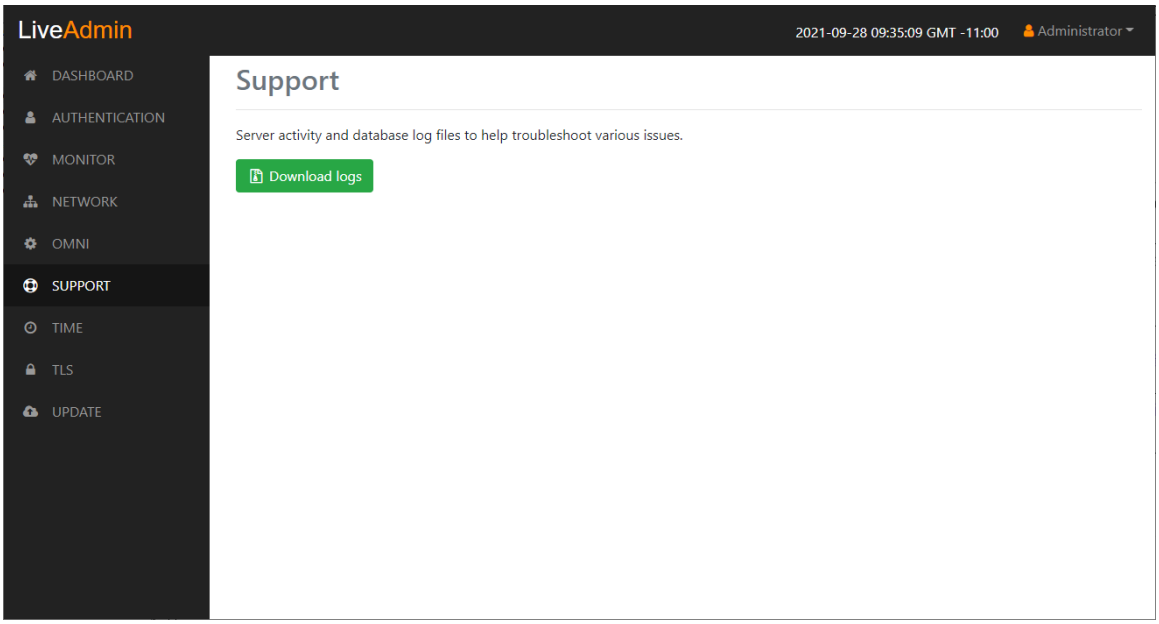
Restore allows you to restore to LiveWire Virtual a backup that was previously performed on LiveWire Virtual. To perform a restore, you will need the backup file you want to restore and any password associated with the backup.



- *Application settings*: Select this option to restore the appliance application settings and customizations.
- *Application and system settings*: Select this option to restore the appliance, application settings, and customizations.
- *File*: Click **Browse** to select the backup file you are restoring.
- *Password*: Enter the password for the backup you are restoring.
- *Restore*: Click to start the restore.

Support

The Support view lets you download logs from LiveWire Virtual that would be helpful in troubleshooting issues.



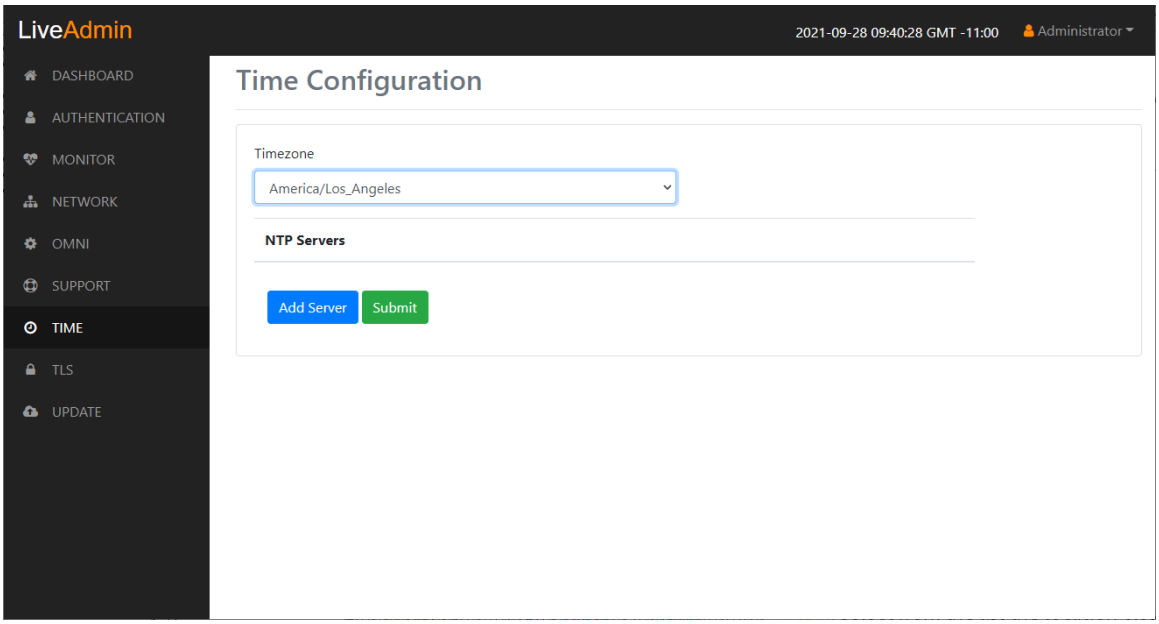
- *Download logs*: Click to download the *logs.tgz* file to your default location.

  The *log.tgz* file will consist of the following information and files:

  - */proc/mounts*
  - */proc/meminfo*
  - */proc/net/dev*
  - */var/log/auth.log*
  - */var/log/boot.log*
  - */var/log/dmesg*
  - */var/log/dms.log*
  - */var/log/dmsd.log*
  - */var/log/kern.log*
  - */var/log/live*
  - */var/log/liveflow*
  - */var/log/nginx*
  - */var/log/omniperf.log*
  - */var/log/omnitrace.log*
  - */var/log/routermap_to_interface.log*
  - */var/log/syslog*

Time

The *Time Configuration* view lets you configure the system's Timezone and NTP servers.

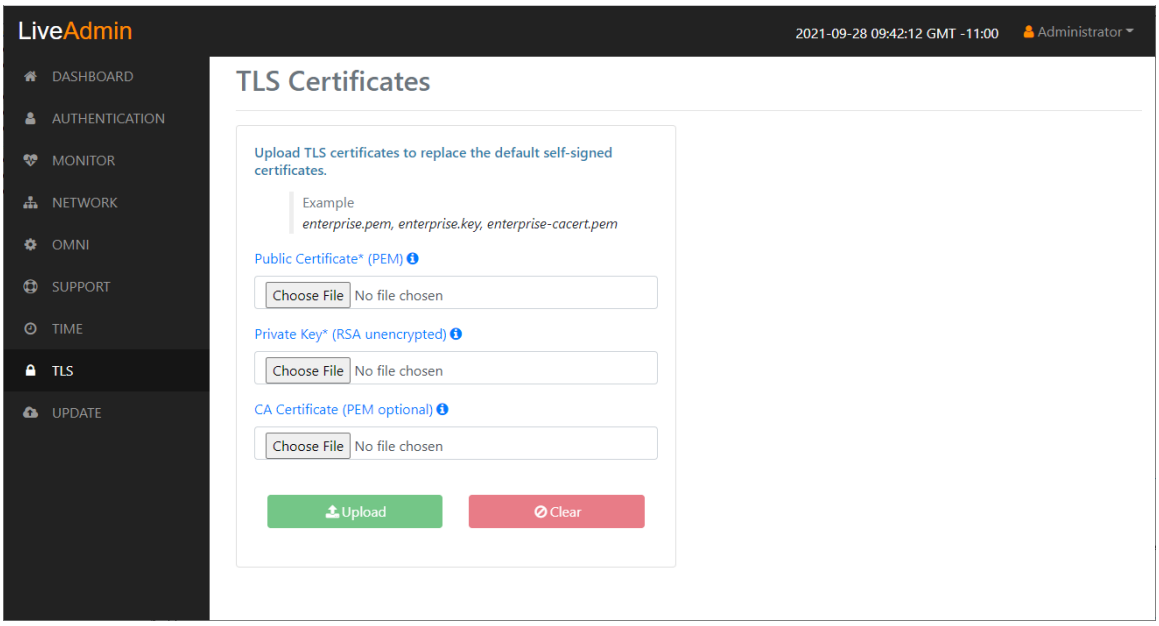


- *Timezone*: The Timezone setting lets you specify the physical location of LiveWire Virtual. Select from the list the location closest to your LiveWire Virtual.
- *NTP Servers*: The NTP (Network Time Protocol) server setting displays the NTP servers used to synchronize the clocks of computers over a network. Many features of LiveWire Virtual require accurate timestamps to properly analyze data.

  To synchronize the LiveWire Virtual clock, you can specify the IP address of an NTP server located on either the local network or Internet. Once an NTP server is added to LiveWire Virtual, you can update (edit) or delete a server displayed in the list.
- *Add Server*: Click to add a new NTP server to the list. Enter the IP address of the NTP server and click **Save** to save the server to the list. Multiple NTP servers can be defined.
- *Submit*: Click to save your changes to LiveWire Virtual.

TLS

The *TLS Certificates* view lets you change the self-signed certificates that Omnipeek and LiveAdmin use for HTTPS.

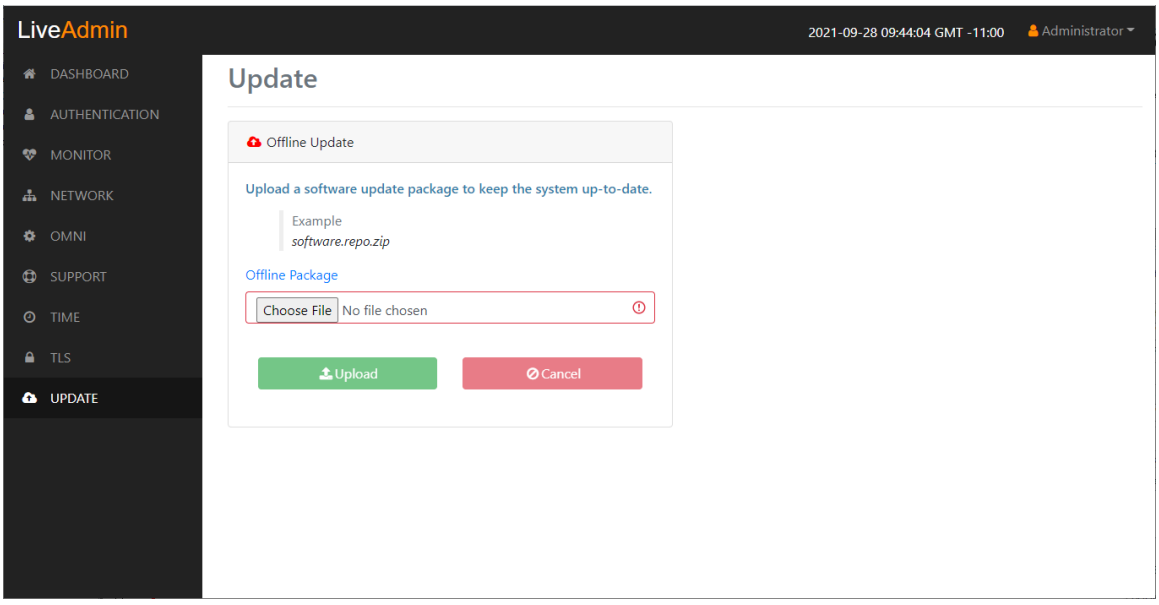


- *Public Certificate* (PEM)*: Click **Choose File** to browse and select your Public Certificate file. Click the information icon to display an example of the file.
- *Private Key* (RSA unencrypted)*: Click **Choose File** to browse and select your Private Key file. Click the information icon to display an example of the file.
- *CA Certificate (PEM optional)*: Click **Choose File** to browse and select your CA Certificate file. Click the information icon to display an example of the file.
- *Upload*: Click to upload the selected files to LiveWire Virtual.

Update

The Update view lets you update the appliance using the software update package.

Note Updating the software will cause the system to reboot.



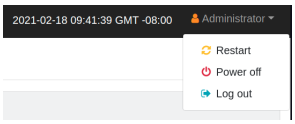
To update the software:

1. Download the latest software update package to your system.
2. Click **Choose File** and select the software update package.
3. Click **Upload** to upload the package and begin the update process.

   Once the update process is complete, the system restarts. A restart message is broadcast to all users connected to the appliance.

Restart and power off

The *Administrator* context menu at the top of the LiveAdmin utility has options that let you restart and power off LiveWire Virtual and log out from the utility.



To restart LiveWire Virtual:

1. Click the *Administrator* context menu and select **Restart**.
2. Click **Yes, restart now!** to confirm the restart.

To power off LiveWire Virtual:

1. Click the *Administrator* context menu and select **Power off**.
2. Click **Power Off** to confirm you want to power off.

To log out of the LiveAdmin utility:

- Click the *Administrator* context menu and select **Log out**.

Using DMS to manage and configure LiveAction appliances

If you have one or more LiveAction appliances, you can use the Device Management Server (DMS) to manage and configure these appliances from the cloud. In order to use the DMS server for the LiveAction appliance, you must first enable the *Enable DMS* option in the LiveAdmin utility as described in *Omni* on page 43.

Note When DMS is enabled, you can make local changes to the LiveAction appliance using the LiveAdmin utility; however, changes made with the DMS will overwrite any local changes made with the utility.

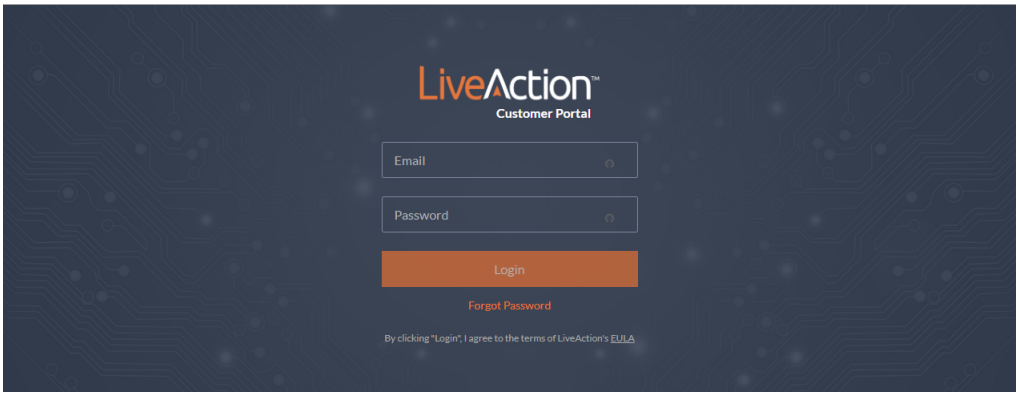
Note All DMS communications require that the LiveAction appliance has Internet access and is able to access various websites including *https://mypeek.liveaction.com* and *https://cloudkeys.liveaction.com* using TCP over port 443. If necessary, configure a DNS server to resolve the URLs above.

Additionally, all DMS communications are initiated by the LiveAction appliance, so it is not necessary to open a port in the firewall for communications.

To use DMS to manage and configure LiveAction appliances:

1. Log into the LiveAction Customer Portal at *https://cloudkeys.liveaction.com/*.

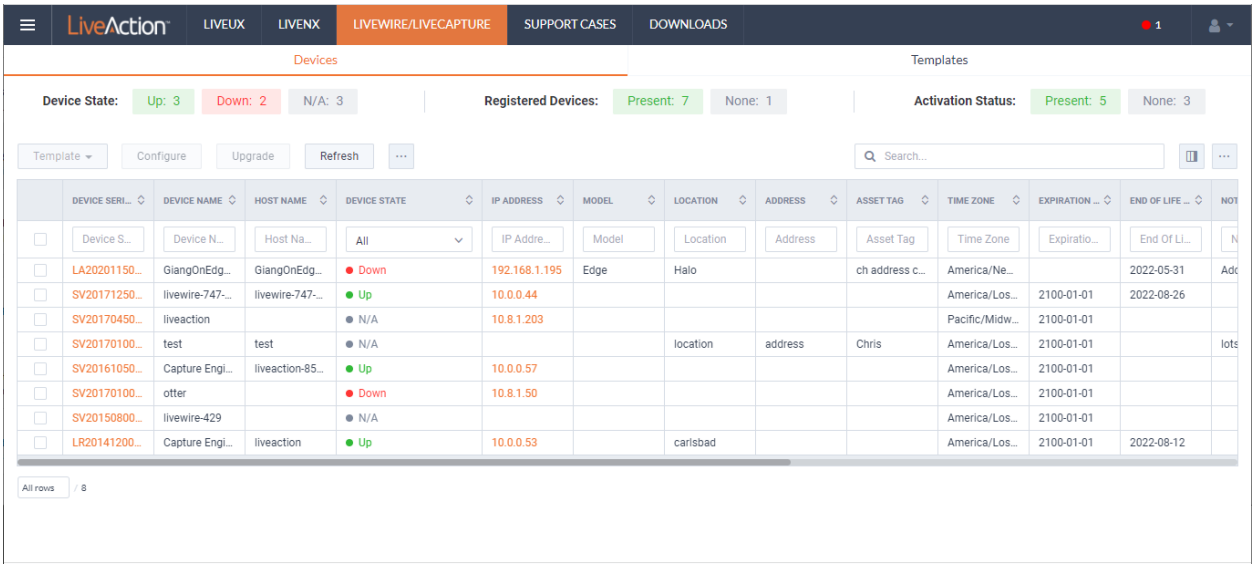
Note A link to the LiveAction Customer Portal and a temporary password is emailed to the customer whenever a LiveAction appliance is purchased. Use the customer email and temporary password to log into the customer portal. You will be required to change the temporary password upon first login.



2. Click the **LIVEWIRE/LIVECAPTURE** tab at the top of the portal to configure the appliances. The LiveAction appliances associated with the user account are displayed.

DMS Devices tab

The DMS Devices tab displays the LiveWire Virtual devices associated with user's account. A description of each of the available options and settings in the *Devices* tab is provided below:



Device State

The *Device State* displays whether the device is able to connect to the DMS portal.

- *Up*: Displays the number of devices that were able to connect the DMS portal.
- *Down*: Displays the number of devices the DMS portal has not heard from in the last two intervals. The default interval is 10 minutes.
- *N/A*: Displays the number of devices that are not available to the DMS portal.

Registered Devices

The *Registered Devices* displays the number of devices that have registered with the DMS portal.

- *Present*: Displays the number of devices that have registered with the DMS portal.
- *None*: Displays the number of devices that have not registered with the DMS portal.

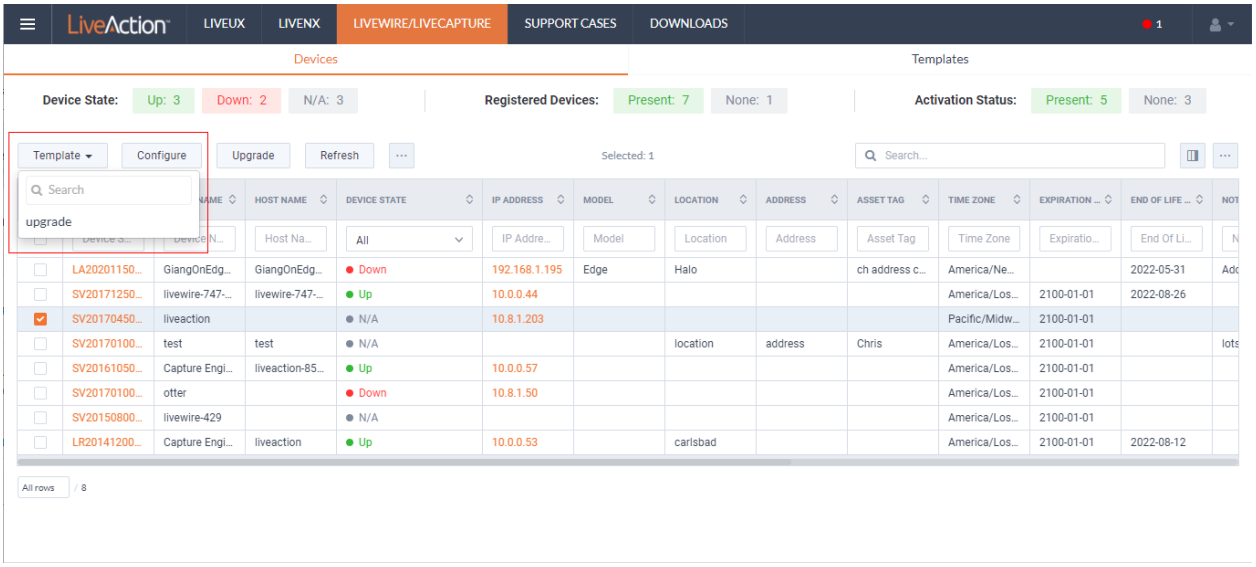
Activation Status

The *Activation Status* displays the number of devices that have been activated.

- *Present*: Displays the number of devices that have been activated with the DMS portal.
- *None*: Displays the number of devices that have not been activated with the DMS portal.

Template

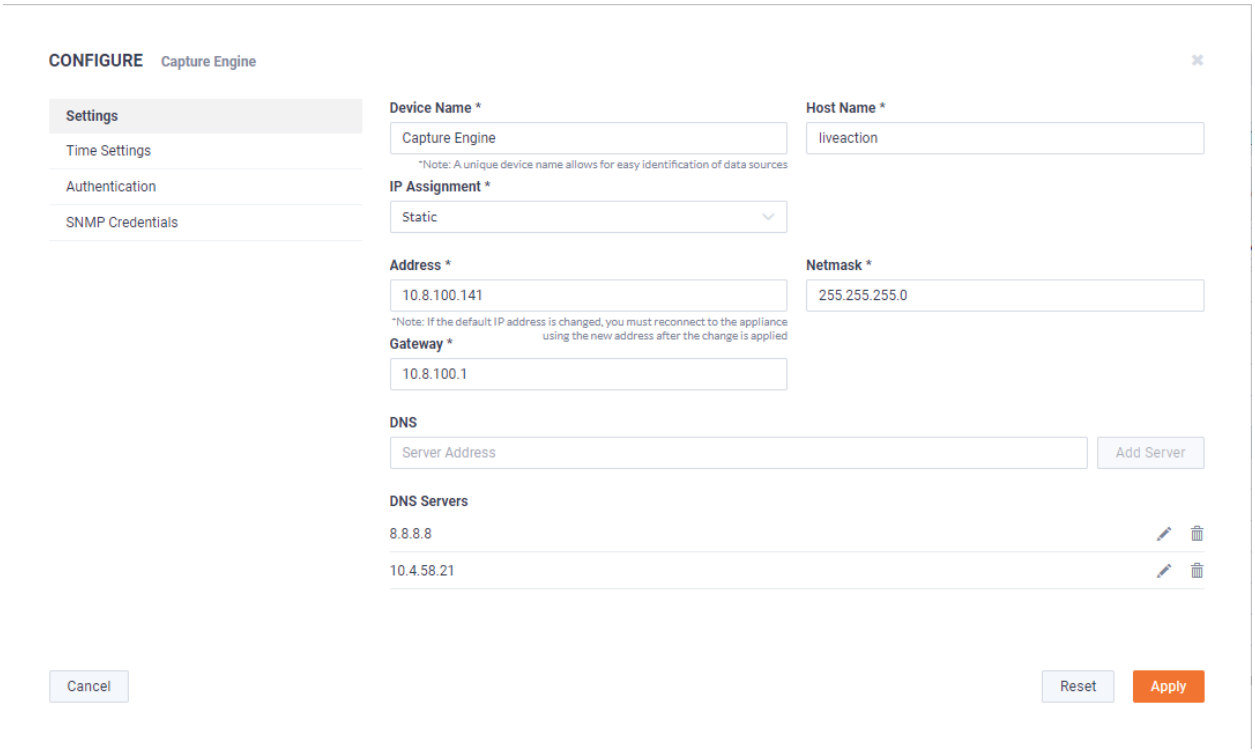
Click the **Template** button to select a template to apply to the selected devices. Templates allow you to apply version-specific settings to one or more devices. To create a template or modify an existing template, see *DMS Templates tab* on page 66.



Configure

Click the *Configure* button to configure the selected devices. If multiple devices are selected, certain configuration options will not be available and greyed out; for example, the *Device Name*. There are tabs available for configuring *Settings*, *Time Settings*, and *Authentication*.

Settings



- *Device Name*: Displays the unique name given to the device. Type a new name to change the name.
- *Host Name*: Displays the host name of the device used by DNS. Type a new name to change the name.
- *IP Assignment*: Displays the current IP assignment for the device. You can select either *DHCP* or *Static*. If the IP Assignment is *DHCP*, then the IP assignment is configured automatically via the DHCP server. If the IP Assignment is *Static*, then the options below are available:

Important! LiveWire Virtual is pre-configured to obtain an IP address automatically from a DHCP server; however, we strongly recommend the use of a static IP address for LiveWire Virtual. If DHCP is selected as the *IP Assignment*, and if the address should change on a new DHCP lease, then the user must look up the new IP address assigned to LiveWire Virtual.

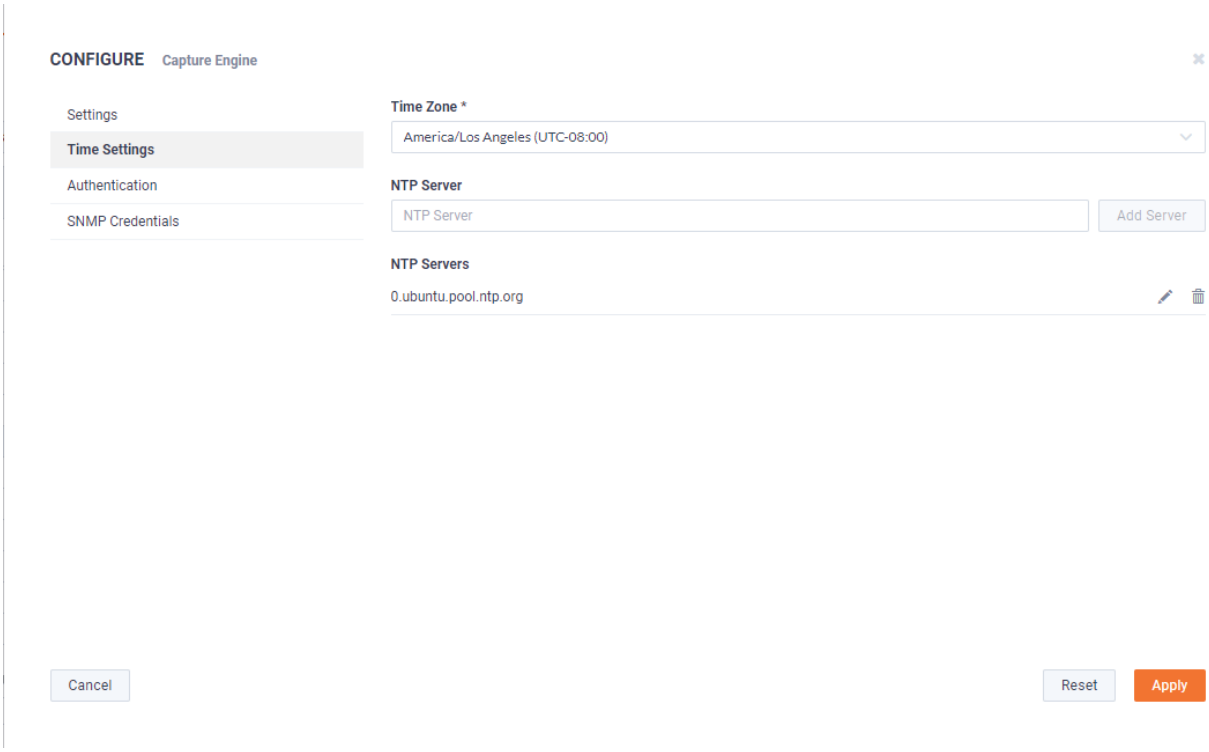
Note If *DHCP* is selected, you have approximately two minutes to connect LiveWire Virtual to your network in order for the DHCP server to assign an IP address. If an IP address is not assigned to LiveWire Virtual by the DHCP server within two minutes of being connected to the network, LiveWire Virtual defaults to a static address of 192.168.1.21. Please make sure LiveWire Virtual is connected to your network within the two minute time period from the time you click **Apply**. If you reboot LiveWire Virtual, the two minute clock is also reset.

- *Address*: Displays the IP address assigned to the device. Type a new address to change the IP address.
- *Netmask*: Displays the netmask address assigned to the device. A netmask address, combined with the IP address, defines the network associated with device. Type a new address to change the netmask address.
- *Gateway*: Displays the gateway address, also known as 'default gateway,' assigned to the device. When the device does not have an IP route for the destination, the IP packet is sent to this address as it does not know how to direct it locally. Only a single default gateway can be defined. Type a new address to change the gateway address.

- *DNS*: Enter the address of any DNS (Domain Name Server) servers to add to the configuration. A Domain Name Server translates domain names (e.g., www.liveaction.com) into an IP address. To add a DNS server, enter the address of the server, and click **Add Server**. Multiple DNS name servers can be defined. You can also edit or delete any defined DNS servers.
- *Add Server*: Click to add the DNS server to the configuration.
- *DNS Servers*: Displays the DNS servers added to the configuration.
- *Edit DNS*: Click to edit or update the DNS server in the configuration.
- *Delete DNS*: Click to delete the DNS server from the configuration.

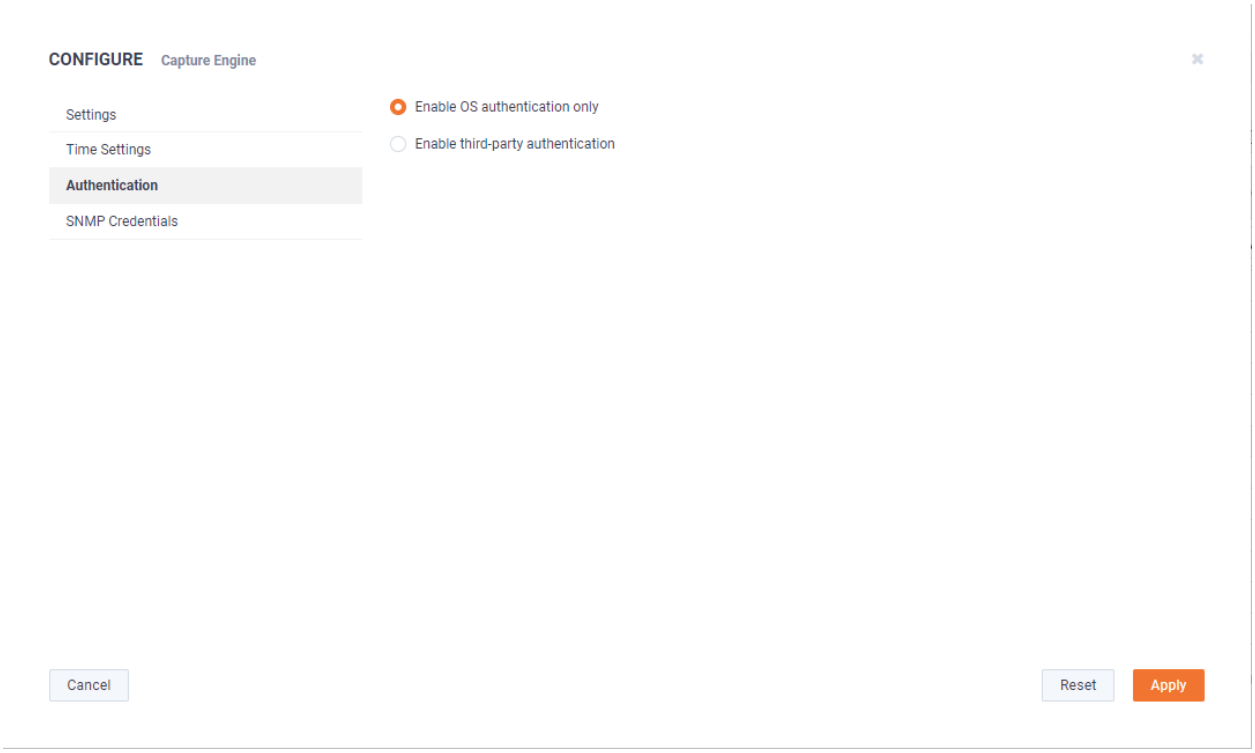
- *DHCP Timeout*: Displays the amount of time (in seconds) the device will wait for a DHCP address.

Time Settings



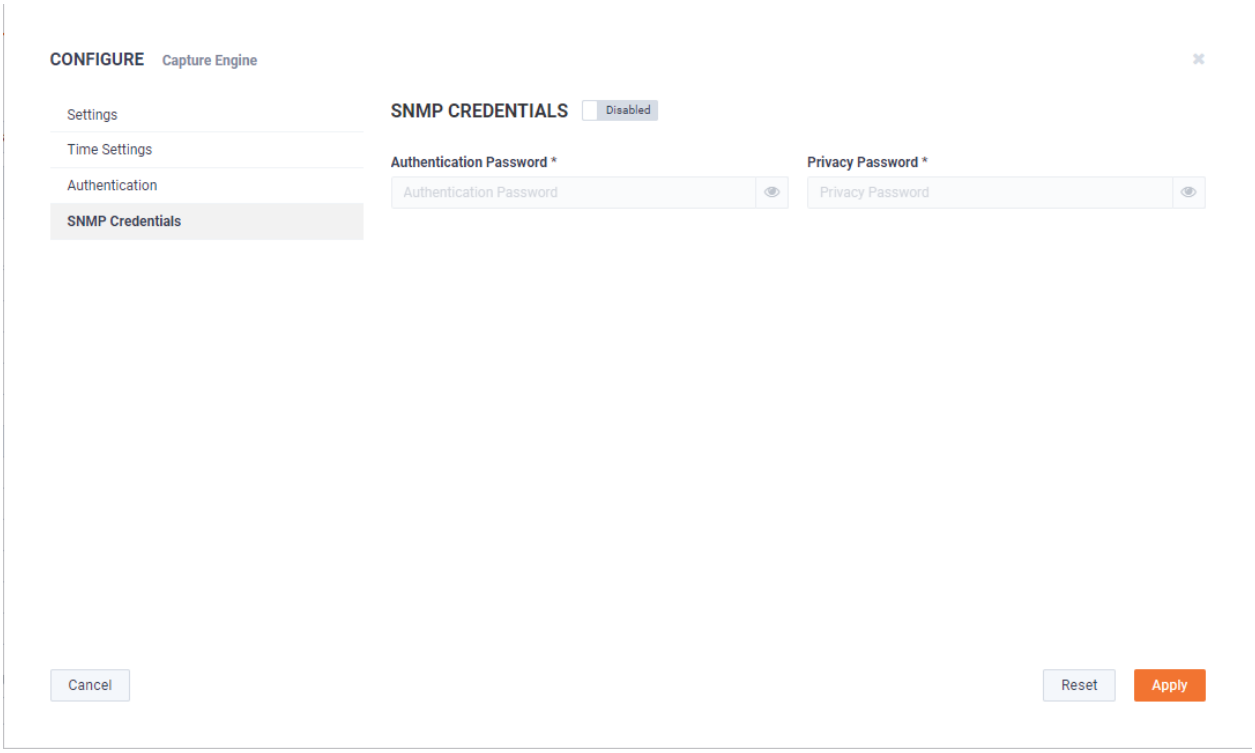
- *Time Zone*: Displays the time zone of the device. Select a different time zone to change the time zone.
- *NTP Server*: Enter the address of any NTP servers to add to the configuration, and then click **Add Server**.
- *NTP Servers*: Displays the list of NTP servers added to *Time Settings*. You can click the **Edit** icon to edit an NTP server in the list, or click the **Trash** icon to remove an NTP server from the list.

Authentication



- *Enable OS authentication only*: Select this option to use the local OS authentication.
- *Enable third-party authentication*: Select this option to use TACACS+ or RADIUS authentication. If this option is selected, click **Add** to configure the new authentication setting.
  - *Add*: Click to add a new authentication setting. You will need to configure the new authentication setting.
  - *Search*: Enter the text string to search the list of authentication settings.
  - *Name*: Displays the name of the authentication setting.
  - *Type*: Displays the type of authentication, which can be either 'RADIUS' or 'TACACS+.'
  - *Host*: Displays the host of the authentication setting.
  - *Port*: Displays the port of the authentication setting.
  - *Secret*: Displays the secret key of the authentication setting.
  - *In Use*: Displays whether or not the authentication setting is in use.
  - *Action*: Click the *Edit* icon to edit the authentication setting, or click the *Trash* icon to delete the authentication setting.
  - *Apply*: Click to save the authentication setting.

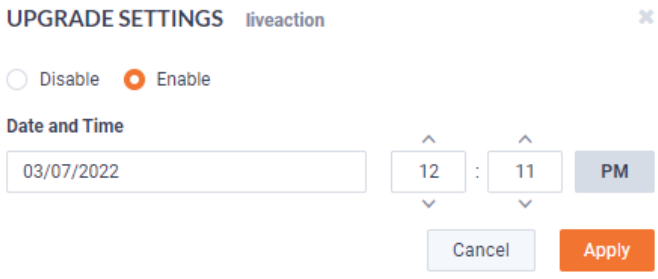
SNMP Credentials



- *Enabled/Disabled*: Select to enable or disable the *SNMP Credentials* configured below for the *Authentication Password* and *Privacy Password*.
- *Authentication Password*: Type a new *Authentication Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in *LiveFlow* on page 87.
- *Privacy Password*: Type a new *Privacy Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in *LiveFlow* on page 87.

Upgrade

Click the **Upgrade** button to upgrade the selected appliance remotely through the DMS. The version that the appliance is upgraded to is the latest shipping version of the appliance. There is no capability to upgrade to a previously released version.



- *Disable*: Select to disable the upgrade on the selected devices.
- *Enable*: Select to enable the upgrade on the selected devices. If you enable the upgrade, you are presented with settings to specify the date and time the upgrade should take place. Because all communications are initiated from the device once every ten minutes, the upgrade will happen as the result of the device communicating with the network, sometime on or after the selected time.

- *Apply*: Click to save the changes to the selected devices.

Refresh

Click the **Refresh** button to refresh the list of devices.

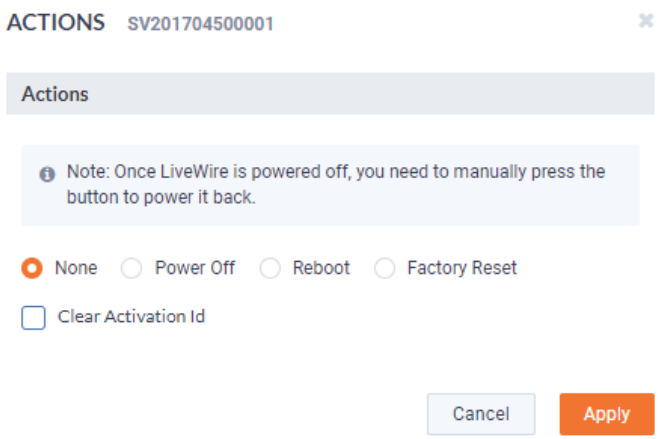
Elipsis (...)

Click the **Elipsis** (...) to view the following options:

- Power and Reset
- Change Password
- Edit Additional Info
- Backup Settings
- Restore Backup
- Share
- Create Template
- Compare Configurations
- iDRAC Settings

Power and Reset

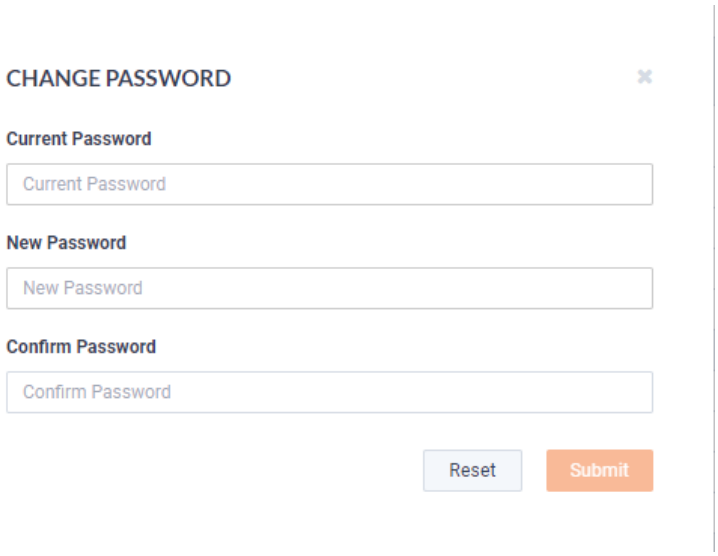
Select the *Power and Reset* option to perform the actions below on the device.



- *None*: Select to not perform an action on the selected appliances.
- *Power Off*: Select to power off the selected device. Once the device is powered off, you must manually press the power-on button on each of the devices to power them back on.
- *Reboot*: Select to reboot the selected appliances.
- *Factory Reset*: Select to reset the selected appliances to their factory default settings.
- *Clear Activation ID*: Select the check box to clear the activation ID.

Change Password

Select the *Change Password* option to change the password of the selected devices.

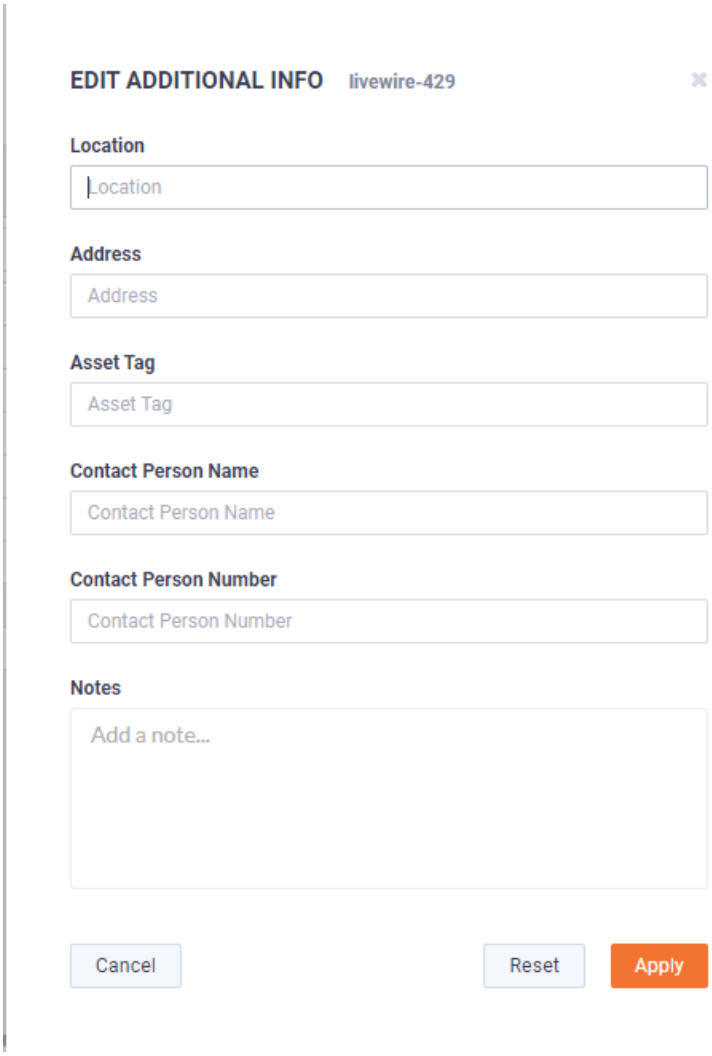


- *Current Password*: Enter the current password.
- *New Password*: Enter the new password. The new password must meet the following requirements:

  Must have 5 different characters than the last password.
  Must be at least 6 characters.
  Must contain at least 1 number
  Must contain at least 1 uppercase character.
  Must contain at least 1 lowercase character.
  Must contain at least 1 special character.
- *Confirm Password*: Enter the new password again.

Edit Additional Info

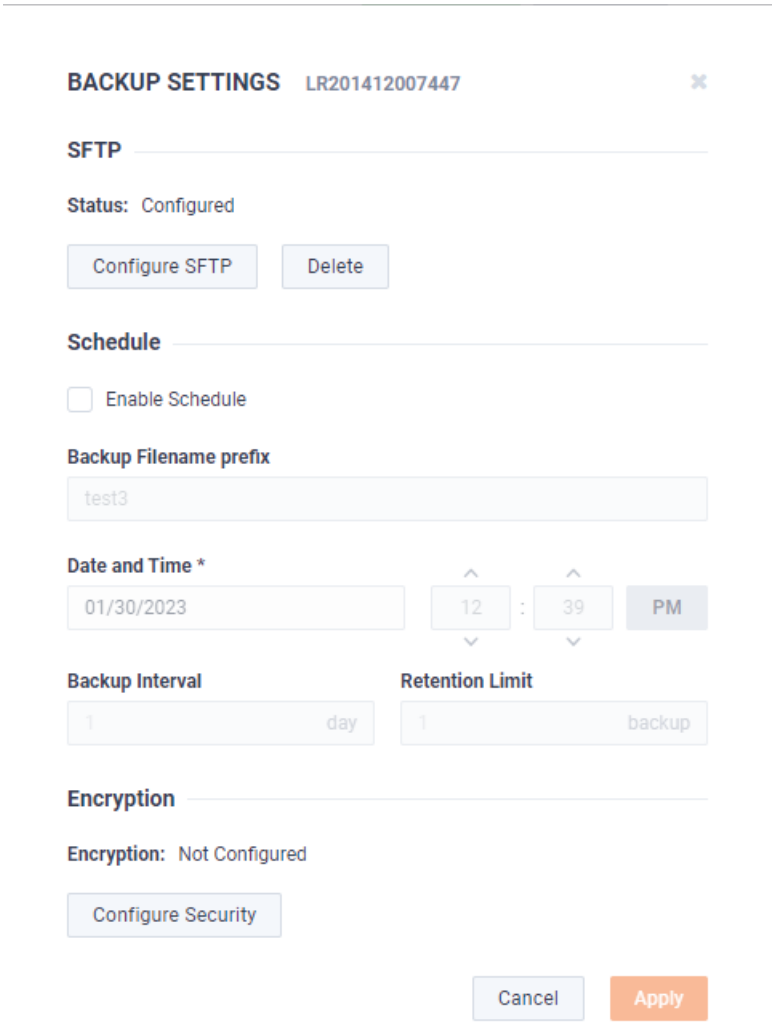
Select *Edit Additional Info* to edit various settings of the selected devices.



- *Location*: Displays the general location of the device. Type a new location to change the location. We suggest entering the physical location of the device for the organization. For example, 'Office.'
- *Address*: Displays the mailing address of the device. For example, 123 Main St., New York, NY. Type a new address to change the address.
- *Asset Tag*: Displays the asset tag of the device. Type a new asset tag to change the asset tag.
- *Contact Person Name*: Displays the contact person of the device. Type a new name to change the contact person.
- *Contact Person Number*: Displays the phone number of the contact person. Type a new number to change the phone number.
- *Notes*: Displays any notes for the device. Type any new notes to update the notes.
- *Reset*: Click to clear the *Edit Additional Info* values.
- *Apply* Click to apply the additional info to the device.

Backup Settings

Select *Backup Settings* to set up and configure a backup for the selected device. See *Backup and restore* on page 75 for instructions on performing an actual backup.



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *Hostname*: Type the IP address of the SFTP server.
  - *Port*: Type the port used for the SFTP Server.
  - *Username*: Type a username.
  - *Password*: Type a password for the SFTP server.
  - *Directory*: Type the directory where backups are saved on the SFTP server.
- *Delete*: Click to delete the configured SFTP server for the backup.

Schedule

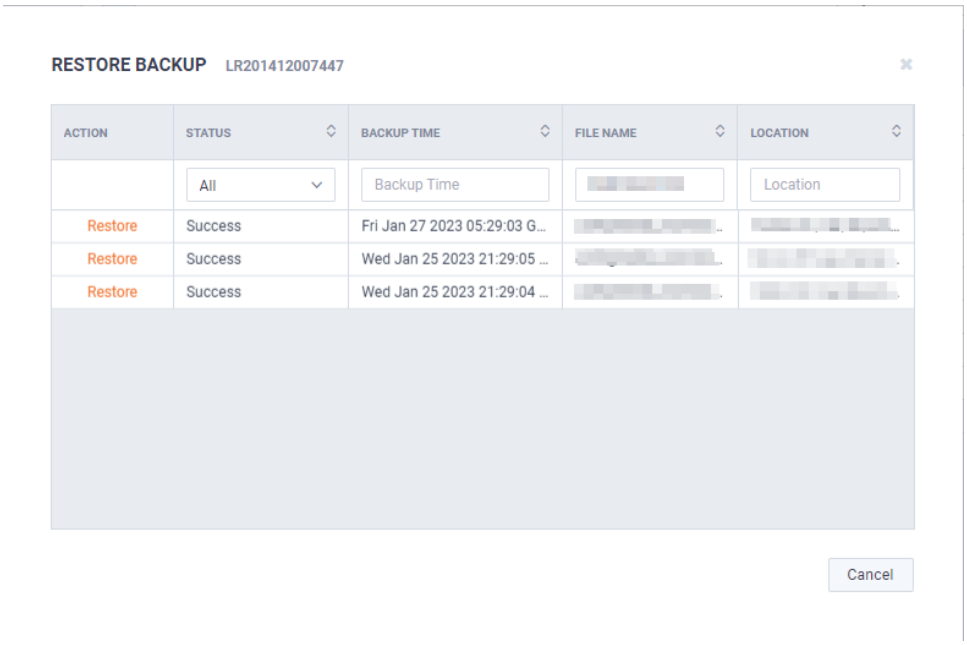
- *Enable Schedule*: Click to enable scheduling for the backup.
- *Backup Filename prefix*: Type a prefix filename for the backup. Each scheduled backup that is created will append the prefix to the beginning of the backup filename.
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between YADA.
- *Retention Limit*: Type the number backups to YADA.

Encryption

- *Encryption*: Displays whether or not encryption is configured for each scheduled backup.
- *Configure Security*: Click to configure security settings to encrypt each scheduled backup.
  - *Encrypt backups*: Select this option to encrypt each scheduled backup.
  - *Password*: Type the password to YADA. The password must be YADA
  - *Repeat Password*: Tye the password again to verify the password.

Restore Backup

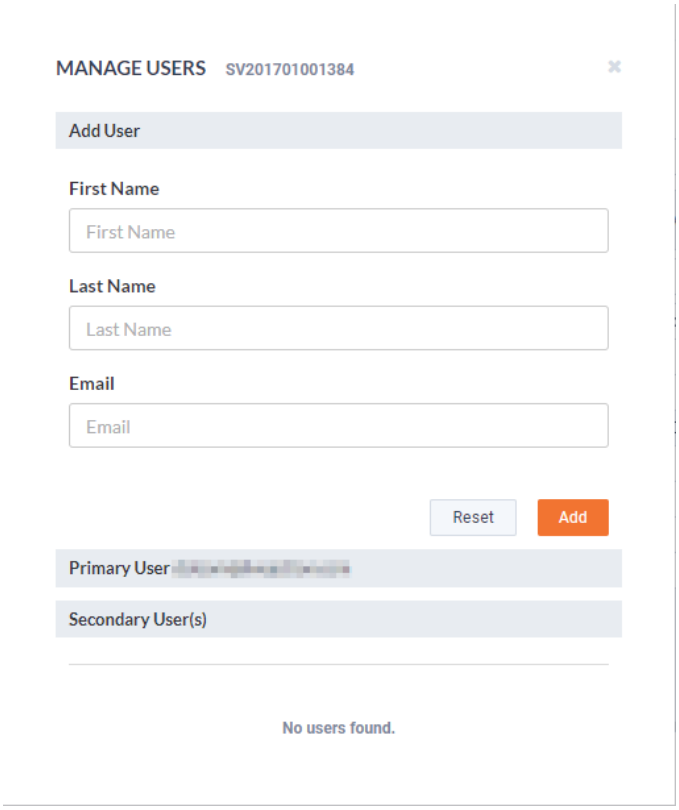
Select *Restore Backup* to restore a backup from an earlier backup. See *Backup and restore* on page 75 for instructions on performing an actual restore.



- *Action*: Click **Restore** to restore a backup for the device. You will need to select to restore either *Application Settings* or *Application and System Settings*.
  - *Application Settings*: Select this option to restore all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins. .
  - *Application and System Settings*: Select this option to restore all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins. Additionally, all system settings are restored and include all new and/or updated users, SNMP, NTP, network, time zone, and host customizations.
  - *Password*: Type the password of the backup you are restoring.
  - *Restore*: Click to perform the restore.
- *Status*: Displays the status of the backup.
- *Backup TIme*: Displays the date and time the backup was completed
- *File Name*: Displays the name of the backup.
- *Location*: Displays the location of the backup.

Share

Select the *Share* option to share the selected devices with other users who manage and configure appliances. You will need to add a user by completing the *Manage Users* dialog.



- *First Name*: Type the first name of the user.
- *Last Name*: Type the last name of the user.
- *Email*: Type the email address of the user.
- *Reset*: Click to clear the *Add User* values.
- *Add*: Click to add the user to the list of secondary users.
- *Primary User*: Displays the primary user of the device when the device was registered with LiveAction. If multiple appliances are selected in the list of devices, the *Primary User* is not displayed.
- *Secondary User(s)*: Displays any secondary users assigned to the device. If multiple appliances are selected in the list of devices, the *Secondary User(s)* are not displayed.

Create Template

Select the *Create Template* option to create a template based on the configuration of the selected device. Once created, the template can be selected when you click the **Template** button. See also *Template* on page 51 and *DMS Templates tab* on page 66.

Compare Configurations

Select the *Compare Configurations* option to compare details between two selected devices. This option is available only when two devices are selected.

iDRAC Settings

Select the *iDRAC Settings* option to configure various options for LiveWire Virtual that would normally be configured by using the iDRAC utility on LiveWire Virtual. See also *Integrated Remote Access Controller (iDRAC)* on page 69.

Note Only selected options available from the iDRAC utility are available and configurable below.

- *Hostname*: Displays the *Hostname* of the device. Type a new *Hostname* to change it.
- *Domain Name*: Displays the *Domain Name* of the device. Type a new *Domain Name* to change it.
- *Time Zone*: Displays the *Time Zone* of the device. Select a new *Time Zone* to change it.
- *DNS Server 1*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *DNS Server 2*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *Web Server TLS Version*: Displays the TLS protocol version support used by the device. You can select from the following: TLS 1.1 and Higher, TLS 1.2 and Higher, and TLS 1.3
    - *Host Header Check*: Select to enable *Host Header Check* requests.

Network Settings:

- *NIC IP Address*: Displays the static *NIC IP Address* of the device. Type a new *NIC IP Address* to change it.
- *NIC Gateway*: Displays the *NIC Gateway* of the device. Type a new *NIC Gateway* to change it.
- *NIC Subnet Mask*: Displays the *NIC Subnet Mask* of the device. Type a new *NIC Subnet Mask* to change it.

Authentication:

- *Username*: Displays the *Username* of the device. Type a new *Username* to change it.
- *Password*: Configures the *Password* of the device. Type a new *Password* to change it.

Update Settings:

- *Enable Updates*: Select to enable updates on the device. If enabled, you must configure the Update Proxy Server, Update Proxy User, and Update Proxy Password.
- *Update Proxy Server*: Displays the *Update Proxy Server* of the device. Type a new *Update Proxy Server* to change it.
- *Update Proxy User*: Displays the *Update Proxy User* of the device. Type a new *Update Proxy User* to change it.
- *Update Proxy Password*: Displays the *Update Proxy Password* of the device. Type a new *Update Proxy Password* to change it.

SNMP:

- *Enable SNMP*: Select to enable the SNMP Agent on the iDRAC. If enabled, you must configure the *SNMP Community.*
    - *SNMP Community*: Configures the *SNMP Community* name used for SNMP Agents. Type a new *SNMP Community* name to change it
- *Enable SNMP Alert 1*: Select to enable the *SNMP Alert 1* on the iDRAC. If enabled, you must configure the *Alert 1 Target Address*.
    - *Alert 1 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.
- *Enable SNMP Alert 2*: Select to enable the *SNMP Alert 2* on the iDRAC. If enabled, you must configure the *Alert 2.* If enabled, you must configure the *Alert 2 Target Address*.
    - *Alert 2 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.

NTP:

- *Enable NTP*: Select to enable an *NTP* server on the iDRAC. If enabled, you must configure the *NTP Server*.

- *NTP Server*: Displays the name or IP address of the *NTP Server*. Type a new name or IP address to change it.

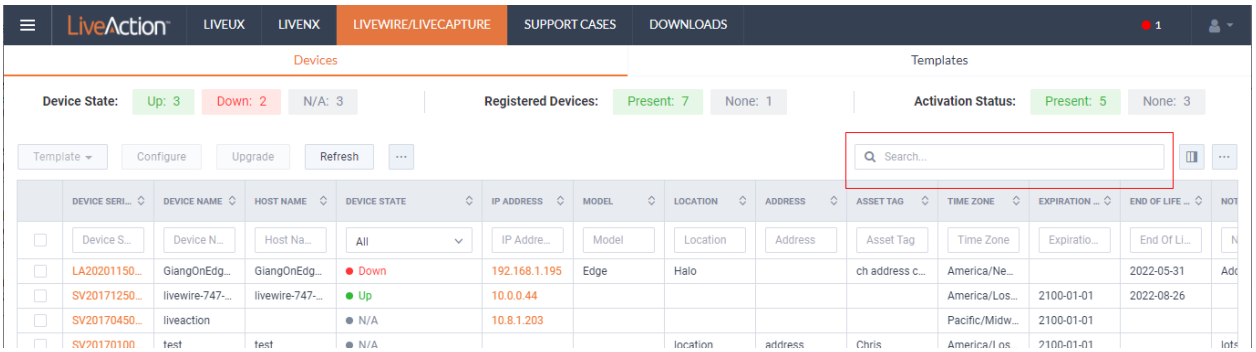
Event Filters:

- *Alert*: Displays any iDRAC Event filters configured for the device.
- *Add*: Click to add a new Event filter configured in the text box. You must provide any parameters by defining what you want to be alerted to and how you want to be notified. You can configure as may event filter commands as you want. The general format of an alert category:

  idrac.alert.category.[subcategory].[severity]

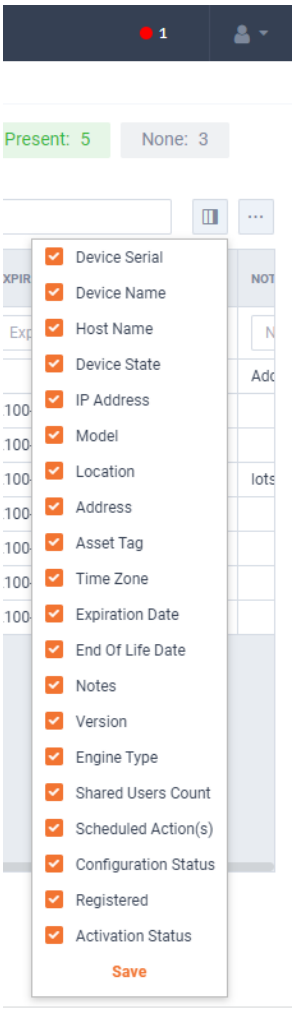
Search

Use the *Search* field to locate a specific device in the list of devices. Simply enter a text string to display all appliances that match the text string.



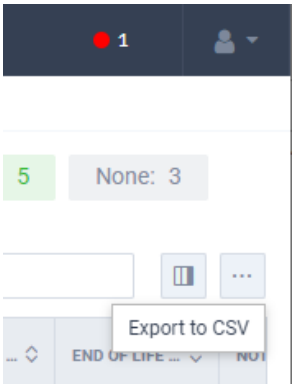
Display Columns

Click the **Display Columns** icon and then select the columns you want to display in the list of devices.



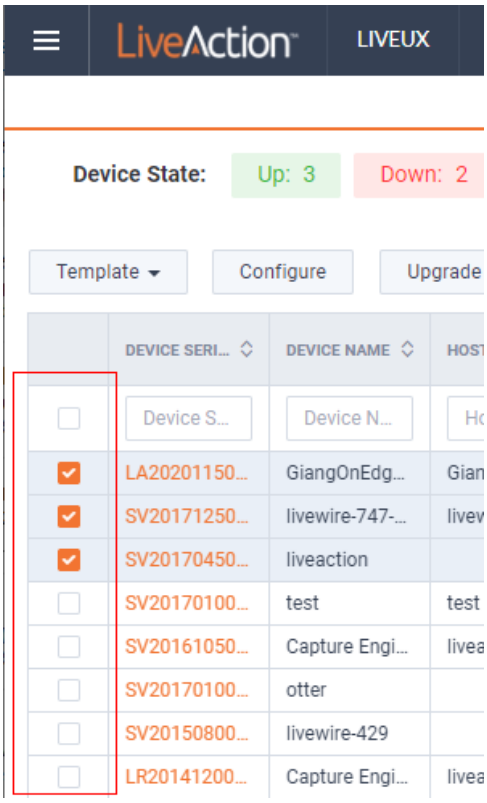
Export to CSV

Click the **Export to CSV** icon (...) to display an option for exporting the list of devices to a *.csv* file.



Check Box

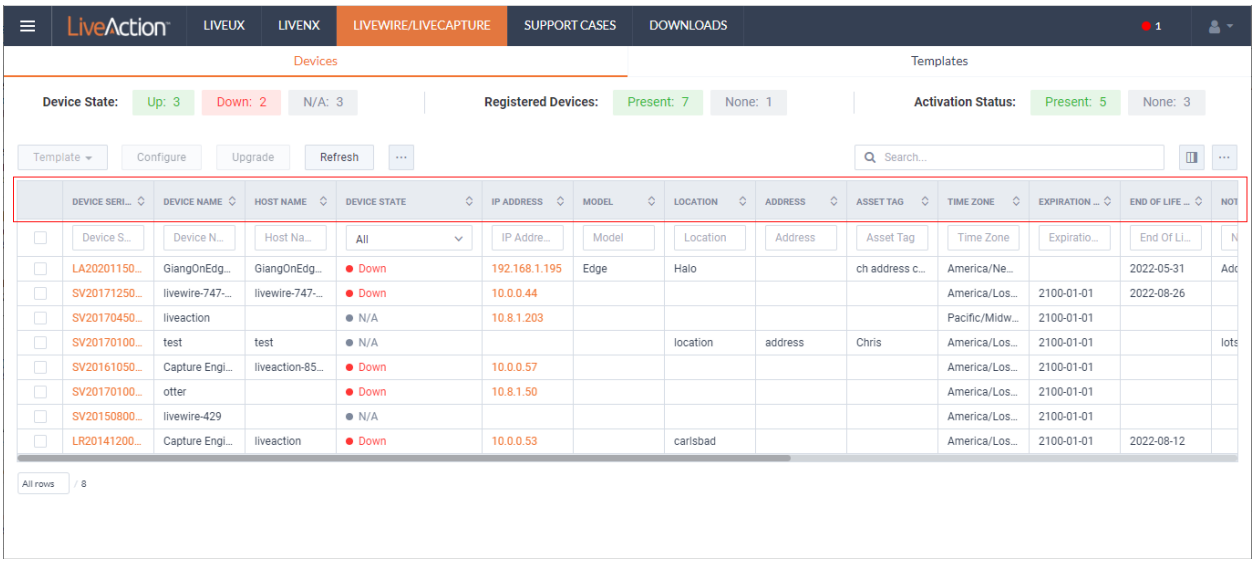
To select a device in the list of devices, select the check box of the desired devices. Selecting the check box at the top of the column allows you to select or clear the check boxes of all devices in the list of devices.



Devices column headings

Descriptions of the columns displayed in the list of devices are provided below.

Tip Below each of the column headings is either a text box or list box that you can use to filter the devices displayed in the list of Devices. To filter using the text box, simply enter a text string to display the devices that match the text string. To filter using a list box, click the box and select an option to display the devices that match that option.

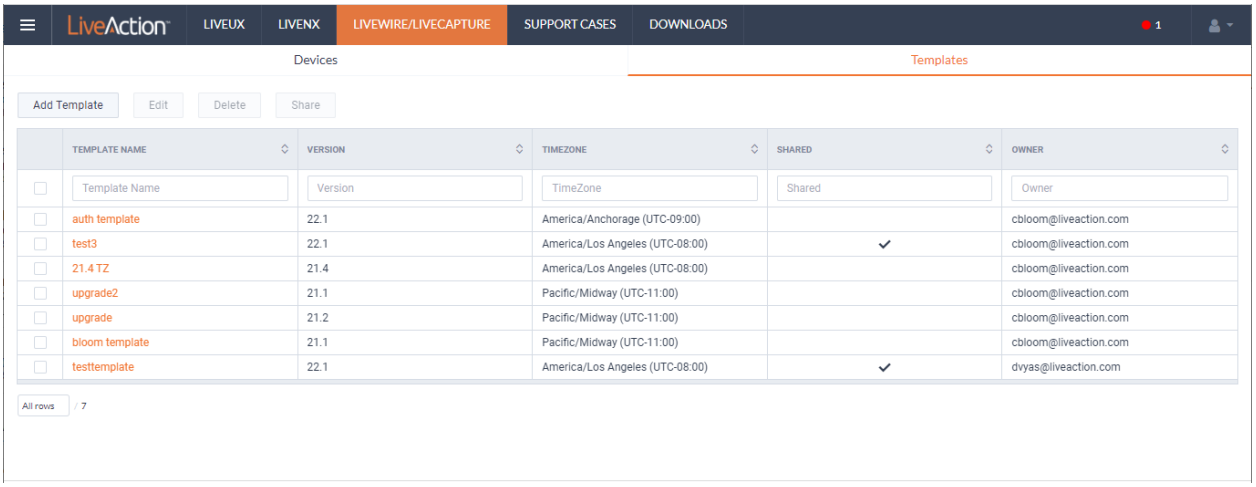


- *Device Serial*: Displays the serial number of the device.
- *Device Name*: Displays the name of the device.
- *Host Name*: Displays the host name of the device used by DNS.

- *Device State*: Displays whether the device is *Up* or *Down*. A device is up if it has contacted the DMS in the last 25 minutes.
- *IP Address*: Displays the IP address of the device. The *IP Address* value is a link which can be used to connect directly to Omnipeek running on the device. This makes it easy to use the DMS as a launch pad to access all of the devices being managed. It can also be used to discover the *IP Address* in the case where the device is set to DHCP, or for some other reason the *IP Address* is not known. The *IP Address* is provided by the device every time the device connects back to the portal, which by default is every 10 minutes. This way, if the *IP Address* of the device changes, the *IP Address* value displayed in the DMS portal will reflect that.
- *Model*: Displays the model of the device (*Edge*, *1100*, *3100*, or *Virtual*).
- *Location*: Displays the location of the device.
- *Address*: Displays the address of the device. Typically, this is the mailing address where the device is located.
- *Asset Tag*: Displays the asset tag of the device.
- *Time Zone*: Displays the time zone of the device.
- *Expiration Date*: Displays the date that the maintenance on the device will expire. Once the expiration date has passed, you can still access the DMS and use it to manage most of the device configuration; however, until the maintenance is renewed, the device cannot be upgraded to a newer version. As LiveAction releases new versions a few times a year with significant improvements, we recommend keeping the devices up to date with the latest releases of the software.
- *End Of Life Date*: Displays the date for when the device should be replaced.
- *Notes*: Displays any notes entered for the device.
- *Version*: Displays the version number of the software installed on the device.
- *Engine Type*: Displays the type of device, which can be *LiveWire*, *LiveCapture*, or *LiveWire Virtual*.
- *Shared Users Count*: Displays the number of secondary users that have access to the device.
- *Scheduled Action(s)*: Displays any 'Actions' scheduled for the device.
- *Configuration Status*: Displays any status associated with configuration of the device.
- *Registered*: Displays a check mark if the device has been registered with LiveAction.
- *Activation Status*: Displays a check mark if the license on the device is valid and not expired.

DMS Templates tab

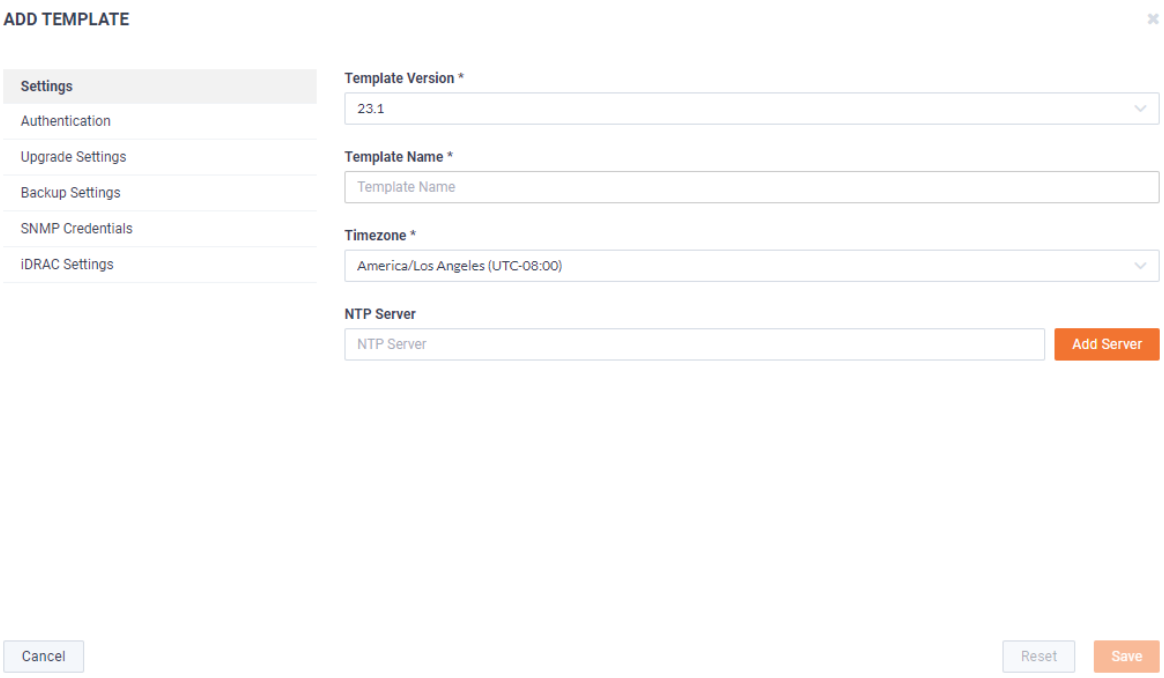
The DMS *Templates* tab displays the templates associated with your account. Templates allow you to configure settings independent of a particular device, and then apply the template, and thus the settings, to a device, or multiple devices in bulk at the same time. A description of each of the available options and settings in the *Templates* tab is provided below:



Add Template

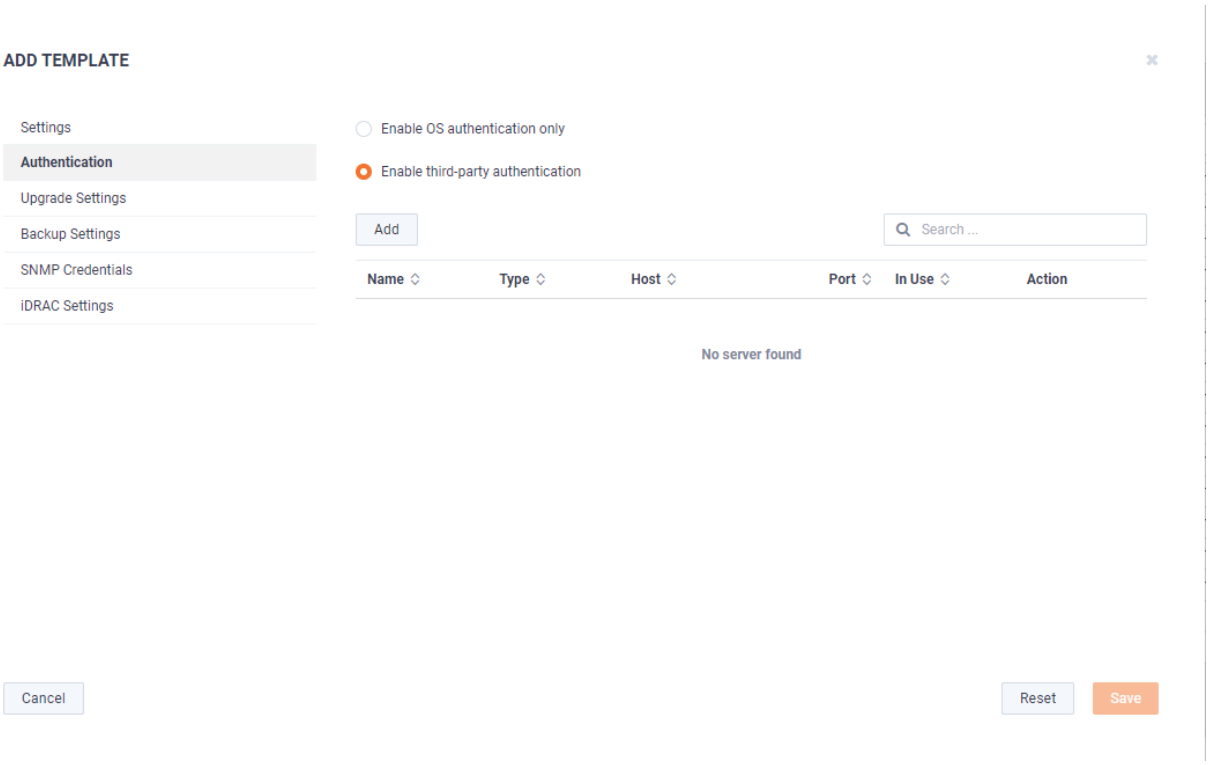
Click the **Add Template** button to display the *ADD TEMPLATE* dialog to add a new template to the configuration.

Settings



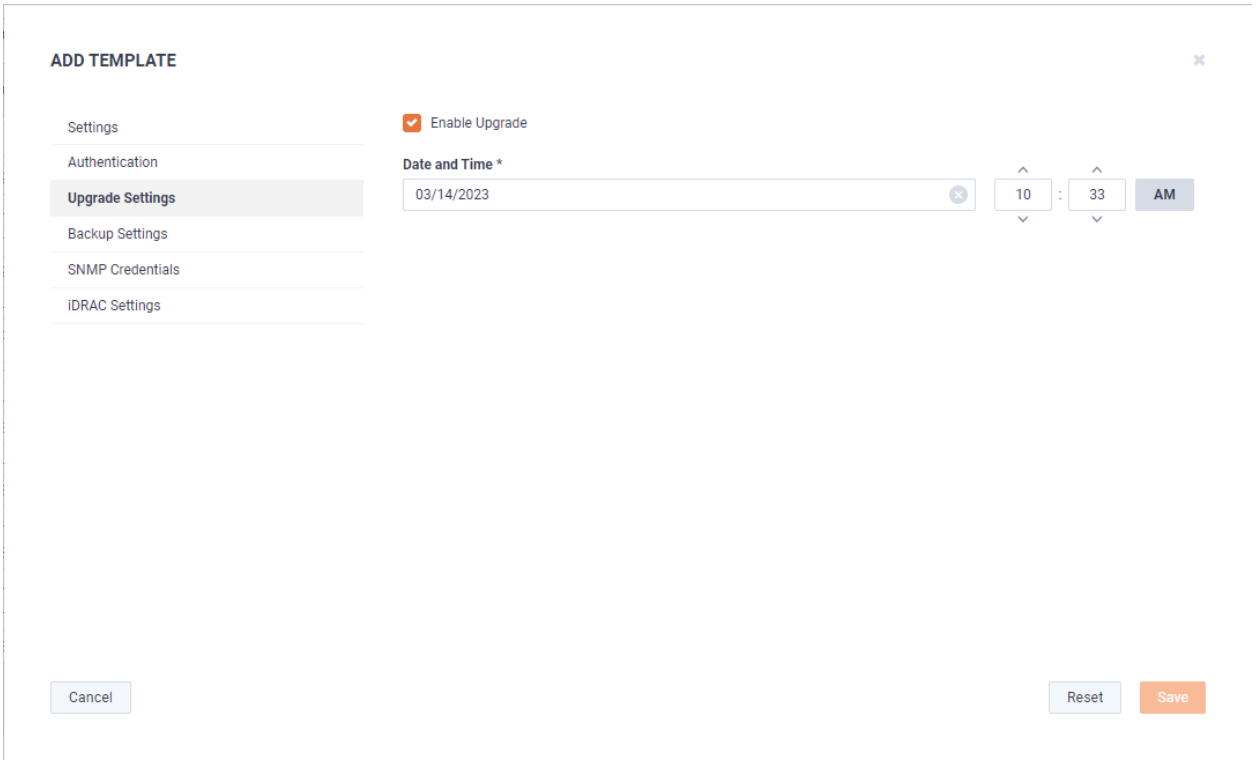
- *Template Version*: Click to select the version of the template you are configuring.
- *Template Name*: Type a name for the template.
- *Timezone*: Click to select the timezone for the template.
- *NTP Server*: Enter the address of any NTP servers to add to the configuration, and then click **Add Server**.
- *NTP Servers*: Displays the list of NTP servers added to *Settings*. You can click the **Edit** icon to edit an NTP server in the list, or click the **Trash** icon to remove an NTP server from the list.

Authentication



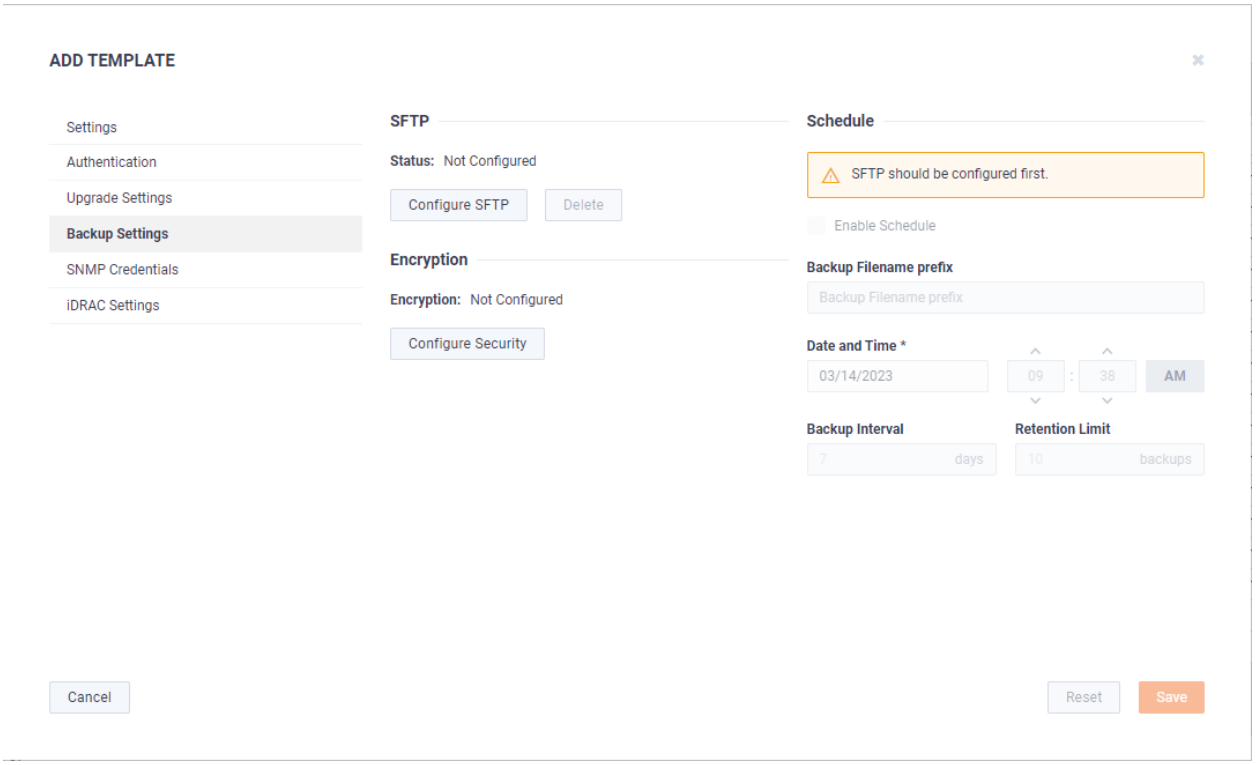
- *Enable OS authentication only*: Select this option to use the local OS authentication.
- *Enable third-party authentication*: Select this option to use TACACS+ or RADIUS authentication. If this option is selected, click **Add** to configure the new authentication setting.
  - *Add*: Click to add a new authentication setting. You will need to configure the new authentication setting.
    - *Name*: Displays the name of the authentication setting.
    - *Type*: Displays the type of authentication, which can be either 'RADIUS' or 'TACACS+.'
    - *Host*: Displays the host of the authentication setting.
    - *Port*: Displays the port of the authentication setting.
    - *Secret*: Displays the secret key of the authentication setting.
    - *Use*: Displays whether or not the authentication setting is in use.
    - *Save*: Click to save the authentication setting.
  - *Search*: yadayada.

Upgrade Settings



- *Enable Upgrade*: Select to enable the upgrade on the selected templates. If you enable the upgrade, you are presented with settings to specify the date and time the upgrade should take place.

Backup Settings



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *Hostname*: Type the IP address of the SFTP server.

- *Port*: Type the port used for the SFTP Server.
- *Username*: Type a username.
- *Password*: Type the password again to verify the password.
- *Directory*: Type the directory where backups are saved on the SFTP server.

- *Delete*: Click to delete the configured SFTP server for the backup.

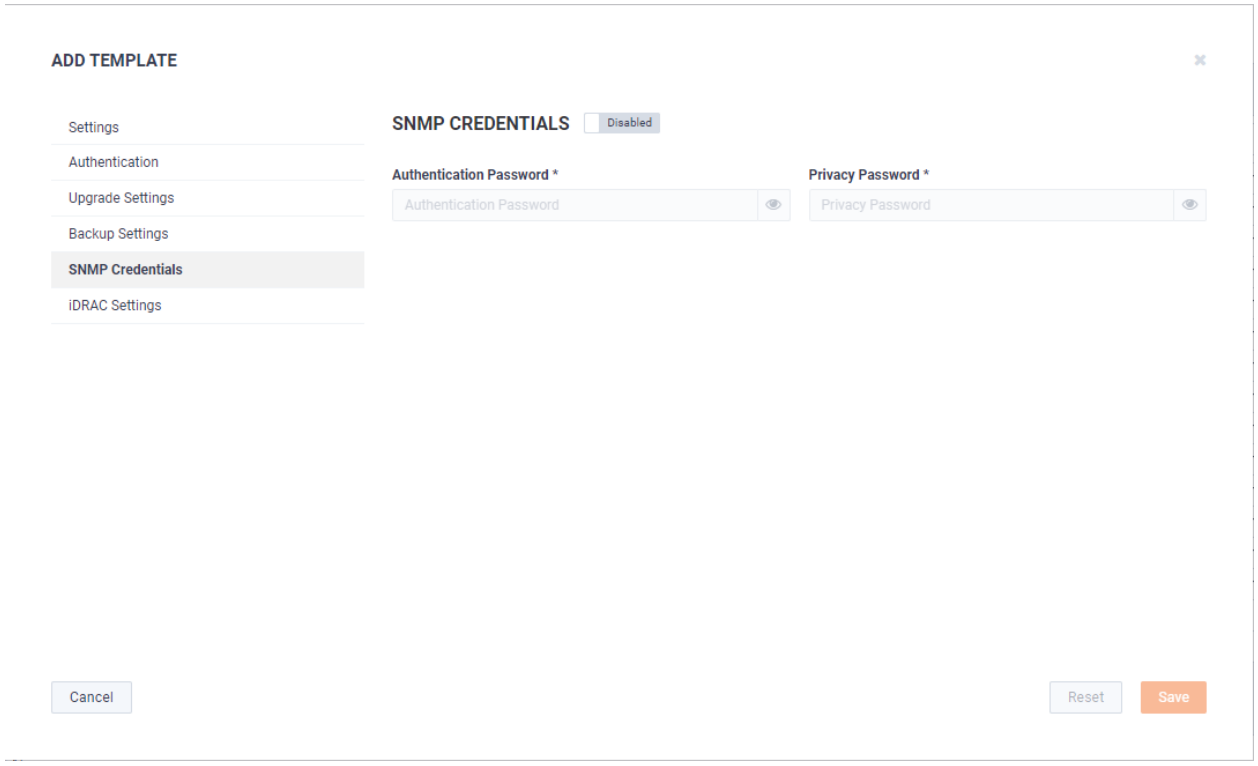
Schedule

- *Enable Schedule*: Click to enable scheduling for the backup.
- *Backup Filename prefix*: Type a prefix filename for the backup. Each scheduled backup that is created will append the prefix to the beginning of the backup filename.
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between YADA.
- *Retention Limit*: Type the number backups to YADA.

Encryption

- *Encryption*: Displays whether or not encryption is configured for each scheduled backup.
- *Configure Security*: Click to configure security settings to encrypt each scheduled backup.
  - *Encrypt backups*: Select this option to encrypt each scheduled backup.
  - *Password*: Type the password to YADA.
  - *Repeat Password*: Tye the password again to verify the password.

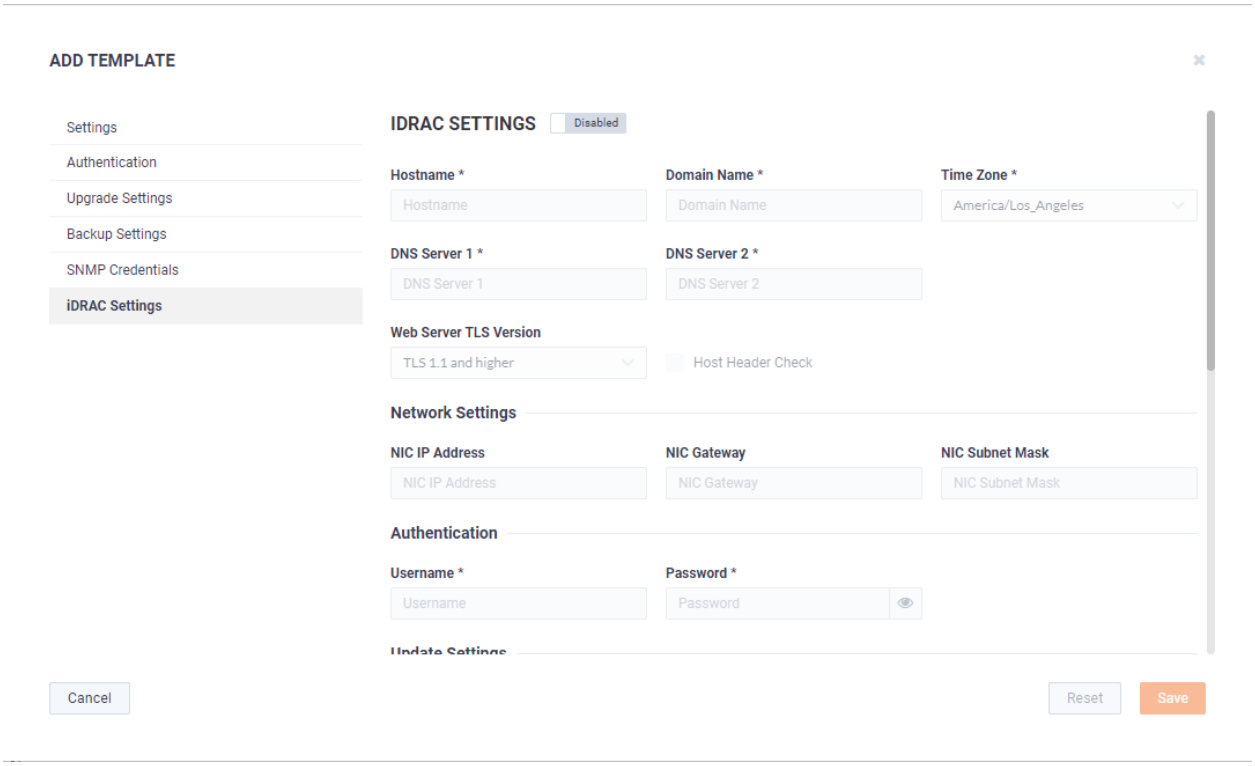
SNMP Credentials



- *Enabled/Disabled*: Select to enable or disable the *SNMP Credentials* configured below for the *Authentication Password* and *Privacy Password*.
- *Authentication Password*: Type a new *Authentication Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in *LiveFlow* on page 87.

- *Privacy Password*: Type a new *Privacy Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in *LiveFlow* on page 87.

iDRAC Settings



Note Only selected options available from the iDRAC utility are available and configurable below. See also *Integrated Remote Access Controller (iDRAC)* on page 69.

- *Hostname*: Displays the *Hostname* of the device. Type a new *Hostname* to change it.
- *Domain Name*: Displays the *Domain Name* of the device. Type a new *Domain Name* to change it.
- *Time Zone*: Displays the *Time Zone* of the device. Select a new *Time Zone* to change it.
- *DNS Server 1*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *DNS Server 2*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *Web Server TLS Version*: Displays the TLS protocol version support used by the device. You can select from the following: TLS 1.1 and Higher, TLS 1.2 and Higher, and TLS 1.3
    - *Host Header Check*: Select to enable *Host Header Check* requests.

Network Settings:

- *NIC IP Address*: Displays the static *NIC IP Address* of the device. Type a new *NIC IP Address* to change it.
- *NIC Gateway*: Displays the *NIC Gateway* of the device. Type a new *NIC Gateway* to change it.
- *NIC Subnet Mask*: Displays the *NIC Subnet Mask* of the device. Type a new *NIC Subnet Mask* to change it.

Authentication:

- *Username*: Displays the *Username* of the device. Type a new *Username* to change it.
- *Password*: Configures the *Password* of the device. Type a new *Password* to change it.

Update Settings:

- *Enable Updates*: Select to enable updates on the device. If enabled, you must configure the Update Proxy Server, Update Proxy User, and Update Proxy Password.
- *Update Proxy Server*: Displays the *Update Proxy Server* of the device. Type a new *Update Proxy Server* to change it.
- *Update Proxy User*: Displays the *Update Proxy User* of the device. Type a new *Update Proxy User* to change it.
- *Update Proxy Password*: Displays the *Update Proxy Password* of the device. Type a new *Update Proxy Password* to change it.

SNMP:

- *Enable SNMP*: Select to enable the SNMP Agent on the iDRAC. If enabled, you must configure the *SNMP Community.*
  - *SNMP Community*: Configures the *SNMP Community* name used for SNMP Agents. Type a new *SNMP Community* name to change it
- *Enable SNMP Alert 1*: Select to enable the *SNMP Alert 1* on the iDRAC. If enabled, you must configure the *Alert 1 Target Address*.
  - *Alert 1 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.
- *Enable SNMP Alert 2*: Select to enable the *SNMP Alert 2* on the iDRAC. If enabled, you must configure the *Alert 2*. If enabled, you must configure the *Alert 2 Target Address*.
  - *Alert 2 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.

NTP:

- *Enable NTP*: Select to enable an *NTP* server on the iDRAC. If enabled, you must configure the *NTP Server*.
  - *NTP Server*: Displays the name or IP address of the *NTP Server*. Type a new name or IP address to change it.

Event Filters:

- *Alert*: Displays any iDRAC Event filters configured for the device.
- *Add*: Click to add a new Event filter configured in the text box. You must provide any parameters by defining what you want to be alerted to and how you want to be notified. You can configure as may event filter commands as you want. The general format of an alert category:

  idrac.alert.category.[subcategory].[severity]

Edit

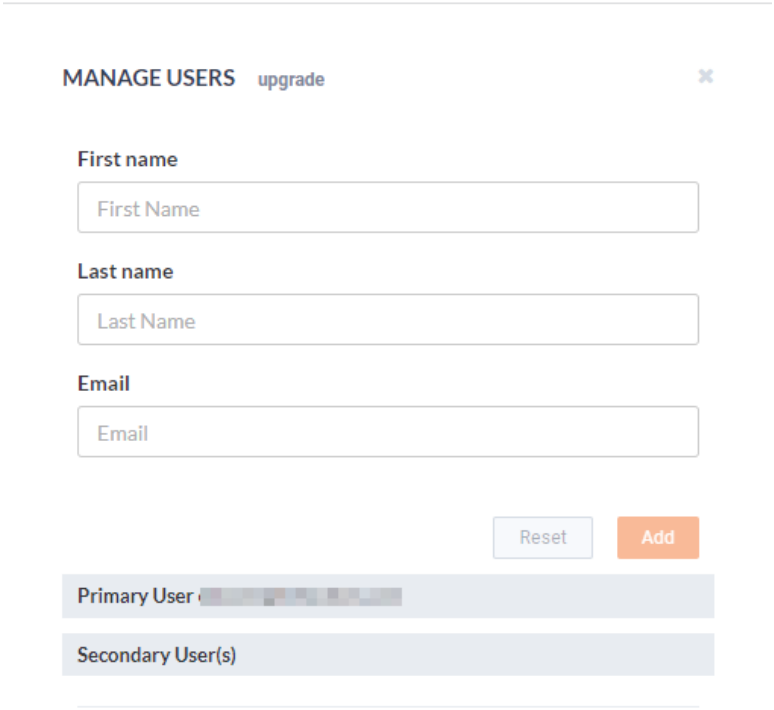
Click the **Edit** button to edit the selected template. See also *Add Template* on page 67.

Delete

Click the **Delete** button to delete the selected template.

Share

Click the **Share** button to share the selected template with other users who manage and configure appliances. You will need to add a user by completing the *Manage Users* dialog.

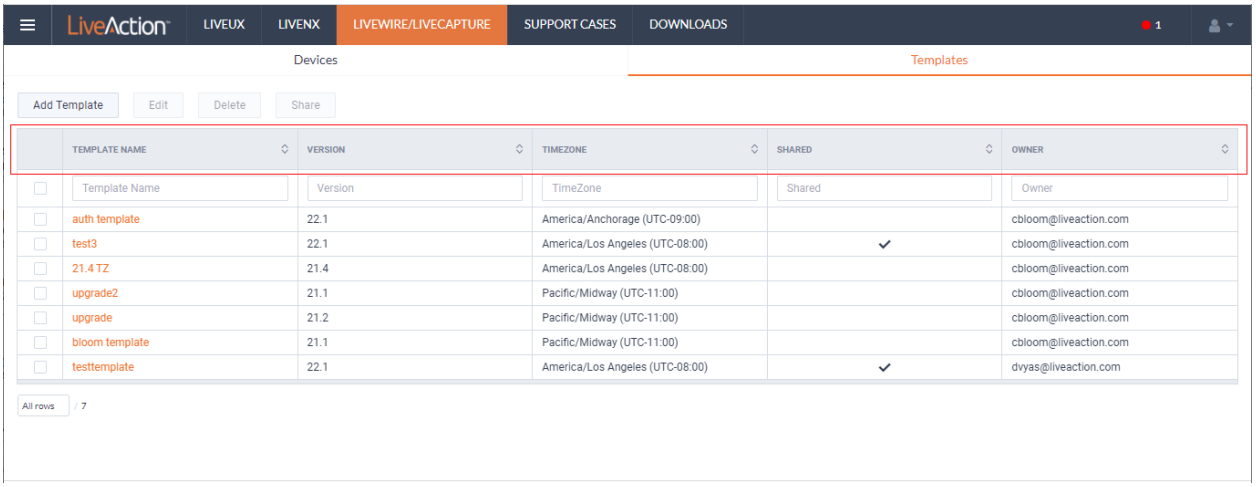


- *First Name*: Type the first name of the user.
- *Last Name*: Type the last name of the user.
- *Email*: Type the email address of the user.
- *Reset*: Click to clear the *Manage User* values.
- *Add*: Click to add the user to the list of secondary users.
- *Primary User*: Displays the primary user of the device when the device was registered with LiveAction. If multiple appliances are selected in the list of devices, the *Primary User* is not displayed.
- *Secondary User(s)*: Displays any secondary users assigned to the device. If multiple appliances are selected in the list of devices, the *Secondary User(s)* are not displayed.

Template column headings

Descriptions of the columns displayed in the list of templates are provided below.

Tip Below each of the column headings is a text box you can use to filter the templates displayed in the list of templates. To filter using the text box, simply enter a text string to display the templates that match the text string.



- *Template Name*: Displays the name of the template. Click the name to display details about the template.
- *Version*: Displays the version number of the template.
- *Timezone*: Displays the time zone of the template.
- *Shared*: Displays the users that have been shared with the device. Shared users can fully configure a device from DMS.
- *Owner*: Displays the owner of the device. There can only be one owner of the device.

Backup and restore

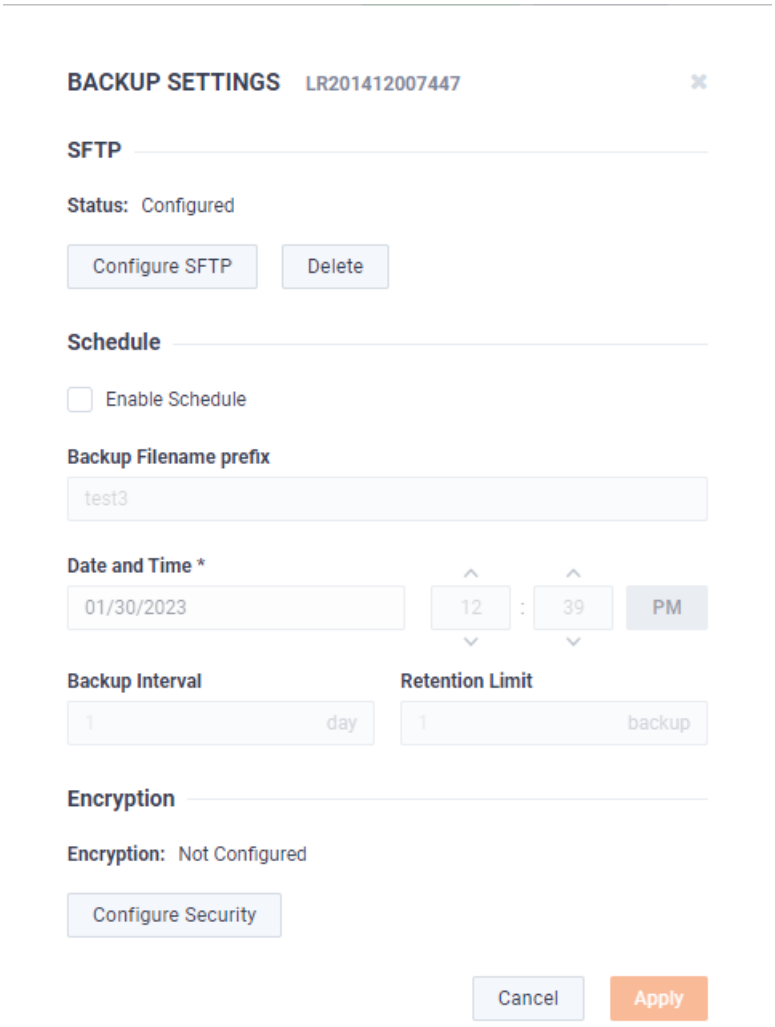
The *Backup Settings* in DMS lets you configure and designate an SFTP (Secure FTP) server for backing up the application and system settings on the LiveWire device. Once a backup is created, you can use the *Restore Backup* settings to restore either the application settings, or both the application and system settings to the same or different LiveWire device.

Here are descriptions of the *Application* and *System* settings that are included in a backup:

- *Application* settings: These are all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins.
- *System* settings: These are new and/or updated users, SNMP, NTP, network, time zone, and host customizations.

Creating a backup

1. Click the **Elipsis** (...) in DMS and select *Backup Settings*. The *Backup Settings* dialog appears. See *Backup Settings* on page 58 for a description of each of the settings.



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *Hostname*: Type the IP address of the SFTP server.

- *Port*: Type the port used for the SFTP server.
- *Username*: Type a username for the SFTP server.
- *Password*: Type a password for the SFTP server.
- *Directory*: Type the directory where backups are saved on the SFTP server.

- *Delete*: Click to delete the configured SFTP server for the backup.

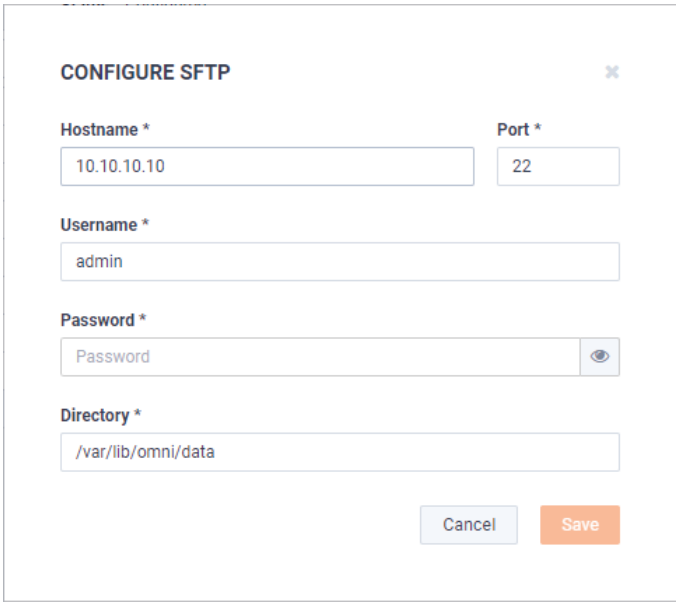
Schedule

- *Enable Schedule*: Click to enable scheduling for the backup.
- *Backup Filename prefix*: Type a prefix filename for the backup. Each scheduled backup that is created will append the prefix to the beginning of the backup filename.
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between when backups are performed.
- *Retention Limit*: Type the number backups to save before a backup is deleted.

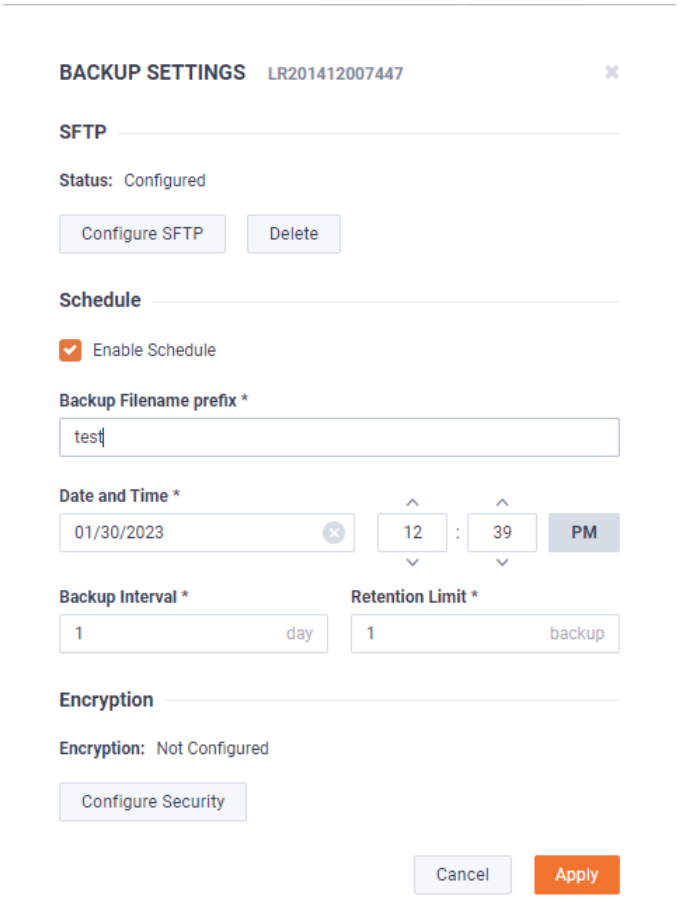
Encryption

- *Encryption*: Displays whether or not encryption is configured for each scheduled backup.
- *Configure Security*: Click to configure security settings to encrypt each scheduled backup.
  - *Encrypt backups*: Select this option to encrypt each scheduled backup.
  - *Password*: Type a password for the encrypted backup.
  - *Repeat Password*: Tye the password again to verify the password.
- *Apply*: Click to apply the backup settings on the device.

2. Click **Configure SFTP** to configure the SFTP (Secure FTP) server for the backup.The *Configure SFTP* dialog appears.

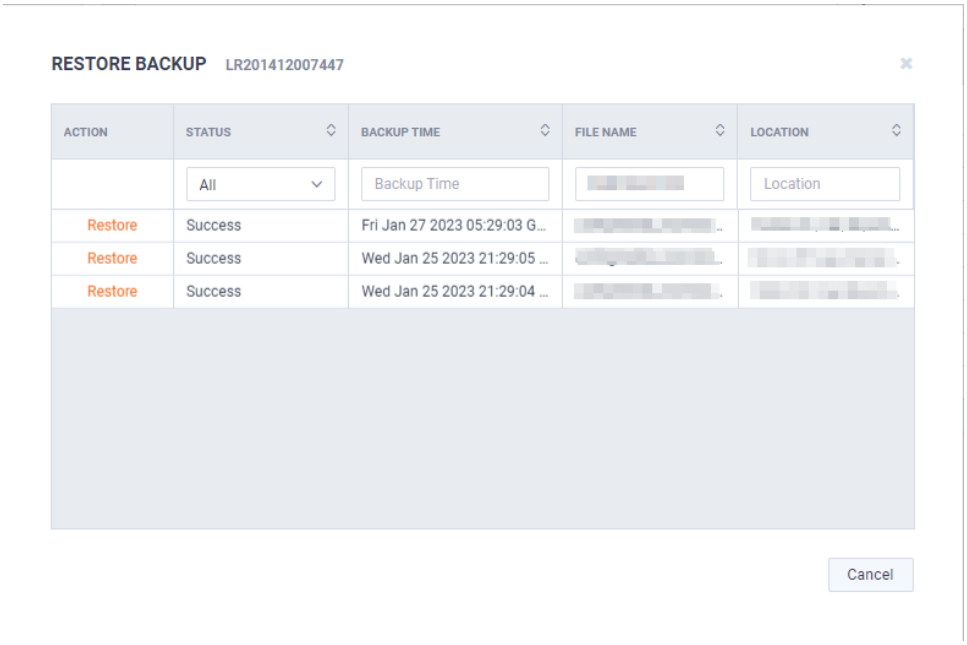


3. Configure the SFTP server you want to use as the backup server. You will need to configure the *Hostname*, *Port*, *Username*, *Password*, *Directory*, and click **Save**.
4. On the *Backup Settings* dialog, select the *Enable Schedule* check box. You will need to configure the *Backup Filename Prefix*, *Date and Time*, *Backup Interval*, *Retention Limit*, *Encryption*, and click **Apply**.

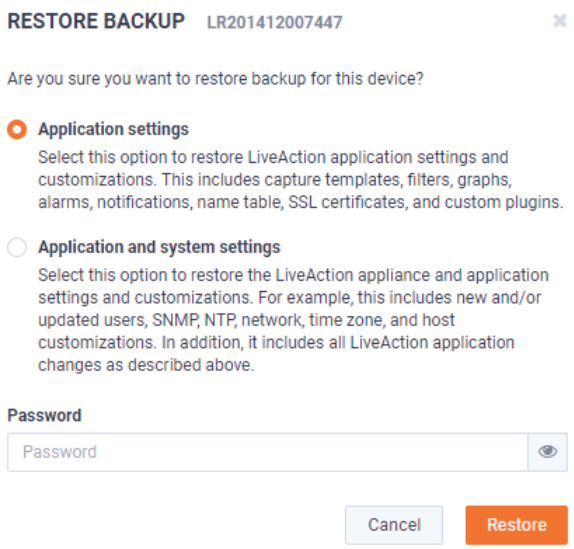


Restoring a backup

1. Click the **Elipsis** (...) in DMS and select **Restore Backup**. The *Restore Backup* dialog appears.



2. In the *Action* column, select the backup you want to restore. The second *Restore Backup* dialog appears.



3. Select either the *Application Settings* or *Application and System Settings* option, enter the *Password* for the backup, and click **Restore**.

Configuring network settings by command script

You can configure LiveWire Virtual network settings by using the 'omni-interface' command script from the 'root' user command prompt (*root@LiveWire*). To get to the '**root**' user command prompt, enter the following command from the command prompt and enter '**admin**' as the password when prompted:

#sudo su

Here are the commands to configure the network settings from the command prompt:

Usage: *omni-interface [options]*

options:

-a, --adapter	adapter to modify
-f, --wifi	enable or disable Remote AP Capture capability [on|off]
-c, --dhcp	configure dhcp
-s, --static	configure static
-l, --manual	configure manual
-r, --address	static adapter address
-m, --netmask	static adapter netmask
-b, --broadcast	static adapter broadcast address
-w, --network	static adapter network address
-g, --gateway	static adapter gateway address
-h, --hwaddress	static adapter mac address
-d, --dns	static dns servers (comma separated)

Important! The Ethernet ports can be configured to obtain an IP address automatically from a DHCP server by specifying 'dhcp' instead of 'static' settings; however, we strongly recommend the use of static IP addresses for the Ethernet ports. If DHCP is used, and if the address should change on a new DHCP lease, then the user must restart the Capture Engine service to see the new IP addresses in the 'Adapters' capture options in Omnipeek.

Additionally, if you specify 'dhcp' instead of 'static' settings, and there is no DHCP server available, you must allow the command to time-out.

Using LiveWire Virtual with Omnipeek

Any computer on the network with the Omnipeek Windows software installed can now access the Capture Engine running on LiveWire Virtual. From the **Capture Engine** window in Omnipeek, you can configure, control, and view the results of the Capture Engine remote captures.

For more information on how to view and analyze remote captures from within the Omnipeek console, please see *Using Capture Engines with Omnipeek* on page 117, and also the *Omnipeek User Guide* or Omnipeek online help.

CHAPTER 3

Sending Telemetry to LiveNX and ThreatEye

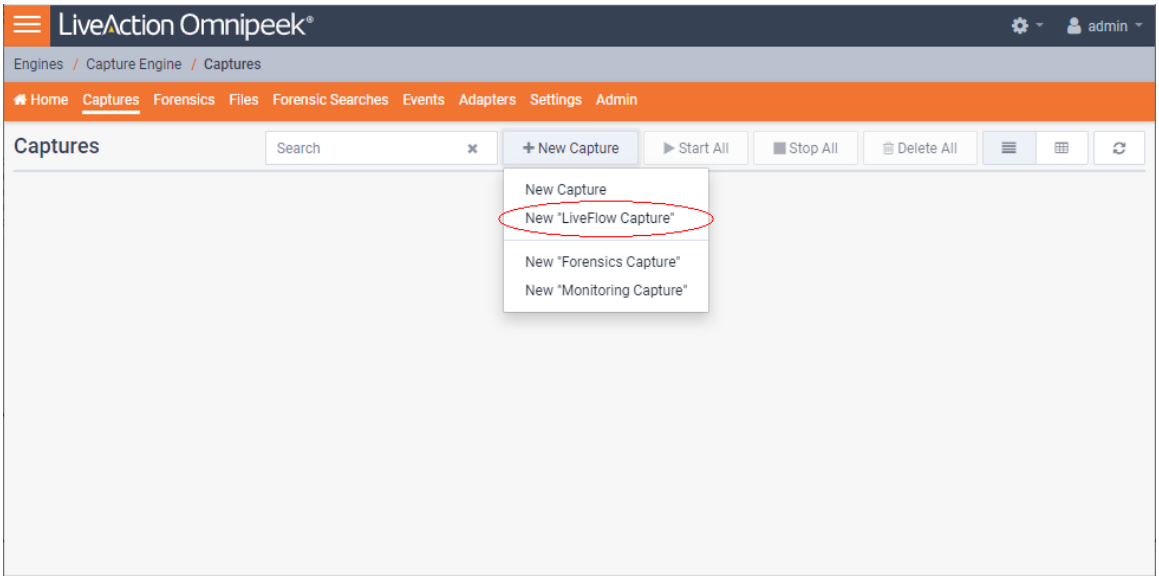
In this chapter:

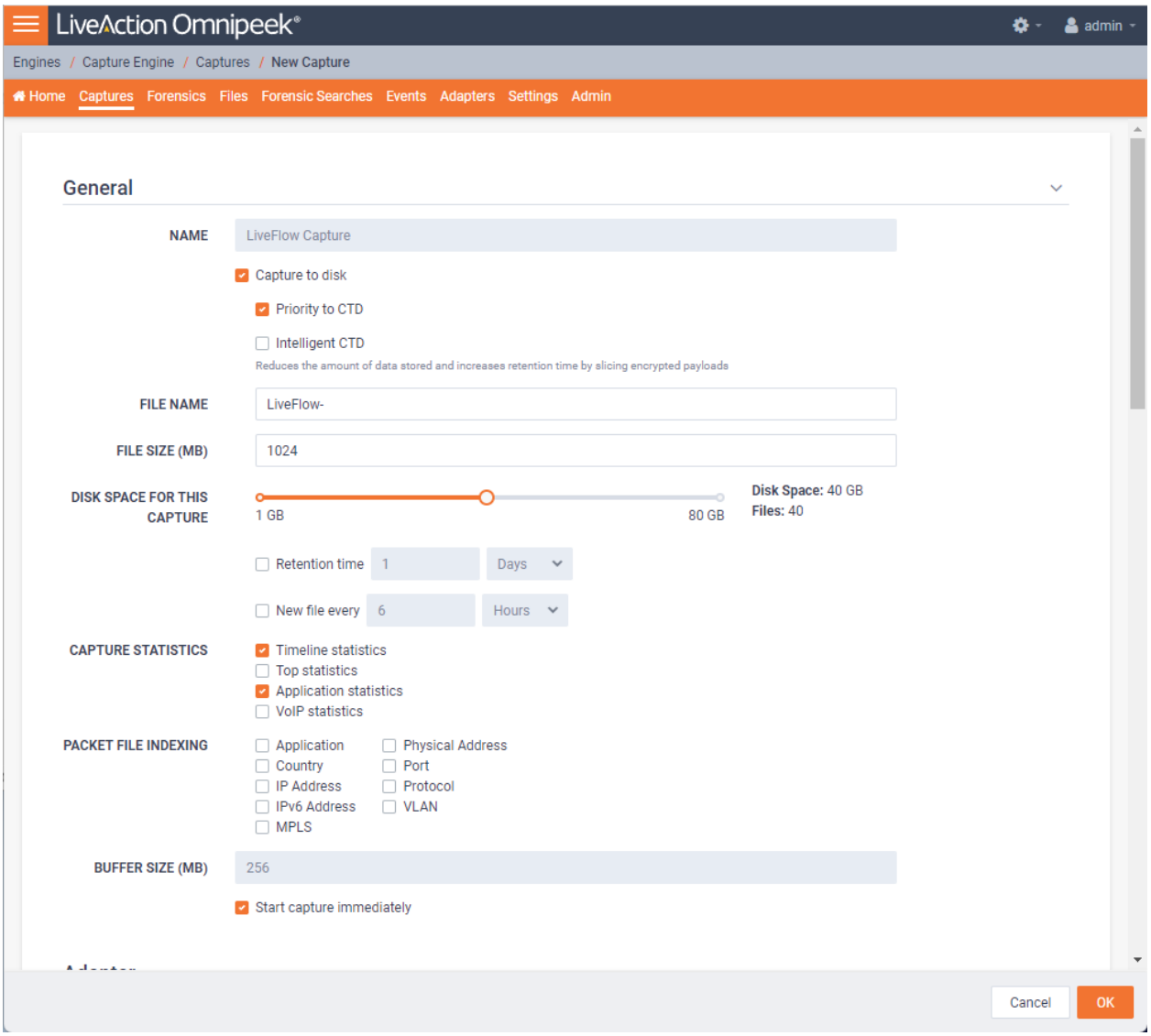
About sending telemetry to LiveNX and ThreatEye

LiveWire Virtual is designed to send LiveFlow telemetry data to LiveAction's LiveNX and ThreatEye platforms. LiveNX is a network and application performance monitoring platform with patented end-to-end visualization for a global view of the network and the ability to drill-down to individual devices. ThreatEye is a Network Detection & Response platform, unfazed by encrypted network traffic, that uses advanced behavioral analysis and machine learning for threat detection and security compliance. This chapter describes the tasks you must perform in order to properly send LiveFlow telemetry data from LiveWire Virtual to LiveNX and ThreatEye.

Configuring LiveFlow telemetry

To send the LiveFlow telemetry data that LiveNX or ThreatEye uses for its platform, you must use Omnipeek to first create a new LiveFlow capture and then configure the settings for that capture to send LiveFlow telemetry to either the LiveNX and/or ThreatEye platforms.

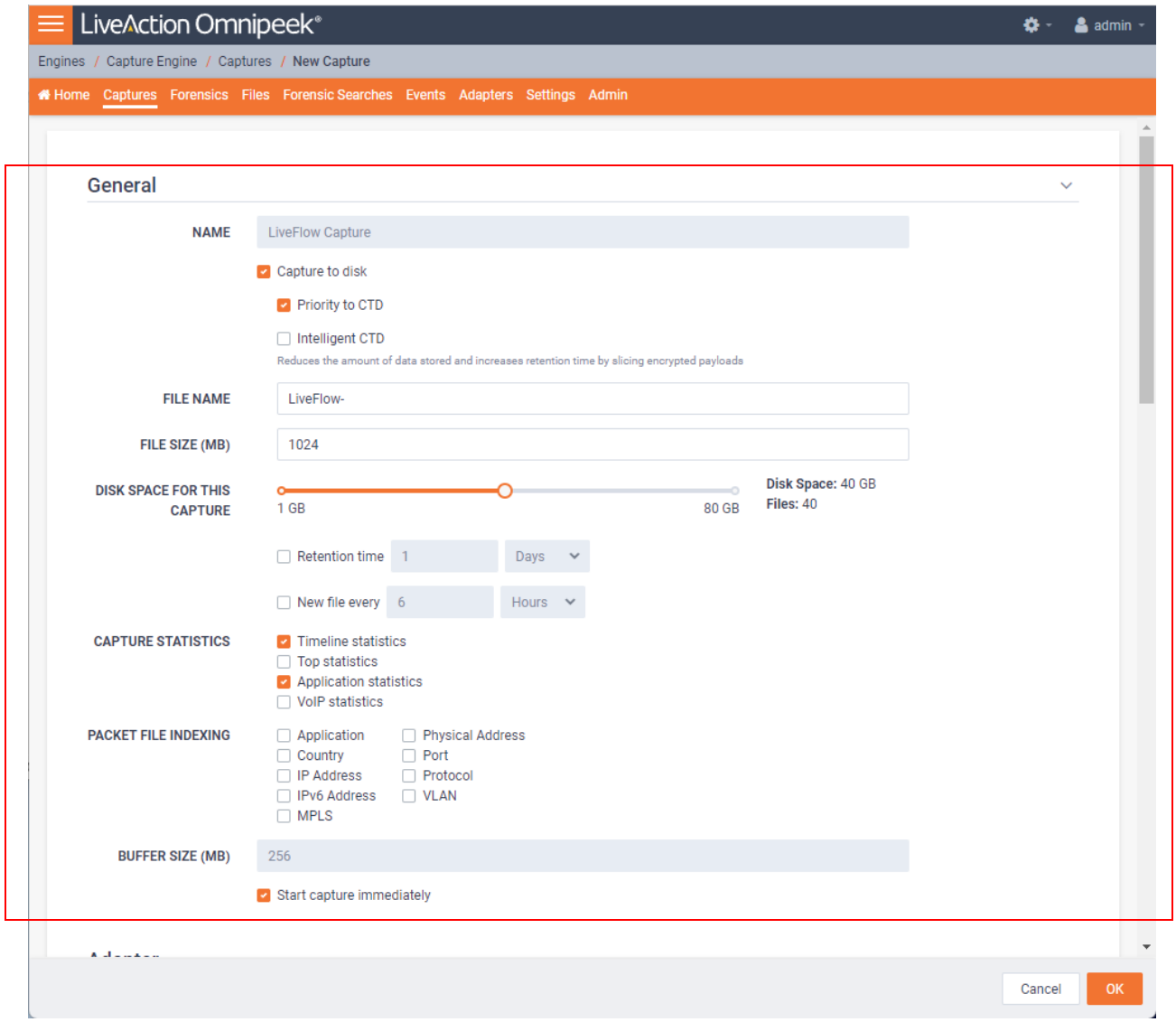




Note Scroll down in the capture options to see LiveFlow settings for *Template Refresh Interval* and *Options Template Refresh Interval*. These settings let you configure the amount of time (in seconds) LiveWire Virtual sends template information to LiveNX. The templates provide the instructions to LiveNX on how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). If you make any changes to your template settings, it will take the specified number of seconds for the changes to take effect. If you recently connected LiveWire Virtual to the network, it may take up to 600 seconds for LiveNX and ThreatEye to see the LiveFlow data from LiveWire Virtual. You may want to adjust the settings to the desired intervals.

General

The *General* settings let you set up and configure the LiveFlow capture.



- *Name:* Type a descriptive name for the capture. Unique names can help you to identify and organize your captures.
- *Capture to disk:* Select this option to save packet files on your disk. Packet files saved to your hard disk (and the individual packets/packet decodes in each of the files) can be opened and analyzed at a later time with Omnipeek. If you are more interested in speeding up analysis of the data and conserving hard disk space, you may want to disable *Capture to disk*.
  - *Priority to CTD:* Select this option so that real-time analysis doesn't impact the capture-to-disk (CTD) performance. When this option is enabled, it is less likely that packets are dropped when they are captured to disk. If capturing all the packets to disk is desirable, enable *Priority to CTD*. If analysis is more important, disable *Priority to CTD*.
  - *Intelligent CTD:* Select this option to reduce the amount of data stored to disk and increase your retention time by intelligently slicing off encrypted payloads. It does this by tracking flows—if a flow is encrypted, the full data for the first 20 packets is kept and the payload from the rest of the packets is sliced. It keeps the first 20 without slicing so the certificate exchange is always included.

    Intelligent CTD is an advanced feature that provides significant benefits to network security and data retention. It reduces the amount of data stored on disk and increases retention time by intelligently slicing off encrypted payloads, which helps to conserve storage space and improve system performance.

The way *Intelligent CTD* works is by tracking flows on the network. When a flow is detected as encrypted, *Intelligent CTD* keeps the full data for the first 20 packets and slices the payload from the rest of the packets. This ensures that the certificate exchange is always included in the data, which is critical for identifying encrypted traffic and providing context for analysis.

The benefits of *Intelligent CTD* are numerous. Firstly, it helps to optimize storage usage, as the system doesn't store unnecessary data. This helps to reduce the cost of storage and improve system performance by reducing the amount of data that needs to be processed.

Secondly, *Intelligent CTD* helps to improve retention time. By conserving storage space, it enables organizations to retain data for longer periods, which can be critical for compliance and regulatory requirements. This also enables organizations to perform more in-depth analysis of data, which can provide valuable insights into network activity and help to identify potential threats.

Thirdly, *Intelligent CTD* helps to maintain privacy and compliance. By keeping the certificate exchange in the data, it ensures that the system can identify encrypted traffic and provide context for analysis, without compromising the privacy of users. This helps organizations to comply with privacy regulations and maintain the trust of their users.

Overall, *Intelligent CTD* is a powerful feature that provides numerous benefits to network security and data retention. By intelligently slicing off encrypted payloads, it helps to optimize storage usage, improve retention time, and maintain privacy and compliance.

- *File Name:* Type the name used as a base file name prefix for each capture file that is created using the *Capture to disk* option. Additionally, each capture file is appended with a timestamp indicating the date and time the file was saved. The format of the timestamp is *YYYY-MM-DD-HH.MM.SS.mmm*.
- *File Size (MB):* Enter or select the maximum file size before a new file is created.
- *Disk Space For This Capture:* Move the slider control to set the amount of hard disk space allocated for the capture. The minimum value of the slider is the minimum size of disk space a capture can occupy.
  - *Retention time*: Select this option to configure how long CTD files can remain on disk. You will need to configure the amount of minutes, hours, or days. For example, if you specify 3 days as the retention time, you'll only see the CTD files written within the past 3 days regardless of how much disk space you reserve for the capture.
  - *New file every*: Select this option to create a new CTD file at a specific time interval rather than when the CTD file size specified is reached. You will need to configure the amount of minutes, hours, or days. For example, if you specify that you want a new file every 1 minute with a 4 GB CTD file size, there will be a new CTD file every 1 minute even if the CTD file is only 1 GB in size. If the 4 GB size limit is reached before the 1 minute mark, then the *New file every* option doesn't come into effect.
- *Capture Statistics:* Select the type of statistics desired for the capture:
  - *Timeline Statistics:* Select this option to populate the capture engine database with capture data and basic network statistics such as utilization, size, distribution, etc. These statistics are then made available through the *Capture Engine Forensics* tab.
  - *Top Statistics:* Select this option to populate the capture engine database with top nodes and top protocols statistics. These statistics are then made available through the *Capture Engine Forensics* tab.
  - *Application Statistics:* Select this option to populate the capture engine database with applications statistics which are made available through the various 'application' displays.
  - *VoIP Statistics:* Select this option to populate the capture engine database with VoIP call quality and call volume statistics. These statistics are then made available through the *Capture Engine Forensics* tab.

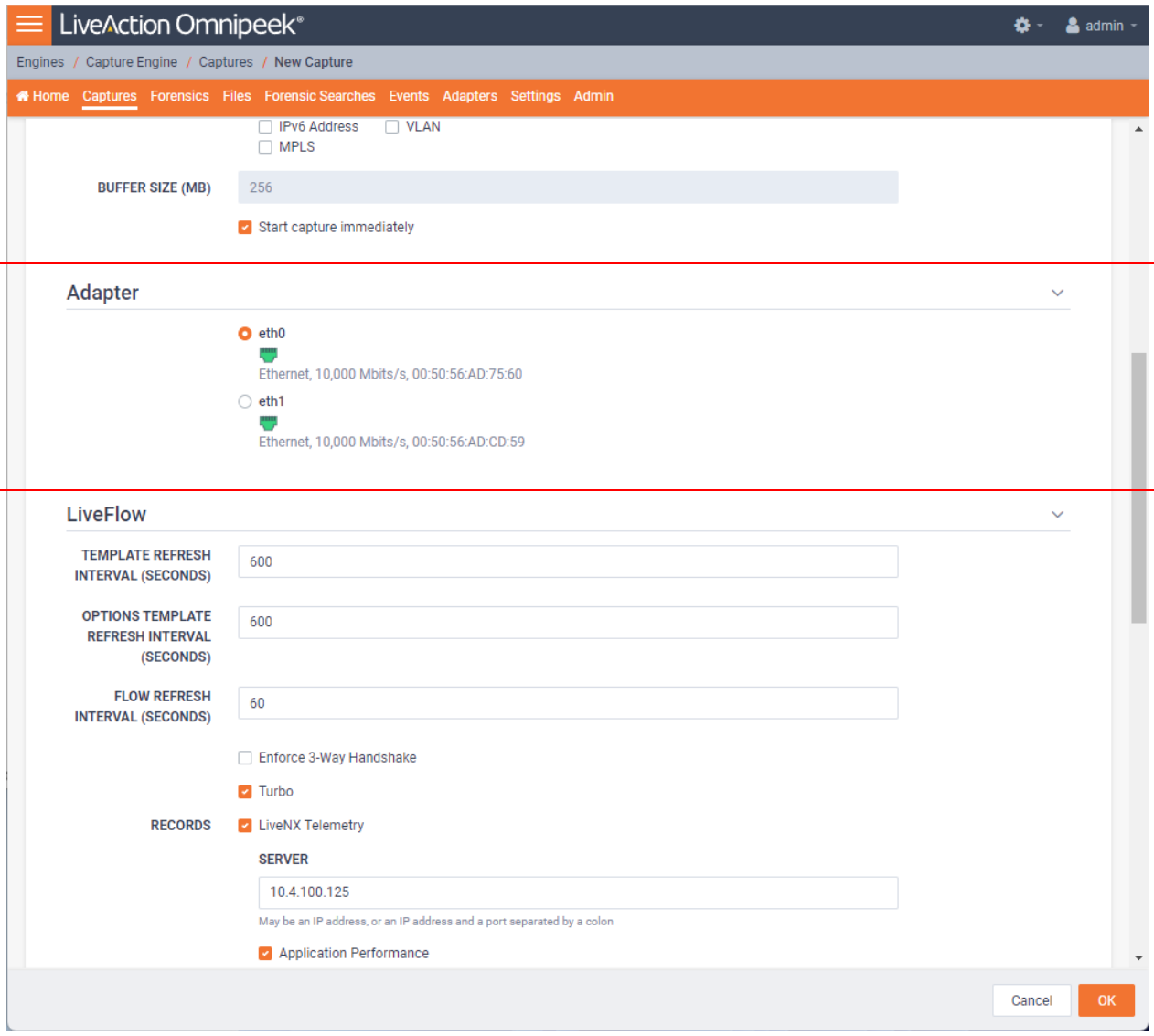
Note Selecting the *VoIP Statistics* option may affect capture performance, especially when there are more than 2000 simultaneous calls on the network. Selecting the *Top Statistics* option may

affect capture performance, especially when there are more than 10,000 active nodes captured on the network.

- *Packet File Indexing:* Under certain conditions, *Packet File Indexing* increases performance for forensic searches that use software filters. Overall capture-to-disk performance can degrade slightly, but forensic search results may be returned significantly faster if the packet elements being filtered are contained in the index and the packet characteristic is sparsely located within the packet files being searched. Enable the packet characteristics below you are most likely to use in a forensic search software filter.
  - *Application*
  - *Country*
  - *IP Address*
  - *IPv6 Address*
  - *MPLS*
  - *Physical Address*
  - *Port*
  - *Protocol*
  - *VLAN*
- *Buffer Size (MB):* Enter a buffer size, in megabytes, for the amount of memory dedicated for the capture buffer. The capture buffer is where packets are placed for analysis. The default is 256 megabytes. A larger buffer can reduce or eliminate packet loss due to spikes in traffic. When *Capture to disk* is enabled, the *Buffer Size* option is unavailable.
  - *Start Capture Immediately:* Select this option to immediately begin capturing packets once you click **OK**.

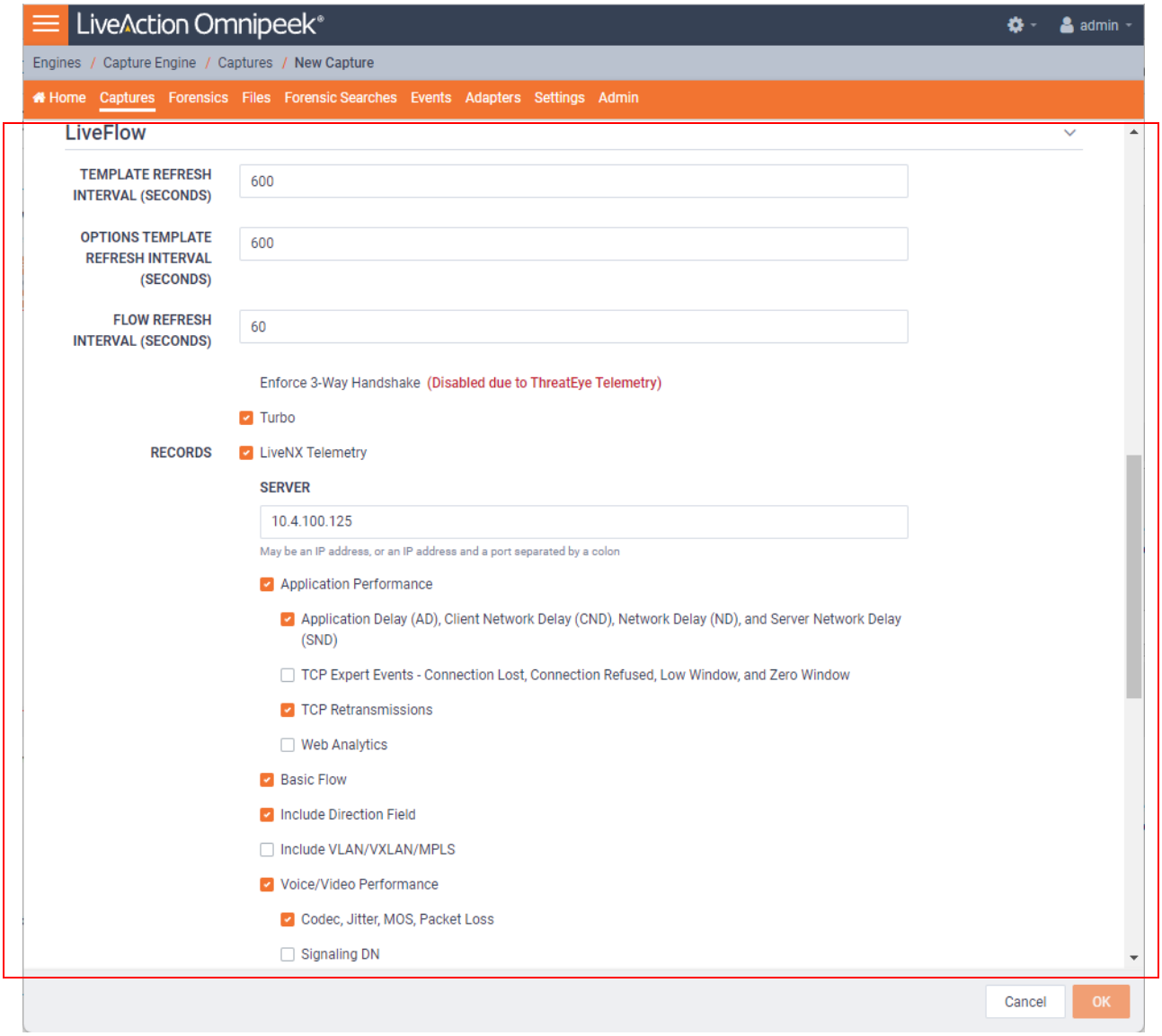
Adapter

The *Adapter* settings display the capture adapters available on LiveWire Virtual. Select the desired adapter for the LiveFlow capture.


LiveAction Omnipeek
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
IPv6 Address
VLAN
MPLS
BUFFER SIZE (MB)
256
Start capture immediately
Adapter
eth0
Ethernet, 10,000 Mbits/s, 00:50:56:AD:75:60
eth1
Ethernet, 10,000 Mbits/s, 00:50:56:AD:CD:59
LiveFlow
TEMPLATE REFRESH INTERVAL (SECONDS)
600
OPTIONS TEMPLATE REFRESH INTERVAL (SECONDS)
600
FLOW REFRESH INTERVAL (SECONDS)
60
Enforce 3-Way Handshake
Turbo
RECORDS
LiveNX Telemetry
SERVER
10.4.100.125
May be an IP address, or an IP address and a port separated by a colon
Application Performance
Cancel
OK

LiveFlow

The *LiveFlow* settings lets you further configure the LiveFlow data of the capture.



Template Refresh Interval

- *Template Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire Virtual generates and sends IPFIX template records to LiveNX. The templates provide the instructions to LiveNX on how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.

> **Note** If you recently connected LiveWire Virtual to the network, it may take up to 600 seconds for LiveNX to see the LiveFlow data from LiveWire Virtual. You may want to adjust this setting to the desired intervals.

Options Template Refresh Interval

- *Options Template Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire Virtual generates and sends IPFIX option template records to LiveNX. The templates provide the

instructions to LiveNX on how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.

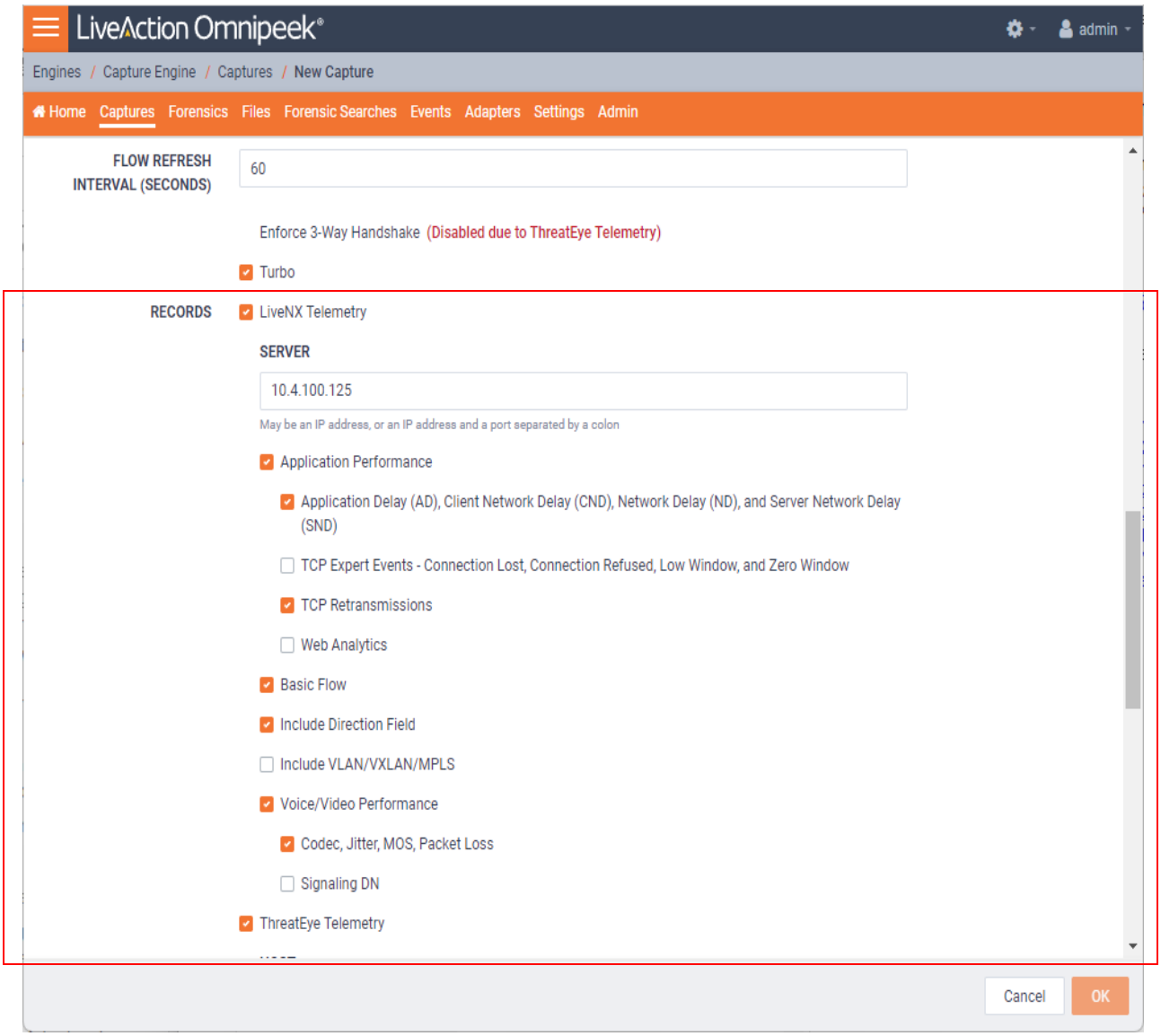
Note If you recently connected LiveWire Virtual to the network, it may take up to 600 seconds for LiveNX to see the LiveFlow data from LiveWire Virtual. You may want to adjust this setting to the desired intervals.

Flow Refresh Interval

- *Flow Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire Virtual generates and sends IPFIX data records to LiveNX. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.
  - *Enforce 3-way Handshake*: Select this option to require a 3-way handshake (SYN, SYN-ACK, ACK) for a TCP flow in order for it to be included in processing and analyzing. If *ThreatEye Telemetry* is enabled below, then *Enforce 3-way Handshake* is automatically disabled.
  - *Turbo*: Select this option to enable multi-stream CTD (also called Turbo mode) which is done in the capture template. This option will only be configurable (and enabled by default) for virtual capture engines with the *Large* or *Unlimited LiveFlow* activation feature.

Records

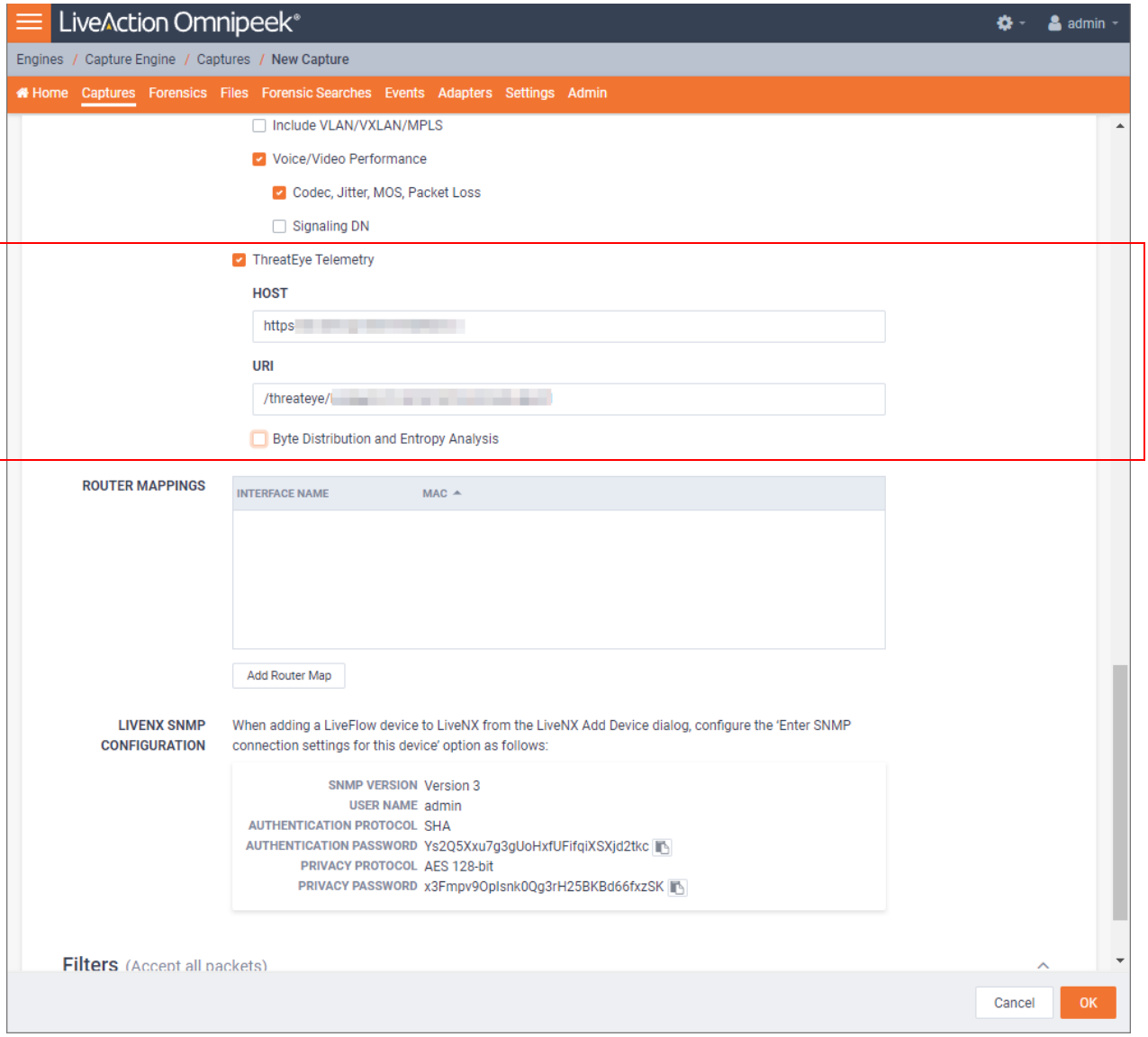
- *LiveNX Telemetry*: Select this option to send LiveFlow telemetry to a specific LiveNX server configured below.



- *Server*: Displays the IP address of the LiveNX server receiving the LiveFlow data from LiveWire Virtual. To change the IP address, enter the IP address of the desired LiveNX server.
- *Application Performance*: Select this option to generate AVC IPFIX records.
  - *Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)*: Select this option to perform and report latency analysis when AVC IPFIX records are generated.
  - *TCP Expert Events -Connection Lost, Connection Refused, Low Window, and Zero Window*: Select this option to perform TCP quality analysis (Expert) when AVC IPFIX records are generated.
  - *TCP Retransmissions*: Select this option to perform TCP retransmission analysis (Expert) when AVC IPFIX records are generated.
  - *Web Analytics*: Select this option to perform web analytics when AVC IPFIX records are generated.

    • *Decrypt Packets*: Select this option to perform decryption on HTTPS packets when *Web Analytics* is enabled.
- *Basic Flow*: Select this option to generate FNF IPFIX records.

- *Include Direction Field*: Select this option to send the 'flowDirection' key in unidirectional IPFIX records indicating the flow direction (0 for ingress, 1 for egress).
- *Include VLAN/VXLAN/MPLS*: Select this option to perform MPLS, VLAN, and VXLAN analysis when AVC, FNF, or MediaNet IPFIX records are generated.
- *Voice/Video Performance*: Select this option to generate MediaNet IPFIX records.
  - *Codec, Jitter, MOS, Packet Loss*: Select this option perform RTP analysis when MediaNet IPFIX records are generated.
  - *Signaling DN*: Select this option to generate Signaling DN IPFIX records when MediaNet IPFIX records are generated.
- *ThreatEye Telemetry*: Select this option to send LiveFlow telemetry to a specific ThreatEye host configured below.



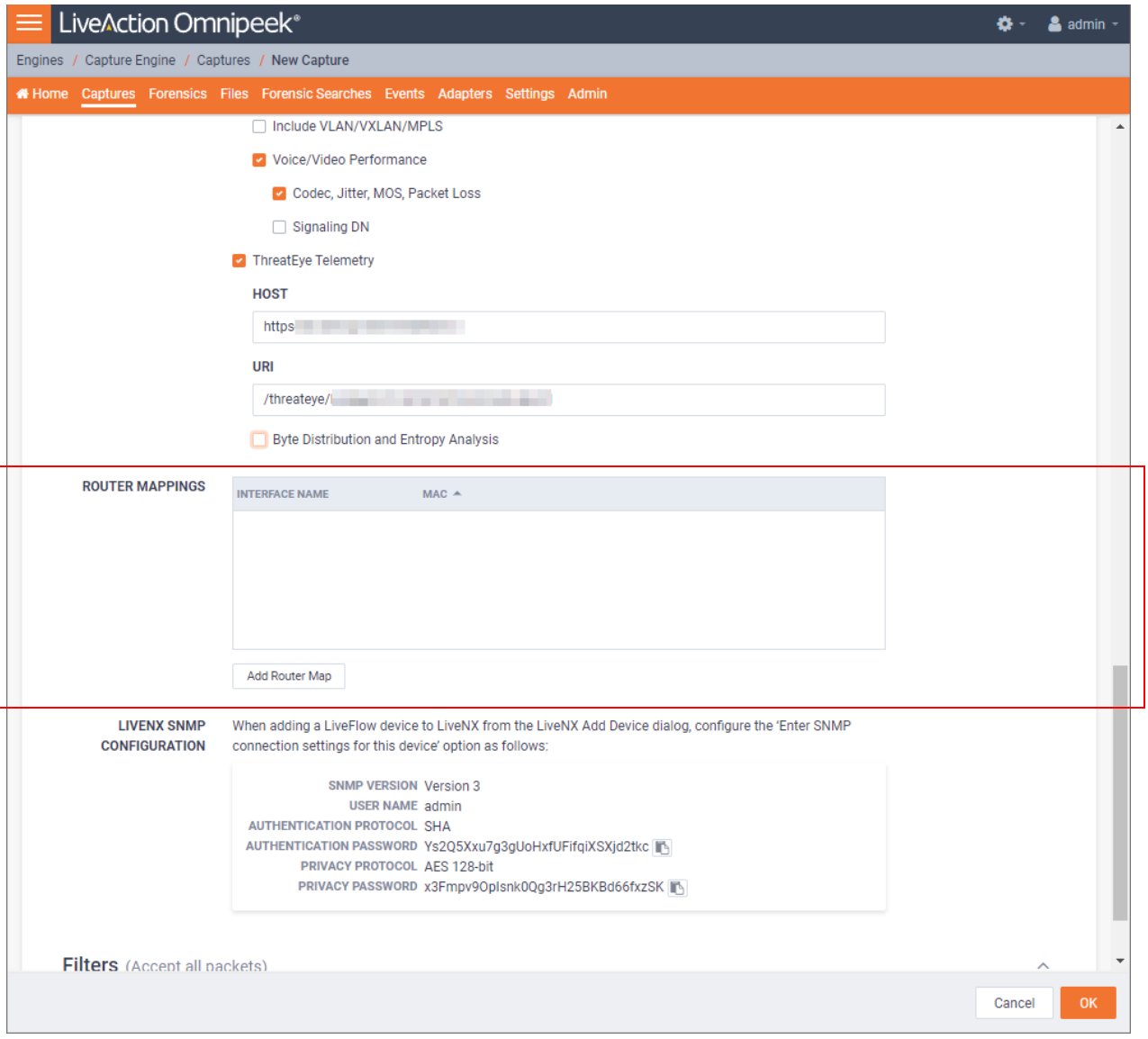
- *Host*: The *Host* (together with the *URI)* specifies the location of the ThreatEye analyzer and indicates where to send ThreatEye telemetry. The *Host* is provided by LiveAction and is made available as part of the licensing process. The *Host* must be configured if *ThreatEye Telemetry* is enabled.

- *URI*: The *URI* (together with the *Host)* specifies the location of the ThreatEye analyzer and indicates where to send ThreatEye telemetry. The *URI* is provided by LiveAction and is made available as part of the licensing process. The *URI* must be configured if *ThreatEye Telemetry* is enabled.
- *Byte Distribution and Entropy Analysis*: Select this option to enable the collection of byte distribution and entropy analysis metadata for Encrypted Traffic Analysis (ETA). This data is used to identify malware communications in encrypted traffic.

Note You must enable a *LiveNX Telemetry* and/or *ThreatEye Telemetry* record type; otherwise, the **OK** button is disabled.

Router Mappings

- *Router Mappings:* Router mappings are used exclusively when you are exporting LiveFlow data to LiveNX, and are used by LiveNX to display aggregated traffic from different segments as separate interfaces per the router map entries you enter in the *Router Mappings* settings.



To add a router map entry for any adapter, you will need to specify an interface name (ifname) and a MAC address of the gateway or router separated by a forward slash (e.g., *router_1/22:33:44:55:66:77*). The interface name can be up to 15 characters, and can include letters, numbers, and underscores. This will

tell LiveNX to display aggregated traffic from different segments as separate interfaces per the router map entries.

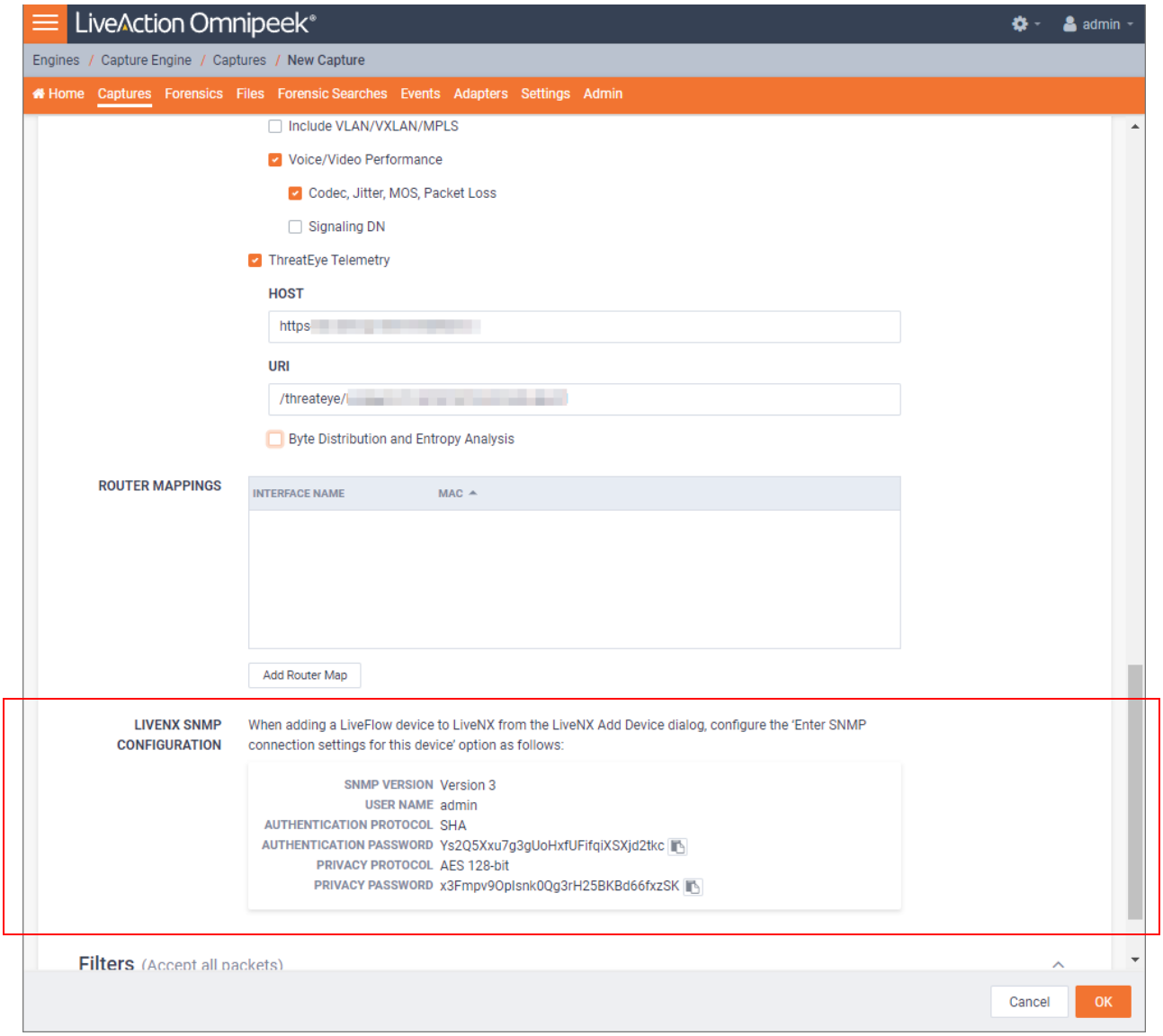
To find the MAC address of the gateway or router, the CLI can be used; otherwise, capture some traffic, or do a Forensics search and look at the *Nodes* view in hierarchical mode. The top level addresses should be the MAC addresses of the gateways and routers for each segment being captured.

Note Although the CLI may display the MAC address using the abbreviated dot notation, the address must be formatted in full colon notation in the LiveWire *Router Mapping* entry dialog.

- *Interface Name:* Displays the interface name of the router. All interface names must be unique, must not be empty, must not be more than 15 characters long, and may only include the following characters: numbers, letters and an underscore (_).
- *MAC:* Displays the MAC address of the router. All MAC addresses must be unique and must be a valid MAC address.
- *Add Router Map:* Click to add a new router mapping. You can add an unlimited number of router mappings.

LiveNX SNMP Configuration

- *LiveNX SNMP Configuration:* For each LiveWire Virtual device that you want to use with LiveNX, you must use the Web client in LiveNX to add the device to LiveNX (see the LiveNX documentation). Since you are most likely adding LiveWire Virtual as an SNMP device to LiveNX, you will need the information provided below when adding the LiveWire Virtual device.



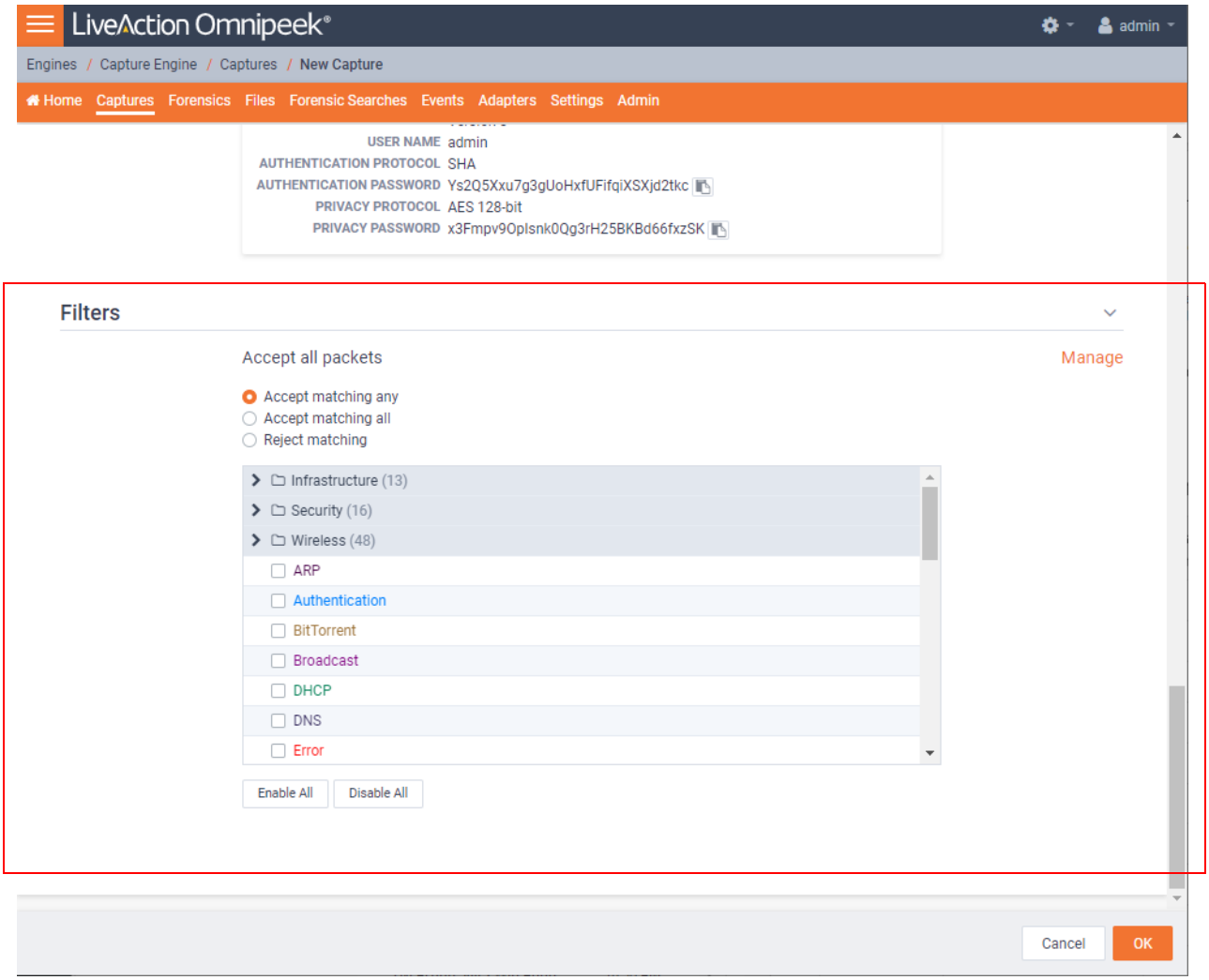
When configuring the '*Enter SNMP connection settings for this device*' option from the **Add Device** dialog in LiveNX client, configure the option as follows:

SNMP Version: **Version 3**
User Name: **admin**
Authentication Protocol: **SHA**
Authentication Password: **Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc**
Privacy Protocol: **AES 128-bit**
Privacy Password: **x3Fmpv9OpIsnk0Qg3rH25BKBd66fxzSK**

Note You can configure and change the *Authentication Password* and *Privacy Password*. See 'SNMP Credentials' in *Configure* on page 51.

Filters

The *Filters* settings let you enable or disable filters used when capturing packets or opening packet files. Select the filters you want to enable and then click *Accept Matching Any*, *Accept Matching All*, or *Reject Matching*.



- *Accept Matching Any:* When you choose *Accept Matching Any*, only those packets which match the parameters of at least one of the enabled filters are placed into the capture buffer.
- *Accept Matching All:* When you choose *Accept Matching All*, only those packets which match the parameters of all the enabled filters are placed into the capture buffer.
- *Reject Matching:* When you choose *Reject Matching*, only those packets which do not match any of the enabled filters are placed into the capture buffer.
- *Enable All:* Click to enable all filters.
- *Disable All:* Click to disable all filters.

Recommendations for better performance at higher data rates

- At high data rates the capture file can roll over multiple times every second. For higher data rates, the File Size should be increased. This will decrease how often the capture file has to be rolled over, and indirectly increase the performance.

- Forensic Searches use the same partition as the capture files, so leave some disk space available for the Forensic Search. Typically, 10-20 GB is sufficient, but the right setting will depend on the size of the forensic searches, and how many there are.
- Packet File Indexing is used to potentially increase Forensic Search performance when relevant filters are used. However, packet file indexing also decreases capture performance and can take a considerable amount of disk space.
- The file size and file indexes are related in that the smaller the file size the more packet indexes there will be. When there are more addresses, this can lead to large index files. A larger file size will generate fewer indexes.

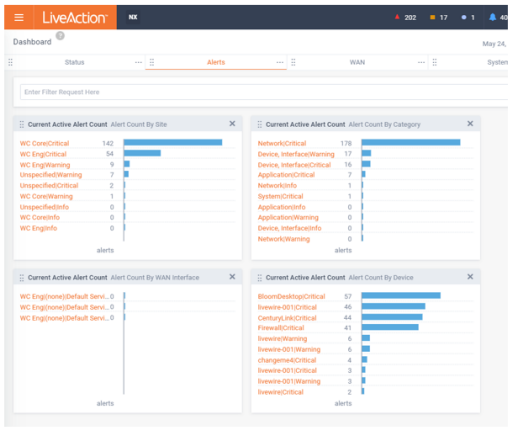
An example of using LiveWire Virtual, LiveNX, and Omnipeek

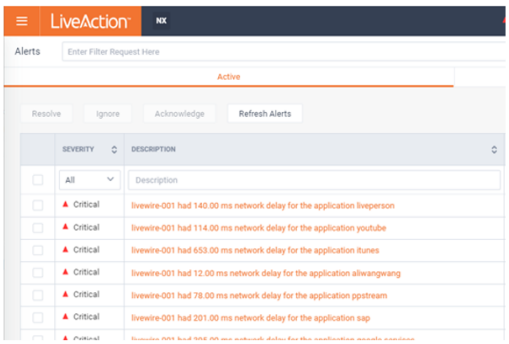
A web-based version of LiveAction's Omnipeek Network Analysis Software is available from LiveNX. You can easily start and use Omnipeek whenever you identify an interesting alert or flow in LiveNX that needs further investigation and you want to analyze the packet level details more closely in Omnipeek.

Note Omnipeek can be used independently of LiveNX, directly from the LiveWire Virtual appliance by entering the IP address of the LiveWire Virtual appliance into a web browser.

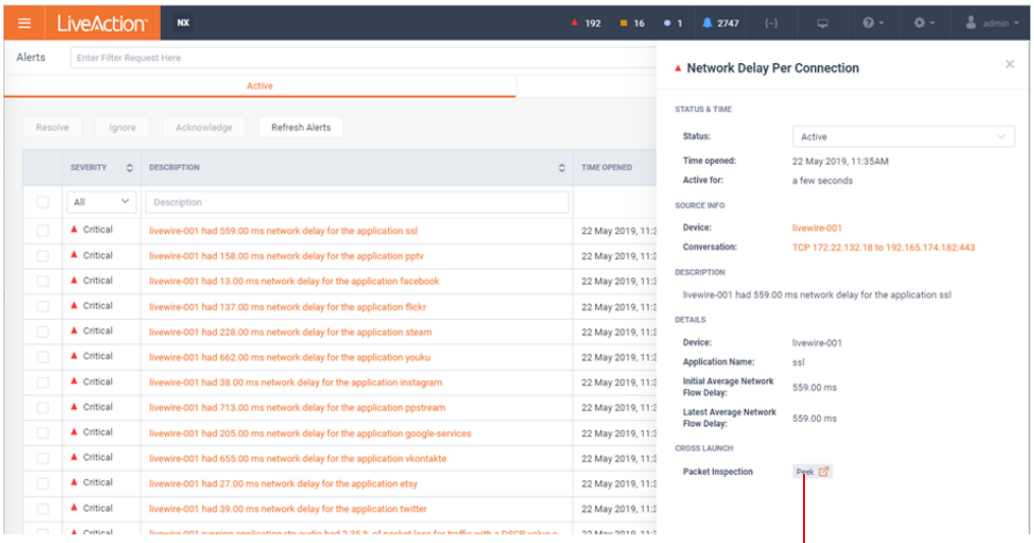
For example, a user on your network experiences poor call quality during a portion of their teleconference meeting. Since you have LiveNX and are populating it with both NetFlow from infrastructure routers as well as LiveFlow from LiveWire Virtual appliance, you can visualize any flow, including this teleconference call, from end to end.

Since the user did not want to disrupt their meeting to report the issue, you find out after the call has ended that the user experienced problems. Based on the user's information, you can quickly find the flow in LiveNX and see critical metrics regarding the call, including jitter and latency. The screen below shows alerts generated by LiveFlow sent from LiveWire Virtual.

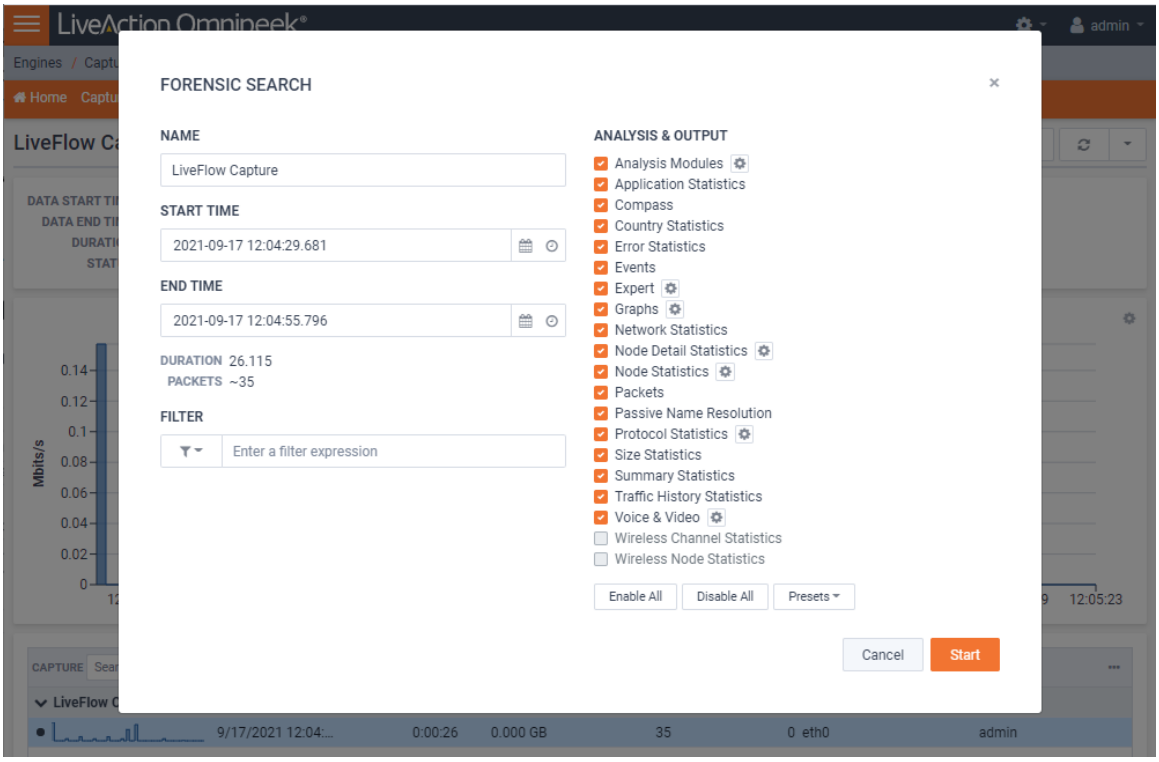




You also notice that an alert was triggered for excessive delay. This alert confirms the user's report, but you'd like to dig in even deeper to perform a root cause analysis of the issue. The best way to do this is with the network packets themselves, and since this call was captured by a LiveWire Virtual appliance you can simply click the 'Peek' button with the alert and immediately see all of the network packets for that teleconference session.



When the Peek button is clicked to cross-launch to packets, a new tab will open in the browser, and a Forensic Search dialog will appear with various options. This allows you to perform detailed analysis on the call in Omnipeek and determine exactly when the jitter was bad, and correlate that with other activity on the network, to determine the root cause.

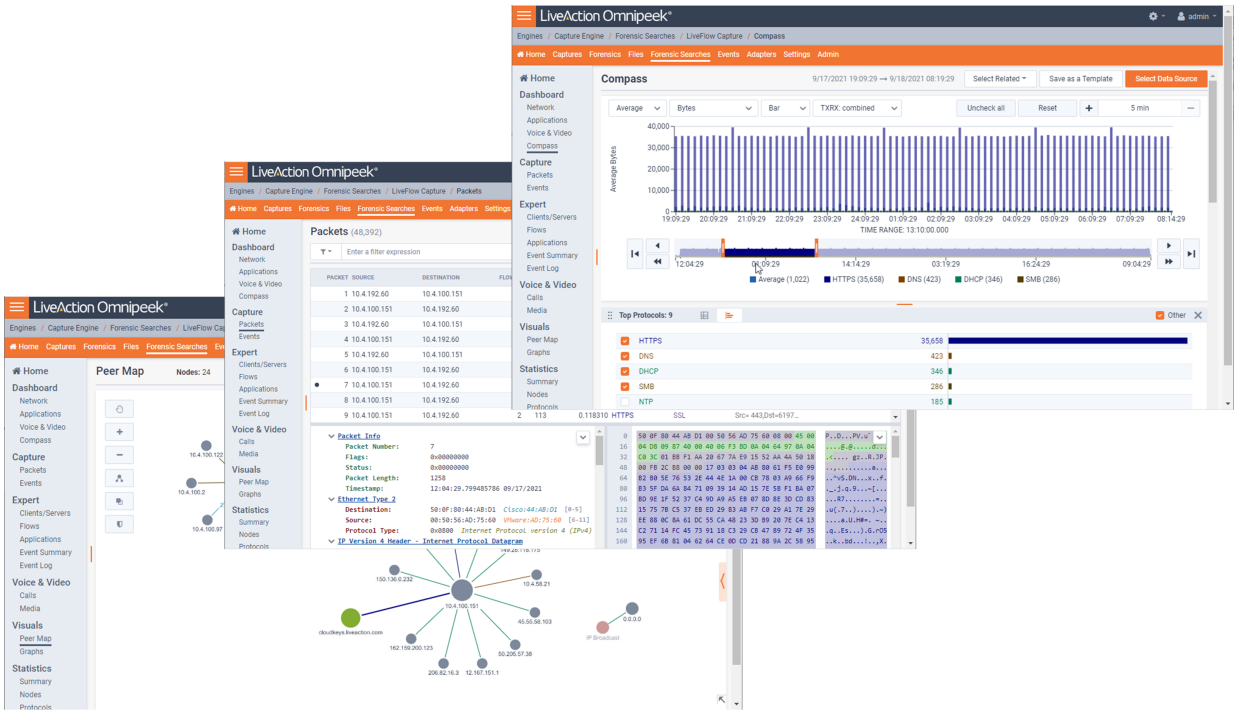


The default filter in the Forensic Search dialog includes the source and destination IP addresses of the flow. The filter can be changed to include more packets in the result, providing insight into what other traffic may be related or affecting the quality of the flow in question.

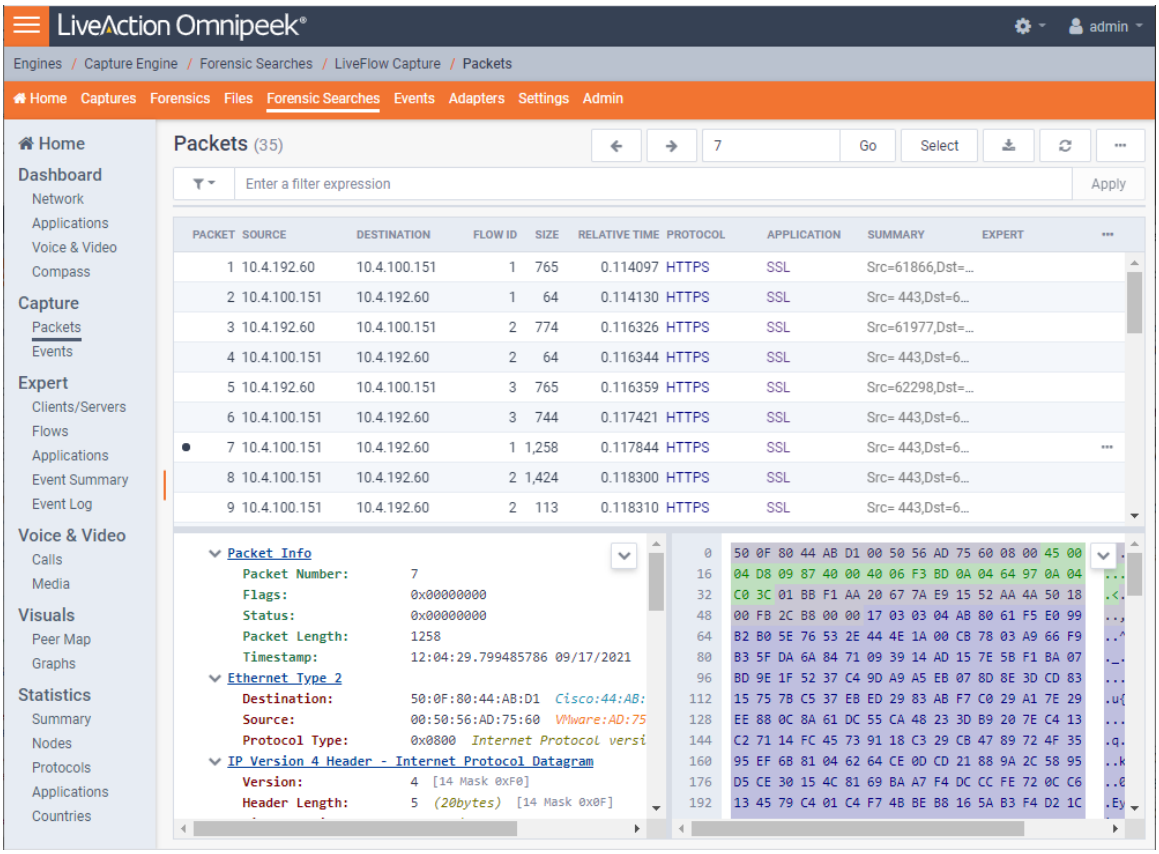
The time range can be adjusted to include more (or less) packets. This can work in conjunction with the filter, which when widened, will include more packets from the other flows between the source and destination IP.

The *Analysis & Output* options are used to include more or less analysis. The less analysis, the faster the forensic search will be. For example, if all you want are the packets, to load into Omnipeek, then just enable the packets option. Multiple forensic searches can be performed at the same time, and left running for others to use collaboratively. Keep in mind that a forensic search exists on the appliance, using memory and hard disk. When you are done using a forensic search it should be deleted.

The screen below shows various analysis views in Omnipeek which are good places to start understanding the problem as well as drill-down to the packets view.



The screen below shows the *Packets* view in Omnipeek which displays the list of packets and various other details about them, including the Experts, decode, and Hex view for each one.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Forensic Searches / LiveFlow Capture / Packets
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Home
Dashboard
Network
Applications
Voice & Video
Compass
Capture
Packets
Events
Expert
Clients/Servers
Flows
Applications
Event Summary
Event Log
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Summary
Nodes
Protocols
Applications
Countries
Packets (35)
Go
Select
Enter a filter expression
Apply
PACKET SOURCE DESTINATION FLOW ID SIZE RELATIVE TIME PROTOCOL APPLICATION SUMMARY EXPERT
1 10.4.192.60 10.4.100.151 1 765 0.114097 HTTPS SSL Src=61866,Dst=...
2 10.4.100.151 10.4.192.60 1 64 0.114130 HTTPS SSL Src= 443,Dst=6...
3 10.4.192.60 10.4.100.151 2 774 0.116326 HTTPS SSL Src=61977,Dst=...
4 10.4.100.151 10.4.192.60 2 64 0.116344 HTTPS SSL Src= 443,Dst=6...
5 10.4.192.60 10.4.100.151 3 765 0.116359 HTTPS SSL Src=62298,Dst=...
6 10.4.100.151 10.4.192.60 3 744 0.117421 HTTPS SSL Src= 443,Dst=6...
7 10.4.100.151 10.4.192.60 1 1,258 0.117844 HTTPS SSL Src= 443,Dst=6...
8 10.4.100.151 10.4.192.60 2 1,424 0.118300 HTTPS SSL Src= 443,Dst=6...
9 10.4.100.151 10.4.192.60 2 113 0.118310 HTTPS SSL Src= 443,Dst=6...
Packet Info
Packet Number: 7
Flags: 0x00000000
Status: 0x00000000
Packet Length: 1258
Timestamp: 12:04:29.799485786 09/17/2021
Ethernet Type 2
Destination: 50:0F:80:44:AB:D1 Cisco:44:AB:
Source: 00:50:56:AD:75:60 VMware:AD:75
Protocol Type: 0x0800 Internet Protocol versi
IP Version 4 Header - Internet Protocol Datagram
Version: 4 [14 Mask 0xF0]
Header Length: 5 (20bytes) [14 Mask 0x0F]
0 50 0F 80 44 AB D1 00 50 56 AD 75 60 08 00 45 00
16 04 D8 09 87 40 00 40 06 F3 BD 0A 04 64 97 0A 04
32 C0 3C 01 BB F1 AA 20 67 7A E9 15 52 AA 4A 50 18
48 00 FB 2C B8 00 00 17 03 03 04 AB 80 61 F5 E0 99
64 B2 B0 5E 76 53 2E 44 4E 1A 00 CB 78 03 A9 66 F9
80 B3 5F DA 6A 84 71 09 39 14 AD 15 7E 5B F1 BA 07
96 BD 9E 1F 52 37 C4 9D A9 A5 EB 07 8D 8E 3D CD 83
112 15 75 7B C5 37 EB ED 29 83 AB F7 C0 29 A1 7E 29
128 EE 88 0C 8A 61 DC 55 CA 48 23 3D B9 20 7E C4 13
144 C2 71 14 FC 45 73 91 18 C3 29 CB 47 89 72 4F 35
160 95 EF 68 81 04 62 64 CE 0D CD 21 88 9A 2C 58 95
176 D5 CE 30 15 4C 81 69 BA A7 F4 DC CC FE 72 0C C6
192 13 45 79 C4 01 C4 F7 4B BE B8 16 5A B3 F4 D2 1C

Capture Engines

In this chapter:

About Capture Engine

Pre-installed on LiveWire Virtual, Capture Engine captures and analyzes network traffic in real time and records that traffic for post-capture analysis. With Capture Engine, network engineering teams can monitor distributed networks remotely and quickly identify and remedy performance bottlenecks without leaving the office.

Capture Engine works in conjunction with Omnipeek, a separate software program required for the monitoring and analysis of the packets captured remotely by . For more information on how to view and analyze remote captures from within the Omnipeek console, please see *Using Capture Engines with Omnipeek* on page 117, and also the *Omnipeek User Guide* or Omnipeek online help.

Using the Capture Engine Manager

The Capture Engine Manager is installed by default when you install Omnipeek. You can run the Capture Engine Manager from the Omnipeek computer to do the following:

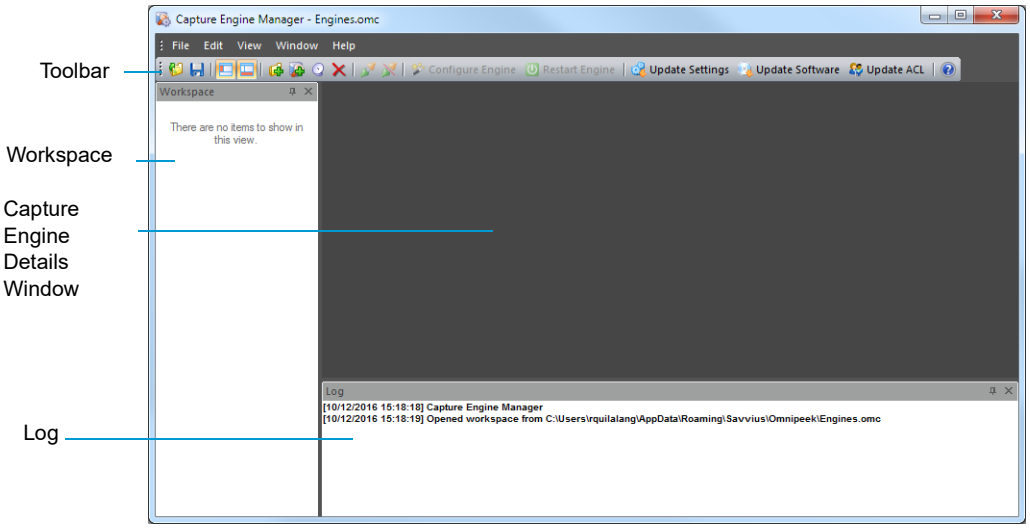
- Update and configure the Capture Engine on
- Display the status and configuration of Capture Engines
- Update settings for filters, alarms, remote graph templates, and capture templates
- Distribute security settings to all Capture Engines running within the same domain
- View the Audit log

Navigating the Capture Engine Manager window

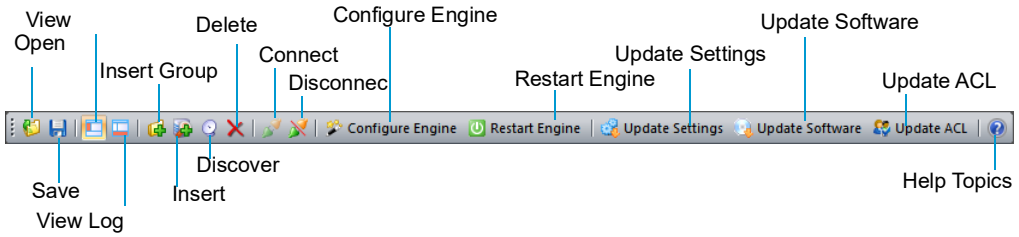
To start the Capture Engine Manager from the Omnipeek computer:

- Choose **Start** > **All Programs** > **LiveAction** > **LiveAction Capture Engine Manager for Omnipeek**. The **Capture Engine Manager** appears.
- On the **Start** menu, click **LiveAction Capture Engine Manager for Omnipeek**. The Capture Engine Manager appears.

The parts of the **Capture Engine Manager** window are described below.



- *Toolbar:* The toolbar allows you to control the following program functions:



- *Open:* Click to open a Capture Engine Manager Workspace *(*.omc)* file.

Note Opening a Capture Engine Manager Workspace *(*.omc)* file other than the *engines.omc* default file (located in *C:\Users\<username>\AppData\Roaming\LiveAction\Omnipeek)*, will no longer synchronize the list of Capture Engines displayed in Omnipeek and Capture Engine Manager.

- *Save:* Click to save the Capture Engine Manager Workspace *(*.omc)* file.
- *View Workspace:* Click to hide/show the Workspace pane.
- *View Log Window:* Click to hide/show the Log pane.
- *Insert Group:* Click to insert a new Capture Engine group.
- *Insert:* Click to insert a new Capture Engine.
- *Discover:* Click to discover Capture Engines via UDP multicast. See *Discover Capture Engines* on page 105.
- *Delete:* Click to delete the selected Capture Engine group or single Capture Engine.
- *Connect*: Click to display the **Connect** dialog, allowing you to connect to the selected Capture Engine. See *Connecting to a Capture Engine* on page 102.
- *Disconnect*: Click to disconnect the Capture Engine Manager from the Capture Engine displayed in the active window.
- *Configure Engine:* Click to start the **Capture Engine Configuration Wizard** to configure the Capture Engine. See *Configuring a Capture Engine* on page 106.
- *Restart Engine*: Click to restart the Capture Engine. See *Reconnect button* on page 105.
- *Update Settings:* Click to update the settings for **Filters**, **Alarms**, or **Graphs** for the Capture Engine. See *Updating Capture Engine settings* on page 111.
- *Update Software:* Click to update the Capture Engine software for one or more Capture Engines using the Update Service.
- *Update ACL:* Click to distribute a single Access Control List (ACL) to multiple Capture Engines running on machines belonging to the same Domain. See *Updating Capture Engine ACL settings* on page 112.
- *Help Topics:* Click to display online help for the Capture Engine Manager application.

- *Workspace:* This area displays the list of currently defined Capture Engines. Both Omnipeek and Capture Engine manager maintain the same list of Capture Engines. Making a change in either program automatically updates the list in the other program.

Note Right-click inside the Workspace to display a context-menu with additional options for displaying the list of Capture Engines; inserting and discovering Capture Engines; editing, deleting, or renaming Capture Engines; connecting and disconnecting Capture Engines; forgetting all passwords; and importing and exporting Capture Engines.

- *Capture Engine Details window:* This area displays the details and tabbed views for the Capture Engine. Each Capture Engine window can also have an **Analysis Modules** and **Audit Log** view, in addition to **Status, Filters, Alarms,** and **Graphs** views. Double-click any Capture Engine in the Workspace to view the details for that Capture Engine.
- *Log:* This area shows the messages sent to the Log file, including program start and the status of update tasks.
  - You can right-click inside the log to save, copy, or clear the contents of the Log file.
  - Choose **File** > **Save log** to save the Log file as a text file.

> **Tip** You can float the Workspace and Log panes, or drag either to dock it in a different location. To toggle between floating and docking, double-click the title bar of the window.

Creating new engine groups

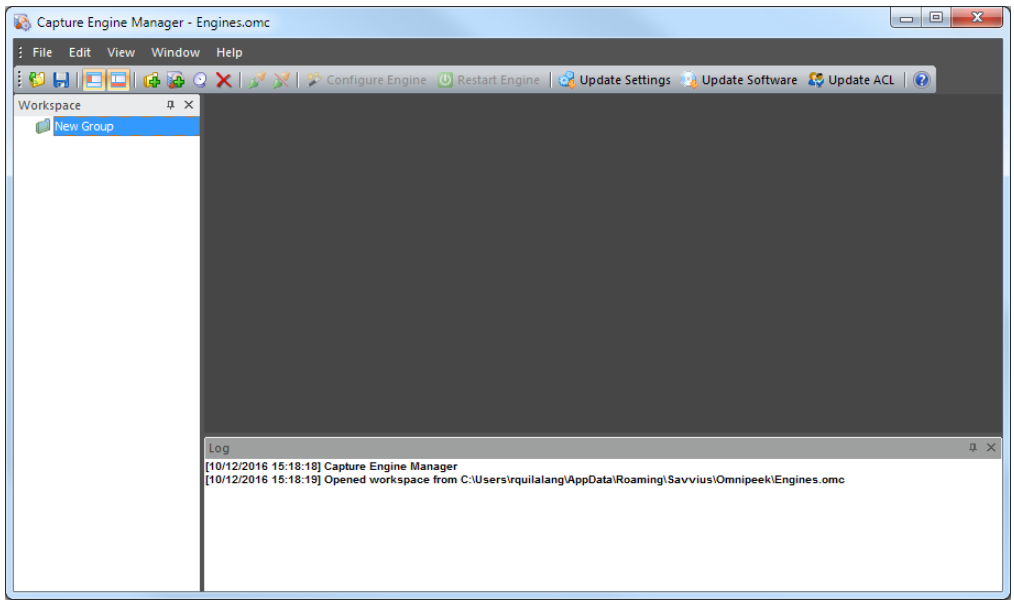
You can organize Capture Engines in groups or add single Capture Engines one at a time to the Workspace.

To create a new group in the Workspace:

1. Select the location in the Workspace under which the new group should appear.
2. Click **Insert Group** in the toolbar.

   The new group appears with its default name (*New Group*) ready to edit.

> **Tip** To change the name of a group in a Workspace file, right-click and choose **Rename**.

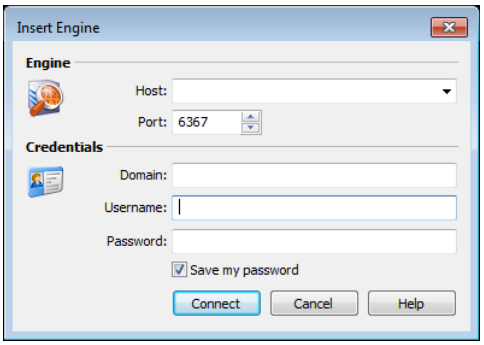


Connecting to a Capture Engine

You can connect to a Capture Engine and add it to the Workspace.

To add a Capture Engine to the Workspace:

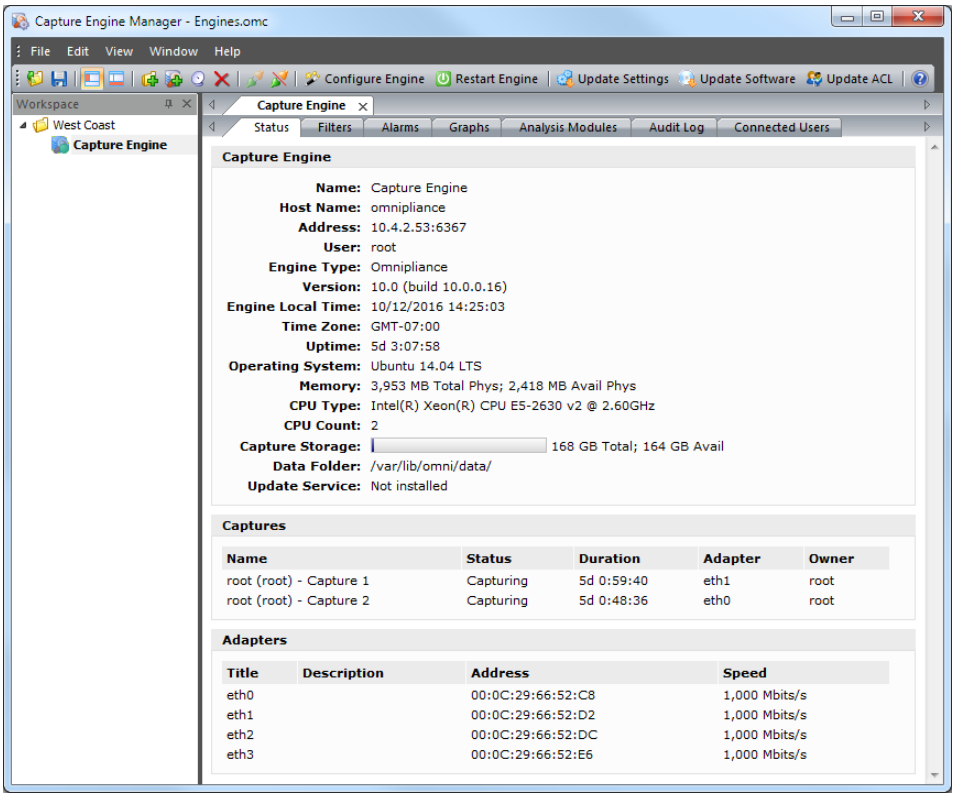
1. Select the location in the Workspace under which the new Capture Engine should appear.
2. Click **Insert Engine**. The **Insert Engine** dialog appears.



3. Complete the dialog:
   - *Host:* Enter the IP address or DNS name of the engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
   - *Username:* Type the Username for login to the Capture Engine.
   - *Password:* Type the Password for login to the Capture Engine.

Note If you leave the *Username* and *Password* fields blank, the Capture Engine Manager attempts to log in using the current Windows login credentials.

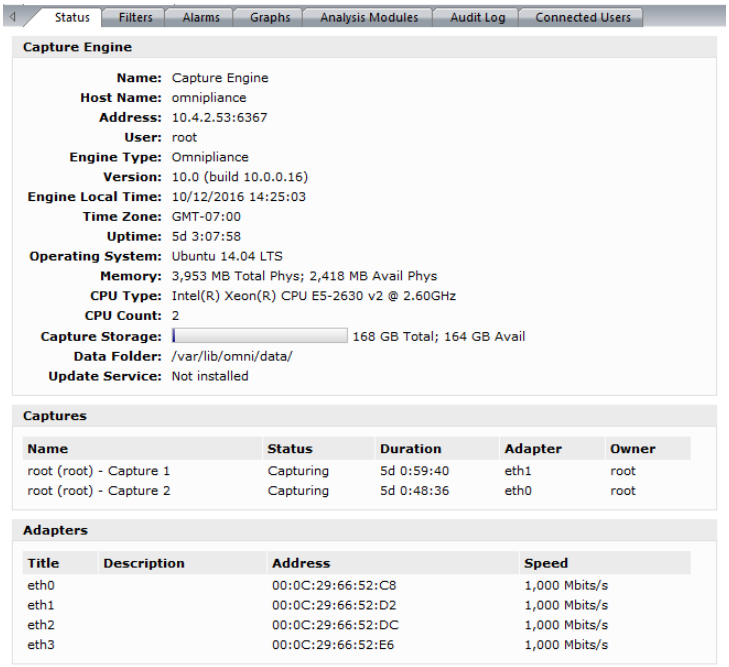
4. Click **Connect**. When the connection is established, the Capture Engine is added to the Workspace and its **Capture Engine** window is displayed showing details for that Capture Engine. See *Capture Engine details windows* on page 104.



Note When you close the **Capture Engine Manager** window, you are automatically disconnected from any Capture Engine displayed in the Capture Engine Manager. When you start the Capture Engine Manager again, all Capture Engines are in a disconnected state. You will need to reconnect to any Capture Engine that you want to configure or update.

Capture Engine details windows

A **Capture Engine** details window displays status information about the Capture Engine and lists the filter, alarm, and graph settings that can be distributed from the Capture Engine to other Capture Engines using the Capture Engine Manager. A Capture Engine details window can have the following tabs: **Status**, **Filters**, **Alarms**, **Graphs, Analysis Modules**, and **Audit Log** and **Connected Users**.



- The **Status** tab displays details about the connected Capture Engine. It includes the *Name*, *IP Address* and *Port* configured for the Capture Engine, *User*, product and file *Version* for the Capture Engine, and whether or not the *Update Service* is running.
  - *Captures:* Shows all the captures defined for the Capture Engine, including the Name, Status (Capturing or Idle), Duration, Adapter it is using, and the Owner.
  - *Adapters:* Shows all the adapters available to the Capture Engine, including the Title, Description, physical Address, and the network Speed.

Tip To print the **Status** tab of a Capture Engine window, make it the active window and choose **File** > **Print...**.

- The **Filters** tab lists all the filters defined for the Capture Engine
- The **Graphs** tab lists all the remote graph templates defined for the Capture Engine
- The **Analysis Modules** tab displays summary information about each analysis module installed on the Capture Engine
- The **Audit Log** tab lists all available information regarding events taking place on the Capture Engine. You can go to the first and last page of the log, and you can search the log.

- The **Connected Users** tab lists all users currently connected to the Capture Engine. Click **Refresh** to refresh the list.

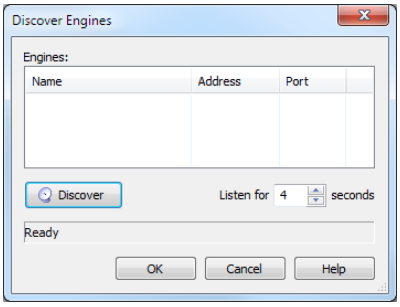
You can distribute settings from the **Filters**, **Alarms**, and **Graphs** tabs to other Capture Engines. For details, see *Updating Capture Engine settings* on page 111.

Discover Capture Engines

When you click **Discover** in the toolbar, the **Discover Engines** dialog appears. This dialog lets you search for Capture Engines installed on the local segment of your network. You can then insert one or more of the Capture Engines that are found into the Workspace.

To discover Capture Engines:

1. Click **Discover** in the toolbar. The **Discover Engines** dialog appears.



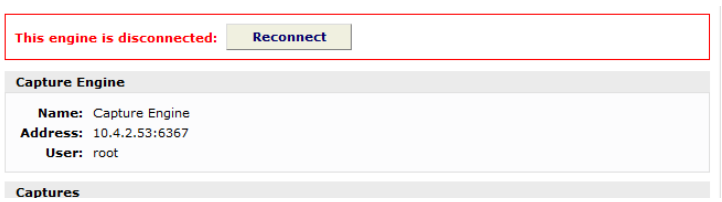
   - *Engines:* Displays the Capture Engines found on the local segment of your network.
   - *Discover:* Click to search for Capture Engines installed on the local segment of your network. The status message will change from *Listening...* to *Finished* when all network-available Capture Engines are discovered.
   - *Listen time:* Enter the number of seconds that the Capture Engine Manager will listen for responses to the discovery request. You can enter a minimum of 2 and a maximum of 60 seconds.
2. Click **Discover** on the dialog. All Capture Engines found on the local segment of your network are displayed in the Engines list.
3. Discovered Capture Engines have the check box next to their name selected. Clear the check boxes of the Capture Engines that you do not want to add to the Workspace and click **OK**. Only the selected Capture Engines are added to the Workspace.

> **Tip** Right-click in the *Engines* pane of the **Discover Engines** dialog and select **Uncheck all** to deselect all Capture Engines.

Reconnect button

To reconnect to a Capture Engine listed in the Workspace:

1. Open the **Status** tab of the **Capture Engine** window for the desired Capture Engine.
2. Click **Reconnect**.



When you click **Reconnect**, the Capture Engine Manager applies the most recently used login information for the selected Capture Engine.

Note If you wish to log in under a different *Username*, or if the configuration for the IP address and/or port have changed since your last login in the same session, you must use the **Connect** dialog directly. See *Connecting to a Capture Engine* on page 102.

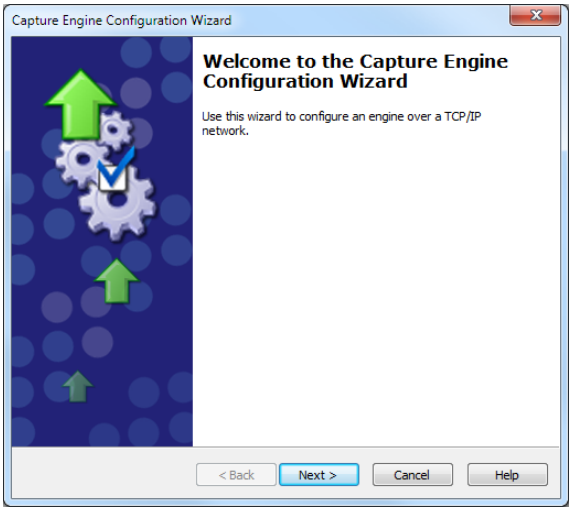
Configuring a Capture Engine

To configure a Capture Engine, you must use the **Capture Engine Configuration Wizard** of the Capture Engine Manager.

Note The **Capture Engine Configuration Wizard** of the Capture Engine Manager also appears when you first install a Capture Engine and are prompted to configure it.

To configure a Capture Engine from the Omnipeek computer:

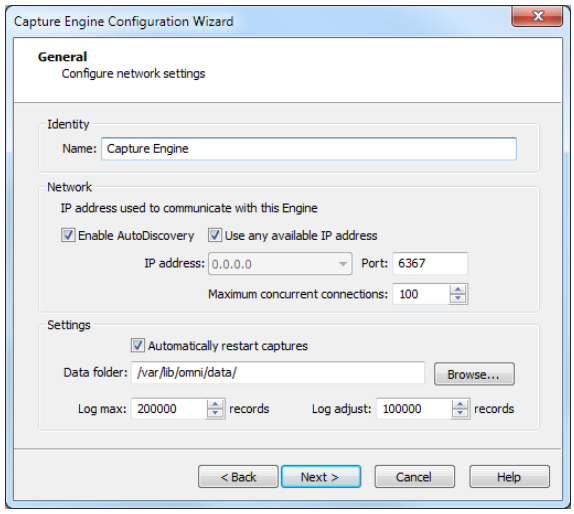
1. Choose **Start** > **All Programs** > **LiveAction** > **LiveAction Capture Engine Manager for Omnipeek**. The **Capture Engine Manager** window appears.
2. Connect to a Capture Engine in the Workspace (see *Connecting to a Capture Engine* on page 102) and click **Configure Engine** in the toolbar. The **Capture Engine Configuration Wizard** appears.



3. Click **Next**. The **General** view of the **Capture Engine Configuration Wizard** appears.
4. Configure the settings in the **General**, **Security**, and **Edit Access Control** views. See *Engine Configuration—General* on page 106; *Engine Configuration—Security* on page 107; and *Engine Configuration—Edit Access Control* on page 109.
5. When prompted, click **Yes** to send the configuration changes to the Capture Engine. The configuration changes won't take effect until the Capture Engine is restarted.

Engine Configuration—General

The **General** view of the **Capture Engine Configuration Wizard** lets you configure the name, address, capture restart, local disk use, and log settings for the Capture Engine.

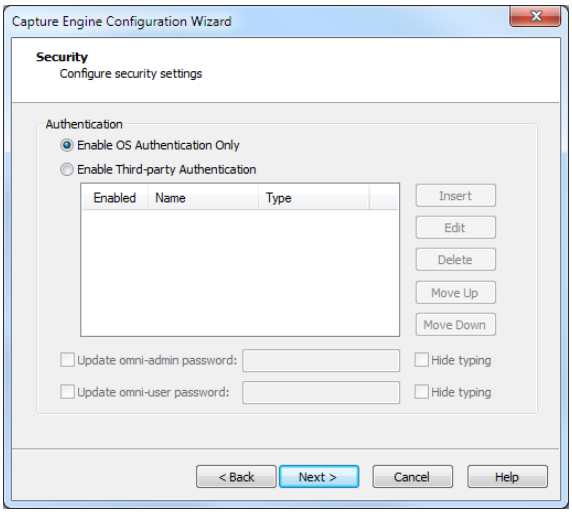


- *Name:* Type a name for the Capture Engine. This name appears in the **Capture Engines** window in Omnipeek.
- *Enable AutoDiscovery:* Select this check box to enable the Capture Engine to respond to autodiscovery requests which arrive from the Capture Engine Manager.
- *Use any available IP address:* Select this check box to accept communications on any and all IP addresses assigned to the computer on which the Capture Engine is installed.
- *IP address:* Select the IP address used to communicate with the Capture Engine. The Capture Engine will respond to communications only on that address. This option is not available when *Use any available IP address* is selected.
- *Port:* Type a port used for communications. The default port is 6367.
- *Maximum concurrent connections:* Type or select the maximum number of concurrent Omnipeek connections allowed for the Capture Engine.
- *Automatically restart captures:* Select this check box to automatically restart captures whenever the Capture Engine restarts. When enabled, the Capture Engine remembers any capture (active or idle) defined for it, and restores the capture whenever the Capture Engine itself is restarted.
- *Data folder:* Type or browse to the location for the data folder. The Capture Engine uses this location to store packet files created when the *Capture to Disk* option is used. The contents of the data folder appear in the **Files** tab of the Omnipeek **Capture Engines** window.
- *Log max:* Select or enter the maximum number of records in the application log. These are the log records you see in the Capture Engine log view. You can enter a range between 100,000 to 100,000,000 records (do not include commas). The default is 200000.
- *Log adjust:* Select or enter the number of application log records that are deleted (the oldest records are deleted first) when the maximum number of log records is reached. You can enter a range between 10,000 to 100,000,000 messages (do not include commas). The default is 100000.

Note Setting the *Log max* or *Log adjust* value to a large number of records or messages can slow down the performance of entries written to the log.

Engine Configuration—Security

The **Security** view of the **Capture Engine Configuration Wizard** lets you set security and authentication settings.



- *Authentication:*
  - *Enable OS Authentication Only:* Select this check box to use the Operating System authentication only, and to disable all other third-party authentication mechanisms.
  - *Enable Third-party Authentication:* Select this check box to enable third-party authentication using an Active Directory, RADIUS, or TACACS+ authentication server. For more information on enabling Third-party authentication, see *Third-party authentication with Capture Engines* on page 120.
  - *Insert:* Click to display the **Edit Authentication Setting** dialog, which allows you to name the setting and select from one of the following *Third-party Authentication* types:
    - *Active Directory:* Select this type to enable Active Directory authentication, and then configure the host information: *Host* (domain controller) and *Port* settings (Capture Engine (Windows)); or *Realm* (domain controller) and *KDC* settings (Capture Engine (Linux)).
    - *RADIUS:* Select this type to enable RADIUS authentication, and then configure the *Host* (IP address), *Port*, and *Secret* settings (select *Hide Typing* to hide the settings) for the RADIUS authentication server.
    - *TACACS+:* Select this type to enable TACACS+ authentication, and then configure the *Host* (IP address), *Port*, and *Secret* settings (select *Hide Typing* to hide the settings) for the TACACS+ authentication server.
  - *Edit:* Click to edit the selected authentication setting.
  - *Delete:* Click to delete the selected authentication setting.
  - *Move Up:* Click to move the selected authentication setting higher up in the list.
  - *Move Down:* Click to move the selected authentication setting lower up in the list.

Note The order of the authentication settings in the list determines the order an authentication server is authenticated against.

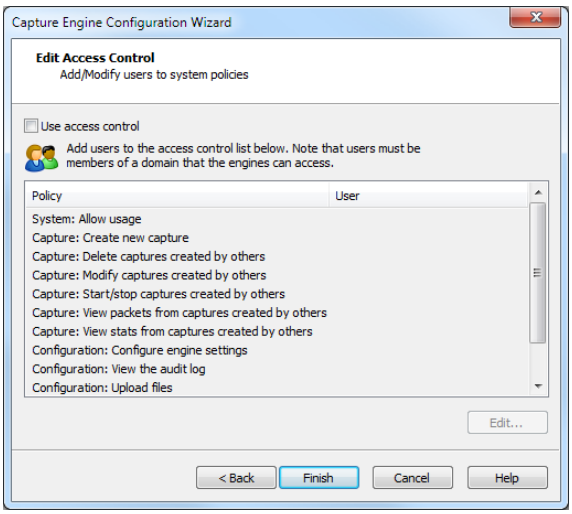
Authentication settings are attempted in groups in a top/down order. For example, if the first setting at the top is a RADIUS setting, then all RADIUS settings in the list are attempted first before attempting the next group type in list. If an authentication server can not be reached because of either an incorrect or unreachable server IP, incorrect port, or incorrect shared secret, then the next setting in the group is attempted. If communication with the authentication server is good, but the user cannot be authenticated because of either an incorrect username, password, or a disabled account, then the next group type is attempted (if authenticating a RADIUS or TACACS+ setting), or the next setting in the list is attempted (if authenticating an Active Directory setting).

Note The Capture Engine operates within the security environment configured in the operating system. Refer to your operating system documentation for instructions on configuring security settings for your operating system.

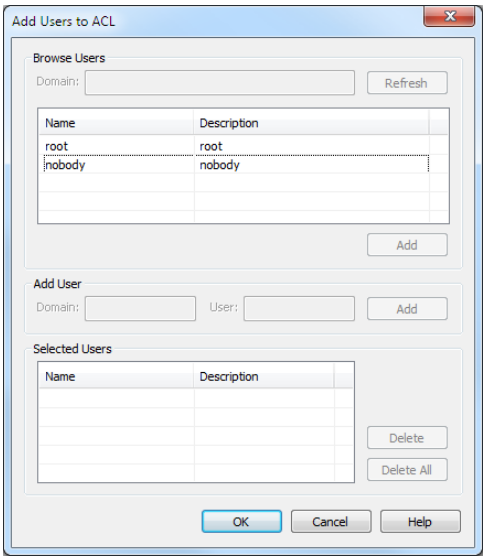
Engine Configuration—Edit Access Control

The **Edit Access Control** view of the **Capture Engine Configuration Wizard** lets you define which users have access to a Capture Engine and which classes of actions (policies) each user is allowed to perform.

Note There are several ways to create a new user in your operating system. Refer to your operating system documentation for instructions on creating new user profiles.



- *Use access control:* Select this check box to enable Access Control.
- The *Policy* column lists the predefined policies:
  - *System: Allow usage*
  - *Capture: Create new capture*
  - *Capture: Delete captures created by others*
  - *Capture: Modify captures created by others*
  - *Capture: Start/Stop captures created by others*
  - *Capture: View packets from captures created by others*
  - *Capture: View stats from captures created by others*
  - *Configuration: Configure engine settings*
  - *Configuration: View/modify matrix switch settings (Capture Engine (Windows) only)*
  - *Configuration: View the audit log*
  - *Configuration: Upload files*
- The *User* column lists which users have access to a certain policy.
- *Edit:* Select a policy and then click **Edit** to define which users have access to the policy. The **Add Users to ACL** dialog appears:



Browse Users

- *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
- *Refresh:* Click to poll the Domain controller to retrieve the list of users.

Note Large Domains with hundreds of users may take several minutes to load.

- *Name/Description:* Displays the name and description for each defined user. Both the name and the description are taken from the operating system security settings (local or Domain).
- *Add:* Click to add the selected user to the *Selected Users* table.

Add User

Note If the Capture Engine is not a member of any Domain, you can ignore *Add User*.

- *Domain:* Type the Domain for the Capture Engine.
- *User:* Type the name of the User you wish to add to the *Selected Users* table.
- *Add:* Click to add the selected user to the *Selected Users* table.

Selected Users

- *Name/Description:* Displays the name and description of users allowed to perform the selected policy.
- *Delete:* Click to remove the selected user from the *Selected Users* table.
- *Delete all:* Click to remove all users from the *Selected Users* table.

Tip A *Policy* that has no users associated with it is effectively reserved for users with Administrator or root level privileges.

Considerations when configuring Access Control

Please note the following when configuring Access Control:

- Users with Administrator or root level privileges always have access to all features of the Capture Engine.

- If the Capture Engine is installed on a machine under local control, the local user with Administrator or root level privileges (and equivalents) has access to the Capture Engine regardless of the settings in the **Edit Access Control** view.
- If the Capture Engine is installed on a machine under Domain control, the Domain Administrator always has access regardless of the settings in the **Edit Access Control** view.
- When *Use access control* is selected and no other users are added to the **Edit Access Control** view (the initial default settings), then only the user with Administrator (local or Domain, depending on the computer setup) or root level privileges has access to the Capture Engine.

Considerations when disabling Access Control

When access control is disabled, the only restrictions on the use of the Capture Engine are those imposed by the operating system security settings. Examples of relevant permissions controlled by operating system security settings include:

- **Login privilege:** A user must be able to log in to the machine on which the Capture Engine is running in order to use the program.

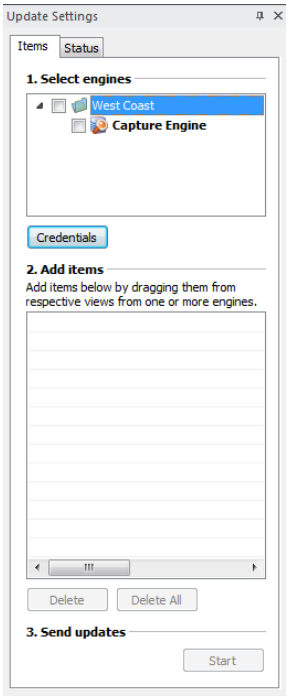
Updating Capture Engine settings

The Capture Engine Manager lets you distribute settings for filters, alarms, and graphs from one or more connected Capture Engines to one or more selected Capture Engines.

Important! You must have Administrator or root level privileges for the Capture Engine where you are distributing settings.

To update settings for one or more Capture Engines:

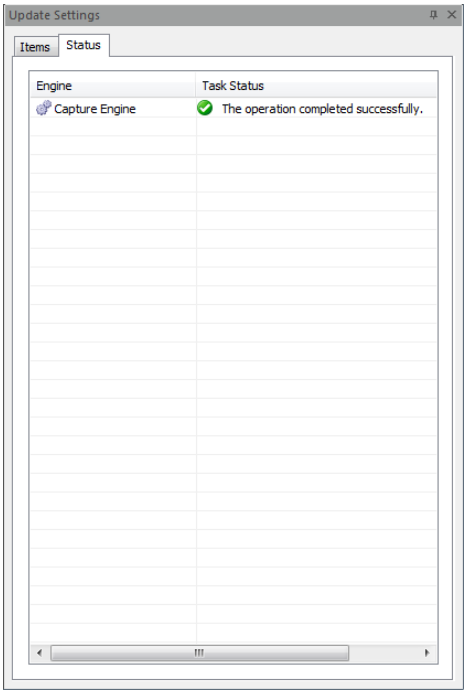
1. Click **Update Settings** in the toolbar. The **Update Settings** dialog appears and lists the Capture Engines defined in the Workspace.



2. Select the check box of the Capture Engines you are updating. You can right-click inside the view to expand all/collapse all lists, or check all /uncheck all Capture Engines.

Note You can click **Credentials** to enter the login credentials that can be used to connect to one or more Capture Engines when distributing software updates or new settings. See *Credentials dialog* on page 116.

3. Open the Capture Engine window of any connected Capture Engine in the Workspace and select the **Filters**, **Alarms**, or **Graphs** tab.
4. Drag-and-drop an item from the **Filters**, **Alarms**, or **Graphs** tab to the *Add items* section of the **Update Settings** dialog. You can add any combination of filters, alarms, or graphs settings.
5. Click **Start** to send the settings to the selected Capture Engines.
6. Click the **Status** tab to see the current status of all configuration updates for each target Capture Engine.



Note To update the settings for a target Capture Engine that has *Use access control* enabled, you must log in either as a user associated with the *System: Allow usage* policy or as a user with Administrator or root level privileges (local or Domain) for the host machine. If the target Capture Engine does not have *Use access control* enabled, any user with read/write privileges to the Data folder directory of the target Capture Engine can use the **Update Settings** dialog.

Updating Capture Engine ACL settings

The Access Control List (ACL) limits access to a Capture Engine by associating *Users* (defined in the operating system) with classes of tasks on the Capture Engine, called *Policies*. These associations are set in the configuration of each Capture Engine.

The Capture Engine Manager also lets you add the same Domain username and Policy associations to the ACLs of multiple Capture Engines, all of which are operating under the same Domain control.

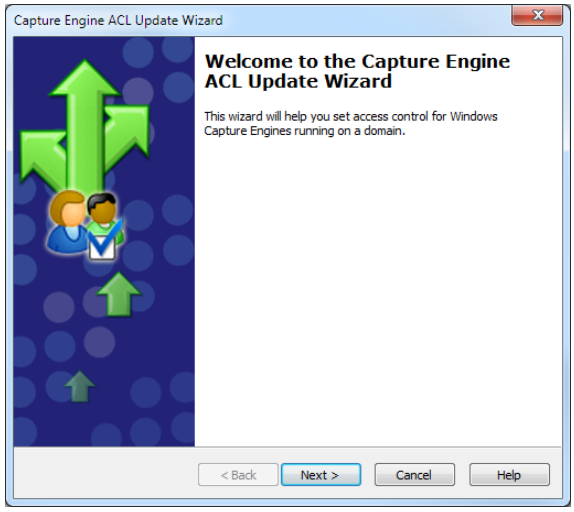
Note To use the ACL with Omnipliance Linux, you must first add the user to the Linux OS and then add the same user to the first ACL policy, "System: Allow usage." You can then limit that user's permission by adding the user to any of the other ACL policies.

Important! The Capture Engine Manager must be able to log in to each target Capture Engine as a user with the correct permissions to update the ACL on that Capture Engine, as described above. For detailed login information, see *Credentials dialog* on page 116.

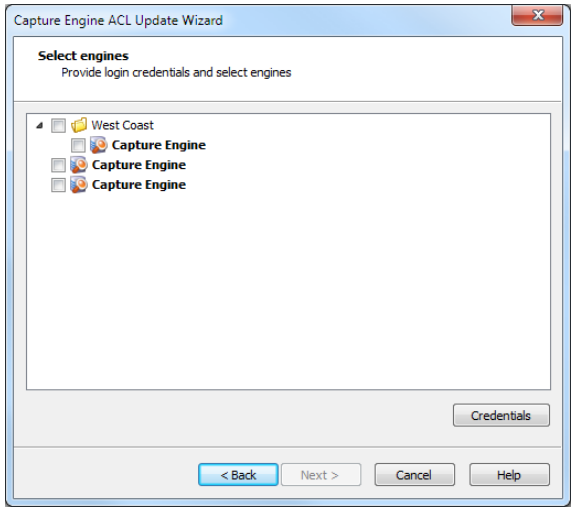
Note To use the **Capture Engine ACL Update Wizard**, you must present the correct login credentials for each target machine. For a Capture Engine with *Use access control* enabled, any user associated with both the *System: Allow usage* and *Configuration: Configure engine settings* policies can configure the Capture Engine. Any user with Administrator privileges (local or Domain) on the target machine can configure the Capture Engine, regardless of any settings in its ACL.

To distribute an ACL update to one or more Capture Engines in a single domain:

1. Click **Update ACL** in the toolbar. The **Capture Engine ACL Update Wizard** appears.



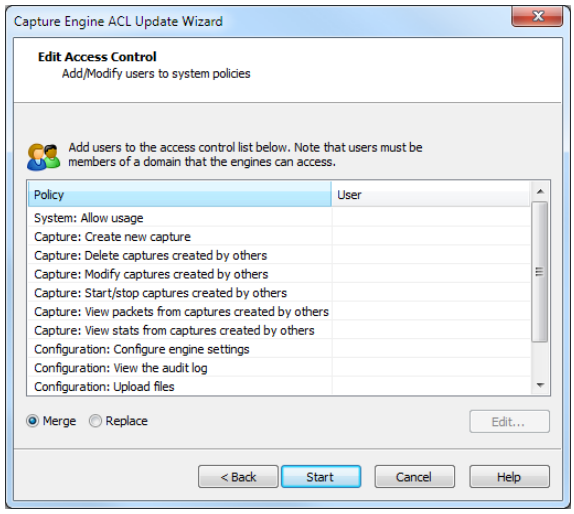
2. Click **Next**. The **Select engines** view appears and lists the Capture Engines defined in the Workspace.



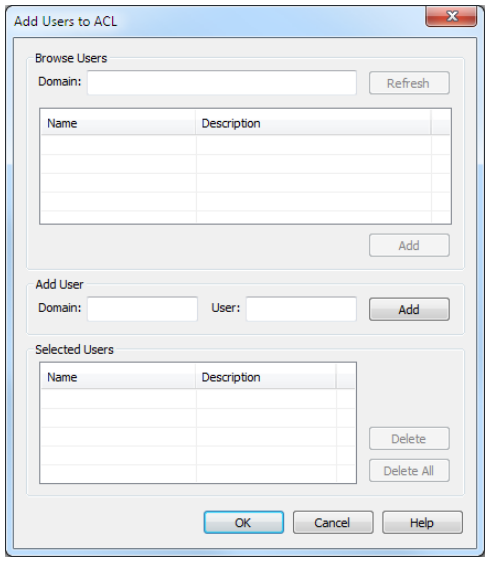
3. Select the check box of the Capture Engines you are updating. You can right-click inside the view to expand all / collapse all lists, or check all / uncheck all Capture Engines.

Note You can click **Credentials** to enter the login credentials that can be used to connect to one or more Capture Engines when distributing software updates or new settings. See *Credentials dialog* on page 116.

4. Click **Next** to open the **Edit Access Control** view. From this view, you can associate any *User* defined for the current Domain with any *Policy* defined for the selected Capture Engines.



5. Select a *Policy* in the list and click **Edit**. The **Add Users to ACL** dialog appears.



Browse Users

- *Domain* (Capture Engine (Windows) only)*:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
- *Refresh:* Click to poll the Domain controller to retrieve the list of users.

Note Large Domains with hundreds of users may take several minutes to load.

- *Name/Description:* Displays the name and description for each defined user. Both the name and the description are taken from the operating system security settings (local or Domain).
- *Add:* Click to add the selected user to the *Selected Users* table.

Add User (Capture Engine (Windows) only)

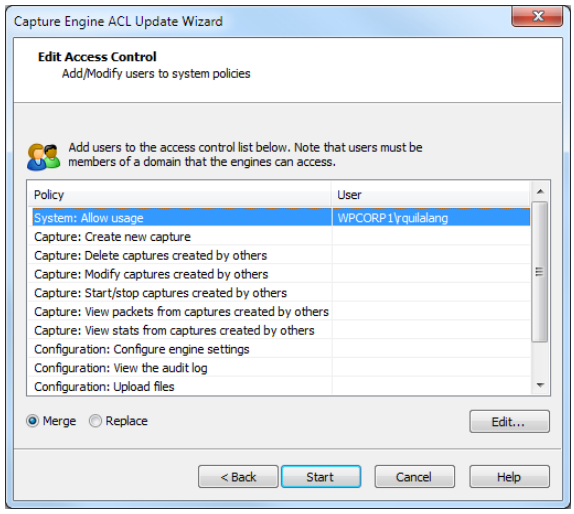
- *Domain:* Type the Domain for the Capture Engine.
- *User:* Type the name of the User you wish to add to the *Selected Users* table.
- *Add:* Click to add the selected user to the *Selected Users* table.

Selected Users

- *Name/Description:* Displays the name and description of users allowed to perform the selected policy.
- *Delete:* Click to remove the selected user from the *Selected Users* table.
- *Delete all:* Click to remove all users from the *Selected Users* table.

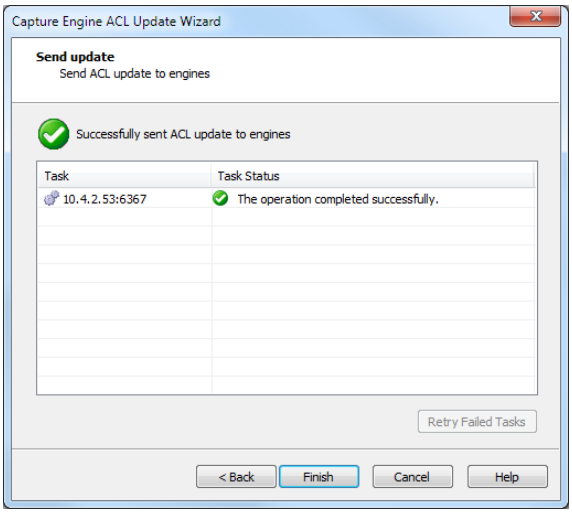
Tip A *Policy* that has no users associated with it is effectively reserved for users with Administrator or root level privileges.

6. Enter the name of the *Domain* and click **Refresh**. The dialog will poll the Domain controller to retrieve a list of users.
7. Select a user you want to associate with the current Policy and click **Add**. The user will appear in the *Selected Users* table of the dialog. Repeat this step until you have added all the users you wish to associate with the current Policy.
8. Click **OK** to close the dialog and return to the **Edit Access Control** view. The users from the *Selected Users* table appear in the *Users* column beside the appropriate *Policy*. You can choose to *Merge* users to the existing Access Control List, or *Replace* the existing Access Control List with a new list defined here.



9. Continue in this manner until you have fully defined the ACL.
10. Click **Start** to begin distributing the ACL to the listed Capture Engines. The **Send update** dialog appears and displays the task status.

Tip If at least one task fails, you can click **Retry Failed Tasks** to send the update again to the Capture Engines that did not complete the task successfully.



Note In order to be able to retrieve the list of Domain users, you must be logged on as a user with Administrator privileges (local or Domain). Additionally, you must have logged on to a computer under the Domain control of the target Domain during the current session of Windows. Your Domain login can have been as a Domain user of any kind, Administrator or otherwise.

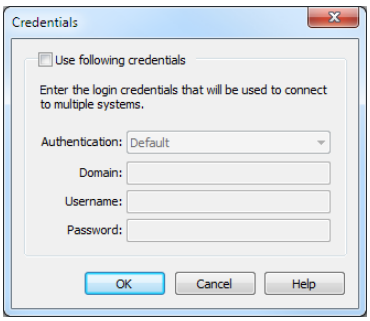
11. Click **Finish** to close the **Capture Engine Update ACL Wizard**.

Credentials dialog

The **Credentials** dialog lets you present a single set of credentials when you distribute software updates, setting updates, or ACL updates to Capture Engines.

To open the Credentials dialog:

1. Click **Credentials...** in any of the following views:
   - the **Items** tab of the **Update Settings** dialog (see *Updating Capture Engine settings* on page 111).
   - the **Select engines** view of the **Capture Engine Update ACL Wizard** (see *Updating Capture Engine ACL settings* on page 112).



2. Select the *Use following credentials* check box to enable credentials.
3. Complete credential information for *Authentication*, *Domain*, *Username*, and *Password*. See *Connecting to a Capture Engine* on page 102 for details.
4. Click **OK** to accept your changes.

Using Capture Engines with Omnipeek

Capture Engines have no user interface of their own and rely on an Omnipeek console to provide a user interface through the **Capture Engines** window. The **Capture Engines** window in Omnipeek is used for interaction between Omnipeek and a Capture Engine.

Connecting to a Capture Engine from Omnipeek

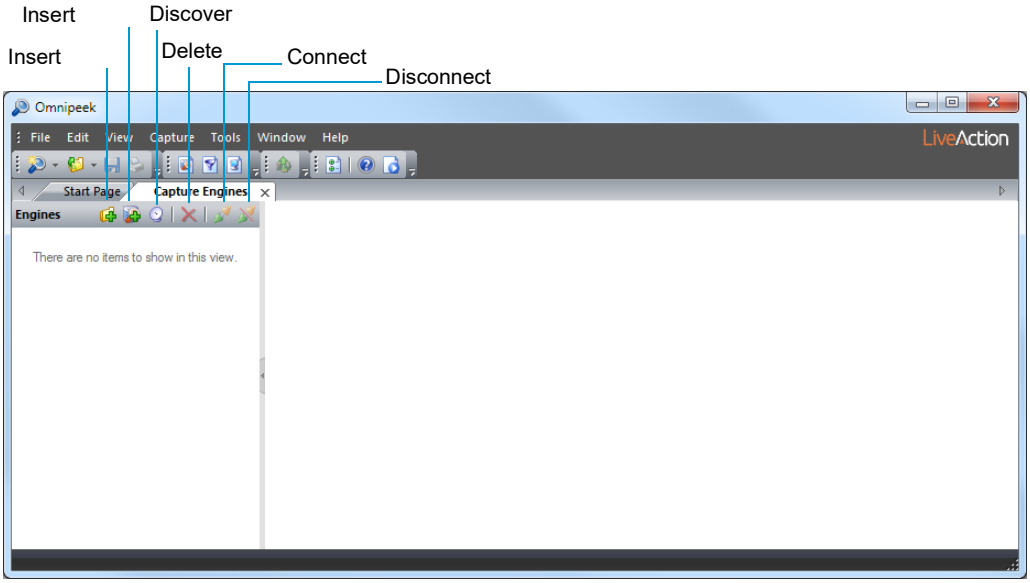
In order to view packets and data from a Capture Engine, you must first connect to the Capture Engine from the **Capture Engines** window.

To connect to a Capture Engine from Omnipeek:

1. Do one of the following to display the **Capture Engines** window:
   - Choose **View** > **Capture Engines**.
   - Click **View Capture Engines** on the Start Page.

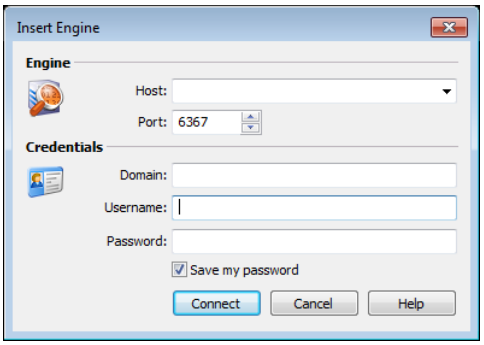
   The **Capture Engines** window appears and displays the list of currently defined Capture Engines.

> **Note** Both Omnipeek and Capture Engine Manager maintain the same list of Capture Engines. Making a change in either program automatically updates the list in the other program.

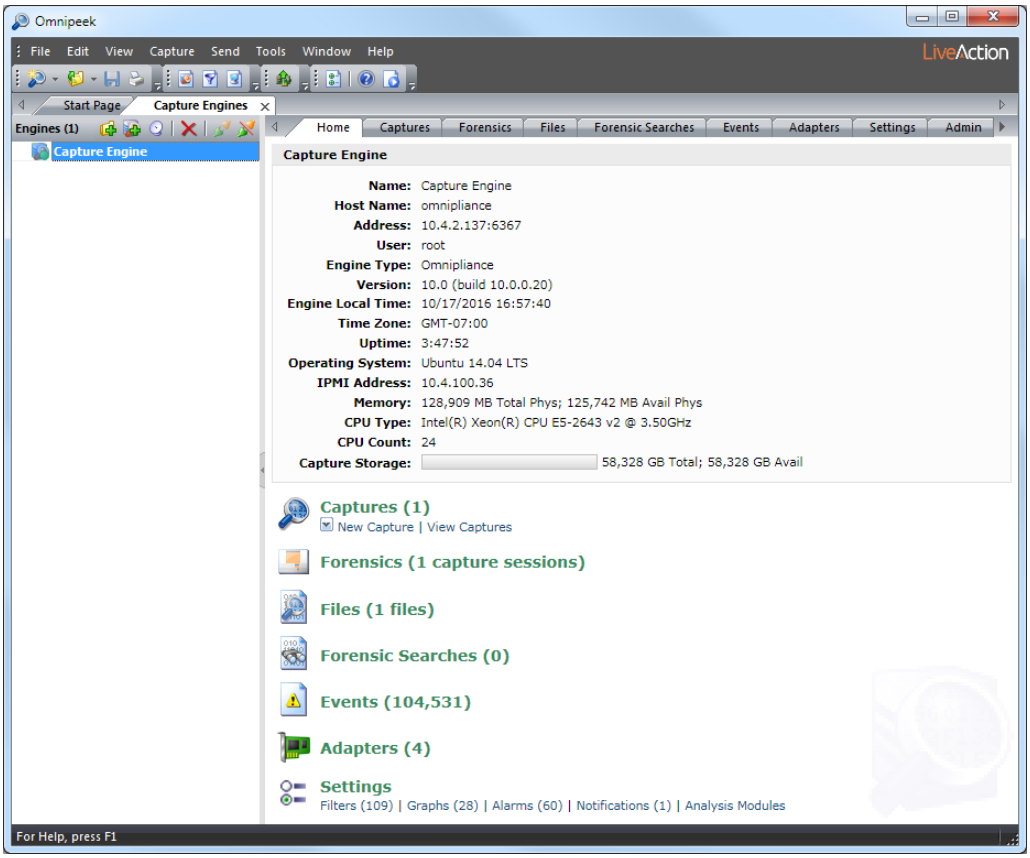


2. Click **Insert Engine**. The **Insert Engine** dialog appears.

> **Note** You can also click **Discover Engine** in the toolbar to find all of the Capture Engines available on your network segment. See *Discover Capture Engines* on page 105 for details.

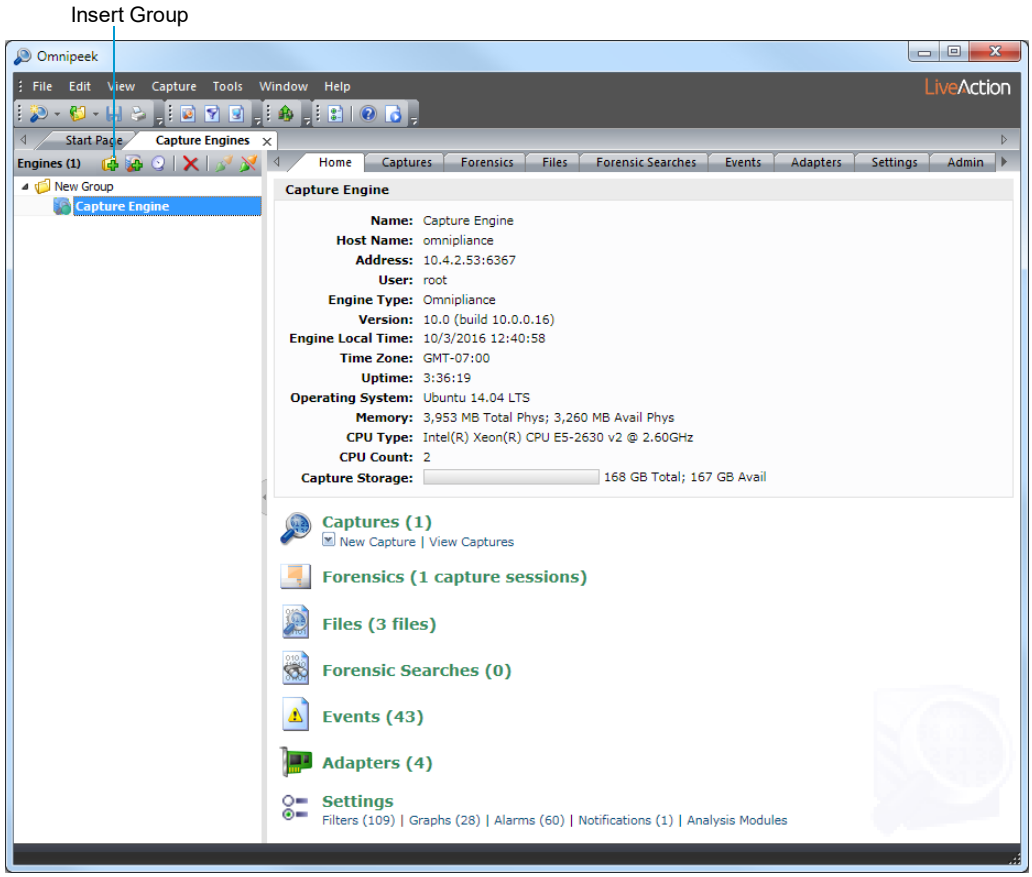


3. Complete the dialog:
   - *Host:* Enter the IP address of the Capture Engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
   - *Username:* Type the Username for login to the Capture Engine.
   - *Password:* Type the Password for login to the Capture Engine.
4. Click **Connect**. When the connection is established, the Capture Engine appears in the **Capture Engines** window.



Tip You can add multiple Capture Engines to the **Capture Engines** window by clicking **Insert Engine**.

5. Click **Insert Group** to add a group of Capture Engines to the **Capture Engines** window.
6. Select the Capture Engine group and then click **Insert Engine** to add an Capture Engine to the group.



Capturing from a Capture Engine

You can select from the following options to capture packets from a Capture Engine:

- *New Capture...*: This option lets you create a new capture window based on the capture settings that you define.
- *New "Forensics Capture"*: This option lets you create a new capture window based on pre-configured capture settings optimized for post-capture forensics analysis.
- *New "Monitoring Capture"*: This option lets you create a new capture window based on pre-configured capture settings optimized to produce higher level expert and statistical data in a continuous capture.
- *Edit Capture Templates*: This option opens the **Capture Templates** dialog and allows you to create new or edit existing capture templates.

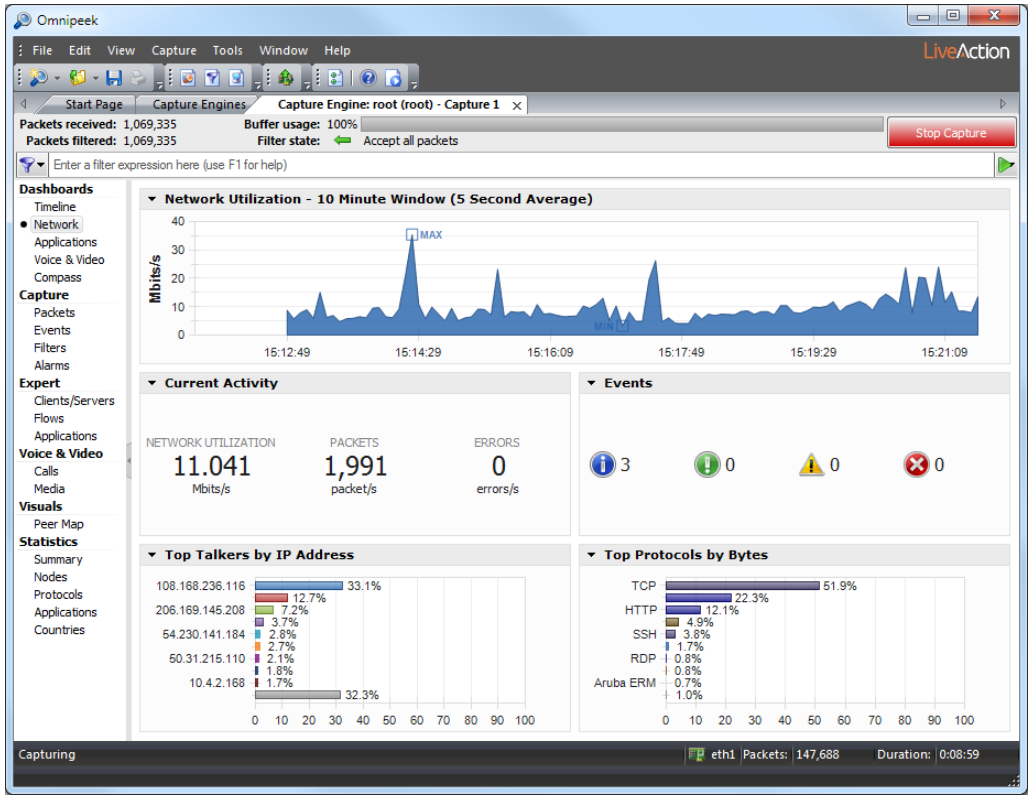
> **Note** For more information about each of the optimized capture formats, please see the *Omnipeek User Guide* or online help.

To begin a remote capture from a Capture Engine:

1. Do one of the following:
   - On the **Home** tab, select the type of remote capture to perform by selecting *New Capture* under the *Captures* heading.
   - On the **Captures** tab, select the type of remote capture to perform by clicking the small arrow next to **Insert**.
   - On the **Adapters** tab, select the type of remote capture to perform by selecting *New Capture* under the name of the adapter you wish to use.

   The remote **Capture Options** dialog appears.

2. Make any desired changes to the capture option settings.
3. Click **OK**. A Capture Engine capture window appears.



Note The views in the left-hand navigation pane that are available in a Capture Engine capture window depend on the type of Capture Engine that is connected, and the *Analysis Options* capture settings configured for that capture window. See the *Omnipeek User Guide* or online help for details on using the features available from Capture Engine capture windows.

4. Click **Start Capture** to begin capturing packets. **Start Capture** changes to **Stop Capture.**
5. Click **Stop Capture** when you want to stop collecting packets into the remote capture buffer.

Third-party authentication with Capture Engines

Third-party authentication of Capture Engines allows administrators of Capture Engines to easily manage logon credentials (after a set of Capture Engines have been deployed), without having to make changes on every Capture Engine individually.

Administrators and users can also sign on to Capture Engines with one set of credentials without requiring the same account on every Capture Engine computer. You can use Active Directory, RADIUS, and TACACS+ authentication to maintain logon credentials.

To use third-party authentication, you must first set up third-party authentication on the Capture Engine (using Capture Engine Manager from the Omnipeek computer), and then log in to the Capture Engine from Omnipeek.

Setting up third-party authentication on the Capture Engine:

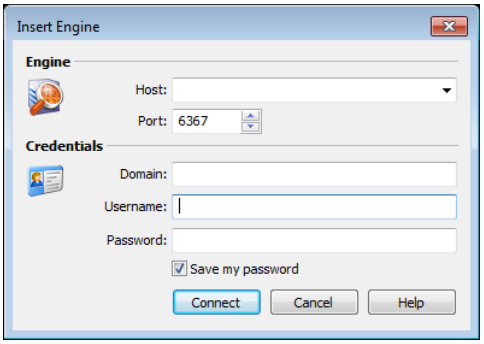
1. Start the Capture Engine Manager from Omnipeek, connect to the Capture Engine, and then add the Capture Engine to the Workspace. See *Using the Capture Engine Manager* on page 100.
2. Click *Configuration* to run the **Capture Engine Configuration Wizard**.

3. When the **Capture Engine Configuration Wizard** appears, click **Next** twice. The **Security** view of the wizard appears.

   The **Security** view of the **Capture Engine Configuration Wizard** allows you to configure the third-party authentication settings that allow the Capture Engine to communicate with, and authenticate to, the authentication servers. See *Engine Configuration—Security* on page 107.

Logging in to the Capture Engine from the Omnipeek computer:

1. From Omnipeek, click **Insert Engine** in the **Capture Engines** window. The **Insert Engine** dialog appears.



2. Complete the dialog:
   - *Host:* Enter the IP address of the Capture Engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Leave this field blank. This field is not used for Capture Engine (Linux).
   - *Username:* Type the Username for login to the Capture Engine using the specified credentials.
   - *Password:* Type the Password for login to the Capture Engine using the specified credentials.
3. Click **Connect.** The Omnipeek console sends the credentials to the Capture Engine over an encrypted channel.

   The Capture Engine decrypts the credentials, and then sends a request to the specific authentication server:
   - A negative response will prompt the Capture Engine to send an error message back to the console (**Access Denied**).
   - An affirmative response allows the user to log on.