



lighthouse

5.1.1

user guide

Revision 1.0.0

1. Terminology

1.1 The Lighthouse table of names

In the *Lighthouse User Manual* various terms are used to define different elements and concepts of the Lighthouse system. These are listed in the table below

Term	Definition
Enrollment	<i>Enrollment</i> is the process of connecting a node to Lighthouse
Enrollment Bundle	An <i>Enroll menu Bundle</i> is used to assign a number of tags to a set of nodes when they are enrolled. During enrollment, the bundle is specified using its name, and a bundle-specific enrollment token
Enrolled Node	An <i>Enrolled Node</i> is a node that has been connected to Lighthouse, and is ready for use.
Enrollment Token	An <i>Enrollment Token</i> is a password, used when performing Node-based, or ZTP enrollment, that authorizes the Node with Lighthouse.
Lighthouse Ironman	<i>Lighthouse Ironman</i> refers to the 5.1 and newer releases of Lighthouse. Re-written from the ground up, it provides a solid basis for accessing, managing and monitoring Opengear console servers.
Lighthouse VPN	The <i>Lighthouse VPN</i> is the OpenVPN based connections that the Lighthouse instance has with the nodes it is managing
Managed Device	A <i>Managed Device</i> is a device that is managed via a Node through a Serial, USB, or Network connection.
Node	A <i>Node</i> is a device that can be enrolled with Lighthouse, allowing it to be accessed, managed, and monitored. Currently, Opengear Console Servers are supported on a standard license, with support for other vendors Console Servers available as an add-on.
Pending Node	A <i>Pending Node</i> is a node that 1) has been connected to Lighthouse and 2) has been configured with a VPN Tunnel, but which has not yet been approved for access, monitoring, or management. The approval operation can be automated by configuring Lighthouse to auto-approve nodes.
Role	A <i>Role</i> defines a set of access rights for a particular group. Currently, 3 Roles are defined within Lighthouse Ironman: Lighthouse Administrator, Node Administrator, and Node User.
Smart Group	A <i>Smart Group</i> is a dynamic filter used to search for particular nodes, or for defining the access rights of a group of users. Smart Groups use node properties, as well as tags defined by users.
Tag	A <i>Tag</i> is a user-defined attribute and value that is assigned to one or more Nodes. Tags are used when creating Smart Groups for filtering views or access to Nodes

2. Lighthouse overview

2.1 Opengear Lighthouse VM 5.1.0 or later host requirements

Opengear Lighthouse deploys as an application running in a Linux-based virtual machine (VM). The Opengear Lighthouse binary is available in both open (for VM managers such as *Boxes*, *KVM*, and *VirtualBox*) and VMware-specific Virtual Machine formats.

To run an Opengear Lighthouse VM, your host computer must be able to run a VM manager and at least one, full, 64-bit Linux-based virtual machine.

To host Lighthouse, the VM needs to be configured to support:

- 10GB SCSI disk.
- 1 x network interface card (Realtek rtl8139 or Intel e1000), bridged.
- VGA console for initial setup.
- To dimension CPU and RAM resources, follow the guidelines below.

CPU and RAM utilization increase with the number of enrolled nodes.

For small deployments (less than 100 nodes), allocate:

- 2 x 64-bit CPU cores.
- 4GB RAM.

For large deployments (between 100 and 1000 nodes), allocate:

- 4 x 64-bit CPU cores.
- 16GB RAM.

For very large deployments (more than 1000 nodes), allocate:

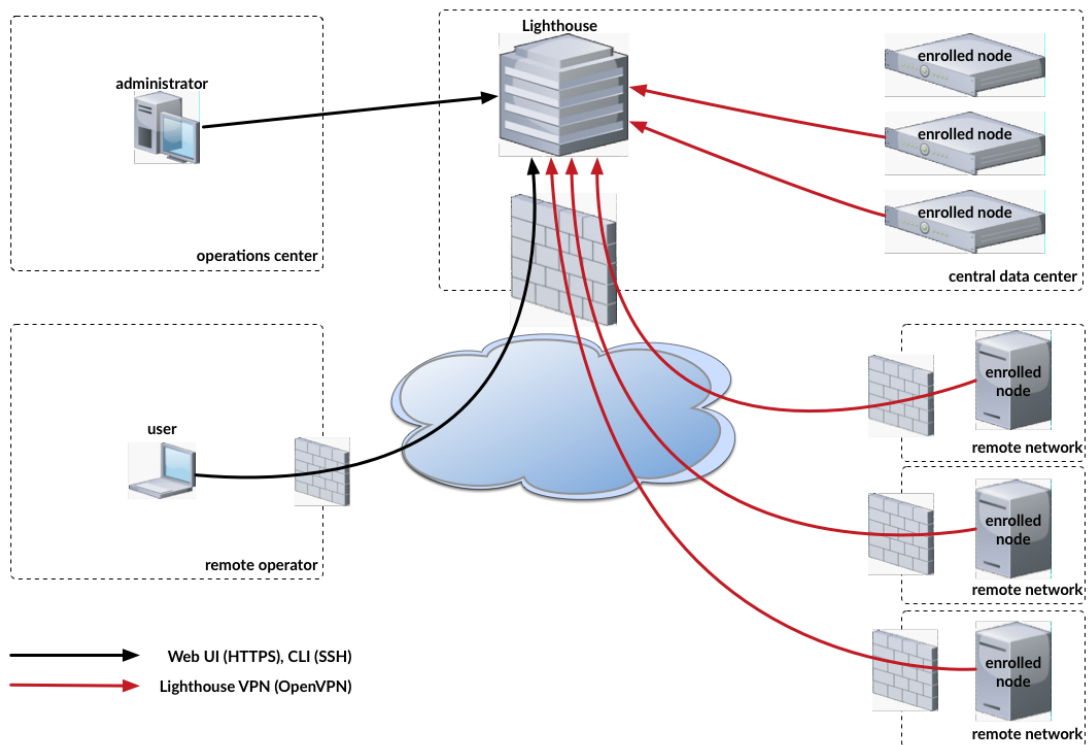
- 8 x 64-bit CPU cores.
- 32GB RAM.

For large and very large deployments, please get in touch for guidance on your deployment options, including low and zero-touch enrollment. The performance and limitations is dependent on network deployment.

2.2 Lighthouse architecture

Opengear Lighthouse 5.1 or later provides a platform for centrally accessing, managing, and monitoring Opengear console servers.

Console servers connect to a central Lighthouse instance over an OpenVPN tunnel, and are accessed, managed, and monitored via services transported over the VPN tunnel. In Lighthouse terminology, the console server is referred to as the *Node*.



2.2.1 Lighthouse to Node interactions

For management and monitoring operations, Lighthouse queries and pushes data to and from a REST API on the node.

When a node is initially enrolled in Lighthouse, Lighthouse generates an X.509 certificate. This certificate authenticates the OpenVPN tunnel, and provides the node access to the Lighthouse REST API. The node also imports a Certificate Authority from Lighthouse, and uses that to allow Lighthouse access to the node's REST API. Lighthouse also provides a public SSH key to the node, which allows Lighthouse to access the node's serial ports via SSH.

For serial access, a node's serial port subsystem is connected via SSH. Users can also access the node's Web UI, which is reverse proxied through the VPN tunnel.

2.2.2 User to Lighthouse interactions

Users interact with Lighthouse via an *Ember.js* JavaScript application, which communicates with Lighthouse via a REST API. This REST API can integrate Lighthouse into other systems. Documentation for this API is available to allow for direct customer use.

Lighthouse 5.1.1 or later has two REST API versions, v1 and v1.1. Some of the endpoints have been deprecated, meaning the functionality and expected request body is different for v1. The v1.1 version of the API has modified endpoint parameters and some new endpoints.

2.2.3 Node organization and filtering

To help search, organize, and filter access to nodes, Lighthouse has a concept called **Smart Groups**, which allow node properties, as well as user supplied **tags** (which consist of a tag name and value) to be compiled into a search expression.

These search expressions can be saved and used to filter the various lists of nodes in the WebUI (for example, when selecting a serial port to connect to, or to connect to the node's WebUI). They can also be used for selecting the nodes that a particular group of users will have access to.

3. Opengear Lighthouse VM installation

3.1 Opengear Lighthouse VM 5.1.0 or later components

Opengear Lighthouse VM 5.1.0 or later comes in one of four formats:

01. An Open Volume Format file – `lighthouse-5.1.1-ovf.zip` – inside a PKZip archive. This is for use with virtual machine managers such as KVM and Virtual Box.
02. A VMware configuration file – `lighthouse-5.1.1-vmx.zip` – also inside a PKZip archive. This is for use with virtual machine managers from VMware.
03. A raw (.hdd) file, `lighthouse-5.1.1-raw.hdd.xz`. This file has been compressed with xz and is for use with hosting services such as ElasticHosts.
04. An Open Virtual Appliance file – `lighthouse-5.1.1.ova`. This is for use with virtual machine managers such as VM and Virtual Box as well as for use with virtual machine managers from VMware.

Not every possible combination of host platform and virtual machine manager is, as yet, documented. Also, if an install procedure is not documented in this manual it does not mean a particular combination of host and virtual machine manager won't be supported when Opengear Lighthouse 5.1.0 or later is formally released.

Note: the *Lighthouse 5.1.0 or later user manual* uses *macOS* to denote the operating system shipped with Apple's desktop and notebook computers. At the time of writing *macOS Sierra 10.12.4* and *OS X El Capitan 10.11.6* are both still supported by Apple. Unless specifically noted, a reference to *macOS* should be read as referring to both of Apple's currently supported operating systems (ie 10.12, macOS, and 10.11, OS X).

3.2 VMWare vSphere 6.0 via the VMWare vSphere 6.0 client on Windows

Note: This procedure assumes VMWare vSphere 6.0 is installed and running on available hardware. It also assumes you have access to a Windows computer on which the VMWare vSphere 6.0 client is installed and that this installed client application can connect to and manage the VMWare Sphere 6.0 instance noted above. Finally, this procedure assumes a copy of the Lighthouse 5.1 binary in Open Volume Format (the .ovf file) is available. In particular, the procedure assumes the binary has been copied to the Windows computer running the VMWare vSphere 6.0 client. Having the binary available via a URL will also work, however.

Note: this procedure was tested using the VMWare Sphere Client 6.0 running on *Windows 7 Enterprise SP 1*.

3.2.1 Launch the vSphere Client and connect to a vSphere instance.

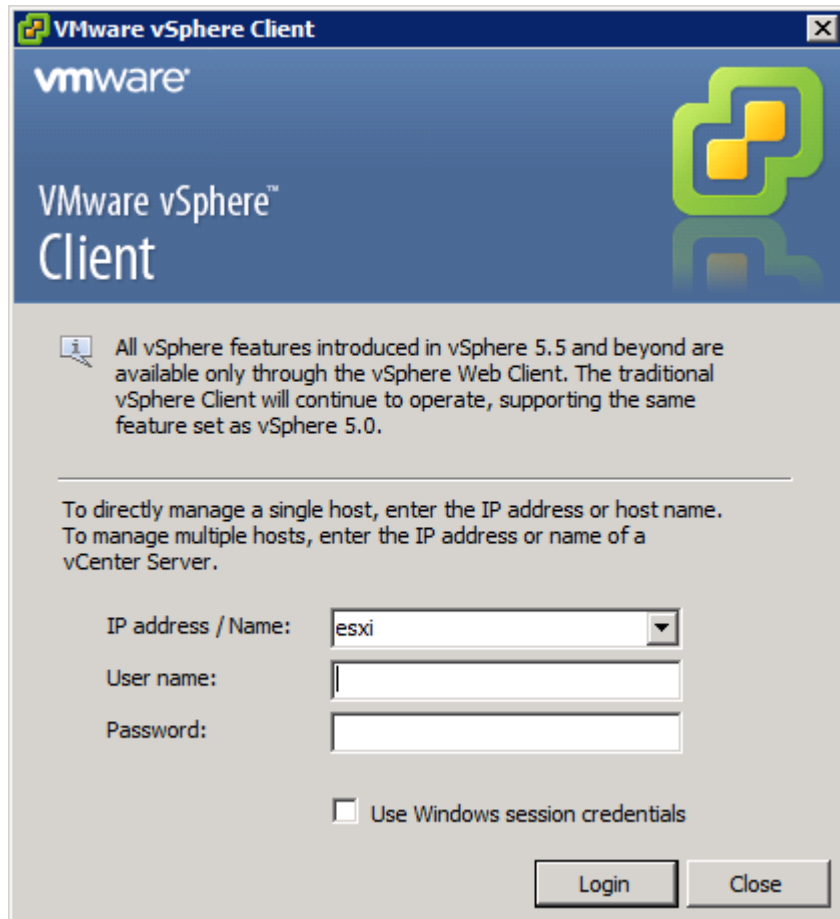
01. launch the *VMware vSphere Client*.

When *VMware Sphere 6.0 Client* is installed, a shortcut to the client is, by default, added to the Start Menu as follows:

Start > All Programs > VMware > VMware vSphere Client

Depending on any customization performed or previous actions taken, other means of launching the client may be available but the default shortcut location should work.

01. The *VMware vSphere Client* presents a login prompt.



01. Select the *IP address* or *Name* of the VMware vSphere instance onto which you wish to install *Lighthouse 5.1.1* from the *IP address/Name* pop-up menu.
02. Enter the *user name* and *password* required to gain management privileges to the selected VMware vSphere instance in the *User name* and *Password* fields.
03. Click the **Login** button, or press **Return**.
04. The login window displays progress text in the bottom left corner. For example:
 - Connecting...
 - Loading inventory...
 - Loading main form...
 - Displaying main form...

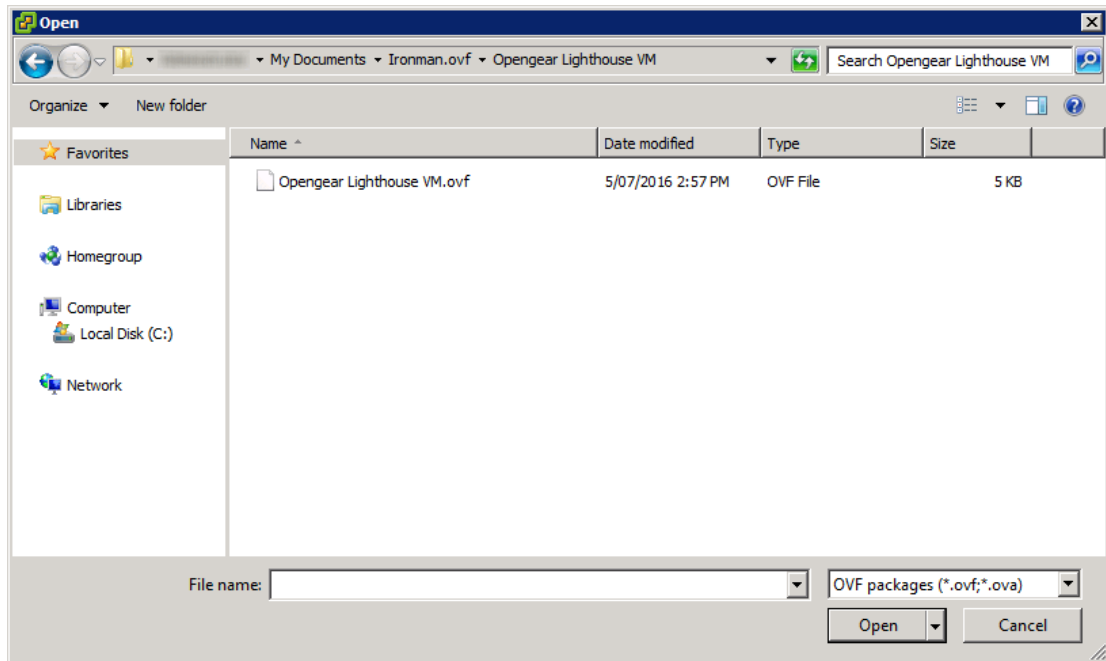
01. The vSphere *main form* window opens.

3.2.2 Import the Lighthouse 5.1.1 VM Open Volume Format (.ovf) image

01. From the *vSphere Client* menu bar choose *File > Deploy OVF Template...*
02. The **Deploy OVF Template** window presents, with the first stage, *Source*, pre-selected.
03. Click the **Browse...** button.
 - An **Open** dialogue box presents.

01. Navigate to the directory containing the file `Opengear Lighthouse VM.ovf`.

In the screenshot below, for example, this file is in `c:\Users\%USERNAME%\My Documents\Ironman.ovf\Opengear Lighthouse VM\`.



01. Select the file *Opengear Lighthouse VM.ovf* and click **Open**.

02. The **Deploy OVF Template** window presents again, with the *Opengear Lighthouse VM.ovf* file listed in the *Deploy from a file or URL* combo-box.

Note: if the required *.ovf* file is not stored on the computer running the vSphere Client, but is, instead, available on a remote computer via a URL, enter said URL in the *Deploy from a file or URL* field rather than taking steps 3 through 6 above.

01. Click **Next**.

02. The *OVF Template Details* stage presents, showing basic information about the *Opengear Lighthouse VM* encapsulated by the *.ovf* file.

03. Click **Next**.

04. The *Name and Location* stage presents with the *Name* field pre-populated and pre-selected.

05. The default name is *Opengear Lighthouse VM*.

To change this, type a new name (by default the *Name* text field is active and the default name is selected).

01. Click **Next**.

02. The *Disk Format* stage presents, showing which data-store the *Opengear Lighthouse VM*'s virtual disk uses, how much free space the virtual disk has available and which provisioning scheme is being used.

03. Click **Next**.

04. The *Network Mapping* stage presents, showing which Destination (or inventory) network the *Opengear Lighthouse VM*'s virtual network is mapped to.

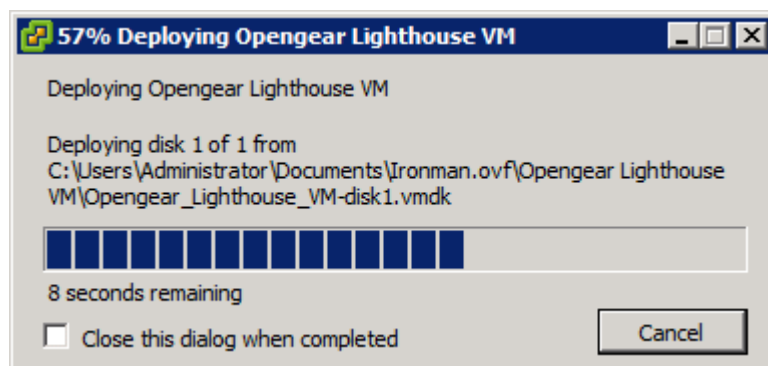
05. Click **Next**.

06. The *Ready to Complete* stage presents, listing the basic properties of the about-to-be-deployed virtual machine.

07. Click **Finish**.

To power-up the new virtual machine immediately after deployment, check the *Power on after deployment* check-box and then click **Finish**.

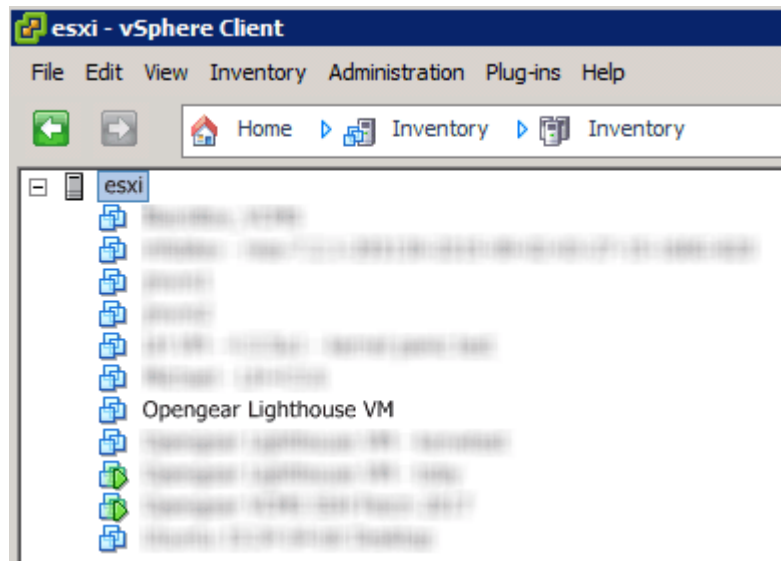
01. The *Deploying Opengear Lighthouse VM* progress bar presents.



01. Once deployment has finished the *Deployment Completed Successfully* alert appears.

02. Click **Close**.

03.The new virtual machine is now deployed and appears in the inventory list.



3.2.3 Launch the Opengear Lighthouse 5.1.0 or later virtual machine

The vSphere Client provides at least three ways of launching a Virtual Machine hosted on a vSphere instance.

All three ways begin with the same first step:

01.Select the *Opengear Lighthouse VM* from the vSphere Client's inventory list.

The selected VM can then be launched by doing one of the following:

01.Select **Inventory > Virtual Machine > Power > Power On**.

02.Press **Ctrl-B**.

03.Click the *Power on the virtual machine* link in the **Basic Tasks** section of the **Getting Started** tab.

This option requires the **Getting Started** tab be front-most. If it is not already the front-most tab, make it active by clicking it.

01.Select **Inventory > Virtual Machine > Open Console** and then:

Click the **Power On** button in the console tool bar or

Choose **VM > Power > Power On** from the console menu bar or

Press **Ctrl-B**.

Note: only the fourth option above results in the running virtual machine being accessible from within the vSphere Client. The first three boot the *Opengear Lighthouse VM* and get it running headless.

3.2.4 Access the console of a running but headless Opengear Lighthouse instance

If direct interaction with a running but headless *Opengear Lighthouse VM* is required, open a console window by

01.Select the running *Opengear Lighthouse VM* in the vSphere Client's inventory list.

Then do one of the following:

01.Select **Inventory > Virtual Machine > Open Console** or

02.Right-click and select **Open Console** from the contextual menu that presents.

Note: a running Opengear Lighthouse VM is almost certainly running a bash shell with no other interactive options. As a consequence, when the vSphere Client opens its console window, the Opengear Lighthouse VM will capture the mouse pointer, making it unavailable for use by any other window. To release the pointer, press **CTRL+ALT**.

3.3 VMware Workstation Player on Windows as host

Note: this procedure assumes *VMware Workstation Player* is already installed on the host Windows machine. This procedure also assumes VMware-ready virtual machine files are stored in `c:\Users\%USERNAME%\Virtual Machines\`. This is the location selected by default by VMware Workstation Player. If another location is preferred, adjust this procedure as required.

Prepare the Opengear Lighthouse VM file for import into VMware Workstation Player.

01.move the `lighthouse-5.1.1-vmx.zip` archive to `c:\Users\%USERNAME%\Virtual Machines\`.

02.right-click the `lighthouse-5.1.1-vmx.zip` archive and select **Extract all...** from the contextual menu.

03.A *Select a Destination and Extract Files* dialogue will open. By default the location is the same folder as the archive is in: `c:\Users\%USERNAME%\Virtual Machines\`. Leave this as the destination folder.

04.Uncheck the *Show extracted files when complete* check box and then click **Extract**.

05.A folder called `ironman` will be created inside `c:\Users\%USERNAME%\Virtual Machines\`.
Import the Opengear Lighthouse VM file into VMware Workstation Player.

01.Launch VMware Workstation Player.

02.Click **Open a Virtual Machine**.

03.navigate to `c:\Users\%USERNAME%\Virtual Machines\ironman\`.

VMware Workstation Player points to *Libraries > Documents* by default and, also by default, this library includes `c:\Users\%USERNAME%\My Documents\`.

Assuming this is the case, double-click *Virtual Machines* and then double-click *Ironman*.

01.If only one file – *Ironman* – presents, double-click it to add the Lighthouse 5.1.0 or later virtual machine to the VMware Workstation 12 Player virtual machines list. If more than one file presents, double-click *Ironman.vmx*.

02.The Lighthouse 5.1.0 or later virtual machine is added to the VMware Workstation 12 Player virtual machines list.

03.With **Opengear Lighthouse VM** selected in the VMware Workstation 12 Player virtual machine list, click **Play virtual machine** to boot Opengear Lighthouse 5.1.0 or later.

3.4 VMware Workstation Pro on Windows as host

Note: this procedure assumes *VMware Workstation Pro* is already installed on the host Windows machine. This procedure also assumes VMware-ready virtual machine files are stored in `c:\Users\%USERNAME%\Virtual Machines\`. This is the location selected by default by VMware Workstation Pro. If another location is preferred, adjust this procedure as required.

Prepare the Opengear Lighthouse VM file for import into VMware Workstation Pro.

01.Move the `lighthouse-5.1.1-vmx.zip` archive to `c:\Users\%USERNAME%\Virtual Machines\`.

02.Right-click the `lighthouse-5.1.1-vmx.zip` archive and select **Extract all...** from the contextual menu.

03.A *Select a Destination and Extract Files* dialogue will open. By default the location is the same folder as the PKZip archive is in: `C:\Users\%USERNAME%\Virtual Machines\`. Leave this as the destination folder.

04.Uncheck the *Show extracted files when complete* check box and then click **Extract**.

05.A folder called `ironman` will be created inside `C:\Users\%USERNAME%\Virtual Machines\`.

Import the Opengear Lighthouse VM file into VMware Workstation Pro.

01.Click **Open a Virtual Machine**.

02.navigate to `C:\Users\%USERNAME%\Virtual Machines\ironman\`.

VMware Workstation Pro points to *Libraries > Documents* by default and, also by default, this library includes `C:\Users\%USERNAME%\My Documents\`.

Assuming this is the case, double-click *Virtual Machines* and then double-click *Ironman*.

03.If only one file – *Ironman* – presents, double-click it to add the Lighthouse 5.1.0 or later virtual machine to the VMware Workstation Pro virtual machines list. If more than one file presents, double-click *Ironman.vmx*.

04.The Lighthouse 5.1.0 or later virtual machine is added to the VMware Workstation Pro virtual machines list.

05.With the **Opengear Lighthouse VM** selected in the *My Computer* listing and the subsequent **Opengear Lighthouse VM** tab open, click **Power on this virtual machine** to boot Opengear Lighthouse 5.1.0 or later.

3.5 VMware Workstation Player or Pro on Fedora Workstation as host

As of the preparation of the *Lighthouse 5.1.0 or later user guide*, VMware Workstation Player 12 could not be installed on Fedora 25 without substantial reconfiguration of a base Fedora Workstation setup. Moreover, the reconfiguration leaves Fedora Workstation in a state that is entirely unsupported by any external entity.

Once appropriately re-configured, it seems likely that Lighthouse 5.1.0 or later will run in VMware Workstation Player 12 on Fedora Workstation. At this stage, however, Opengear is not supporting this particular combination of host operating system and virtual machine manager.

3.6 VMware Workstation Player with Custom Hardware

Note: this procedure assumes *VMware Workstation Player* is already installed on the host Windows machine. This procedure also assumes VMware-ready virtual machine files are stored in `c:\Users\%USERNAME%\Virtual Machines\`. This is the location selected by default by VMware Workstation Player. If another location is preferred, adjust this procedure as required.

Prepare the Opengear Lighthouse VM file for import into VMware Workstation Player.

01.Move the `lighthouse-vmx.zip` archive to `c:\Users\%USERNAME%\Virtual Machines\`.

02.Right-click the `lighthouse-vmx.zip` archive and select **Extract all...** from the contextual menu.

03.A *Select a Destination and Extract Files* dialogue will open. By default the location is the same folder as the PKZip archive is in: `C:\Users\%USERNAME%\Virtual Machines\`. Leave this as the destination folder.

04.Uncheck the *Show extracted files when complete* check box and then click **Extract**.

05.A folder called `ironman` will be created inside `C:\Users\%USERNAME%\Virtual Machines\`.

06. You will need to update the vmx file to use the **vmxnet3** network card instead of the default e1000, by:

1. Changing the line 'ethernet0.virtualDev = "e1000"' to 'ethernet0.virtualDev = "vmxnet3"':

2. Adding the following lines to enable pci:

```
pciBridge0.present = "TRUE"
pciBridge4.present = "TRUE"
pciBridge4.virtualDev = "pcieRootPort"
pciBridge4.functions = "8"
pciBridge5.present = "TRUE"
pciBridge5.virtualDev = "pcieRootPort"
pciBridge5.functions = "8"
pciBridge6.present = "TRUE"
pciBridge6.virtualDev = "pcieRootPort"
pciBridge6.functions = "8"
pciBridge7.present = "TRUE"
pciBridge7.virtualDev = "pcieRootPort"
pciBridge7.functions = "8"
```

Import the Opengear Lighthouse VM file into VMware Workstation Player.

01. Launch VMware Workstation Player.

02. Click **Open a Virtual Machine**.

03. Navigate to C:\Users\%USERNAME%\Virtual Machines\ironman\.

VMware Workstation Player points to *Libraries > Documents* by default and, also by default, this library includes C:\Users\%USERNAME%\My Documents\.

Assuming this is the case, double-click *Virtual Machines* and then double-click *Ironman*.

04. If only one file – Ironman – presents, double-click it to add the Lighthouse 5.1.0 or later virtual machine to the VMware Workstation 12 Player virtual machines list. If more than one file presents, double-click Ironman.vmx.

05. The Lighthouse 5.1.0 or later virtual machine is added to the VMware Workstation 12 Player virtual machines list.

06. With the **Opengear Lighthouse VM** selected in the VMware Workstation 12 player virtual machine list, click **Play virtual machine** to boot Opengear Lighthouse 5.1.0 or later.

07. Inspection of syslog on the VM should show that the vmxnet3 driver is being loaded for the network card.

3.7 VirtualBox on Windows as host

Note: this procedure assumes VirtualBox is already installed on the host machine. This procedure also assumes the required PKZip archive, lighthouse-5.1.1-ovf.zip is in c:\Users\%USERNAME%\Downloads, the default location for files downloaded from remote sources to a computer running Windows.

01. Unzip ironman-ovf (it may appear as lighthouse-5.1.1-ovf.zip depending on your Windows Explorer preference settings).

Right-click the ironman-ovf archive and select **Extract all...** from the contextual menu.

02. A *Select a Destination and Extract Files* dialogue will open. The destination will be c:\Users\%USERNAME%\Downloads\Ironman-ovf.

03. Uncheck the *Show extracted files when complete* checkbox and edit the destination by removing Ironman-ovf from the path.

04. Click **Extract**.

05. A folder called ironman-ovf will be created inside c:\Users\%USERNAME%\Downloads\.

06. Launch Virtual Box

The **Oracle VM VirtualBox Manager** window appears.

07. Choose **File > Import Appliance...**

The **Appliance to import** dialogue box opens.

08. Click the **Expert Mode** button.

The **Appliance to import** dialogue box changes from *Guided Mode* to *Expert Mode*.

09. Click the icon of a folder with an upward pointing arrow superimposed. This icon is to the far-right of the *Appliance to import* field.

The *Open File* dialogue box opens. By default, it opens with C:\Users\%USERNAME%\Documents as the current folder.

10. Navigate to c:\Users\%USERNAME%\Downloads\Ironman.ovf\Opengear Lighthouse VM\.

11. Select the file Opengear Lighthouse VM and click **Open**.

12. Double-click the text 'vm' in the *Name* row and *Configuration* column to make it editable.

13. Type Opengear Lighthouse VM and hit Enter.

14. Click the **Import** button.

A new virtual machine, called **Opengear Lighthouse VM** is added to the list of virtual machines available to Virtual Box.

15. Select **Opengear Lighthouse VM** from the list.
16. Choose **Machine > Settings...** (Alternatively, click the **Settings** icon in the VirtualBox Manager toolbar, or press Control-S.)
The *Opengear Lighthouse VM – Settings* dialogue box presents.
17. Click the *System* option in the list of options running down the left-hand side of the dialogue box.
The majority of the dialogue box presents the *System* options available as three tabs: *Motherboard*, *Processor*, and *Acceleration*. (Depending on the underlying hardware platform, *Acceleration* may be greyed-out and unavailable). The *Motherboard* tab is pre-selected by default.
18. In the *Motherboard* tab, check the *Hardware Clock in UTC Time* checkbox.
19. Click **OK** or press Return.
20. Select **Opengear Lighthouse VM** from the list and click **Start** in the **Oracle VM VirtualBox Manager** toolbar to boot Opengear Lighthouse 5.1.0 or later. (Double-clicking **Opengear Lighthouse VM** in the list also boots Opengear Lighthouse 5.1.0 or later.)

Note: Checking the *Hardware Clock in UTC Time* check-box is necessary because Lighthouse expects the hardware clock to be set to UTC, not local time. Unlike other Virtual Machine Managers, *Virtual Box* both exposes this option as a user-adjustable setting and does not set it to UTC by default.

3.8 VirtualBox on macOS as host

Note: this procedure assumes VirtualBox is already installed on the host macOS machine. This procedure also assumes the required PKZip archive, `lighthouse-5.1.1-ovf.zip` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running macOS.

01. Unzip `lighthouse-5.1.1-ovf.zip`.

This creates a folder – `Ironman-ovf` – in `~/Downloads` that contains the following files and folders:

```
Ironman-ovf
├── Opengear Lighthouse VM
│   ├── Opengear Lighthouse VM.ovf
│   └── Opengear_Lighthouse_VM-disk1.vmdk
```

02. Launch Virtual Box.
The **Oracle VM VirtualBox Manager** window appears.
03. Choose **File > Import Appliance...** or press Command-I.
The **Appliance to import** dialogue sheet slides down from the **Oracle VM VirtualBox Manager** toolbar.
04. Click the **Expert Mode** button.
The **Appliance to import** dialogue sheet changes from *Guided Mode* to *Expert Mode*.
05. Click the icon of a folder with an upward pointing arrow superimposed. This icon is to the far-right of the *Appliance to import* field.
The **Open File** dialogue sheet slides down from the **Oracle VM VirtualBox Manager** toolbar. By default, this sheet opens with `~/Documents` as the current folder.
06. Navigate to `~/Downloads/Ironman.ovf/Opengear Lighthouse VM/`.
07. Select `Opengear Lighthouse VM` and click **Open**. (Depending on your Finder Preferences settings, the file may present as `Opengear Lighthouse VM.ovf`.)
08. Double-click the text 'vm' in the *Name* row and *Configuration* column to make it editable.
09. Type `Opengear Lighthouse VM` and hit Return.
10. Click the **Import** button.
A new virtual machine, called **Opengear Lighthouse VM** is added to the list of virtual machines available to Virtual Box.
11. Select **Opengear Lighthouse VM** from the list.
12. Choose **Machine > Settings...** (Alternatively, click the **Settings** icon in the VirtualBox Manager toolbar, or press Command-S.)
The *Opengear Lighthouse VM – Settings* dialogue box presents.
13. Click the *System* option in the dialogue box's toolbar.
The dialogue box presents the *System* options available as three tabs: *Motherboard*, *Processor*, and *Acceleration*. (Depending on the underlying hardware platform, *Acceleration* may be greyed-out and unavailable). The *Motherboard* tab is pre-selected by default.
14. In the *Motherboard* tab, check the *Hardware Clock in UTC Time* checkbox.
15. Click **OK** or press Return.

16. Select **Opengear Lighthouse VM** from the list and click **Start** in the **Oracle VM VirtualBox Manager** toolbar to boot Opengear Lighthouse 5.1.0 or later. (Double-clicking **Opengear Lighthouse VM** in the list also boots Opengear Lighthouse 5.1.0 or later.)

Note: Checking the *Hardware Clock in UTC Time* check-box is necessary because Lighthouse expects the hardware clock to be set to UTC, not local time. Unlike other Virtual Machine Managers, *Virtual Box* both exposes this option as a user-adjustable setting and does not set it to UTC by default.

Note: by default, VirtualBox stores virtual machines in `~/VirtualBox VMS`. If this is the first virtual machine setup by VirtualBox it will create the `VirtualBox VMS` folder in the current user's home-directory and create a further folder – `Opengear Lighthouse VM` – inside the `VirtualBox VMS` folder. Inside `Opengear Lighthouse VM` are the files and folders which make up Opengear Lighthouse 5.1.0 or later when run under Virtual Box.

3.9 VirtualBox on Ubuntu as host

Note: this procedure assumes VirtualBox and all required support files are already installed on the host machine. This procedure also assumes the required PKZip archive, `lighthouse-5.1.1-ovf.zip` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running Ubuntu.

01. Unzip `lighthouse-5.1.1-ovf.zip`.

This creates a folder – `Ironman.ovf` – in `~/Downloads` that contains the following files and folders:

```
Ironman.ovf
├── Opengear Lighthouse VM
│   ├── Opengear Lighthouse VM.ovf
│   └── Opengear_Lighthouse_VM-disk1.vmdk
```

02. Launch Virtual Box.

The **Oracle VM VirtualBox Manager** window appears.

03. Choose **File > Import Appliance...**

The **Appliance to import** dialogue box opens.

04. Click the **Expert Mode** button.

The **Appliance to import** dialogue box changes from *Guided Mode* to *Expert Mode*.

05. Click the icon of a folder with an upward pointing arrow superimposed. This icon is to the far-right of the *Appliance to import* field.

A file-navigation dialogue box, headed **Please choose a virtual appliance to import** opens. By default, it opens with `~/Documents` as the current folder.

06. Navigate to `~/Downloads/Ironman.ovf/Opengear Lighthouse VM/`.

07. Select `Opengear Lighthouse VM.ovf` and click **Open**.

08. Double-click the text 'vm' in the *Name* row and *Configuration* column to make it editable.

09. Type `Opengear Lighthouse VM` and hit Return.

10. Click the **Import** button.

A new virtual machine, called **Opengear Lighthouse VM** is added to the list of virtual machines available to Virtual Box.

11. Select **Opengear Lighthouse VM** from the list and click **Start** in the **Oracle VM VirtualBox Manager** toolbar to boot Opengear Lighthouse 5.1.0 or later. (Double-clicking **Opengear Lighthouse VM** in the list also boots Opengear Lighthouse 5.1.0 or later.)

Note: by default VirtualBox stores virtual machines in `~/VirtualBox VMS`. If this is the first virtual machine setup by VirtualBox it will create the `VirtualBox VMS` folder in the current user's home-directory and create a further folder – `Opengear Lighthouse VM` – inside the `VirtualBox VMS` folder. Inside `Opengear Lighthouse VM` are the files and folders which make up Opengear Lighthouse 5.1.0 or later when run under Virtual Box.

3.10 VirtualBox on Fedora Workstation as host

Note: this procedure assumes VirtualBox and all required support files are already installed on the host machine. This procedure also assumes the required PKZip archive, `lighthouse-5.1.1-ovf.zip` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running Fedora.

01. Unzip `lighthouse-5.1.1-ovf.zip`.

This creates a folder – `Ironman.ovf` – in `~/Downloads` that contains the following files and folders:

```
Ironman.ovf
├── Opengear Lighthouse VM
│   ├── Opengear Lighthouse VM.ovf
│   └── Opengear_Lighthouse_VM-disk1.vmdk
```

02. Launch Virtual Box.

The **Oracle VM VirtualBox Manager** window appears.

03. Choose **File > Import Appliance...** or press Control-I.
The **Appliance to import** dialogue box opens.
 04. Click the **Expert Mode** button.
The **Appliance to import** dialogue box changes from *Guided Mode* to *Expert Mode*.
 05. Click the icon of a folder with an upward pointing arrow superimposed. This icon is to the far-right of the *Appliance to import* field.
The **Open File** dialogue box opens. By default, it opens with `~/Documents` as the current folder.
 06. Navigate to `~/Downloads/Ironman.ovf/Opengear Lighthouse VM/`.
 07. Select `Opengear Lighthouse VM` and click **Open**.
 08. Double-click the text 'vm' in the *Name* row and *Configuration* column to make it editable.
 09. Type `Opengear Lighthouse VM` and hit Return.
 10. Click the **Import** button.
A new virtual machine, called **Opengear Lighthouse VM** is added to the list of virtual machines available to Virtual Box.
 11. Select **Opengear Lighthouse VM** from the list and click **Start** in the **Oracle VM VirtualBox Manager** toolbar to boot Opengear Lighthouse 5.1.0 or later. (Double-clicking **Opengear Lighthouse VM** in the list also boots Opengear Lighthouse 5.1.0 or later.)
- Note:** by default VirtualBox stores virtual machines in `~/VirtualBox VMs`. If this is the first virtual machine setup by VirtualBox it will create the `VirtualBox VMs` folder in the current user's home-directory and create a further folder – `Opengear Lighthouse VM` – inside the `VirtualBox VMs` folder. Inside `Opengear Lighthouse VM` are the files and folders which make up Opengear Lighthouse 5.1.0 or later when run under Virtual Box.

3.11 Virtual Machine Manager (KVM) on Ubuntu as host

Note: this procedure assumes Virtual Machine Manager and all required support files are already installed on the host machine. This procedure also assumes the the .xz archive, `lighthouse-5.1.1-raw.hdd.xz` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running Ubuntu.

01. Expand `lighthouse-5.1.1-raw.hdd.xz`
This creates a file – `lighthouse-5.1.1-raw.hdd` – in `~/Downloads`.
02. launch *Virtual Machine Manager*.
03. Click the **New** button at the top-left of the Virtual Machine Manager window (or choose **File > New Virtual Machine**).
The *Source Selection* window opens.
04. Click the **Select a file** button.
A *Select a device or ISO file* dialogue box slides into view.
05. Navigate to `~/Downloads/`.
06. Select the file `lighthouse-5.1.1-raw.hdd` and click **Open** in the top right-hand corner of the dialogue box.
A *Review* window opens providing basic information about the virtual machine (or 'box', as Boxes calls them) to be created
07. Click the **Create** button in the top-right corner of the *Review* window.
08. A new virtual machine instance, `Opengear_Lighthouse_VM-disk1` is created and presented in the *Boxes* window.
To rename the virtual machine instance, right-click on the machine instance and choose **Properties** from the contextual menu that appears.
Click anywhere in the *Name* field to select and edit the name.
Click the close box to save the changes.

3.12 Boxes on Fedora Workstation as host

Note: this procedure assumes Boxes and all required support files are already installed on the host machine. This procedure also assumes the the required PKZip archive, `lighthouse-5.1.1-ovf.zip` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running Fedora Workstation.

01. Unzip `lighthouse-5.1.1-ovf.zip`
This creates a folder – `Ironman.ovf` – in `~/Downloads` that contains the following files and folders:


```

Ironman.ovf
├── Opengear Lighthouse VM
│   ├── Opengear Lighthouse VM.ovf
│   └── Opengear_Lighthouse_VM-disk1.vmdk
      
```
02. launch *Boxes*.
03. Click the **New** button in the Boxes window title bar

The *Source Selection* window opens.

04. Click the **Select a file** button.

A *Select a device or ISO file* dialogue box opens.

05. Navigate to `~/Downloads/Ironman.ovf/Opengear Lighthouse VM/`.

06. Select the file `Opengear_Lighthouse_VM-disk1.vmdk` and click **Open** in the top right-hand corner of the dialogue box.

A *Review* window opens providing basic information about the virtual machine (or 'box', as Boxes calls them) to be created

07. Click the **Create** button in the top-right corner of the *Review* window.

08. A new virtual machine instance, *Opengear_Lighthouse_VM-disk1* is created and presented in the *Boxes* window.

To rename the virtual machine instance, right-click on the machine instance and choose **Properties** from the contextual menu that appears.

Click anywhere in the *Name* field to select and edit the name.

Click the close box to save the changes.

3.13 Boxes on CentOS as host

Note: this procedure assumes a CentOS installation, complete with the Gnome desktop environment as the host operating system. By default CentOS includes the full complement of KVM-centric virtualization tools including the GUI-based virtualization management tools **Boxes** and **virt-manager** and the shell-based virtualization management tool `virsh`.

This procedure assumes **Boxes** is used to setup and manage the Opengear Lighthouse VM.

Finally, this procedure assumes the required PKZip archive, `lighthouse-5.1.1-ovf.zip` is in `~/Downloads`, the default location for files downloaded from remote sources to a computer running Fedora Workstation.

01. Unzip `lighthouse-5.1.1-ovf.zip`.

This creates a folder – `Ironman.ovf` – in `~/Downloads` that contains the following files and folders:

```
Ironman.ovf
├── Opengear Lighthouse VM
│   ├── Opengear Lighthouse VM.ovf
│   └── Opengear_Lighthouse_VM-disk1.vmdk
```

02. Launch Boxes

03. Click **New** in the Boxes title bar.

04. Navigate to `~/Downloads/Ironman.ovf/Opengear Lighthouse VM/`

05. Select `Opengear Lighthouse VM` and click **Open**.

A new virtual machine, called **Opengear LighthouseVM** is added to the list of virtual machines available to Boxes.

4. First boot of the Opengear Lighthouse VM

During boot, two screens present.

01.The first notes the VM is **Booting to latest installed image**.

The selected image is *Lighthouse Root 1*. Two other images are available: *Lighthouse Root 1* and *Memtest86+*. Do not change the boot image the VM boots from.

02.The second screens asks you to **Select Lighthouse boot mode** and presents four options:

Graphics console boot
Graphics console recovery mode
Serial console boot
Serial console recovery mode

03.*Graphics console boot* is pre-selected and should not be changed.

04.After the first boot has completed a message presents:

Welcome to Ironman. This is software version:
5.1.1

05.And the final procedure in the initial setup presents:

To complete initial setup, please set a new root password.
Press ENTER to continue.

06.After pressing **Enter**, a prompt appears:

Enter new root password:

07.Enter a strong, high-entropy password and press **Enter**.

08.The confirm prompt appears:

Confirm given password

09.Re-enter the password and press **Enter**.

10.Multiple configuration notices present ending with a login prompt:

opengear-lighthouse login:

11.Enter `root` (the only user able to login at this point) and press **Enter**.

12.A password prompt appears:

Password:

13.Enter the newly-set password and press **Enter**.

14.A standard bash shell prompt appears.

root@opengear-lighthouse:~#

5. Initial system configuration

5.1 Loading Opengear Lighthouse

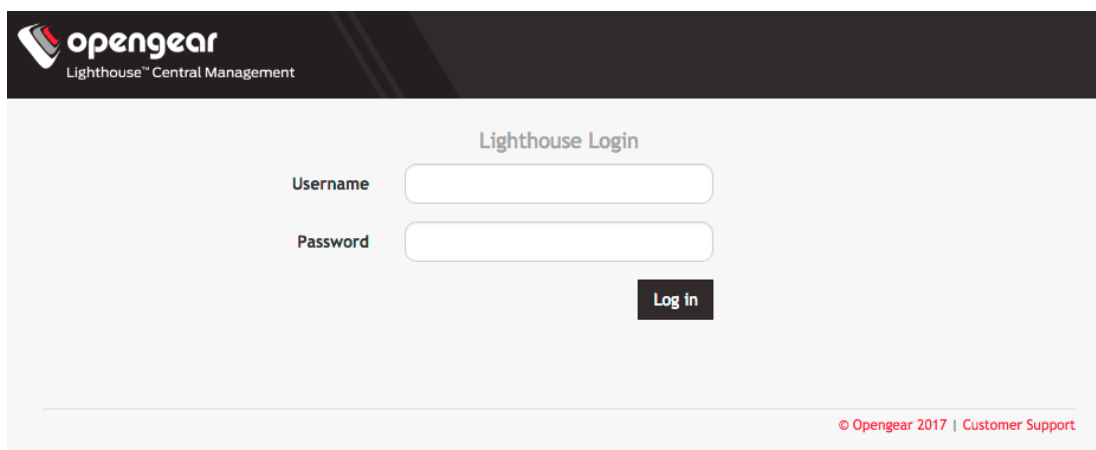
When the *Opengear Lighthouse* VM is booted and running it is addressable at either of two IP addresses:

- 01.the fixed address, **192.168.0.1**, or
- 02.whatever address it is assigned by any DHCP server it finds.

In your browser of choice open a new window or tab and enter

- 01.**https://192.168.0.1/** or **https://[DHCP-supplied address]/** in the address bar
- 02.press **Return**.

The Opengear Lighthouse login page loads.



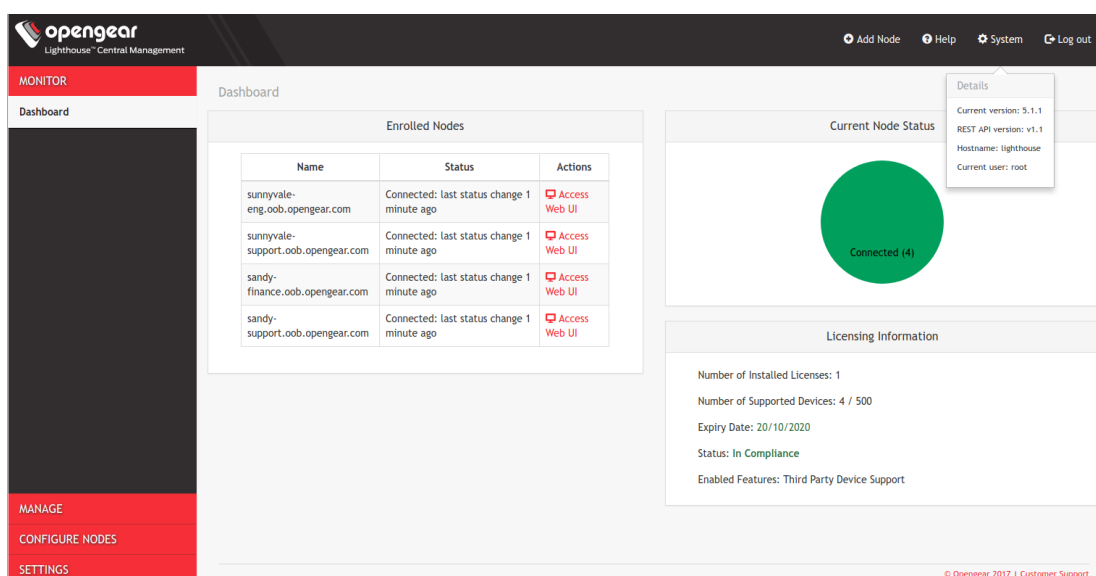
5.2 Login to Opengear Lighthouse

To login to *Opengear Lighthouse*

- 01.Enter a username in the *Username* field.
- 02.enter the username's password in the *Password* field.
- 03.Click **Log In** or press **Enter**.

The *Opengear Lighthouse* **Dashboard** loads.

- 04.Click **System** right top icon to see Current user.



Note: the Dashboard, the Sidebar, and other Lighthouse pages, will present differently depending on the privileges assigned to the logged-in user. In this manual, screenshots such as that of the Lighthouse Dashboard above represent what the `root` user sees. Users with different privileges will see filtered views of available nodes, users, groups, tags and Smart Groups and will have different privileges regards creating and changing settings within Lighthouse. (For example, users other than `root` can edit their own account settings but cannot edit

other user's accounts. Depending on the privileges an account has, a user may also be restricted with regards what they can do with enrolled nodes or what new nodes they can enroll.)

5.3 Setting the Opengear Lighthouse hostname

To set the hostname for a running *Opengear Lighthouse* instance:

01. Select **Settings > System > Administration**.
02. Edit the *Hostname* field as required.

The screenshot shows the Opengear Lighthouse Administration interface. The left sidebar contains navigation options: MONITOR, MANAGE, CONFIGURE NODES, SETTINGS, Network Connections, User Management, Services, Date & Time, System, Licensing, Administration, System Upgrade, and Factory Reset. The main content area is titled 'Administration' and shows the 'Settings' section expanded. The 'Hostname' field is set to 'lighthouse'. The 'SSH Port' is set to '22'. The 'External Network Addresses' section is currently empty, with columns for Order, Address, API Port (default: 443), and VPN Port (default: 1194). An 'Apply' button is located at the bottom right of the settings area.

01. Click **Apply**.

5.4 Adding external IP addresses manually (optional)

Adding a Lighthouse instance's external IP address or addresses to a Lighthouse instance's configuration is an optional step.

To add a single external address:

01. Select **Settings > System > Administration**.

The screenshot shows the same Opengear Lighthouse Administration interface as in the previous screenshot, but with an external IP address added. The 'External Network Addresses' table now contains one entry with the IP address '192.168.254.33'. The 'API Port' is set to '443' and the 'VPN Port' is set to '1194'. The 'Apply' button is still visible at the bottom right.

01. In the *Address* field of the *External Network Addresses* section, enter an IP address.
02. (Optional step) Change the API Port, VPN Port or both, if the ports used on the entered IP address are different from the default (443 and 1194, respectively).
03. Click the **Apply** button.
04. Click **Apply**.

To manually add further external addresses to a Lighthouse instance's configuration:

01. Click the + (add) button.

A second row appears in the **External Network Addresses** section.

02. In the newly presented *Address* field, enter an IP address.

03. (Optional step) Change the API Port, VPN Port or both, if the ports used on the entered IP address are different from the default (443 and 1194, respectively).

04. Add further IP addresses as required by repeating the steps above.

05. Click the **Apply** button.

To change the order in which manually-added IP addresses are sent to remote nodes:

01. Click the up and down arrows in the **Order** column to change the order in which the IP addresses are listed.

The presented order reflects the order in which these addresses are sent out.

02. Click the **Apply** button.

If external IP addresses are manually added to a Lighthouse configuration, these addresses are sent to a remote node during enrollment. If no external IP address is manually added to a Lighthouse configuration, default external IP addresses are used.

The default external IP addresses are sent to a remote node during enrollment in the following order:

01. net1:dhcp

02. net1:static

03. the IP address connected to the default gateway.

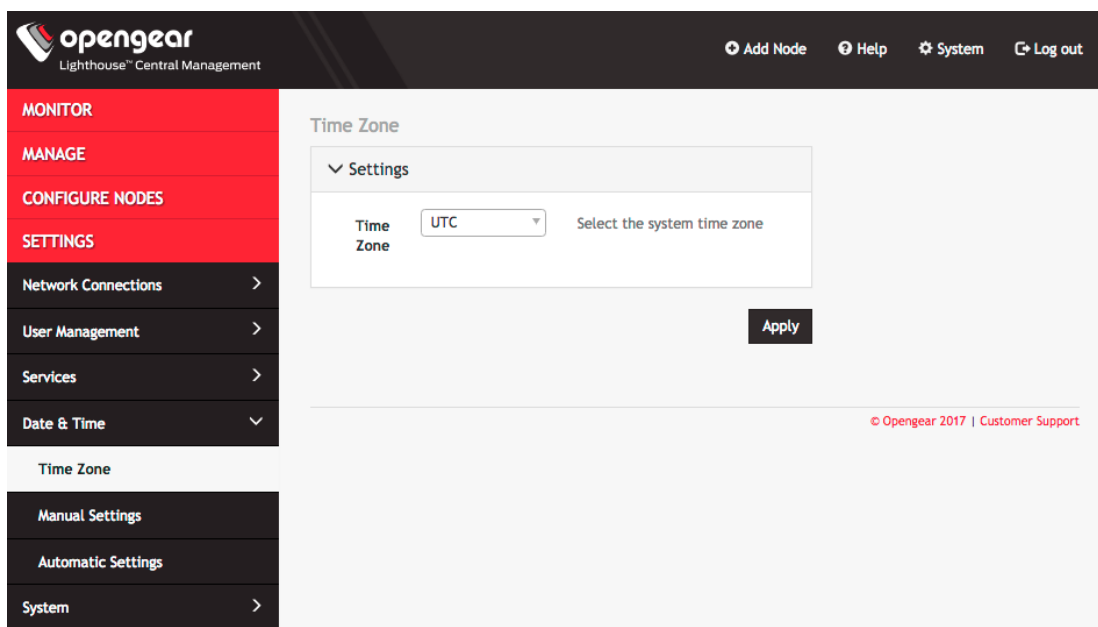
5.5 Setting the Opengear Lighthouse internal clock

To set the time-zone:

01. Select **Settings > Date & Time > Time Zone**.

02. Select the *Lighthouse* instance's time-zone from the *Time Zone* pop-up menu.

03. Click **Apply**.

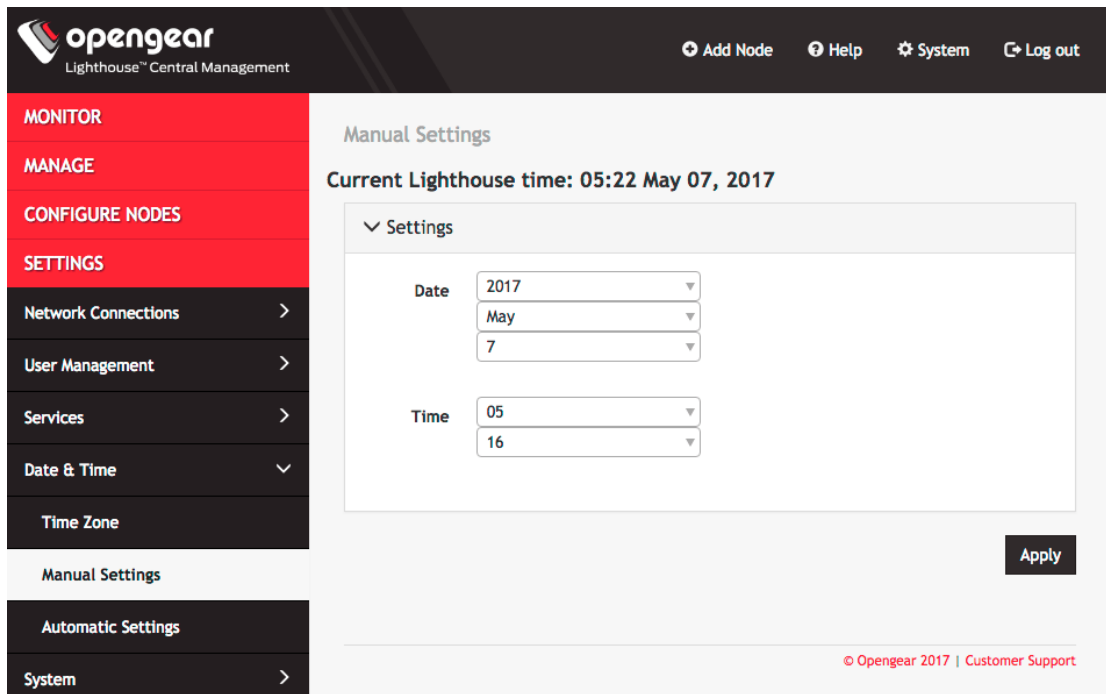


To set the correct time and date either

01. Select **Settings > Date & Time > Manual Settings**.

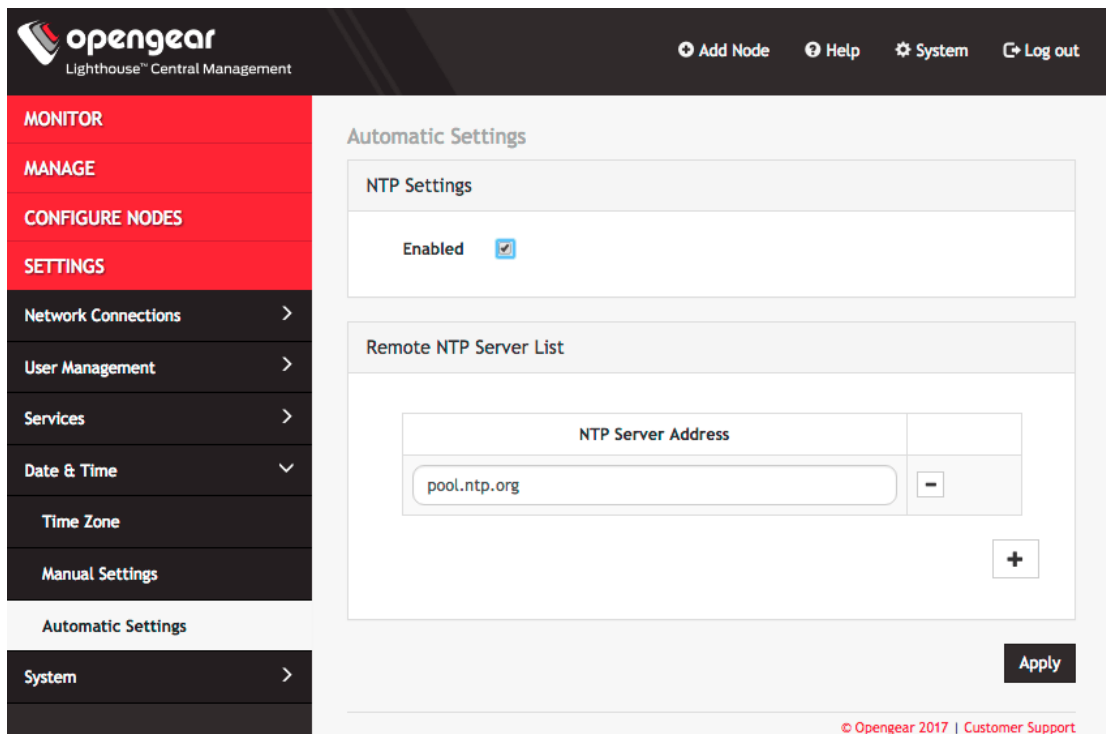
02. Enter the current *Date* and *Time*.

03. Click **Apply**.



or

01. Select **Settings > Date & Time > Automatic Settings**.
02. Click the *Enabled* check-box.
03. Enter a working NTP Server address in the *NTP Server Address* field.
04. Click **Apply**.



5.6 Examine or change the Lighthouse SSL certificate

Lighthouse ships with a private SSL Certificate that encrypts communications between it and your browser.

To examine this certificate, or generate a new Certificate Signing Request:

01. Select **Settings > Services > HTTPS Certificate**.

The screenshot shows the OpenGear Lighthouse Central Management interface. On the left is a navigation sidebar with categories: MONITOR, MANAGE, CONFIGURE NODES, and SETTINGS. Under SETTINGS, there are sub-menus for Network Connections, User Management, Services, Session Settings, HTTPS Certificate (selected), Console Gateway, Lighthouse VPN, Date & Time, and System. The main content area is titled 'HTTPS Certificate' and contains two sections:

- Current SSL Certificate:** A table showing details for the current certificate:

Common Name	default	The full canonical name for this device
Organizational Unit		The group overseeing this device
Organization		The name of the organization to which the device belongs
Locality/City		The city where the organization is located
State/Province		The state or province where the organization is located
Country	US	The country where the organization is located
Email		The email address of a contact person for this device
Key Length (bits)	2048	Length of generated key in bits
Issue Date	Nov 26 08:19:18 2017 GMT	The date at which the certificate becomes valid
Expiry Date	Nov 27 08:19:18 2018 GMT	The date at which the certificate ceases to be valid
- Certificate Signing Request:** A form with the following fields:
 - Common Name:
 - Organizational Unit:
 - Organization:
 - Locality/City:
 - State/Province:
 - Country:
 - Email:
 - Key Length (bits):
 - Challenge Password:
 - Confirm Password:
 - Private Key File:

An 'Apply' button is located at the bottom right of the form.

The details of the **Current SSL Certificate** present.

Immediately below this listing is a **Certificate Signing Request** form, which can be used to generate a new SSL certificate.

5.7 Examine or change the Lighthouse Session Settings

To examine Web and CLI session settings, or to modify them:

01. Select **Settings > Services > Session Settings**.
02. Examine or modify **Web Session Timeout** settings. The maximum value for idle timeout is 1440 minutes.
03. Examine or modify **CLI Session Timeout** settings. Setting the CLI session timeout to 0 will disable the timeout. Changes will take effect the next time a user logs in via the CLI.

The screenshot shows the OpenGear Lighthouse Central Management interface. The top navigation bar includes 'Add Node', 'Help', 'System', and 'Log out'. The left sidebar shows the navigation menu with 'Session Settings' selected under the 'SETTINGS' category. The main content area is titled 'Session Settings' and contains a 'Settings' section with the following configuration:

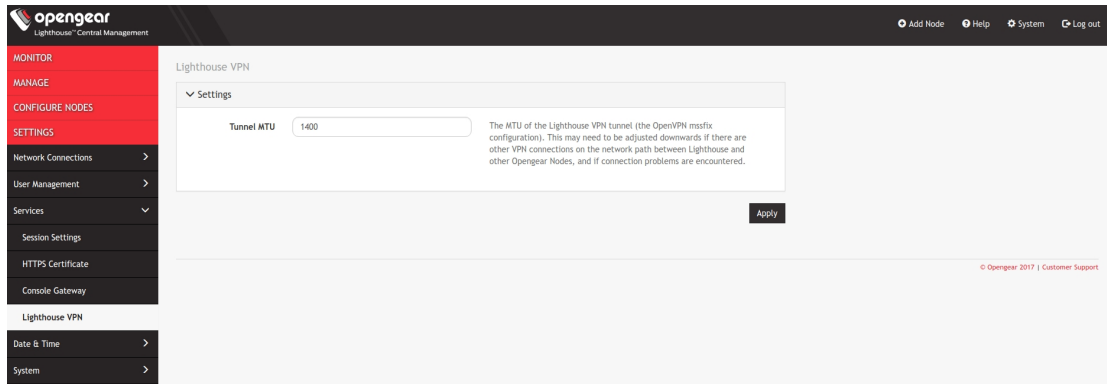
- Web Session Timeout:** Web session idle timeout (in minutes)
- CLI Session Timeout:** CLI session idle timeout (in minutes). Note: To disable the CLI session idle timeout, set it to 0.

An 'Apply' button is located at the bottom right of the settings section.

5.8 Examine or change the MTU of the Lighthouse VPN tunnel

The MTU setting can be configured for traffic that is travelling through the Lighthouse VPN, in an attempt to solve MTU path discovery problems. To examine the MTU of the Lighthouse VPN tunnel, or to modify it:

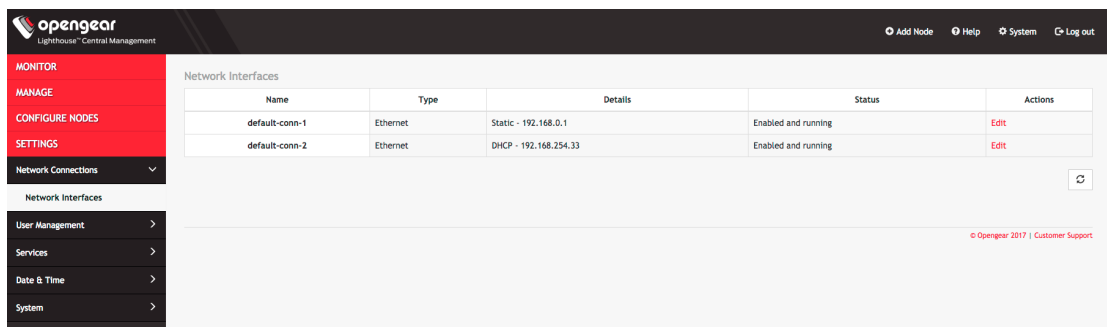
01. Select **Settings > Services > Lighthouse VPN**.
02. Examine or modify **Tunnel MTU** settings. The allowed values are between 1280 and 1500.



5.9 Network connections

To see the network connections available to *Opengear Lighthouse 5.1.0* or later:

01. Select **Settings > Network Connections > Network Interfaces**



This currently presents only two default connections: static and dhcp interfaces.

If you log in to the Lighthouse VM and run `ifconfig`, the two connections listed in Opengear Lighthouse 5.1.0 or later correspond to the following returned interfaces:

default-static is net1:static.

default-DHCP is net1:dhcp.

To edit a given network interface:

01. Select **Settings > Network Connections > Network Interfaces**

02. Click the *Edit* button in the **Actions** section of the network interface to be modified.

03. Make the desired changes in the resultant dialog.

04. Click **Apply**.

The screenshot shows the Opengear Lighthouse Central Management interface. The top navigation bar includes the Opengear logo, 'Lighthouse™ Central Management', and links for 'Add Node', 'Help', 'System', and 'Log out'. The left sidebar contains a menu with categories: MONITOR, MANAGE, CONFIGURE NODES, SETTINGS, Network Connections (expanded), Network Interfaces, User Management, Services, Date & Time, and System. The main content area is titled 'default-conn-1' and features a yellow warning box: 'Editing these settings may break connectivity'. Below this are several sections:

- Status:** Shows 'Status' as 'Running'.
- Common Settings:** Includes an 'Enabled' checkbox (checked) and a 'Description' field with the value 'Default static network'.
- IPv4 Settings:** Contains a 'Configuration Method' dropdown set to 'Static assignment', and input fields for 'IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), 'Gateway', 'Primary DNS', and 'Secondary DNS'.
- Media Settings:** A section with a right-pointing arrow.

 At the bottom right of the configuration area are 'Cancel' and 'Apply' buttons. A footer at the bottom right reads '© Opengear 2017 | Customer Support'.

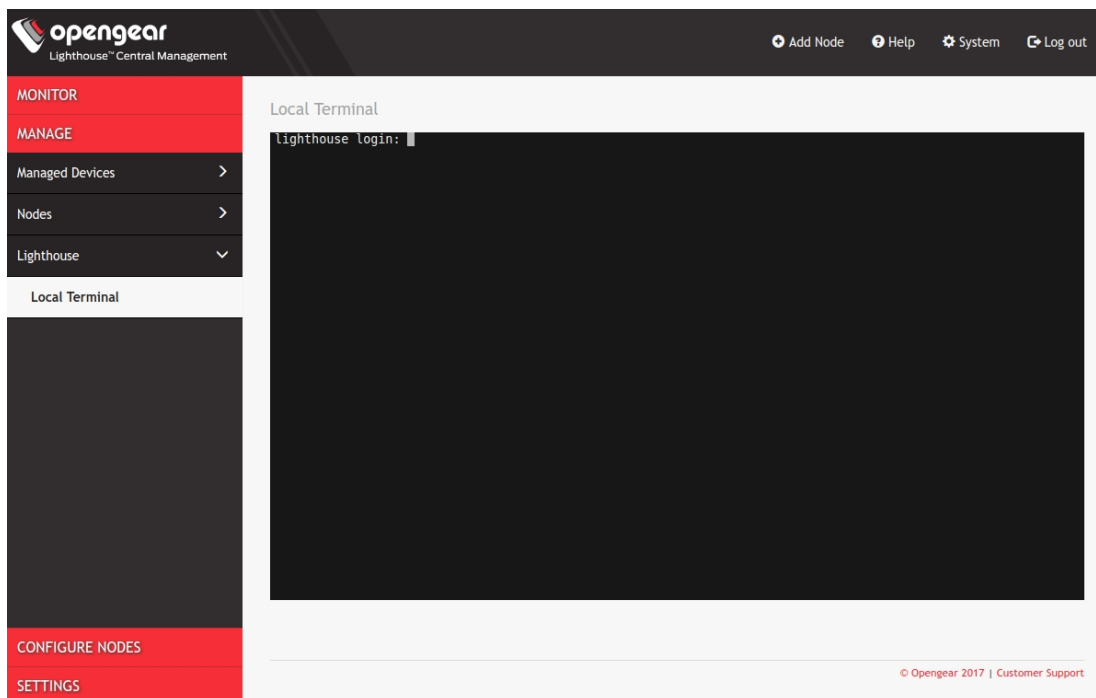
Note: don't change the configuration method. Just disable the interface you don't want to use by unchecking the *Enabled* checkbox. As of this release of *Opengear Lighthouse 5.1.0* or later, if *default-static* and *default-DHCP* are changed to the same configuration method (ie both are set to *Static assignment* or both are set to *DHCP*) neither interface will work.

6. Shut down or restart Opengear Lighthouse

6.1 Shutting down a running Opengear Lighthouse instance

To shutdown a running Opengear Lighthouse instance:

01. Select **Manage > Lighthouse > Local Terminal**



01. At the **Local Terminal** login prompt enter a username with administrative privileges (eg root.)

02. At the Password: prompt, enter that account's password

A *Last login* date and time for that account are returned to STD OUT and a shell prompt for the newly logged in user presents.

01. enter the command `shutdown now` and press **Return**.

The Lighthouse virtual machine shuts down.

6.2 Restarting a running Opengear Lighthouse instance

To restart a running Opengear Lighthouse instance, follow the first three steps of the *Shutting down a running Opengear Lighthouse instance* procedure above then:

01. At the shell prompt enter one or other of the following command strings:

`reboot`

`shutdown -r now`

01. Press **Return**.

The Lighthouse virtual machine shuts down and immediately reboots.

7. Using Opengear Lighthouse

After Opengear Lighthouse has been installed and configured, a small set of nodes should be enrolled, and a set of tags and smart groups should be created, that will allow nodes access to be filtered to the correct subset of users.

Once these nodes are installed, access to the Node's Web UI and serial ports should be tested.

This section will cover

- 01.Licensing third-party nodes before enrollment
- 02.Enrolling nodes
- 03.Creating Smart Groups
- 04.Accessing the node's Web UI
- 05.Accessing the node's serial ports via Console Gateway

7.1 Licensing third-party nodes before enrollment

Lighthouse 5.1.0 or later includes support for managing third-party remote nodes.

Support for third-party remote nodes is not built-in to a new Lighthouse instance, however: it is added via a *license*.

A *license* is an encrypted, RFC 7519-compliant, JSON web token that contains key-value pairs describing the features and entitlements of a given third-party remote node.

Licenses are distributed by Opengear and will be available as encrypted ASCII strings sent by e-mail via a fulfillment procedure.

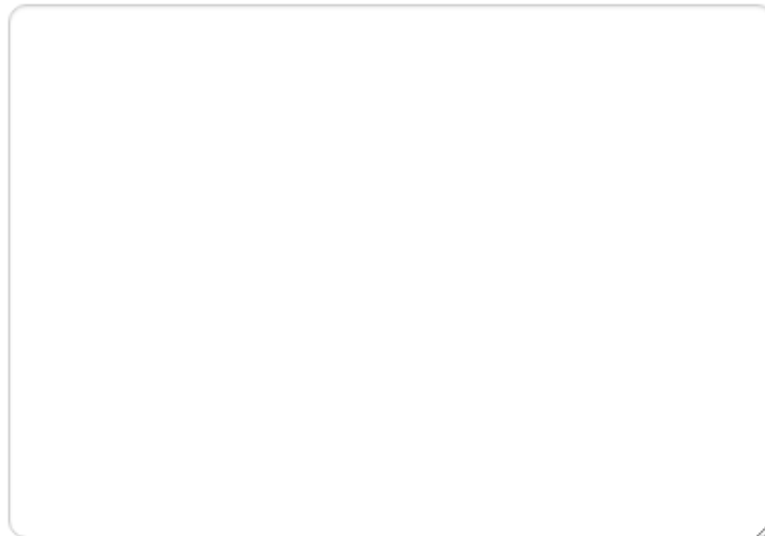
Before enrolling a third-party remote node, its corresponding license must be added to Lighthouse as follows:

7.1.1 Adding a license using the Lighthouse UI

- 01.Select **Settings > System > Licensing**
- 02.Click the + (add) button.

New License

License
body



Cancel

Apply

- 01.Paste the encrypted *license* text string into the *License body* text field.
- 02.Click **Apply**.

7.1.2 Showing installed licenses in the Lighthouse UI

Installed licenses are presented at **Settings > System > Licensing**.

opengear
Lighthouse™ Central Management

Add Node Help System Log out

MONITOR

MANAGE

CONFIGURE NODES

SETTINGS

Network Connections >

User Management >

Services >

Date & Time >

System >

Licensing

Administration

System Upgrade

Factory Reset

Licensing

License Information

OGLH

SKU	OGLH	SKU Code for the license information
Customer Name	Test	The customer name for this license
Email	engineering@opengear.com	The email address of a customer for this license
License Expiry	20/10/2020	The date when license will expire (aggregated date of expiry across all applied licenses for this SKU)
Number of Supported Devices	500	The number of supported devices for this license (aggregated across all applied licenses for this SKU)
License Features	Third Party Device Support	Additional features supported

Show License body

+ refresh

© Opengear 2017 | Customer Support

Installed Licenses are also presented on the Lighthouse Dashboard at **Monitor > Dashboard**.

Dashboard

Enrolled Nodes

Name	Status	Actions
sunnyvale-eng.oob.opengear.com	Connected: last status change 1 hour ago	Access Web UI
sunnyvale-support.oob.opengear.com	Connected: last status change 1 hour ago	Access Web UI
cm7132-2-dac	Connected: last status change 17 minutes ago	Access Web UI
im7216-24u	Connected: last status change 16 minutes ago	Access Web UI

Current Node Status

Connected (4)

Licensing Information

Number of Installed Licenses: 1
 Number of Supported Devices: 4 / 500
 Expiry Date: 20/10/2020
 Status: In Compliance
 Enabled Features: Third Party Device Support

The dashboard also displays messages when:

- 01.The number of nodes supported by a license has been reached or exceeded.
- 02.The maintenance period of a license has expired.

7.1.3 Showing installed licenses via the Local Terminal

oglicdump is a shell-based tool that writes the current licensing status of a Lighthouse instance to STD OUT (or, using the -o switch, a file).

For example:

```
# oglicdump
{
  "OGLH": {
    "contact": {
      "email": "engineering@opengear.com",
      "name": "Test",
```

```

    "phone": "123456"
  },
  "features": {
    "nodes": 500,
    "additional": {
      "thirdpartynodes": "1"
    }
  },
  "maintenance": 1603152000
}
}
}

```

If there are no installed licenses, `oglicdump` returns the following:

```

# oglicdump
No data found

```

7.2 Enrolling nodes

7.2.1 Enrollment overview

Enrolling nodes is the process of connecting nodes to Lighthouse, to make them available for access, monitoring, and management. Enrollment can be performed in a number of ways

01.Enrollment via the Lighthouse Web UI

02.Enrollment via the Node Web UI

03.Enrollment via ZTP

04.Enrollment via USB key

Each of these options will be described in this section

To authenticate either the Lighthouse (during enrollment via the Lighthouse WebUI), or the node (during the other enrollment scenarios) credentials must be provided.

The Lighthouse VPN uses certificate-authenticated OpenVPN tunnels between Lighthouse and remote nodes. These tunnels, in turn, rely on the time being synchronized between the Lighthouse instance and the *console server* or other remote node. If a remote node is not relying on an NTP server to set its own time, when a remote node receives a Lighthouse enrollment request, it inspects the HTTP `Date` header sent by Lighthouse and sets its local time to match that of the Lighthouse instance.

If a remote node *is* relying on an NTP server to set its own time, it still checks the HTTP `Date` header sent by Lighthouse to affect the time synchronization, but it does not set its local time to match that of the Lighthouse instance

When enrolling via Lighthouse, an administration username and password for the node must be provided. When enrolling via the node, an enrollment **Token** must be provided. A default enrollment token can be set on the **Configure Nodes > Enrollment Settings** page, and individual tokens set per enrollment bundle

Enrollment can either be a two-step, or a one-step process. The default is two-step:

01.Once enrollment starts, nodes receive their enrollment package, and establish a VPN connection to Lighthouse.

02.The node is now in the **Pending** state, and needs to be **Approved** before the node will be available for access, management, or monitoring.

This second step can be skipped when a particular enrollment bundle is used by checking the *Auto-approve node* check-box when configuring an enrollment bundle.

7.2.2 Enrollment bundles

An enrollment bundle (aka a provisioning bundle) is a downloadable file that stores provisioning information, allowing for bulk enrollment and manipulation of remote nodes.

Applying an enrollment bundle during enrollment allows tags to be associated with nodes when they're first enrolled, rather than manually assigning tags after the nodes are enrolled.

This is especially useful for larger roll-outs where there will be many nodes deployed with a similar configuration and responsibilities. If relevant Smart Groups and tags have been set up, newly enrolled nodes will be immediately visible for the relevant users to configure and use.

Associating templates with an enrollment bundle allows to run a set of templates on a node, after it has been enrolled. Any template currently defined on the Lighthouse can be added to an enrollment bundle, and each bundle supports any number of templates.

7.2.3 Creating an enrollment bundle

An enrollment bundle or `manifest.og` file contains a series of field-value pairs that an unconfigured device can use to configure itself.

Options that can be set in `manifest.og` include new firmware, custom configuration scripts, `opg config` files, and lighthouse enrollment details.

By default, `manifest.og` includes the following field-value pairs (the values are examples only):

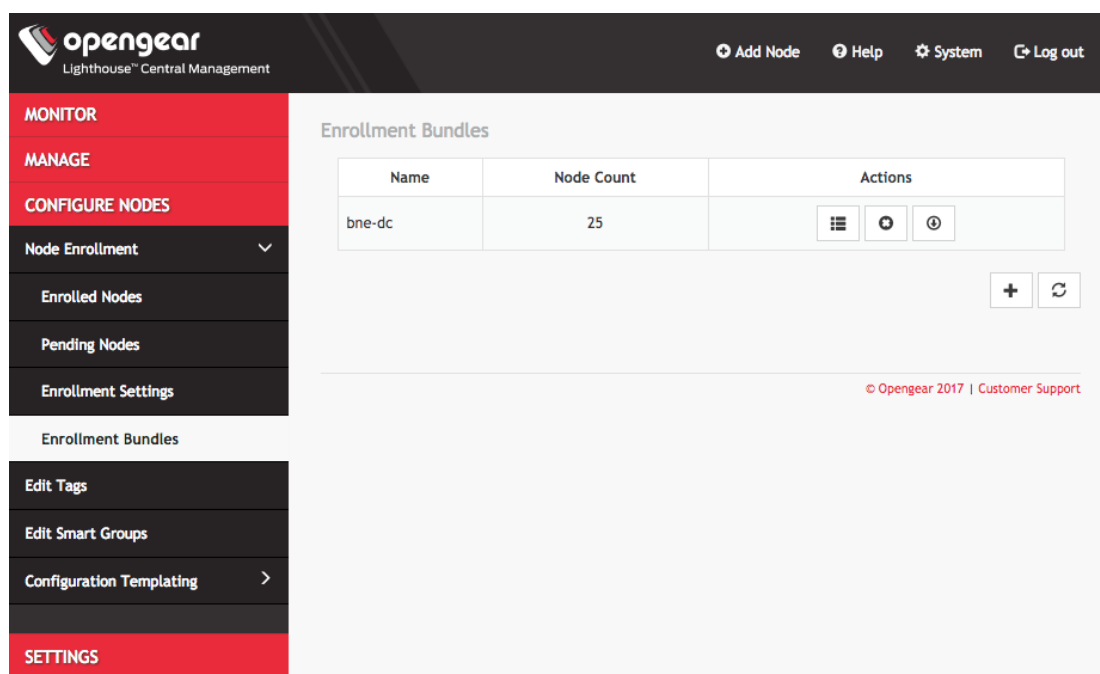
```
address=192.168.88.20
api_port=4443
bundle=bne-dc
password=secret
```

Custom field-value pairs can be added manually (again, the field names are potential field names for a real-world, customized file but the values following each field name are examples only):

```
script=configure_ports.sh
image=acm7000-3.16.6.image
external_endpoints=192.168.1.2:4444,192.168.1.3:4445
```

A provisioning bundle manifest .og file can be created in a Lighthouse instance as follows:

01.Select **Configure Nodes > Enrollment Bundles**



01.Click the + (add) button.

The **Enrollment Bundle Details** dialog box presents.

Enrollment Bundles

Enrollment Bundle Details

Name Descriptive bundle name

Token Authentication token used to request enrollment with this bundle

Auto-approve node Automatically approve enrollment after identification

Enrollment Bundle Node Tags

Tag values specified here will automatically be applied to any nodes enrolled against this bundle.

Templates

Templates selected here will automatically be applied to any nodes enrolled against this bundle in the specified order. Template push operations will stop from continuing if one fails.

Order	Template Type	Template Name	Actions
No Templates have been selected			

01. Enter a *Name* and *Authentication Token* for the bundle in the respective fields.

02. Select the number of *Tags* and *Values* to apply to any nodes that enroll using this enrollment bundle

03. (Optional) Check the *Auto-approve node* check-box.

When this is checked, a device configured using this enrollment bundle is not placed in pending mode during the enrollment process. Instead, it is automatically approved for enrollment after it has been identified.

With the enrollment bundle named, use the **Enrollment Bundle Node Tags** to populate it with the desired name-value pairs by:

01. Select a field name from the left-most pop-up menu.
02. Select or enter a value from the right-most pop-up menu.
03. Click the + (add) button to add a new pair of pop-up menus
04. Select another field name and select or enter another value.
05. Repeat until all desired name-value pairs are displayed.
06. Click the **Apply** button.

With the enrollment bundle named, use the **Templates** to populate it with the desired list of templates to be applied post-enrollment by:

01. Click the + (add) button to add a new pair of pop-up menus.
02. Select a value from the **Template Type** menu. The selected template type will filter the available names to those templates that are of that type. Note that to apply script templates, nodes need to be running firmware version 4.1.1 or later.
03. Select a value from the **Template Name** menu.
04. Repeat until all desired type-name pairs are displayed.
05. Click the **Apply** button.
06. The templates in the table can be re-ordered using the arrow buttons in the far left column of the table, and will be executed in the order they appear. The order buttons will only appear if there is more than one template in the table.

Note: Template push operations will stop from continuing if one template fails.

7.2.4 Enrollment via Lighthouse Web UI

01. Select the **Add Node** shortcut in the top menu bar to bring up the new enrollment dialog.
02. Select the *Product* type from the **Product** pop-up menu.
03. Available options in the **Product** pop-up menu are:

- An Opengear device
- A generic third party device
- An Avocent ACS6000
- An Avocent ACS8000

An Avocent ACS Classic A Cisco 2900 Series

The screenshot shows the 'New Enrollment' form. The 'Product' dropdown menu is open, displaying the following options: 'An Opengear device', 'A generic third party device', 'An Avocent ACS6000', 'An Avocent ACS8000', 'An Avocent ACS Classic', and 'A Cisco 2900 Series'. The 'An Opengear device' option is currently selected. The form includes fields for 'Network Address', 'Username', and 'Password', and a checked 'Auto-approve node' checkbox. 'Cancel' and 'Apply' buttons are located at the bottom right.

01.To enroll an Opengear device, an Avocent ACS6000, an Avocent ACS8000, an Avocent ACS Classic, or a Cisco 2900 Series, enter the *Name*, *Network Address*, *Username*, and *Password* of the Node being enrolled.

Note: Enrolling an Avocent ACS6000, an Avocent ACS8000, an Avocent ACS Classic, or a Cisco 2900 Series requires the device's license to have been added as per the 'Licensing third-party nodes before enrollment' procedure above. If an appropriate license has not been added to Lighthouse, the procedure will return a 'No licenses have been applied' error and the node will not be added to Lighthouse.

Note: the *Name* field does not allow the period (aka full-stop or 'dot') character. Attempting to use this character will fail with a *not a valid common name* error.

The screenshot shows the 'New Enrollment' form with the 'Product' dropdown menu closed. The 'Product' field now displays 'An Opengear device'. The other fields ('Network Address', 'Username', 'Password') and the 'Auto-approve node' checkbox are visible. 'Cancel' and 'Apply' buttons are at the bottom right.

Note: 5.1.1 or later Lighthouse populates the node name field with the hostname of the enrolled node rather than using a user provided value. It is no longer possible for users to specify a custom name, except when enrolling third party nodes. Console servers with firmware 4.1.1 and higher provide their hostname in the node information, with pre-4.1 nodes instead just having their node id used as the name. Nodes enrolled prior to upgrading to 5.1.1 or later have their names switched to the new standard if the node is running 4.1.1 firmware but will retain their old name if older firmware is still installed.

Note: the *Username* and *Password* fields are for the login credentials required by the remote node being enrolled. They are **not** for the login credentials required to login to the Opengear Lighthouse instance.

01.To enroll a generic third-party device, there are three more required fields: *Connection Method*; *Base Protocol Port*; and *Port Count*.

Note: the following procedure assumes the third-party device's license has been added as per the 'Licensing third-party nodes before enrollment' procedure above. If an appropriate license has not been added to Lighthouse, the procedure will return a 'No licenses have been applied' error and the node will not be added to Lighthouse.

New Enrollment

Product	<input type="text" value="A generic third party device"/>	The type of device to enroll
Name	<input type="text"/>	Brief name for this node
Network Address	<input type="text"/>	Current network address for this node
Connection Method	<input type="text" value="SSH"/>	The protocol used to connect to serial ports
Username	<input type="text"/>	Username for a node user with access to all serial ports
Password	<input type="text"/>	Password for a node user with access to all serial ports
Auto-approve node	<input checked="" type="checkbox"/>	Automatically approve enrollment after identification
Base Protocol Port	<input type="text" value="3000"/>	The base number from which network ports for individual serial ports will be derived
Port Count	<input type="text" value="4"/>	The number of serial ports on the target device (maximum 400)

Serial Port Labels

Port Label 1	<input type="text" value="Port 1"/>
Port Label 2	<input type="text" value="Port 2"/>
Port Label 3	<input type="text" value="Port 3"/>
Port Label 4	<input type="text" value="Port 4"/>

01. Choose *SSH* or *Telnet* from the *Connection Method* pop-up menu, as appropriate for the connection method supported by the third-party device.
 02. Enter a base number in the *Base Protocol Port*. By default, this is set to *3000*.
The Base Protocol Port number is the starting port number from which the third-party device's individual serial port network port numbers will be derived.
 03. Enter the number of serial ports the third-party device has in the *Port Count* field.
Below the *Port Count* field is a **Serial Port Labels** section. Whatever number is entered in the *Port Count* field, the *Port Label x* fields in this section will update to match this number in real-time.
 04. Optionally, edit the labels used to identify each serial port in the **Serial Port Labels** section.
01. Click **Apply**.
- Once enrolled, the console server's details are automatically removed from the **Pending Nodes** page and automatically added to the **Configure Nodes > Node Enrollment > Enrolled Nodes** page.

The screenshot shows the OpenGear Lighthouse Central Management web interface. The left sidebar contains navigation options: MONITOR, MANAGE, CONFIGURE NODES, Node Enrollment, Enrolled Nodes, Pending Nodes, Enrollment Settings, Enrollment Bundles, Edit Tags, Edit Smart Groups, and Configuration Templating. The main content area displays a table of enrolled nodes with columns for Name, Status, Description, and Actions. The table lists four nodes, all with a status of 'Connected' and a 'Success' configuration template run status. The nodes are: sunnyvale-eng.oob.opengear.com, sunnyvale-support.oob.opengear.com, sandy-finance.oob.opengear.com, and sandy-support.oob.opengear.com. Each node entry includes detailed information such as Model, Firmware Version, Enrollment Bundle, Management VPN Address, NET1 MAC address, Network, and Serial Number. A search bar and a 'Filtering' section are located at the top of the table. A 'Unenroll Selected' button is visible at the bottom of the table.

Name	Status	Description	Actions
sunnyvale-eng.oob.opengear.com	Connection Status: Connected: last status change 1 hour ago Configuration Template Run Status: Success	Model: IM7208-2-DAC Firmware Version: 4.1.0u2 Enrollment Bundle: Global Management VPN Address: 192.168.128.2 NET1 MAC address: 00:13:c6:01:5e:19 Network: 10.84.1.62 Serial Number: 72000183511477	[List Icon] [Close Icon]
sunnyvale-support.oob.opengear.com	Connection Status: Connected: last status change 1 hour ago Configuration Template Run Status: Success	Model: CM7196A Firmware Version: 4.1.0u2 Enrollment Bundle: Global Management VPN Address: 192.168.128.5 NET1 MAC address: 00:13:c6:00:00:01 Network: 10.84.1.72 Serial Number: N/A	[List Icon] [Close Icon]
sandy-finance.oob.opengear.com	Connection Status: Connected: last status change 25 minutes ago Configuration Template Run Status: Success	Model: CM7132-2-DAC Firmware Version: devbuild Enrollment Bundle: Global Management VPN Address: 192.168.128.4 NET1 MAC address: 00:13:c6:01:51:63 Network: 10.84.1.71 Serial Number: 71320039381442	[List Icon] [Close Icon]
sandy-support.oob.opengear.com	Connection Status: Connected: last status change 24 minutes ago Configuration Template Run Status: Success	Model: IM716-24U Firmware Version: devbuild Enrollment Bundle: Global Management VPN Address: 192.168.128.3 NET1 MAC address: 00:13:c6:01:e0:4d Network: 10.84.1.63 Serial Number: 72000666091618	[List Icon] [Close Icon]

Note: As of Lighthouse 5.1.0 or later, third-party devices are added to the config server but they are not enrolled.

7.2.5 Enrollment via Node Web UI

If the Node is situated behind a firewall, Lighthouse will not be able to initiate an enrollment: it will need to be triggered from the Node WebUI.

To do this:

- 01.log into the Node WebUI.
 - 02.select **Serial & Network > Lighthouse**.
 - 03.Enter the *Server Address*, the *Enrollment Bundle* (if a specific bundle is being used), and the *Enrollment Token* (either the global token or the bundle-specific token).
 - 04.Select **Apply Settings**.
- The enrollment process starts.

7.2.6 Mass Enrollment using ZTP

For mass node enrollments using ZTP, three new custom DHCP fields are handled by ZTP scripts.

These fields contain the **URL**, **Bundle Name** and **Enrollment Password** used in an enrollment which is kicked off immediately after all other ZTP handling is completed. If a reboot is required because of a config file being provided the enrollment will start after the reboot. Otherwise it happens immediately.

A sample configuration file, for the ISC DHCP Server, follows:

```
option space opengear code width 1 length width 1;
option opengear.config-url code 1 = text;
option opengear.firmware-url code 2 = text;
option opengear.enroll-url code 3 = text;
option opengear.enroll-bundle code 4 = text;
option opengear.enroll-password code 5 = text;

class "opengear-config-over-dhcp-test" {
  match if option vendor-class-identifier ~ "^Opengear/";
  vendor-option-space opengear;
  option opengear.config-url "http://192.168.88.1/config.xml";
  option opengear.enroll-url "192.168.88.20";
  option opengear.enroll-bundle "";
  option opengear.enroll-password "default";
}
```

Note: the maximum amount of data allowable as DHCP options is 1200 bytes, including all overhead inherent in the structuring of this data. Individual options are still, however, limited to 255 characters.

7.2.7 Enrollment via USB drive

USB Enrollment enables the configuration of a device using a manifest file copied to a USB drive and inserted into the unconfigured device before it first boots.

Once created (see 'Creating an enrollment bundle' above), `manifest.og` files can be downloaded from a Lighthouse instance as follows:

01. Select **Configure Nodes > Node Enrollment > Enrollment Bundles**.

A list of extant **Enrollment Bundles** presents.

02. In the **Actions** column of the particular bundle to be used, click the **download** button (a downward-pointing arrow in a circle).

03. Depending on your browser's configuration, a `manifest.og` file will either be downloaded to your local system (likely to `~/Downloads` or `c:\Users\%USERNAME%\Downloads\`) or your browser will present a dialogue box asking you to specify which local directory the download should be copied to.

To effect an enrollment via USB drive:

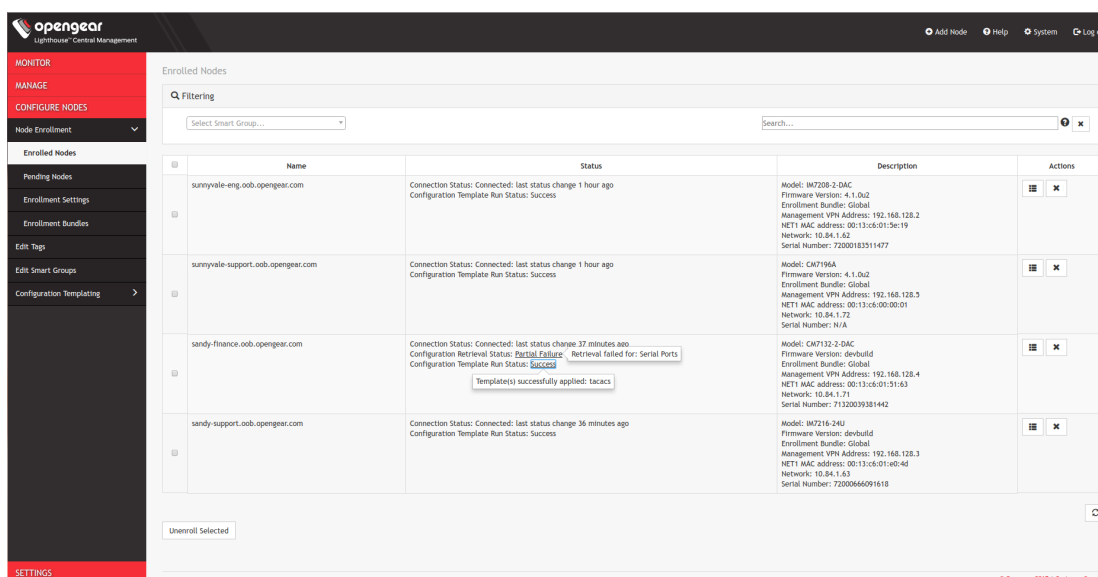
01. Copy `manifest.og` to the root directory on a USB drive.

02. Plug the USB drive into an unconfigured and powered-down *console server*

03. Power the *console server* up.

On first boot, the device looks for a file — `manifest.og` — on any USB drives attached to the device and configures the device based on the contents therein.

7.3 The Enrolled Nodes page



Configure Nodes > Node Enrollment > Enrolled Nodes lists all currently enrolled nodes in the order they are enrolled to *Opengear Lighthouse 5.1.0* or later.

It also presents details about each node (such as model, firmware version, serial number) and status.

Connection Status is the current status of the node and displays either of two things:

01. *Connected: Last status change x [time unit] ago.*

This is the time since *Opengear Lighthouse* connected to the console server.

01. *Disconnected: last status change x [time unit] ago*

This is the time since *Opengear Lighthouse* disconnected from the console server.

Configuration Retrieval Status displays if any configuration retrieval sections failed when performing a configuration sync with this node, such as Groups, Node Description, Authorization or Serial Ports.

Configuration Template Run Status displays the result of the most recent configuration template push on this node, listing which templates finished applying, or failed to apply to the node. This information is displayed until the next template push has completed on this node.

The **Configuration Retrieval Status** and **Configuration Template Run Status** are not displayed if there is no relevant data to display and are only displayed for users with Lighthouse Administrator or Node Administrator permissions.

The detailed information about the **Configuration Retrieval Status** and **Configuration Template Run Status** for each node are summarized as either:

01. "Success": all templates were successfully executed on the node.

02. "Partial Failure": some templates failed to execute on the node, or some config sections failed to synchronize.

03. "Failure": all templates failed to execute on the node, or all config sections failed to synchronize.

The detailed information is shown in a popover that appears when the summary of each status is clicked on, navigated to or hovered over. The format of the detailed information for each status shown on relevant popovers is now as follows:

- 01.Retrieval failed for: section_name, section_name, section_name.
- 02.Template(s) failed to apply: template_name, template_name, template_name.
- 03.Template(s) successfully applied: template_name, template_name, template_name.

7.4 Filtering pages displaying nodes

The **Configure Nodes > Enrolled Nodes** page and the **Configure Nodes > Pending Nodes** page as well as the **Nodes > Node Web UI** and **Nodes > Console Gateway** pages can all be filtered using either the *Search...* text-entry field or the *Smart Groups* pop-up menu.

7.4.1 Filtering using the Search field

The *Search...* text-entry field allows for near real-time filtering of which nodes are presented. Type a string (eg 'finance' or 'london' or 'CM7148') and press **Return** and only the nodes which include that string in their *Name* or *Description* will be displayed.

The *Search...* field treats multiple search terms (ie terms delimited by the space character) as Boolean AND searches.

For example, a search on the string:

london 4.1.1

will return any nodes that have both *london* AND *4.1.1* in searchable fields (eg 'london' in the name field and '4.1.1' in the firmware version field).

To make a search string that contains spaces into a single searched entity, enclose the string in double quotes.

For example, a search on the string:

"london east" 4.1.1

will return nodes that contain *london east* in the name field and *4.1.1* in the firmware version field. It will not return a node with *4.1.1* in the firmware version field if it also only contains *london* in the name field.

7.4.2 Filtering using the Smart Groups pop-up menu

Alternatively selecting from the *Select Smart Group...* pop-up menu will set the page to display the sub-set of nodes that belong to the selected group.

See Creating Smart Groups immediately below for how to create such groups.

Once a particular Smart Group has been selected, further filtering options become available. For example:

The screenshot shows a 'Filtering' interface with two rows of filter criteria. The first row consists of a dropdown menu with 'Office Deployments', a dropdown with 'Location', a dropdown with 'Is', and a dropdown with 'Brisbane', followed by a minus sign button. The second row consists of a dropdown with 'Department', a dropdown with 'Is not', and a dropdown with 'Support', followed by minus and plus buttons. At the bottom right, there are three buttons: 'Clear', 'Save as...', and 'Apply'.

In the example above, the **Configure Nodes > Node Enrollment > Enrolled Nodes** page is being filtered on the *Office Deployments* Smart Group.

It is then being further filtered to only display nodes with a:

Location of *Brisbane*, and a

Department other than *Support*.

Adding further filtering options can be done as follows:

- 01.Click the + (add) button.
An extra row of pop-up menus presents.
- 02.Select the desired tag from the left-most pop-up menu.
- 03.Select the filtering operator from middle pop-up menu.
- 04.Select or enter the value to be filtered against from the right-most pop-up menu.
- 05.Click **Apply**.

7.5 Creating Smart Groups

Smart Groups are saved search parameters used within Lighthouse for grouping related remote nodes.

A given User Group can be linked to a particular Smart Group. When a Group is linked in this fashion, members of the Group inherit rights over all nodes in the group based on the Group's Role. See 'Modifying existing Opengear Lighthouse groups' below for how to set a Group's Role and Linked Smart Group.

Smart Groups can also be used to filter visible nodes on pages that display enrolled nodes (such as **Configure Nodes > Node Enrollment > Enrolled Nodes**) to make it easier to drill down to a particular console.

Smart groups are dynamic, so as more nodes are added to the system, the filters will automatically update.

To create a Smart Group:

01.Navigate to any page which displays the Smart Group search interface, for example **Configure Nodes > Node Enrollment > Enrolled Nodes** or **Manage > Node > Node Web UI**.

The screenshot shows the Opengear Lighthouse Central Management interface. The left sidebar contains navigation menus: MONITOR, MANAGE (with sub-items Managed Devices and Nodes), Node Web UI (with sub-items Console Gateway and Lighthouse), CONFIGURE NODES, and SETTINGS. The main content area is titled 'Node Web UI' and features a 'Filtering' section with a 'Select Smart Group...' dropdown and a search box. Below this is a table with the following data:

Name	Status	Description	Actions
sunnyvale-eng.oob.opengear.com	Connected: last status change 2 hours ago	Model: IM7208-2-DAC Firmware Version: 4.1.0u2 Enrollment Bundle: Global Management VPN Address: 192.168.128.2 NET1 MAC address: 00:13:c6:01:5e:19 Network: 10.84.1.62 Serial Number: 72000183511477	Access Web UI
sunnyvale-support.oob.opengear.com	Connected: last status change 1 hour ago	Model: ACM5504-5-G-W-I Firmware Version: 4.1.1 Enrollment Bundle: Global Management VPN Address: 192.168.128.6 NET1 MAC address: 00:13:c6:00:f2:3d Network: 10.84.1.23 Serial Number: 5500061511353	Access Web UI
brisbane-support.oob.opengear.com	Connected: last status change 1 hour ago	Model: ACM7008-2-LMR Firmware Version: 4.1.1 Enrollment Bundle: Global Management VPN Address: 192.168.128.7 NET1 MAC address: 00:13:c6:01:f9:ef Network: 10.84.1.33 Serial Number: 70000305081677	Access Web UI
brisbane-eng.oob.opengear.com	Connected: last status change 57 minutes ago	Model: ACM7004-5-LMR Firmware Version: 4.1.1 Enrollment Bundle: Global Management VPN Address: 192.168.128.3 NET1 MAC address: 00:13:c6:02:30:d8 Network: 10.84.1.41 Internal Cellular Modem: 120.157.100.201 Serial Number: N/A	Access Web UI

01.Click on the *Select Smart Group...* drop-down

02.select *New Smart Group*.

This populates a number of new drop-downs and text boxes.

01.Click the *Field to search* drop-down to select a Node attribute to filter on.

These attributes include details about the device (*Model, Firmware Version, Serial Number, NET1 MAC Address*), and also include any **tags** that have been configured in the system. For filtering access to devices, tags are generally the most useful attribute to filter on. Note that when a tag is selected, the *Value* text box becomes a drop down with the values for that tag.

01.Click the *Operator* drop-down to select the operator to apply to the *Value*.

Generally, **Is** is the most useful.

01.Select the *Value* to be matched against.

02.Click **Apply** to see the results of the filter.

03.Click **Save As...**

04.type in a name for the search.

This Smart Group can now be used for filtering nodes for display, and for access.

7.6 Editing an existing Smart Group

To edit an existing Smart Group:

01.Select **Configure Nodes > Edit Smart Groups**.

01. Click the X icon to delete an existing Smart Group.

02. Click the **edit** icon to change a Smart Group's name.

Note: As of Lighthouse 5.1.1, editing the parameters of an existing Smart Group cannot be done from this page.

To change the search parameters used by an extant Smart Group:

01. Navigate to a page that presents Smart Groups for filtering (eg **Configure Nodes > Node Enrollment > Enrolled Nodes**).

02. Select the Smart Group which search parameters you wish to change from the **Select Smart Group...** pop-up menu.

03. Change the parameters (eg Tag and Operator values) as required.

04. Click the **Save as...** button.

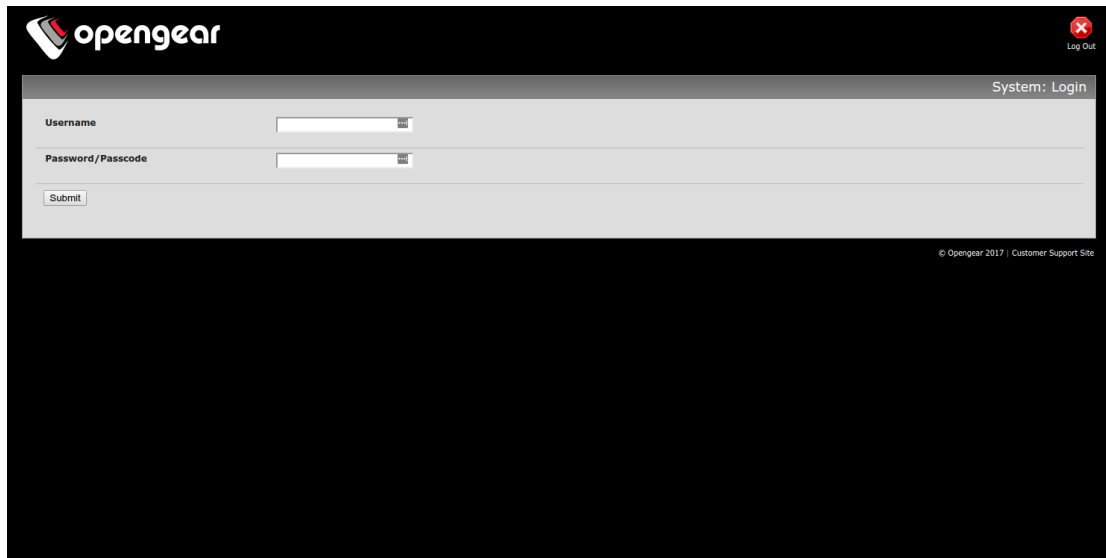
01. Leave the Smart Group name unedited and click **Apply**.

The changed Smart Group will overwrite the existing Smart Group.

7.7 Connecting to a Node's web-management interface

Once a node has been enrolled to *Opengear Lighthouse 5.1.0* or later its own web-management interface can be accessed from within the Lighthouse UI. To connect to an enrolled node's web-management interface:

01. Select **Manage > Nodes > Node Web UI**.
 02. In the *Actions* column, click the **Access Web UI** link for the node you wish to connect to.
The web-based login for that node loads.
01. Authenticate using the username and password required by that node.



This system is being accessed via Lighthouse - [click here to return to Lighthouse](#)

Note: at the bottom of the browser window is a visual indication that the console server session is being mediated through Opengear Lighthouse 5.1.0 or later. This footer also contains a link allowing for a quick return to Opengear Lighthouse 5.1.0 or later.

7.8 Connecting to a Node's serial ports via Console Gateway

Searching for serial ports on Lighthouse can be accomplished in two ways

01. Port-centric searching via the **Manage > Managed Devices > Console Gateway** page
02. Node-centric searching via the **Manage > Node > Console Gateway** page

Port-centric search allows filtering via the port name, and presents a flat list of ports that match the search terms, while Node-centric search allows filtering via Smart Groups, and Node properties, as well as port names. In general, the Port-centric searching offered via the **Manage > Managed Devices > Console Gateway** is recommended

Port-centric searching

01. Select **Manage > Managed Devices > Console Gateway**.
02. Find the console port you wish to access.

Do this by using the *Filtering* options to search for the port name. This search will live update as you type

Node-centric searching

01. Select **Manage > Nodes > Console Gateway**.
02. Find the console port you wish to access.

Do this by using the *Filtering* options to restrict the listed nodes to the particular node that hosts the console port, or by using the *Search* field to search by the port's *name* (aka label).

01. Click the **+** icon in the *Access Console Ports* row adjacent the node you wish to access.

Once the particular serial port is located, serial port access via **Console Gateway** can be accomplished in two ways

01. Access via HTML5 Web Terminal
02. Access via SSH

7.8.1 Access via HTML5 Web Terminal

To provide easy console port access, Lighthouse includes a HTML5 Web Terminal.

Note: The HTML5 Web Terminal includes native cut, copy and paste support. The terminals available on Nodes do not.

To access a console port via the Web Terminal:

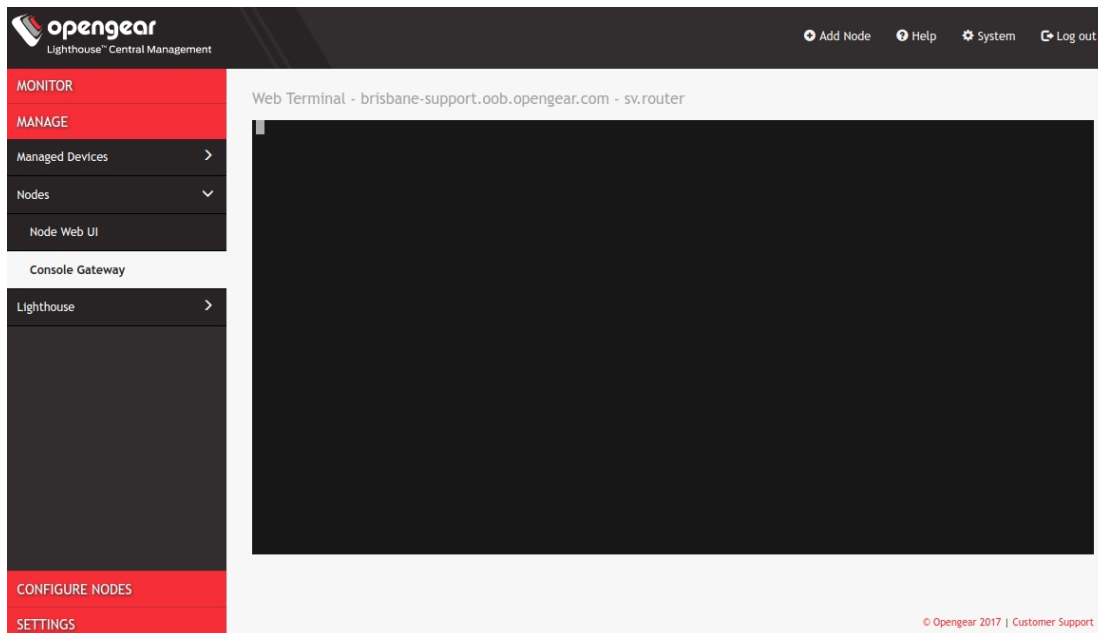
01. Locate the port you wish to access using one of the search techniques discussed above.

02. Click the **Web Terminal** link for the particular port.

A new tab opens, containing the Web Terminal

To close an HTML5 terminal session:

01. Close the tab, or type `~` in the Web Terminal window.



7.8.2 Access via SSH

To access ports via SSH, the user can either use a console chooser menu to select the node and the console port, or use a direct SSH link from the Web UI to connect directly to the port.

To access a console port via a Direct SSH link:

01. Locate the port you wish to access using one of the search techniques discussed above.

02. Click the **SSH** link to connect to the URL.

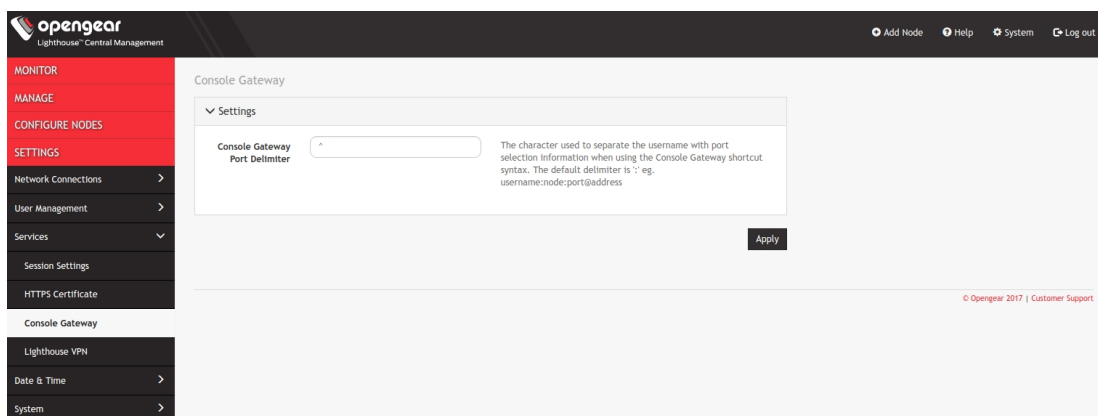
By default, these auto-generated links use the colon (:) as the field-delimiter. That is, the auto-generated SSH link has, by default, the following form:

```
ssh://user-name:console-server-name:port-number@lighthouse-ip-address
```

Some web-browsers, however, treat the colon character as strictly associated with delimiting the protocol at the beginning of a URI. Consequently, they don't pass these auto-generated URIs safely.

To cater for this, the default delimiter character can be changed. To change this character:

01. Select **Settings > Services > Console Gateway**.



01. Enter an alternative delimited character in the *Console Gateway Port Delimiter* text-entry field.

The caret character – ^ – is the most common alternative delimiter for URIs being parsed by browsers.

To use the console chooser menu, use SSH to connect to the Lighthouse appliance, with the username format *user-name:serial*. This will connect to the Lighthouse, and present a list of nodes that the user has access to.

Once the user selects a node, they are presented with a list of console ports they have access to. When one is selected, the user is connected to that port.

For faster access, there are username format shortcuts that give more specific lists of serial ports, or direct access without a menu.

`username:node_name`

When a valid node name is specified, a list of console ports that the user has access to on that node will be presented. If they do not have access to that node, the connection will fail.

`username:node_name:port_name`

When a valid node name and port name are specified, and the user has access to that node and port, the user will be directly connected to that port. If they do not have access to that port, the connection will fail.

`username:port_name`

When a valid port name is specified, the user will be connected to first port with that port name found. If the user does not have access to that port, the connection will fail.

Note: node names and port names are not case sensitive.

7.8.3 Example Console Gateway session:

```
$ ssh adminuser:serial@lighthouse-name-or-ip-here
```

```
1: cm71xx
```

```
Connect to remote > 0
```

```
1: Cisco Console
```

```
2: Port 2
```

```
Connect to port > 1
```

```
router#
```

8. Opengear Lighthouse user management

Lighthouse 5.1 supports locally defined users, and remote users that are authenticated and authorized by AAA.

Users must be members of one or more groups. Each group has a role assigned to it, which determines the level of access that group members will have to the system

These roles are:

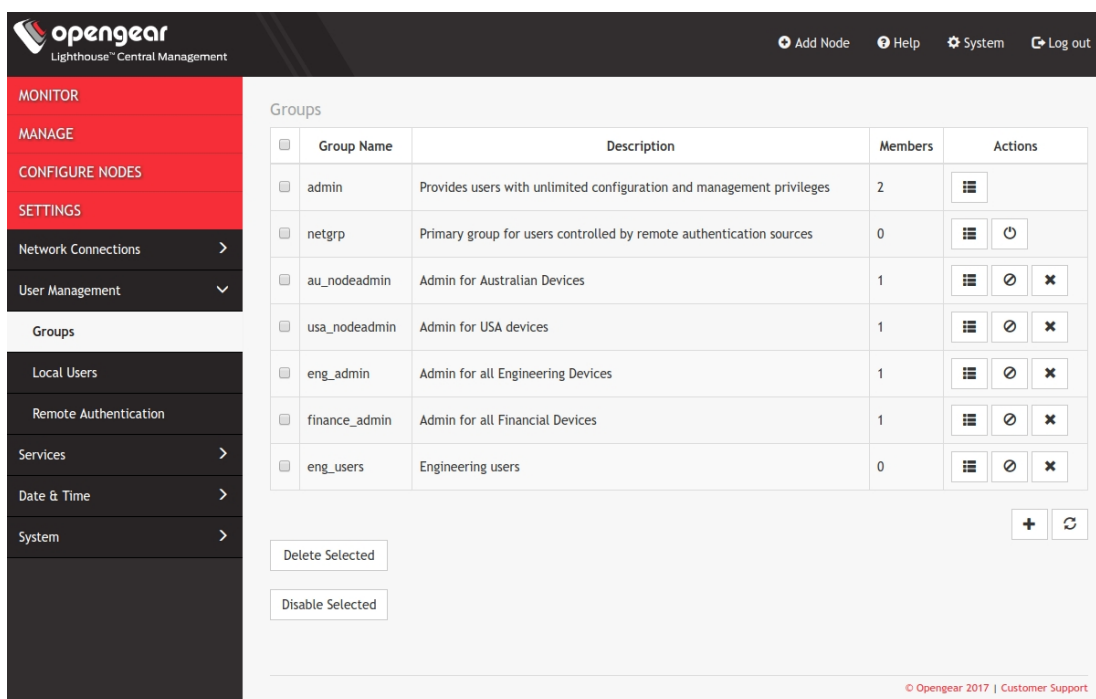
Role	Description
Lighthouse Administrator	The <i>Lighthouse Administrator</i> role is assigned to groups whose members need to manage and maintain the Lighthouse appliance. Members have access to all data on the Lighthouse system
Node Administrator	The <i>Node Administrator</i> role is assigned to groups that need to manage and maintain a set of Nodes. Each group with the <i>Node Administrator</i> role also must have an associated <i>Smart Group</i> which is evaluated to define the set of Nodes that the group members have access to.
Node User	The <i>Node User</i> role is assigned to groups that need to access a set of Nodes. Each group with the <i>Node User</i> role also must have an associated <i>Smart Group</i> which is evaluated to define the set of Nodes that the group members have access to.

Group membership can either be defined locally (for local users), or can be defined on the AAA server. Groups that are assigned by the AAA servers must still exist locally.

8.1 A note on password fields in Opengear Lighthouse

However they are labelled – *Password* or *Confirm password* or other label – password fields in Opengear Lighthouse are, in effect, **write-only**. They accept data from the clipboard or pasteboard but do not pass data out. So, all those strong, high-entropy passwords that you, quite rightly, don't want to either type or re-type, must be copied to your local clipboard or pasteboard from outside Lighthouse. They can then be safely copied in to all such fields in the Lighthouse user-interface.

8.2 Creating new Opengear Lighthouse groups



The screenshot shows the Opengear Lighthouse user management interface. The left sidebar contains navigation options: MONITOR, MANAGE, CONFIGURE NODES, SETTINGS, Network Connections, and User Management. The main content area displays a table of groups with columns for Group Name, Description, Members, and Actions. Below the table are buttons for 'Delete Selected' and 'Disable Selected'.

Group Name	Description	Members	Actions
admin	Provides users with unlimited configuration and management privileges	2	[Grid Icon]
netgrp	Primary group for users controlled by remote authentication sources	0	[Grid Icon] [Power Icon]
au_nodeadmin	Admin for Australian Devices	1	[Grid Icon] [Power Icon] [X Icon]
usa_nodeadmin	Admin for USA devices	1	[Grid Icon] [Power Icon] [X Icon]
eng_admin	Admin for all Engineering Devices	1	[Grid Icon] [Power Icon] [X Icon]
finance_admin	Admin for all Financial Devices	1	[Grid Icon] [Power Icon] [X Icon]
eng_users	Engineering users	0	[Grid Icon] [Power Icon] [X Icon]

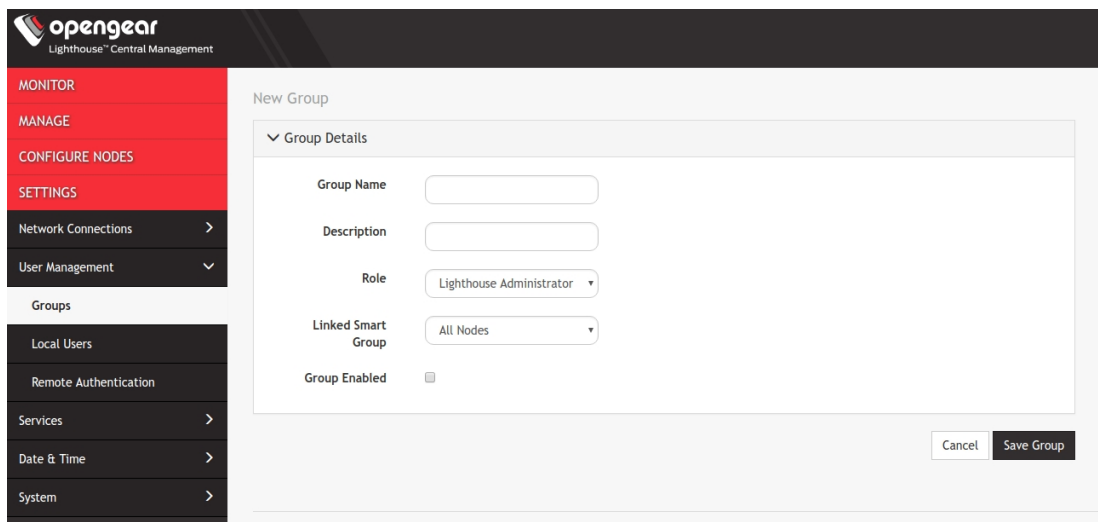
To create a new Opengear Lighthouse group:

01. Select **Settings > User Management > Groups**
02. Click the + button.
03. The New Group dialog loads.
04. Enter a *Group Name*, *Description* and select a *Role* for the group.

Note: Group Name can contain capital letters, numbers, and some alphanumeric characters. It is case sensitive.
When using remote authentication, characters from a user's remote groups that are not allowed on Light-

house will be converted to underscores during the authentication stages. Local groups can be created that take that into account, allowing the authentication to continue.

- 05.If the *Role* selected is *Lighthouse Administrator*, members of the group will automatically be added to the 'All Nodes' *Linked Smart Group*.
- 06.If the *Role* selected is *Node Administrator* or *Node User*, select a *Smart Group* to define the nodes that the group has access to.
- 07.Select **Group Enabled** checkbox to enable group.
- 08.Click **Save Group**.

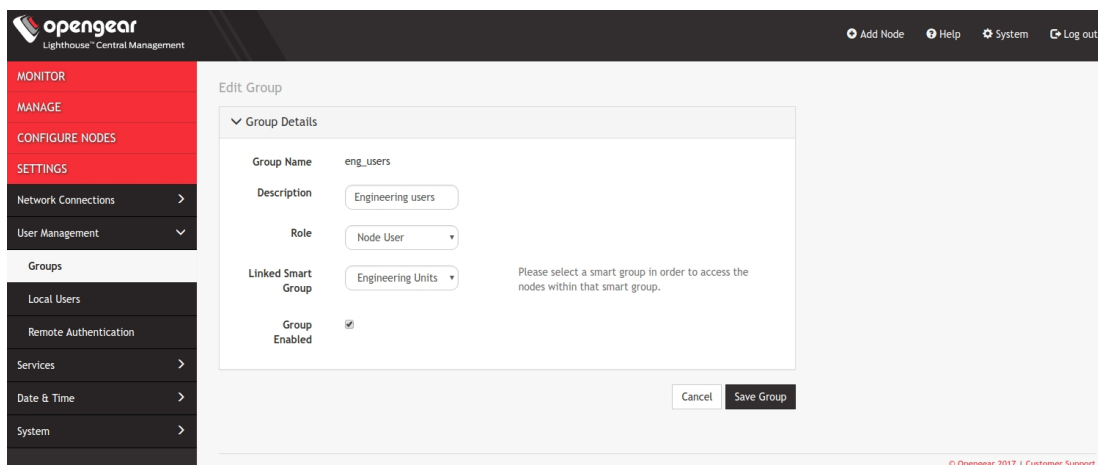


Note: if a new group (or new user) is given the *Lighthouse Administrator* role, members of the group (or individual users) will have access to the `sudo` command. In 'under the hood' terms, groups or users with the *Lighthouse Administrator* role are added to the `admin` group, which is in the list of allowed sudoers. On first boot of a new Lighthouse instance, the `root` user is the only member of the `admin` group and, consequently, the only user with `sudo` access.

8.3 Modifying existing Opengear Lighthouse groups

To modify an existing Opengear Lighthouse group:

- 01.Select **Settings > User Management > Groups**.
- 02.Click *Edit* in the **Actions** section of the group to be modified.
- 03.Make desired changes
- 04.Click **Save Group**.



The Modify Group dialog allows the group's *Description*, *Role*, and *Linked Smart Group* to be set and changed.

Note: If a Group's *Role* is *Lighthouse Administrator*, the group's *Linked Smart Group* is *All Nodes* and this cannot be changed. In equivalent fashion, if a Group has a *Linked Smart Group* other than *All Nodes*, the group's *Role* cannot be set to *Lighthouse Administrator*.

See 'Creating Smart Groups' above for details regarding creating and using Smart Groups.

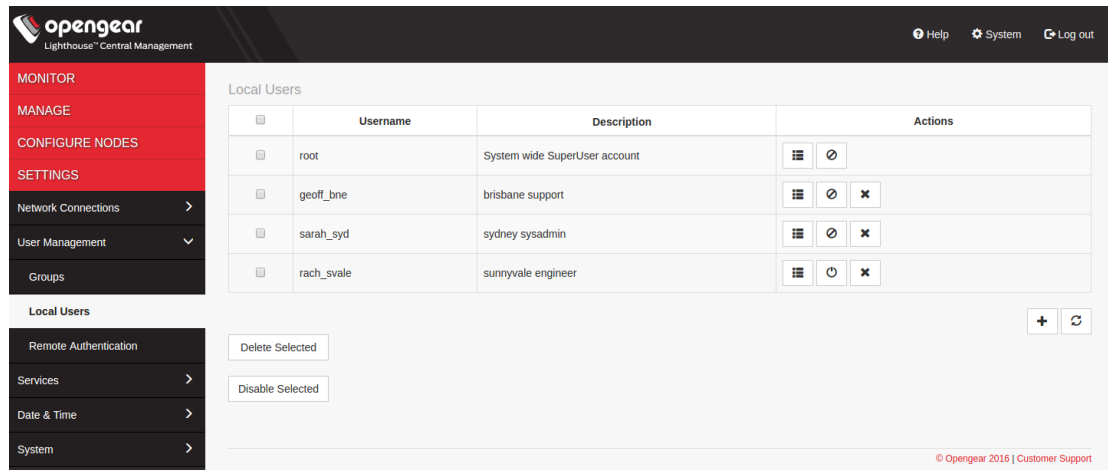
The Modify Group dialog also allows for a group to be deleted. If a group is deleted, however, all users who were members of the group lose any access and administrative rights inherited from the group.

8.4 A note on default netgrp Opendgear Lighthouse group

The "netgrp" group is inherited as the primary group for all remote AAA users who are not defined locally on Lighthouse. By default, "netgrp" has the Lighthouse Administrator role and is disabled - it must be enabled to take effect for remote AAA users.

8.5 Creating new Opendgear Lighthouse users

To create a new Opendgear Lighthouse user:



01. Select **Settings > User management > Local Users**

02. Click the + button.

03. The New User dialog loads.

04. Enter a *Username*, *Description*, and *Password*.

05. Re-enter the *Password* in the *Confirm Password* field.

06. Check the *Enabled* check box.

07. Click Apply.

The root user – which password was reset on the initial boot of the *Opendgear Lighthouse VM* (see 'First boot of the Opendgear Lighthouse VM' above) will already be listed here.

To create a new Opendgear Lighthouse user without password which causes them to fail back to remote authentication:

01. Select **Settings > User management > Remote Authentication**

02. Apply Remote Authentication Settings.

03. Select **Settings > User management > Local Users**

04. Click the + button.

05. The New User dialog loads.

06. Enter a *Username*, *Description*.

07. Check the *Remote Password Only* check box.

08. Check the *Enabled* check box.

09. Click Apply.

8.6 Modifying existing Opendgear Lighthouse users

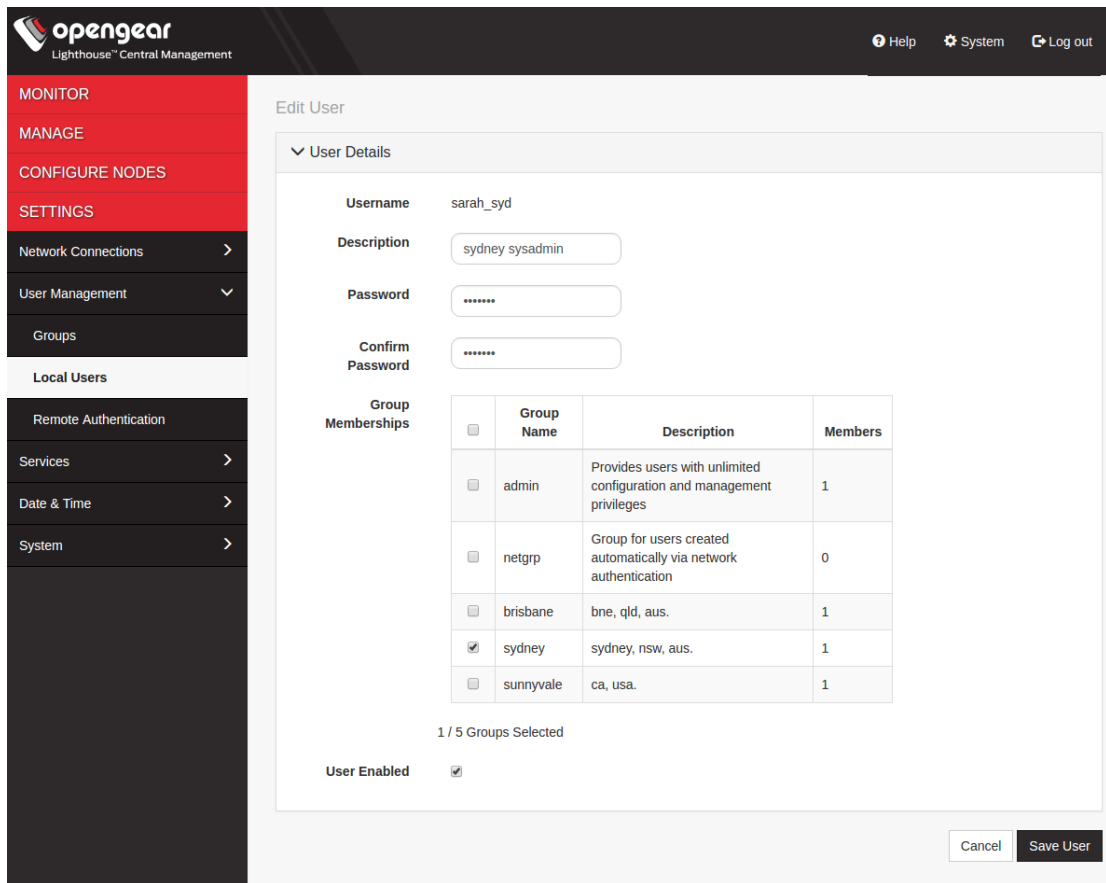
To modify an existing Opendgear Lighthouse user:

01. Select **Settings > User management > Local Users**

02. Click *Edit* in the **Actions** section of the user to be modified.

03. Make desired changes.

04. Click **Save User**.



The Modify Users dialog allows the user's *Description* to be changed and the user's *Password* to be re-set. The user-name cannot be changed. The Modify Users dialog also allows the user to be disabled, by unchecking the *Enabled* check box.

Disabled users cannot login to Lighthouse using either the Web-based interface or via shell-based logins (ie `sshusername-you-disabled@lighthouse-name-or-ip` will not work). The user still exists, however (the `/home/username-you-disabled` directory is still extant in the Opengear Lighthouse VM file-system for example).

8.7 Deleting Opengear Lighthouse users

To delete an Opengear Lighthouse user completely:

01. Select **Settings > User management > Local Users**
02. Click *Delete* in the **Actions** section of the user to be modified.
03. Click **Yes** in the **Confirmation** dialog.

8.8 Disabling Opengear Lighthouse root user

To disable an Opengear Lighthouse root user:

01. Make sure that another user exists that is in a group that has the "Lighthouse Administrator" role.
02. Select **Settings > User management > Local Users**
03. Click *Disable* in the **Actions** section of the root user.
04. Click **Yes** in the **Confirmation** dialog.
05. To enable root user back log in with another user exists that is in a group that has the "Lighthouse Administrator" role and click *Enable* in the **Actions** section of the root user.

Lighthouse supports three AAA systems:

01. LDAP (Active Directory and OpenLDAP)
02. RADIUS
03. TACACS+

Authentication works much the same with each, but group membership retrieval varies. The following sections detail the configuration settings for each provider, and explain how group membership retrieval works.

To begin:

01. Select **Settings > User Management > Remote Authentication**.

8.9 LDAP Configuration

Remote Authentication

Settings

Scheme: LDAP

Remote authentication servers	Address	Port <small>(defaults to 389)</small>	
	<input type="text"/>	<input type="text"/>	<input type="button" value="-"/> <input type="button" value="+"/>

LDAP base DN: The distinguished name of the search base. For example: dc=my-company,dc=com

LDAP bind DN: The distinguished name to bind to the server with. The default is to bind anonymously.

Bind DN password:

Confirm password:

LDAP username attribute: The LDAP attribute that corresponds to the login name of the user (commonly "sAMAccountName" for Active Directory, and "uid" for OpenLDAP).

LDAP group membership attribute: The LDAP attribute that indicates group membership in a user record (commonly "memberOf" for Active Directory, and unused for OpenLDAP).

Apply

01. Select *LDAP* from the *Scheme* drop-down box.

02. Add the *Address* and optionally the *Port* of the LDAP server to query.

03. Add the *Base DN* that corresponds to the LDAP system being queried.

For example, if a user's distinguished name is cn=John Doe, dc=Users, dc=ACME, dc=com, the *Base DN* is dc=ACME, dc=com

01. Add the *Bind DN*.

This is the distinguished name of a user with privileges on the LDAP system to perform the lookups required for retrieving the username of the users, and a list of the groups they are members of.

01. Add the password for the binding user

02. Add the *Username Attribute*.

This depends on the underlying LDAP system. Use *sAMAccountName* for Active Directory systems, and *uid* for OpenLDAP based systems

01. Add the *Group Membership Attribute*.

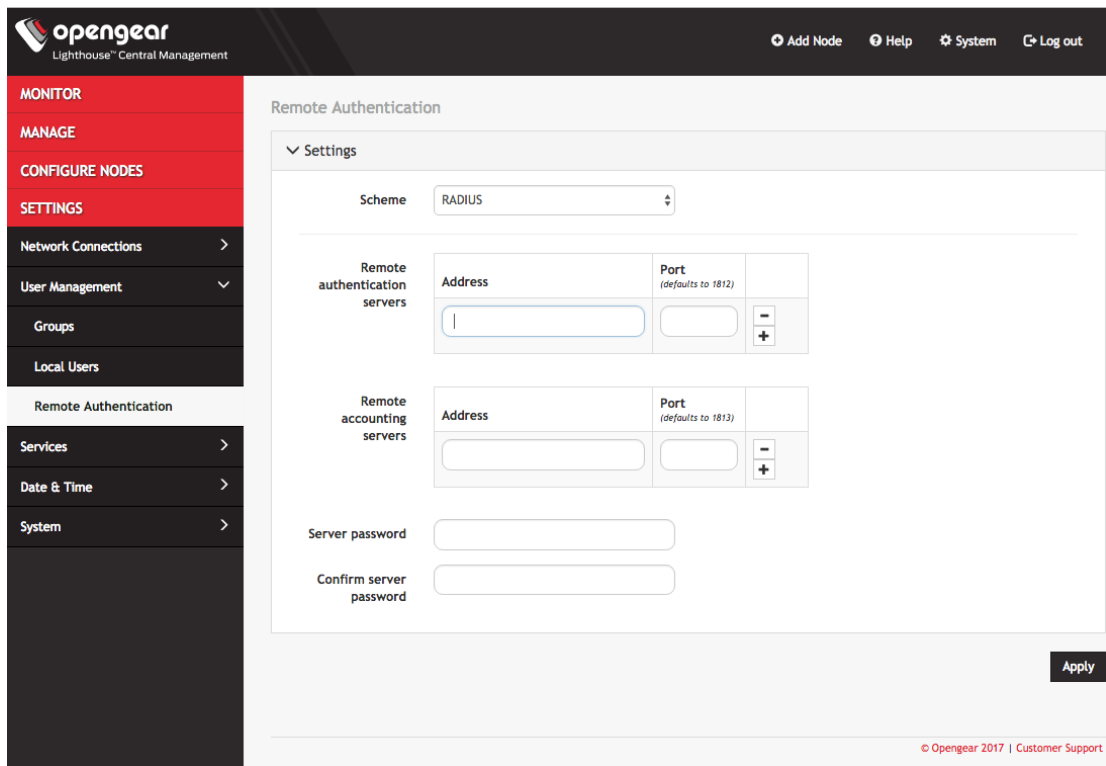
This is only needed for Active Directory, and is generally *memberOf*.

Note: multiple servers can be added. The LDAP subsystem will query them in a round-robin fashion.

8.10 RADIUS Configuration

To configure RADIUS:

01. Select **Settings > User Management > Remote Authentication**.



01. In the **Settings** section, select *RADIUS* from the *Scheme* pop-up menu.
02. Add the *Address* and optionally the *Port* of the RADIUS authentication server to query.
03. Add the *Address* and optionally the *Port* of the RADIUS accounting server to send accounting information to.
04. Add the *Server password* (Also known as the RADIUS Secret).

Note: multiple servers can be added. The RADIUS subsystem will query them in a round-robin fashion.

To provide group membership, RADIUS needs to be configured to provide a list of group names via the Framed-Filter-Id attribute.

The following configuration snippet shows how this can be configured for FreeRADIUS

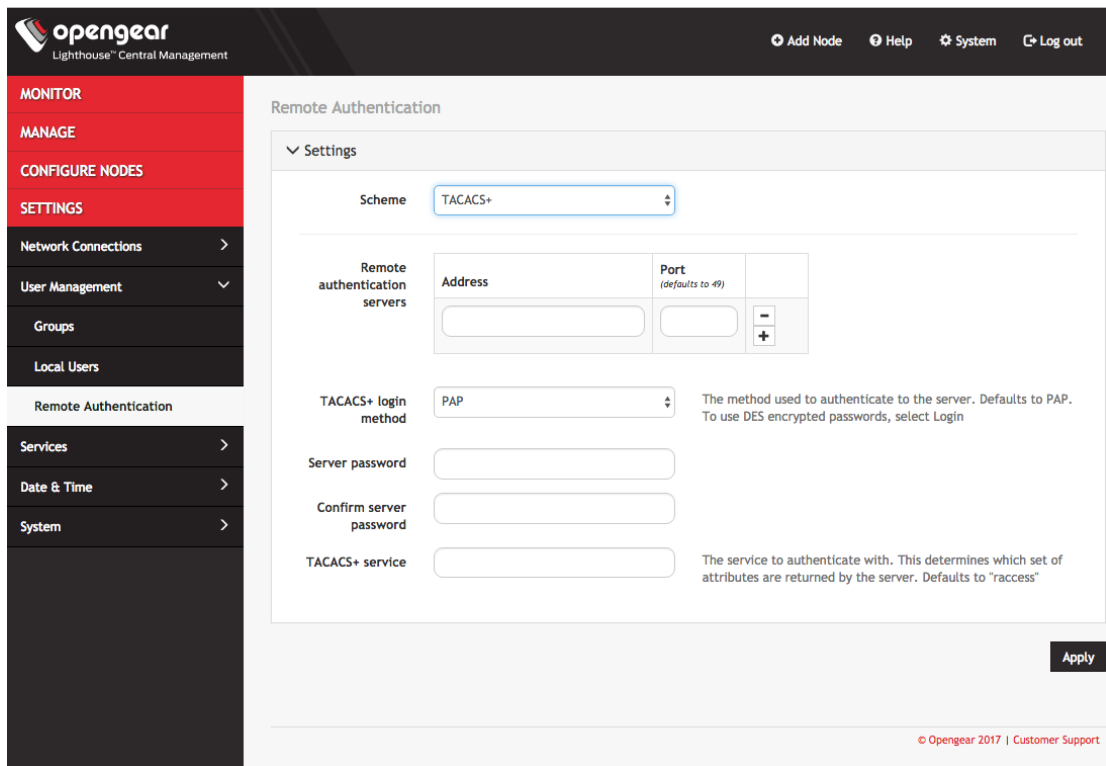
```
operator1 Auth-Type := System
        Framed-Filter-ID = ":group_name=west_coast_admin,east_coast_user:"
```

Note: the Framed-Filter-ID attribute must be delimited by the colon character.

8.11 TACACS+ Configuration

To configure TACACS+:

01. Select **Settings > User Management > Remote Authentication**.



01. Select *TACACS+* from the *Scheme* pop-up menu.

02. Add the *Address* and optionally the *Port* of the TACACS+ authentication server to query.

03. Select the *Login Method*.

PAP is the default method. However, if the server uses DES-encrypted passwords, select *Login*.

01. Add the *Server password* (Also known as the TACACS+ Secret)

02. Add the *Service*. This determines the set of attributes sent back by the TACACS+ server

Note: multiple servers can be added. The TACACS+ subsystem will query them in a round-robin fashion.

To provide group membership, TACACS+ needs to be configured to provide a list of group names

The following configuration snippet shows how this can be configured for a *tac_plus* server.

```

user = operator1 {
    service = raccess {
        groupname = west_coast_admin, east_cost_user
    }
}

```

To do this with Cisco ACS, see [setting up permissions with Cisco ACS 5 and TACACS+](#) on the OpenGear Help Desk.

9. Lighthouse central configuration

Templates are a centralized way of changing the configuration for enrolled Opengear Console Server nodes by pushing pre-defined configuration templates to selected nodes. Lighthouse 5.1 or later supports the creation and execution of Group, Authentication and Script templates.

9.1 Creating new group templates

Only users assigned to the *Lighthouse Administrator* role can access **Configure Nodes > Configuration Templating > Group Templates** and create templates.

A group template contains a list of groups that are set as the list of user-defined groups on the node. Each group has a defined role which determines what privileges group members will have.

The available roles are:

Node Administrator — maps to the administrator role on the nodes.

Node User — maps to the all ports user role, and the pmshe11 role, on the nodes.

To create a new group template:

01. Select **Configure Nodes > Configuration Templating > Group Templates**.

02. Click the + (add) button.

The **New Group Template** dialog loads.

The screenshot shows the 'New Group Template' dialog in the Opengear Lighthouse Central Management interface. The dialog is divided into two main sections: 'Template Details' and 'Set Group List'. In the 'Template Details' section, there are two input fields: 'Name' and 'Description'. The 'Set Group List' section contains a table with two columns: 'Group Name' and 'Actions'. Below the table, there is a note: 'Groups provided in the list will replace any user defined groups on the node'. The table currently shows 'No Groups have been created'. There is a '+ Add' button below the table. At the bottom of the dialog, there are 'Cancel' and 'Save Template' buttons. The interface also shows a sidebar with navigation options like 'MONITOR', 'MANAGE', 'CONFIGURE NODES', and 'SETTINGS'.

01. Enter a *Name* and *Description* for a template in the **Template Details** section.

02. Click the + (add) button in the **Set Group List** section to add a new group.

The **Group Details** dialog loads.

03. Enter a *Group Name*, a *Description*, and select a *Role* for the group.

04. Click **Apply**.

05. Click **Save Template**.

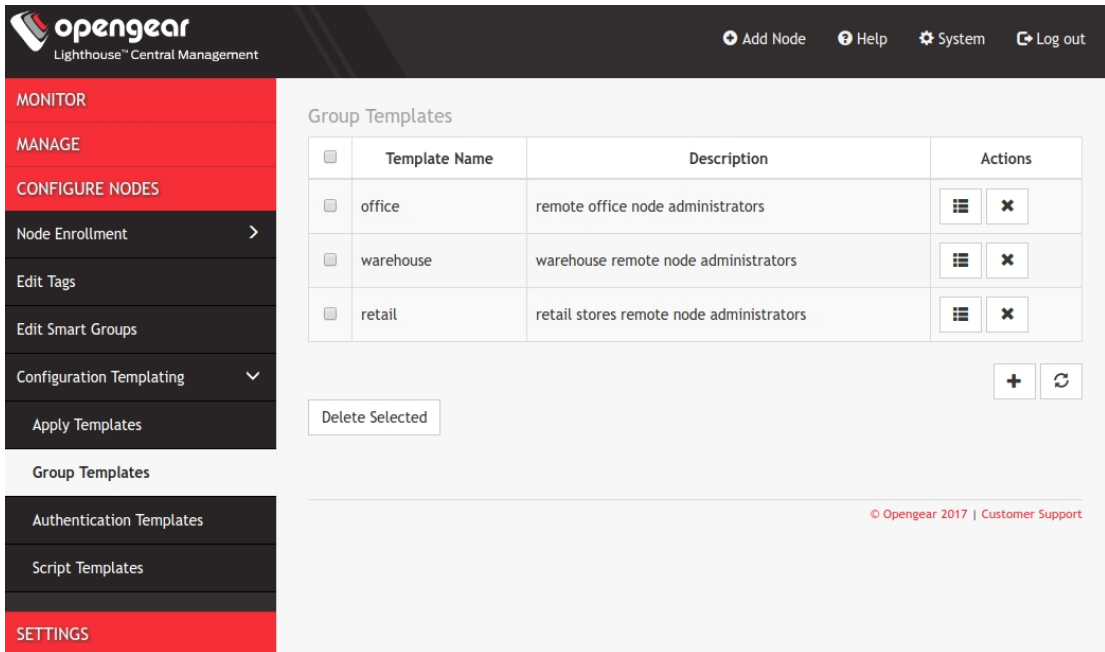
Note: when a group template is pushed to a node, all custom groups on that node are replaced by the groups defined in the template's group list.

9.2 Modifying existing group templates

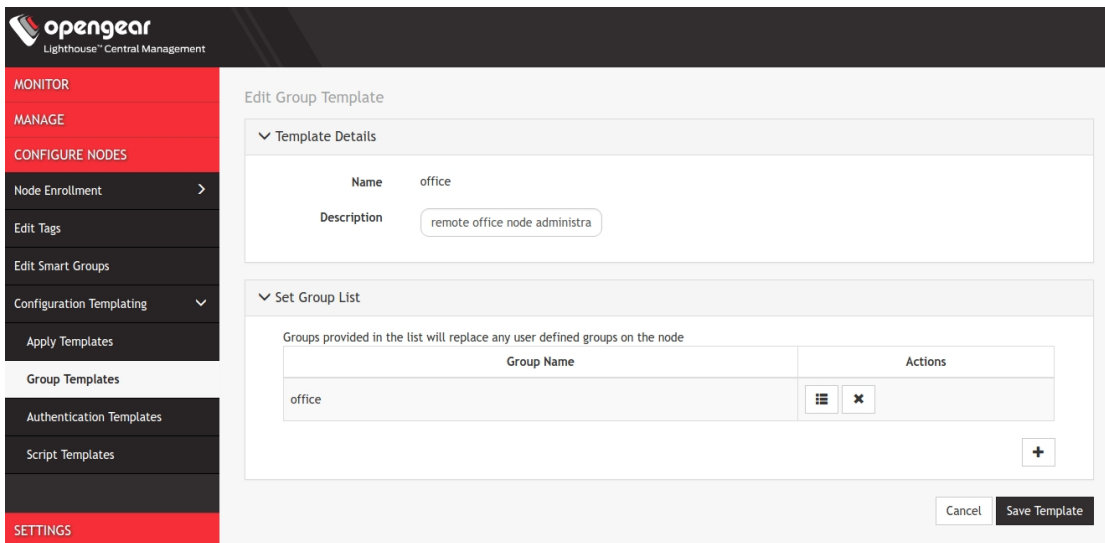
The **Edit Group Template** dialog allows a template's Description and Group List to be set and changed.

To modify an existing group template:

01. Select **Configure Nodes > Configuration Templating > Group Templates**.



01. Click **Edit** in the **Actions** section of the template to be modified.
The **Edit Group Template** dialog presents.



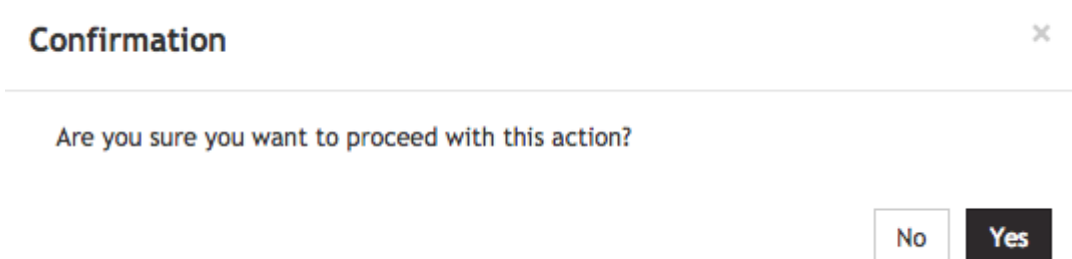
01. Make changes as required.
02. Click **Save Template**.

9.3 Deleting group templates

To delete a group template completely:

01. Select **Configure Nodes > Configuration Templating > Group Templates**.
02. Click **Delete** in the **Actions** section of the template to be removed.

The *Confirmation* alert box appears.



01. Click **Yes** in the **Confirmation** dialog.

The group template is deleted.

9.4 Creating new authentication templates

Only users assigned to the *Lighthouse Administrator* role can access **Configure Nodes > Configuration Templating > Authentication Templates** and create authentication templates.

The supported modes are *Local*, *Radius*, *TACACS+* and *LDAP*. For example, if an authentication template is configured to use *RADIUS* as an authentication source, that corresponds to *RADIUSDownLocal* with *Use Remote Groups* ticked on the downstream node.

To create a new authentication template:

01. Select **Configure Nodes > Configuration Templating > Authentication Templates**.

02. Click the + (add) button.

The **New Authentication Template** dialog loads.

01. Enter a *Name* and *Description* for a template in the **Template Details** section.

02. Select a desired Scheme or click the **Pre-populate** button to pre-populate a template with the current Lighthouse remote authentication configuration.

03. Enter or update authentication settings if required.

See 'Configuring AAA' above for an example.

04. Click **Save Template**.

Note: when an authentication template is pushed to a node, the authentication settings at that node are replaced by the those defined in the authentication template.

Note: the authentication templates do not currently support the full list of settings that the Opengear Console Servers support. However, templates can be applied and then additional settings configured manually.

9.5 Modifying existing authentication templates

The **Edit Authentication Template** dialog allows the template's *Description* and *Authentication Settings* to be set and changed.

To modify an existing authentication template:

01. Select **Configure Nodes > Configuration Templating > Authentication Templates**.

opengear
Lighthouse™ Central Management

MONITOR
MANAGE
CONFIGURE NODES
Node Enrollment
Edit Tags
Edit Smart Groups
Configuration Templating
Apply Templates
Group Templates

Authentication Templates
Script Templates

SETTINGS

Authentication Templates

Template Name	Description	Actions
office	auth settings for remote office nodes	[Grid] [X]
warehouse	auth settings for warehouse nodes	[Grid] [X]
retail	auth settings for retail nodes	[Grid] [X]

Delete Selected

+ Refresh

© Opengear 2017 | Customer Support

02. Click **Edit** in the **Actions** section of the template to be modified.
The **Edit Authentication Template** dialog presents.

opengear
Lighthouse™ Central Management

MONITOR
MANAGE
CONFIGURE NODES
Node Enrollment
Edit Tags
Edit Smart Groups
Configuration Templating
Apply Templates
Group Templates

Authentication Templates
Script Templates

SETTINGS

Edit Authentication Template

Template Details

Name: office
Description: remote office nodes

Authentication Settings

Pre-populate from Lighthouse: Pre-populate
Pre-populate the template fields with the current Lighthouse remote authentication settings.

Scheme: RADIUS

Remote authentication servers
Address: 192.168.1.168
Port (defaults to 1812): 1812

Remote accounting servers
Address: 192.168.1.168
Port (defaults to 1813): 1813

Server password:
Confirm server password:

Cancel Save Template

01. Make required changes.
02. Click **Save Template**.

9.6 Deleting authentication templates

To delete an authentication template completely:

01. Select **Configure Nodes > Configuration Templating > Authentication Templates**.
02. Click **Delete** in the **Actions** section of the template to be removed.

The *Confirmation* alert box appears.

Confirmation



Are you sure you want to proceed with this action?

No

Yes

01. Click **Yes** in the **Confirmation** dialog.
The authentication template is deleted.

9.7 Creating new script templates

Only users assigned to the *Lighthouse Administrator* role can access **Configure Nodes > Configuration Templating > Script Templates** and create script templates.

Script Templates allow the user to upload arbitrary shell scripts to be run on a node. A script may set additional configuration settings not available in other templates, or store additional files onto the node such as certificates, for example. The uploaded script must have a ".sh" extension, and can not be more than 1MB in size. Other than those, there are no other restrictions on the script file to be uploaded. Once saved, the template will store the size and SHA1 checksum of the script. This can be used to verify the script contents of the template once saved. To apply script templates, the selected nodes need to be running firmware version 4.1.1 or later.

To create a new script template:

01. Select **Configure Nodes > Configuration Templating > Script Templates**.
02. Click the + (add) button.

The **New Script Template** dialog loads.

01. Enter a *Name* and *Description* for a template in the **Template Details** section.
 02. Upload a script with *Choose file* button.
 03. Click **Save Template**.
- Note:** Script checksum and Script size will be shown after template with uploaded script as saved.

9.8 Modifying existing script templates

The **Edit Script Template** dialog allows the template's *Description*, *Script timeout* and *Script File* to be uploaded.

To modify an existing script template:

01. Select **Configure Nodes > Configuration Templating > Script Templates**.

opengear
Lighthouse™ Central Management

MONITOR
MANAGE
CONFIGURE NODES
Node Enrollment
Edit Tags
Edit Smart Groups
Configuration Templating
Apply Templates
Group Templates
Authentication Templates
Script Templates
SETTINGS

Script Templates

Template Name	Description	Actions
office	script for office nodes	[List] [X]
warehouse	script for warehouse nodes	[List] [X]
retail	script for retail nodes	[List] [X]

Delete Selected

+ Refresh

© OpenGear 2017 | Customer Support

02. Click **Edit** in the **Actions** section of the template to be modified.
The **Edit Script Template** dialog presents.

opengear
Lighthouse™ Central Management

MONITOR
MANAGE
CONFIGURE NODES
Node Enrollment
Edit Tags
Edit Smart Groups
Configuration Templating
Apply Templates
Group Templates
Authentication Templates
Script Templates
SETTINGS

Edit Script Template

Template Details

Name: office

Description: script for office node

Script timeout: 15
Time to wait for script to complete execution (in minutes). After timeout is reached, script will be stopped

Script checksum: 87181db25fd03cddfcc0819a2e6e08d30bf03775
SHA1 checksum will be shown after template with uploaded script is saved

Script size (kB): 28 bytes
Size will be shown after template with uploaded script is saved

Upload Script File

Script File: Choose file script.sh
Maximum script file size is 1 MB. Script must be in shell executable format (.sh)

Note: To apply script templates, the selected nodes need to be running firmware version 4.1.1 or later.

Cancel Save Template

01. Make required changes.
02. Click **Save Template**.

9.9 Deleting script templates

To delete a script template completely:

01. Select **Configure Nodes > Configuration Templating > Script Templates**.
02. Click **Delete** in the **Actions** section of the template to be removed.

The *Confirmation* alert box appears.

Confirmation



Are you sure you want to proceed with this action?

No

Yes

01. Click **Yes** in the **Confirmation** dialog.

The script template is deleted.

9.10 Apply Templates

Users with Lighthouse Administrator privileges (ie, users with the Lighthouse Administrator role or users who are members of groups with the Lighthouse Administrator role) can access **Configure Nodes > Configuration Templating > Apply Templates** and execute templates affecting any node.

Users with Node Administrator privileges (ie, users with the Node Administrator role or users who are members of groups with the Node Administrator role) can access **Configure Nodes > Configuration Templating > Apply Templates** and execute templates affecting nodes in Smart Groups linked to their role.

Apply Templates consists of four stages, each one a step in the overall 'wizard'. The steps are:

01. Select Template.

02. Select Nodes.

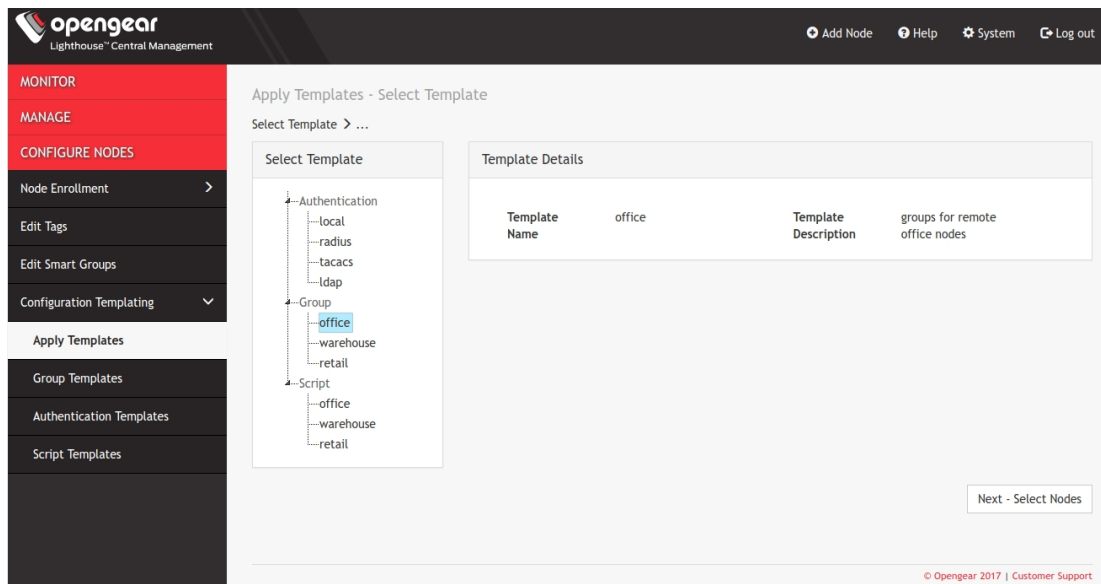
03. Preflight.

04. Execution.

'Preflight' is a test run, simulating what happens if the template is pushed to the selected nodes.

To apply a template:

01. Select **Configure Nodes > Configuration Templating > Apply Templates**.

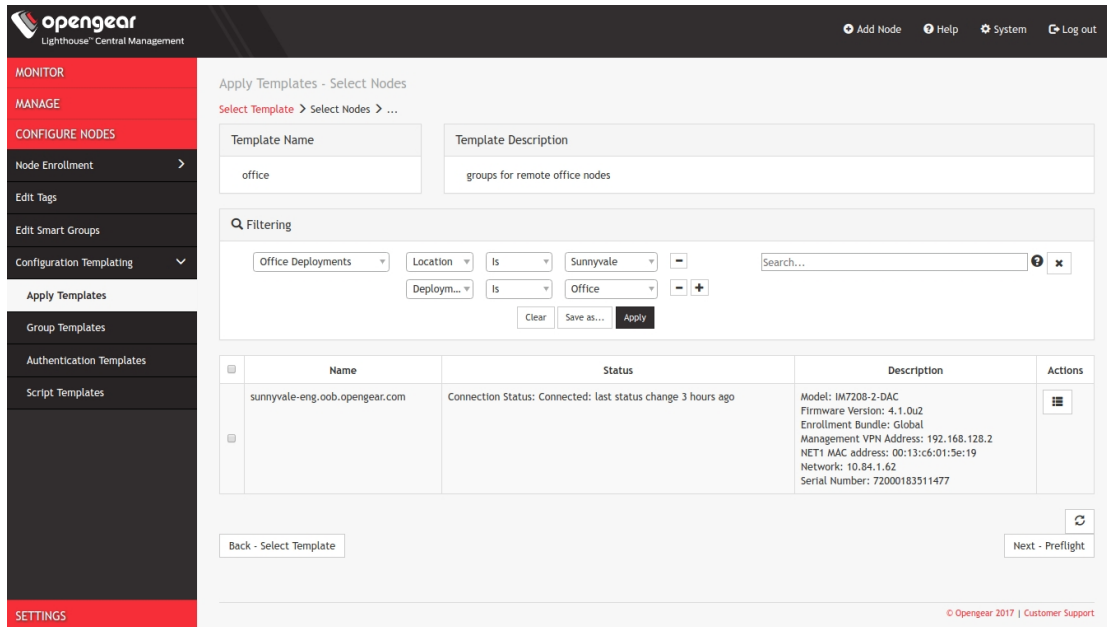


01. Select a template from the existing template tree.

Template Details populates with details from the selected template.

01. Click the **Next — Select Nodes** button.

The **Select Nodes** stage loads.



01. Select nodes from the list of enrolled nodes.

The screenshot above shows filtering being used to set the list of enrolled nodes to match (or closely match) the set of nodes an administrator wishes to deal with.

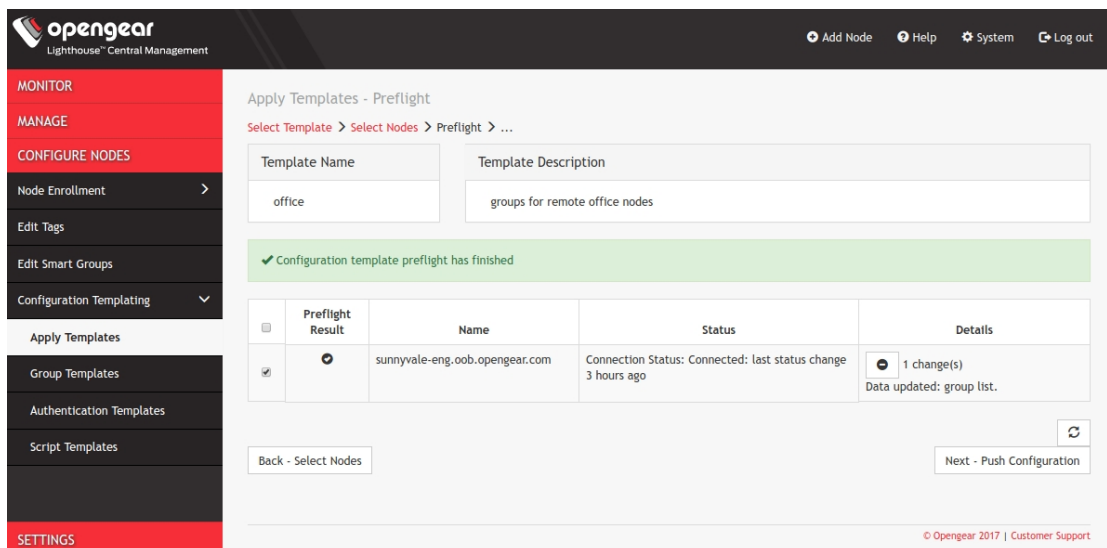
Third party nodes are not supported for template execution.

01. Click the **Next – Preflight** button.

02. The **Preflight** stage loads.

This stage requires manual refresh to retrieve updated **Preflight Result** and **Details**.

After all nodes finish preflight, a success message appears and the **Next – Push Configuration** button becomes active.



01. Select desired nodes for template execution and click the **Next – Push Configuration** button.

The **Configuration Status** stage loads.

This stage requires manual refresh to retrieve updated **Push Result** and **Details**.

After all nodes finish the template push a success message appears.

- MONITOR
- MANAGE
- CONFIGURE NODES
 - Node Enrollment >
 - Edit Tags
 - Edit Smart Groups
 - Configuration Templating ▾
 - Apply Templates
 - Group Templates
 - Authentication Templates
 - Script Templates
- SETTINGS

Apply Templates - Configuration Status

Select Template > Select Nodes > Preflight > Configuration Status

Template Name	Template Description
office	groups for remote office nodes

✔ Configuration template push has finished

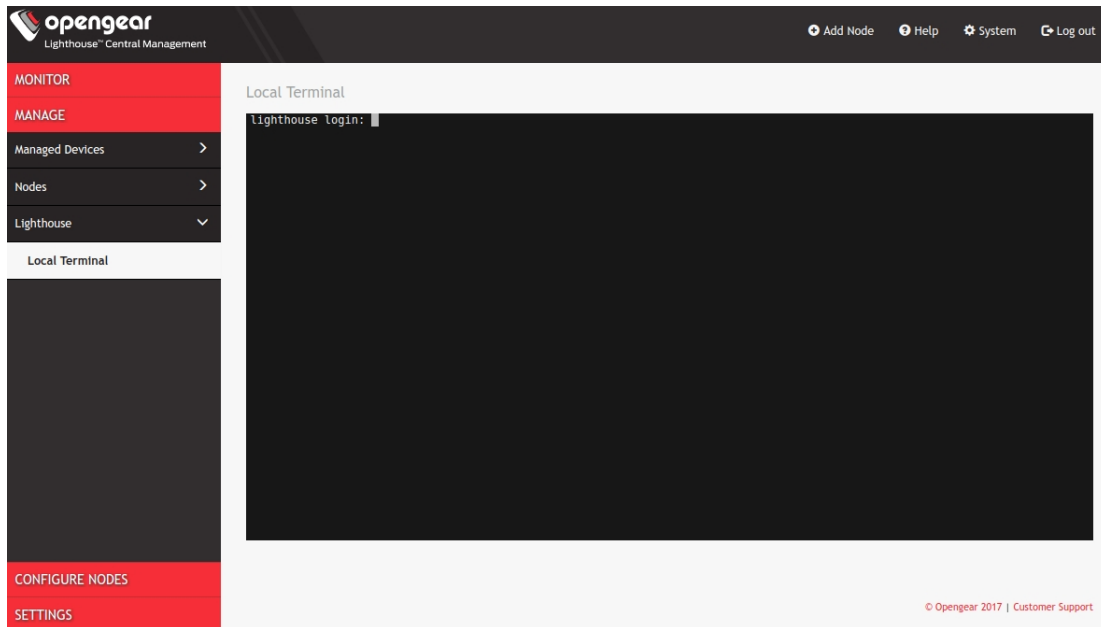
Push Result	Name	Status	Details
✔	sunnyvale-eng.oob.opengear.com	Connection Status: Connected: last status change 3 hours ago Configuration Template Run Status: Success	1 change(s) Data updated: group list.



10. Command line tools

Lighthouse 5.1.0 or later includes a web-based terminal. To access this bash shell instance:

01. Select **Manage > Lighthouse > Local Terminal**.



At the presented login prompt:

01. Enter an administrator's username and press Return.

A Password: prompt appears.

01. Enter the administrator's password and press Return.

A bash shell prompt appears.

This shell supports most standard bash commands and also supports copy-and-paste to and from the terminal.

There are also Lighthouse-specific shell-based tools available, including:

10.1 node-command

The `node-command` tool is used to run commands on managed console servers, allowing administrators to easily run a single CLI command in bulk, on all or on a range of their console server deployment.

Note: to run `node` commands, you must be authorized as an admin group user.

To get started with any of the `node` tools, you can get quick information on how to use it from the command line:

```
node-command --help
```

To see a list of all the registered console servers that the tool can operate on:

```
node-command --list-nodes
```

10.1.1 Example `node-command` Output

```
== node-command ID 2017-05-19T14:08:33.360164_29534 ==
14:08:33 [SUCCESS] BNE-R01-ACM7004-5 192.168.128.2:22
OpenGear/ACM7004-5 Lighthouse 3b90d826 -- Tue May 9 13:42:16 EST 2017

14:08:33 [SUCCESS] BNE-R02-IM7216 192.168.128.3:22
OpenGear/IM72xx Lighthouse 3b90d826 -- Tue Jul 5 13:42:16 EST 2017
```

10.2 node-info

`node-info` is a shell-based tool for pulling more detailed information from *console servers*.

10.2.1 Example `node-info` output

```
$ node-info -A
BNE-R01-ACM7004-5
  address: 192.168.128.2
  id: nodes-1
  ssh port: 22
```

```

description: Brisbane Rack 1
enrollment status: Enrolled
connection status: Connected
BNE-R02-IM7216
address: 192.168.128.3
id: nodes-2
ssh port: 22
description: Brisbane Rack 2
enrollment status: Enrolled
connection status: Connected

```

10.3 node-upgrade

`node-upgrade` is a tool for running bulk firmware upgrades on managed *console servers*.

By passing in required information — such as the firmware version to upgrade to, the location of the firmware image to upgrade with, and the nodes to upgrade — via appropriate flags, `node-upgrade` can upgrade the firmware on multiple *console servers* and report results back to STD OUT with a single command.

`node-upgrade` accepts twelve flags as follows:

<code>-h --help</code>	Display this message
<code>-q --quiet</code>	Suppress command output
<code>-b --batch</code>	Suppress node-command output
<code>-l --list-nodes</code>	List all nodes matching query, or all nodes if none selected
<code>-i --node-id=ID</code>	Select node by config ID
<code>-n --node-name=name</code>	Select node by name
<code>-a --node-address=address</code>	Select node by VPN address
<code>-g --smartgroup=name</code>	Select nodes by the smart group they resolve to
<code>-A --all</code>	Select all available nodes
<code>-f --firmware-dir</code>	The directory of the firmware file(s).
<code>-v --version</code>	The firmware version to upgrade to.
<code>-z --ignore-version</code>	Ignore firmware version warnings for upgrade.

10.3.1 An example node-upgrade run

The following is an example `node-upgrade` command. It sets `/mnt/nvram/` as the directory `node-upgrade` looks to for the firmware image used as the source for all the firmware upgrade attempts. Every *console server* being managed from the active Lighthouse instance is targeted for an upgrade and the target *console servers* are set to upgrade to firmware 4.0.0.

```
# node-upgrade -A -f /mnt/nvram -v 4.1.0
```

When run, `node-upgrade` returns information to STD OUT, such as the following:

```

Upgrading firmware for device family: ACM550X
Upgrading firmware for device family: CM71XX
Upgrading firmware for device family: CM7196
Upgrading firmware for device family: ACM7004-5
Upgrading firmware for device family: IM72XX
im7208: flashing firmware file: im72xx-4.1.0.flash
[FAILURE] acm5508: not upgraded to OpenGear/ACM5508-2 version 4.1.0.
Reason for failure: No firmware available for ACM550X device family.
[FAILURE] cm7148: not upgraded to OpenGear/CM7148-2-DAC version 4.1.0.
Reason for failure: netflash failed due to the same firmware currently
on the device.
[FAILURE] cm7196: not upgraded to OpenGear/CM7196A-2-DAC version
4.1.0. Reason for failure: netflash failed due to the same firmware
currently on the device.
[FAILURE] acm7004: not upgraded to OpenGear/ACM7004-5-LMR version
4.1.0. Reason for failure: netflash failed due to the same firmware
currently on the device.
[SUCCESS] im7208: upgraded to OpenGear/IM7208-2-DAC-LR version 4.1.0.

```

`node-upgrade` also returns status codes 0 (success) or 1 (failure) when particular conditions are met.

Exit code 0 (success) is returned under the following conditions:

- 01.Success
- 02.Successful upgrade of all nodes.
- 03.No nodes selected for upgrade.
- 04.No firmware found in nominated directory.

Exit code 1 (failure) is returned under the following conditions:

- 01.Missing or invalid command line options.
- 02.The current user is not authorized to execute commands on a node.
- 03.The specified firmware directory was invalid (ie it does not exist or is not readable).

04.At least one node upgrade failed.

10.4 ogadduser

ogadduser is a shell-based tool for creating users.

Basic ogadduser usage syntax is as follows:

```
$ ogadduser -u testuser -p mypassword -g admin
```

10.5 ogconfig-cli

ogconfig-cli allows users to inspect and modify the configuration tree from the command line. It is inherently transactional in nature, allowing users to ensure their configuration is correct before pushing it to the configuration server.

From a command line, as the root user, you can start the tool with:

```
ogconfig-cli
```

10.5.1 Commands to try from within the ogconfig-cli tool

```
01.help
02.get
03.print . 2
04.print users[0].username
```

10.5.2 Changing a configuration from within ogconfig-cli

From inside ogconfig-cli:

```
ogcfg> set system.hostname "opengear-lighthouse-new"
ogcfg> push
ogcfg> quit
```

To see that the change has taken effect:

```
$ cat /etc/hostname
```

A configuration change doesn't take effect until it is pushed to the configuration server. For example, from inside ogconfig-cli:

```
ogcfg> set system.hostname "opengear-lighthouse-new-again"
ogcfg> print system.hostname
ogcfg> quit
```

To see that the change did not take effect:

```
$ cat /etc/hostname
```

10.5.3 Configuration validation from within ogconfig-cli

Configuration is internally validated before being applied, so that an incorrect configuration cannot be accidentally set. For example, from inside ogconfig-cli, setting an invalid ethernet link speed is rejected:

```
ogcfg> set system.net.physifs[0].ethernet.link_speed "1GB"
ogcfg> push
Commit failed
  Messages:   String is not in the list of allowed values
             Push command failed
```

```
ogcfg> quit
```

10.6 oglicdump

oglicdump is a shell-based tool for displaying and saving the current third-party licensing status of a Lighthouse instance.

When used without a switch, oglicdump writes the current status to STD OUT.

To write this status out to a file, or in machine readable form, or as a raw license container string, or to write out a sub-set of the licensing information (such as licenses for a given SKU), use one of the switches oglicdump supports:

```
-h           Displays this help.
-v           Display version information
-o <file>   File to write out to. Default is stdout.
```

```

-s <SKU>          Specific SKU code to dump out. Default is all SKU codes.
-f <feature>     Specific feature value to dump out. This is only valid in conjunction with -s.
-c              Output contacts only. This is only valid in conjunction with -s.
-m              Output machine readable, as in compact formatted, not pretty
-r              Output the raw license container strings from config.

```

10.7 cron

Cron service can be used for a scheduled cron jobs runs. Daemon can be managed via the `/etc/init.d/crond` interface, and cron tables managed via `crontab`. `Crontab` supports:

Usage:

```

crontab [options] file
crontab [options]
crontab -n [hostname]

```

Options:

```

-u <user>   define user
-e          edit user's crontab
-l          list user's crontab
-r          delete user's crontab
-i          prompt before deleting
-n <host>   set host in cluster to run users' crontabs
-c          get host in cluster to run users' crontabs
-x <mask>   enable debugging

```

To perform start / stop / restart on `crond` service:

```
/etc/init.d/crond start
```

Note: `crond` doesn't need to be restarted when `crontab` file is modified, it will examine the modification time on all `crontabs` and reload those which have changed.

To verify the current `crond` status:

```
/etc/init.d/crond status
```

To check current cron jobs running with the following command to list all `crontabs`:

```
crontab -l
```

To edit or create a custom `crontab` file:

```
crontab -e
```

This will open a personal cron configuration file. Each line can be defined as one command to run. The following format is used:

```
minute hour day-of-month month day-of-week command
```

For example, append the following entry to run a script every day at 3am:

```
0 3 * * * /etc/config/backup.sh
```

Save and close the file.

10.8 sysflash

`sysflash` is the shell-based tool for upgrading a Lighthouse instance's system.

Basic `sysflash` syntax is as follows:

```
# sysflash [flags] [path/to/system-image.lg_upg | Percent-encoded URL to firmware-image.lg_upg]
```

Image filenames cannot include spaces. And, as the syntax example above notes, URLs must be Percent-encoded.

`sysflash` includes eight flags which modify the standard upgrade behaviour as well as the `-h` or `--help` flag, which returns all the available flags and their affects:

```

-b, --board-name <name>      Override board name (currently lighthouse-vm)
-B, --board-revision <version> Override board revision (currently 1.0)
-V, --vendor <vendor>       Override vendor (currently opengear)
-I, --no-version-check      Do not check software version for upgradability
-m, --no-migration          Do not migrate current config. Start fresh.
-v, --verbose                Increase verbosity (may repeat)
-o, --no-boot-once          Do not modify bootloader (implies --no-reboot)
-r, --no-reboot              Do not reboot after upgrading
-h, --help                  Print this help

```

10.9 Selecting nodes using shell-based tools

There are a number of ways to select nodes (also known as *console servers*) as targets on which to run a command. These can be used multiple times, or together, to select a range of console servers:

Select individually by name, address, Lighthouse VPN address, config index or smart group (as per `--list-nodes` output):

```
node-command --node-name BNE-R01-IM4248
node-command --node-address 192.168.0.33
node-command --node-index nodes-1
node-command --smartgroup="model-acm"
```

10.9.1 Select all nodes

```
node-command --all
```

10.9.2 Running commands on selected nodes

Once nodes are selected, the commands to be run for each can be given. These are run on each managed node, in parallel. Any command you can run from a node shell can be run on each managed node.

Note: all commands are run as root.

For example, to check the version on two specific, configured nodes, selecting one by name and the other by index, run the following command:

```
node-command --node-name BNE-R01-ACM7004-5 --node-index nodes-2 cat /etc/version
```

Note: when using non-trivial selection arguments, check which target nodes have been selected on your initial command pass by using the `--list-nodes` switch rather than the final command.

11. System upgrades

A Lighthouse appliance's system can be upgraded using a .lh_upg image file.

Note: The filename suffix .lh_upg is required.

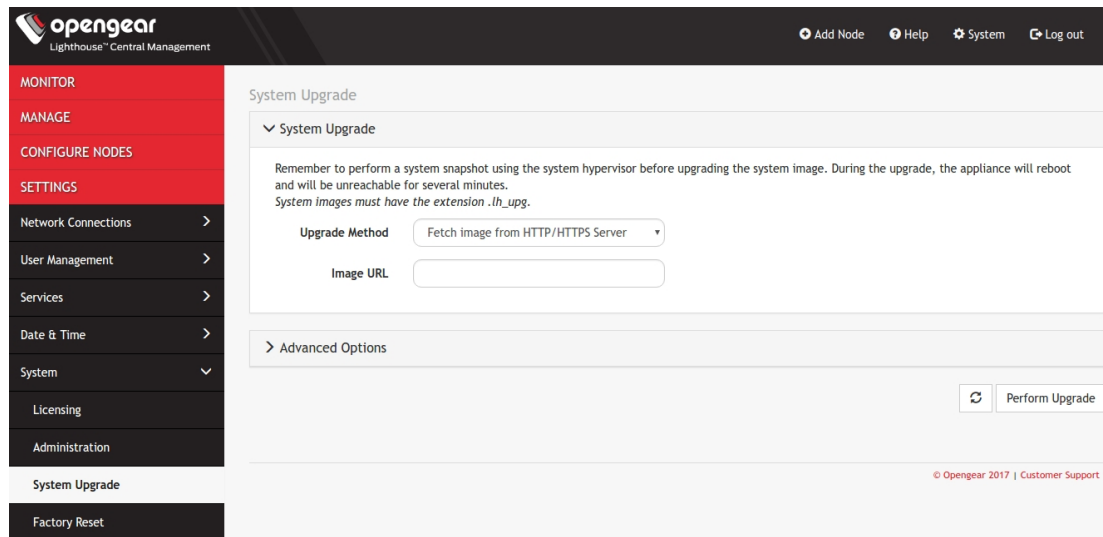
However a system upgrade is carried out, once the upgrade is complete, the Lighthouse instance reboots. It will be unavailable during the reboot process.

11.1 Upgrading the system from within Lighthouse

To upgrade a Lighthouse instance's system using the Lighthouse UI:

01. Select **Settings > System > System Upgrade**.

02. Select the **Upgrade Method** (either *Fetch image from HTTP/HTTPS Server* or *Upload Image*).



If upgrading via *Fetch image from HTTP/HTTPS Server*:

01. Enter the URL for the system image in the **Image URL** text-entry field.

02. Click the **Perform Upgrade** button.

If upgrading via *Upload Image*:

01. Click the **Choose file** button.

02. Navigate to the directory containing the *system-upgrade-image.lh_upg* file.

03. Select the *system-upgrade-image.lh_upg* file and press **Return**.

04. Click the **Perform Upgrade** button.

Note: The **Advanced Options** section, which expands to present an **Upgrade Options** text-entry field, should only be used if a system upgrade is being performed as part of an Opengear Support call. If a specific option is required, the Opengear Support technician will specify it.

Once the upgrade has started, the System Upgrade page displays feedback as to the state of the process.

A system upgrade attempt will return the error *System version was not higher than the current version* if the selected image file is not, in fact, a more recent version than that already installed.

11.2 Upgrading the Lighthouse system via the Local Terminal

Lighthouse includes a shell-based tool — `sysflash` — that allows a user with administrative privileges to upgrade the instance's system from the Local Terminal.

To upgrade Lighthouse instance's system using the Lighthouse Local Terminal:

01. Select **Manage > Lighthouse > Local Terminal**.

02. At the `[hostname] login:` prompt, enter an administrator username and press **Return**.

03. At the `Password:` prompt, enter the administrator's password and press **Return**.

To use `sysflash` in conjunction with a .lh_upg file available via an HTTP or HTTPS server:

01. At the Local Terminal bash shell prompt enter:

```
sysflash http[s]://%3A%2Fdomain.tld%2Fpath%2Fto%2Ffirmware-upgrade-image.lh_upg
```

02. Press **Return**.

Note: as shown in the example URL above, URLs passed to `sysflash` **must** be Percent-encoded (also known as URL encoded).

To use `sysflash` in conjunction with a `.lh_upg` file available via the local file system:

01.At the Local Terminal bash shell prompt enter:

```
sysflash /path/to/system-upgrade-image.lh_upg.
```

02.Press **Return**.

`sysflash` also includes several flags that allow for variations in the standard system upgrade process. For the most part, these flags should not be used unless directed to do so by Opendgear Support.

All nine flags are listed by running either of the following at a Local Terminal bash shell prompt:

01.`sysflash -h` or

02.`sysflash --help`

The same listing is presented in the `sysflash` entry of the Command line tools chapter above.

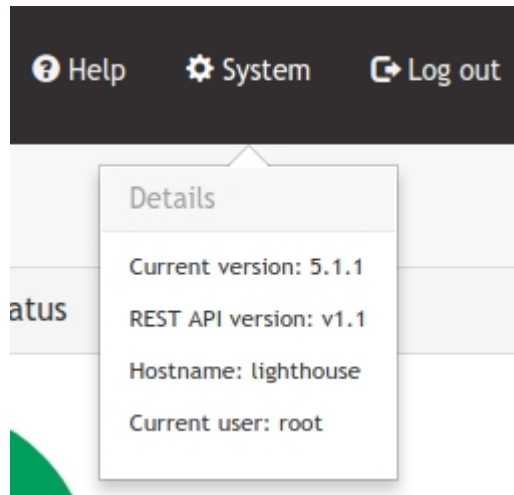
12. Troubleshooting

12.1 Establishing the current Lighthouse instance version

12.1.1 using the web UI

01.click **System** on the top right of the Lighthouse instance's web UI.

02.The *Details* menu appears, listing the Lighthouse instance's **Current version**, **REST API version**, **Hostname**, and **Current user**.



12.1.2 via the local Lighthouse shell

01.Click **Manage > Lighthouse > Local Terminal**

02.At the [hostname] login: prompt, enter an administrator username and press **Return**.

03.At the Password: prompt, enter the administrator's password and press **Return**.

04.At the bash shell prompt, enter `cat /etc/version` and press **Return**.

05.The current Lighthouse instance's version is returned to STD OUT. For example:

```
[administrator-username]@[hostname]:~# cat /etc/version
5.1.1
```

Note: the procedure above uses the Web UI to reach the Lighthouse Local Terminal. This is not the only way to reach the Lighthouse shell and `cat /etc/version` works in any circumstance where an administrator has access to the Lighthouse shell. For example, many of the Virtual Machine Manager applications that can run a Lighthouse instance offer virtual console access. If this is available and an administrator logs in to the Lighthouse shell via this console, the command string will work as expected.

12.1.3 Other information sources related to a Lighthouse instance's version

Two other command strings can be useful when specifics about a particular Lighthouse instance are needed.

Both these commands can be run by an administrator with access to a running Lighthouse instance's bash shell.

First is `cat /etc/sw*`. This command concatenates the following four files to STD OUT:

```
/etc/sw_product
/etc/sw_variant
/etc/sw_vendor
/etc/sw_version
```

For example:

```
# cat /etc/sw*
ironman
release
opengear
5.1.1
```

Second is `cat /etc/issue`. `/etc/issue` is a standard *nix text file which, by default, contains system information for presenting before the system's login prompt. On a Lighthouse instance, `/etc/issue` contains the vendor, and the Ironman/Lighthouse version

```
# cat /etc/issue
Opengear Ironman 5.1.1 \n \l
```

12.2 Technical support reports

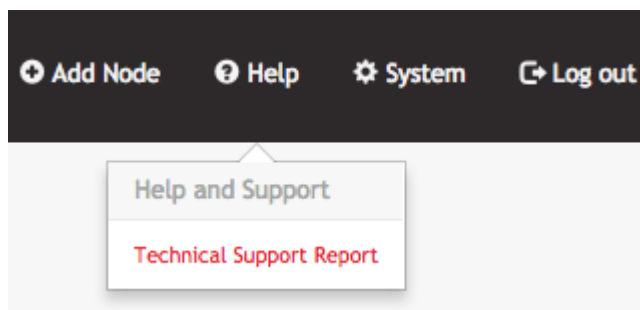
Lighthouse 5.1.0 or later can generate a technical support report that includes Lighthouse configuration information and the current system log for the Lighthouse VM.

If you contact Opengear Technical Support, the support technician may ask for this report.

12.2.1 Generate a support report via the Lighthouse interface

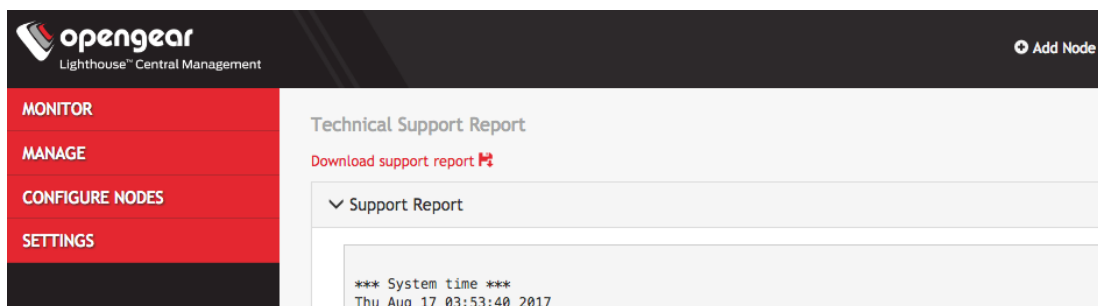
To generate a complete configuration and status report regarding a given *Opengear Lighthouse 5.1.0 VM* or later:

01. Select **Help > Technical Support Report**.



Note: Lighthouse generates this support report on demand and the report includes the current system log. This process can take several minutes.

01. Click **Download support report**.



This downloads a PKZip archive to your local system. The archive's filename is structured as follows:

```
support-[host-name]-[iso-8601-order-date-and-time-stamp].zip
```

It contains two files:

`system.txt` – the configuration information also presented in the **Technical Support Report** window.

`messages` – the current *Opengear Lighthouse 5.1.0 VM* or later system log.

The two files are also presented in the *Support Report* text box below the **Download support report** link. Because the report includes the current system log, this will almost certainly be a long but scrollable presentation. This presentation is, however, searchable using your web browser's built-in search function.

12.2.2 Generate a support report via the local terminal

To generate a complete configuration and status report regarding a given *Opengear Lighthouse 5.1.1 VM* or later:

01. Select **Manage > Lighthouse > Local Terminal**.

02. At the `[hostname] login:` prompt, enter an administrator username and press **Return**.

03. At the `Password:` prompt, enter the administrator's password and press **Return**.

04. At the bash shell prompt, enter

```
support-report -z > /tmp/support.zip
```

and press **Return**

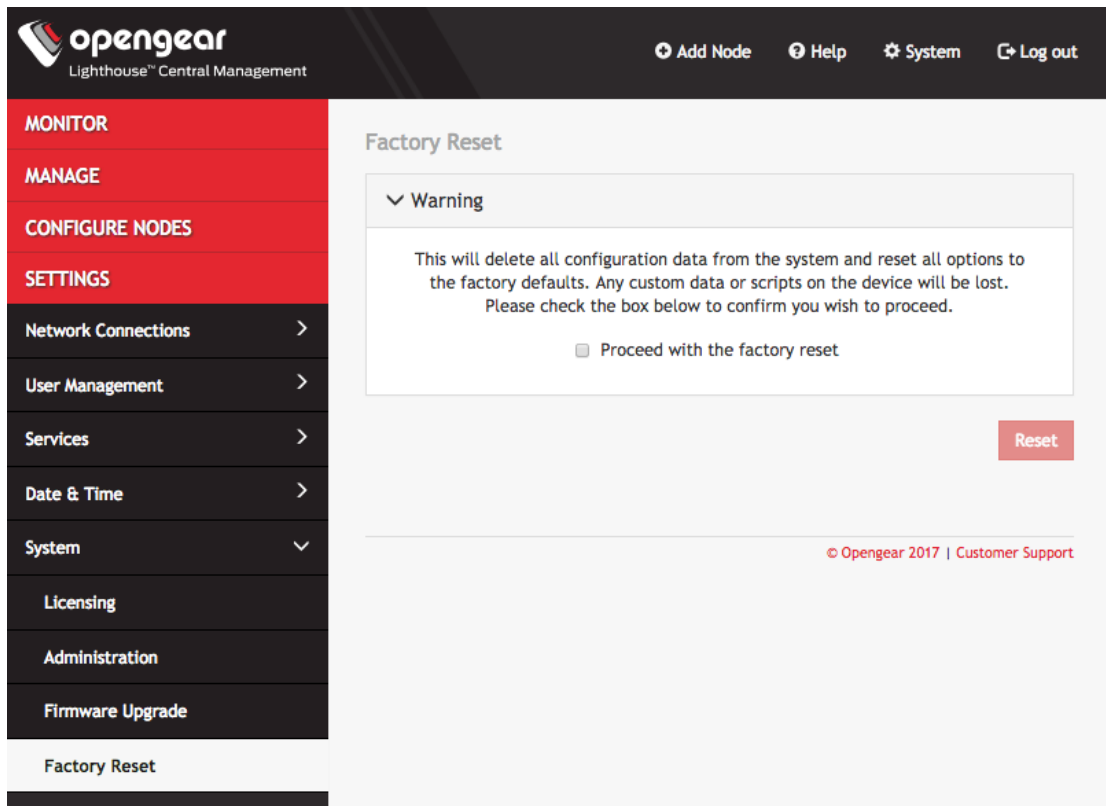
Note: this is the recommended way of running the `support-report` command. The `-z` switch generates the same combined file as produced by the **Download support report** link noted in the Lighthouse UI-specific procedure above. And the redirect saves this generated PKZip file to `/tmp/support.zip` for retrieval at your convenience.

12.3 Returning an Opengear Lighthouse instance to factory settings

To return an enrolled console server to its factory settings using *Opengear Lighthouse 5.1.0* or later:

01. Login to the *Opengear Lighthouse 5.1.0* or later web-based interface as `root`.

02. Select **Settings > System > Factory Reset**.



01. Check the *Proceed with the factory reset* checkbox.

02. Click the **Reset** button.

You must login as `root` for this to work. Other users, even those with full administrative privileges, do not have the permissions required to reset an *Opengear Lighthouse 5.1.0 VM* or later to its factory settings.

Alternatively, the following script, run from a shell, performs a full factory reset:

```
/usr/bin/factory_reset
```

As with the Lighthouse-based procedure, only `root` can run this script. And, again as with the Lighthouse-based procedure, the script prompts for confirmation before performing the factory reset.

This procedure, and the shell script, are equivalent to logging in to console server's web-based management interface (see 'Connecting to a console server's web-management interface' above) and doing the following:

01. Select **Administration**

02. Check the *Config Erase* checkbox.

03. Click **Apply**.

Note: returning a console server to its factory settings in this fashion does **not** un-enroll said server from the *Opengear Lighthouse 5.1.0 VM* or later.

13. Technical support

Purchaser is entitled to twelve (12) months free telephone support and free e-mail support (worldwide) from date of purchase provided that the Purchaser first register their product(s) with Opengear by filling in the on-line form <http://opengear.com/registration.html>.

Direct telephone, help-desk and e-mail support is available from 09:00 to 20:00, US Eastern Time (UTC -5 or UTC -4). Other support options are at <http://opengear.com/support.html>.

Opengear's standard warranty includes free access to Opengear's [Knowledge Base](#) as well as any application notes, white papers and other on-line resources that may become available from time to time.

Opengear reserves the right to stop support for products no longer covered by warranty.

14. End-user license agreements

14.1 Opendgear end-user license agreement

READ BEFORE USING THE ACCOMPANYING SOFTWARE

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING SOFTWARE, THE USE OF WHICH IS LICENSED FOR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE. IF YOU USE ANY PART OF THE SOFTWARE, SUCH USE WILL INDICATE THAT YOU ACCEPT THESE TERMS.

You have acquired a product that includes Opendgear (“Opendgear”) proprietary software and/or proprietary software licensed to Opendgear. This Opendgear End User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and Opendgear for the installed software product of Opendgear origin, as well as associated media, printed materials, and “online” or electronic documentation (“Software”). By installing, copying, downloading, accessing, or otherwise using the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Opendgear is not willing to license the Software to you. In such event, do not use or install the Software. If you have purchased the Software, promptly return the Software and all accompanying materials with proof of purchase for a refund.

Products with separate end user license agreements that may be provided along with the Software are licensed to you under the terms of those separate end user license agreements.

LICENSE GRANT. Subject to the terms and conditions of this EULA, Opendgear grants you a nonexclusive right and license to install and use the Software on a single CPU, provided that, (1) you may not rent, lease, sell, sublicense or lend the Software; (2) you may not reverse engineer, decompile, disassemble or modify the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; and (3) you may not transfer rights under this EULA unless such transfer is part of a permanent sale or transfer of the Product, you transfer at the same time all copies of the Software to the same party or destroy such materials not transferred, and the recipient agrees to this EULA.

No license is granted in any of the Software's proprietary source code. This license does not grant you any rights to patents, copyright, trade secrets, trademarks or any other rights with respect to the Software.

You may make a reasonable number of copies of the electronic documentation accompanying the Software for each Software license you acquire, provided that, you must reproduce and include all copyright notices and any other proprietary rights notices appearing on the electronic documentation. Opendgear reserves all rights not expressly granted herein.

INTELLECTUAL PROPERTY RIGHTS. The Software is protected by copyright laws, international copyright treaties, and other intellectual property laws and treaties. Opendgear and its suppliers retain all ownership of, and intellectual property rights in (including copyright), the Software components and all copies thereof, provided however, that (1) certain components of the Software, including SDT Connector, are components licensed under the GNU General Public License Version 2, which Opendgear supports, and (2) the SDT Connector includes code from JSch, a pure Java implementation of SSH2 which is licensed under BSD style license. Copies of these licenses are detailed below and Opendgear will provide source code for any of the components of the Software licensed under the GNU General Public License upon request.

EXPORT RESTRICTIONS. You agree that you will not export or re-export the Software, any part thereof, or any process or service that is the direct product of the Software in violation of any applicable laws or regulations of the United States or the country in which you obtained them.

U.S. GOVERNMENT RESTRICTED RIGHTS. The Software and related documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights at 48 C.F.R. 52.227-19, as applicable, or any successor regulations.

TERM AND TERMINATION. This EULA is effective until terminated. The EULA terminates immediately if you fail to comply with any term or condition. In such an event, you must destroy all copies of the Software. You may also terminate this EULA at any time by destroying the Software.

GOVERNING LAW AND ATTORNEY'S FEES. This EULA is governed by the laws of the State of Utah, USA, excluding its conflict of law rules. You agree that the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety and does not apply to this EULA. If you acquired this Software in a country outside of the United States, that country's laws may apply. In any action or suit to enforce any right or remedy under this EULA or to interpret any provision of this EULA, the prevailing party will be entitled to recover its costs, including reasonable attorneys' fees.

ENTIRE AGREEMENT. This EULA constitutes the entire agreement between you and Opendgear with respect to the Software, and supersedes all other agreements or representations, whether written or oral. The terms of this EULA can only be modified by express written consent of both parties. If any part of this EULA is held to be unenforceable as written, it will be enforced to the maximum extent allowed by applicable law, and will not affect the enforceability of any other part.

Should you have any questions concerning this EULA, or if you desire to contact Opendgear for any reason, please contact the Opendgear representative serving your company.

THE FOLLOWING DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY IS INCORPORATED INTO THIS EULA BY REFERENCE. THE SOFTWARE IS NOT FAULT TOLERANT. YOU HAVE INDEPENDENTLY DETERMINED HOW TO USE THE SOFTWARE IN THE DEVICE, AND OPENGear HAS RELIED UPON YOU TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.

LIMITED WARRANTY Opengear warrants the media containing the Software for a period of ninety (90) days from the date of original purchase from Opengear or its authorized retailer. Proof of date of purchase will be required. Any updates to the Software provided by Opengear (which may be provided by Opengear at its sole discretion) shall be governed by the terms of this EULA. In the event the product fails to perform as warranted, Opengear's sole obligation shall be, at Opengear's discretion, to refund the purchase price paid by you for the Software on the defective media, or to replace the Software on new media. Opengear makes no warranty or representation that its Software will meet your requirements, will work in combination with any hardware or application software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the Software will be corrected.

OPENGear DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OTHER THAN AS STATED HEREIN, THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. ALSO, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT. IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR THE SOFTWARE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, OPENGear.

NO LIABILITY FOR CERTAIN DAMAGES. EXCEPT AS PROHIBITED BY LAW, OPENGear SHALL HAVE NO LIABILITY FOR COSTS, LOSS, DAMAGES OR LOST OPPORTUNITY OF ANY TYPE WHATSOEVER, INCLUDING BUT NOT LIMITED TO, LOST OR ANTICIPATED PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, EXEMPLARY SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE ARISING FROM OR IN CONNECTION WITH THIS EULA OR THE USE OR PERFORMANCE OF THE SOFTWARE. IN NO EVENT SHALL OPENGear BE LIABLE FOR ANY AMOUNT IN EXCESS OF THE LICENSE FEE PAID TO OPENGear UNDER THIS EULA. SOME STATES AND COUNTRIES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

14.2 GNU general public license (GPL), version 2

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how

to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- 9.If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 10.The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

- 11.If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 1.BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 2.IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

one line to give the program's name and a brief idea of what it does.

Copyright © year name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright © year name of author Gnomovision
comes with ABSOLUTELY NO WARRANTY; for details
type 'show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type 'show c'
for details.
```

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest
in the program ‘Gnomovision’
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU [Lesser General Public License](#) instead of this License.

15. Service

15.1 Standard warranty

Opengear, Inc., its parent, affiliates and subsidiaries, (collectively, "Opengear") warrant your Opengear product to be in good working order and to be free from defects in workmanship and material (except in those cases where the materials are supplied by the Purchaser) under normal and proper use and service for the period of four (4) years from the date of original purchase from an Authorized Opengear reseller. In the event that this product fails to meet this warranty within the applicable warranty period, and provided that Opengear confirms the specified defects, Purchaser's sole remedy is to have Opengear, in Opengear's sole discretion, repair or replace such product at the place of manufacture, at no additional charge other than the cost of freight of the defective product to and from the Purchaser. Repair parts and replacement products will be provided on an exchange basis and will be either new or reconditioned. Opengear will retain, as its property, all replaced parts and products. Notwithstanding the foregoing, this hardware warranty does not include service to replace or repair damage to the product resulting from accident, disaster, abuse, misuse, electrical stress, negligence, any non-Opengear modification of the product except as provided or explicitly recommended by Opengear, or other cause not arising out of defects in material or workmanship. This hardware warranty also does not include service to replace or repair damage to the product if the serial number or seal or any part thereof has been altered, defaced or removed. If Opengear does not find the product to be defective, the Purchaser will be invoiced for said inspection and testing at Opengear's then current rates, regardless of whether the product is under warranty.