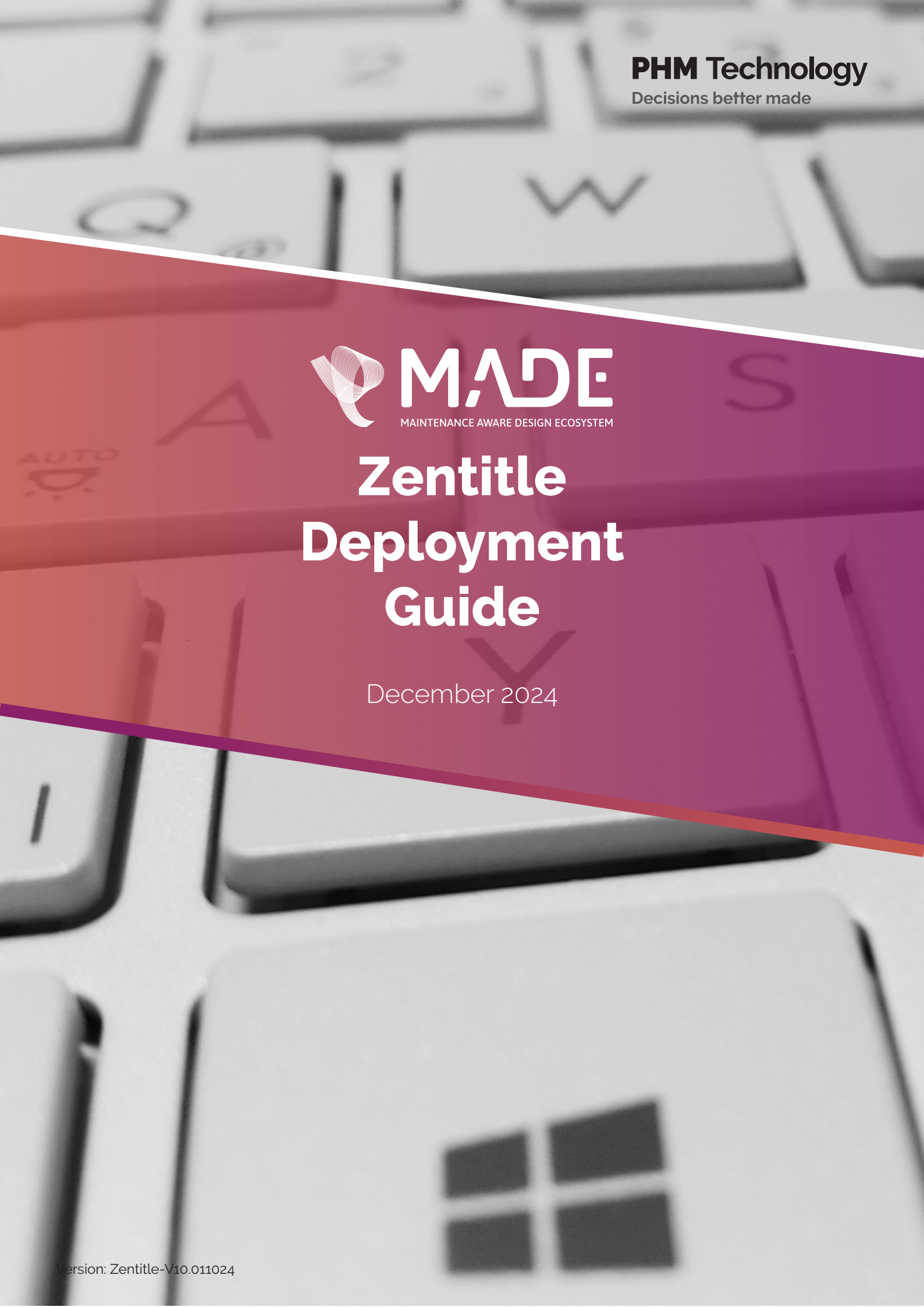
PHM Technology
Decisions better made



MADE
MAINTENANCE AWARE DESIGN ECOSYSTEM

Zentitle Deployment Guide

December 2024

Version: Zentitle-V10.011024

Contents Page

1. Introduction

PHM Technology (PHMT) uses Zentitle, a licensing management service provided by Nalperion (https://www.nalpeiron.com/software-licensing.html), to license its software suite. The Zentitle licensing utilizes a license code which is configured and managed on the cloud by PHMT.

The default Zentitle licensing is a cloud-based activation service – this means that a persistent internet connection is required to activate and use the license. There are periodic heart-beat license checks to maintain usage of the license.
Licenses issued by PHMT are either Node-locked or Network licenses. The license term offered are:

- **Subscription**
- **Perpetual**

Node-locked licenses will be tied to a single computer at any given time and will have access to all modules the license contains. The license code can be shared with other users; however, the license code will need to be returned to the Nalperion Zentitle server first.

Network licenses are installed on a network location (cloud or local), where multiple computers can install the license code. If a license seat is available, users will be able to access the software.

Offline activations for dark environments via Relay Servers and a Local Daemon Server are also supported, for this installation configuration, please contact support@phmtechnology.com.

2. Pre-requisites

The following section outlines the minimum hardware and software requirements for the Nalperion Zentitle license installation.

2.1. Node-locked License

For node-locked licensing, the MADE software will be operating on the computer and this will serve as the minimum requirements as listed below:

- OS: Windows 8.1 (64-bit) or later
- CPU (Desktop): Intel Core i3-6100 or AMD Ryzen 3 1200 or better
- CPU (Laptop): Intel i7-6650U or better
- RAM: 4GB or more
- Disk Space: 50GB or more of available space
- Resolution: 1366x768 HD resolution or better

2.2. Cloud License

Cloud licenses can be deployed with different configurations; cloud, using a relay server, and using a local daemon server.

2.2.1. Cloud

A standard cloud license is used where end-user computers are on a local area network (LAN) and will have persistent internet connection. This enables multiple end-users to access the software from different computers, providing a license is active and available. Standard connections are MADE as an outgoing connection to IP 184.106.60.185 and 20.237.110.18 on ports HTTP/80 and HTTPS/443.

2.2.2. Zentitle Relay Server

Relay server is used where the end-user computers are on a local area network (LAN) and will not have access to the internet, however, the license server computer will have internet access to activate the license from the Zentitle server to hand over the relevant access controls to the end-user computers. Connections from the MADE software to the Relay server can be MADE on LAN ports 16700-16710, with the default configuration set to port 16701.. These ports can be changed if needed in the Relay server configuration. The Relay server will then make the external call to 184.106.60.185 and 20.237.110.18 on HTTP/80 and HTTPS/443.

2.2.3. Zentitle Local Daemon Server (Virtual Machine)

Local Daemon Server (Virtual Machine) is used where end-user computers are on a local area network (LAN) and will not have access to the internet. The Local Daemon Server can use an internet connection to the Zentitle Cloud service to activate the license (one off process for the duration of the license period) or can work totally offline where the license is activated manually (copy and paste of keys in the Local Daemon Server UI). From here, all licensing access is managed by the Local Daemon Server. The Local Daemon Server UI can also provide some basic information on license usage and connected MADE instances. For detailed instructions on this process see section B3. Licensing the Network Daemon.

For relay servers and the local daemon server, the minimum requirement are as follows:

- OS: CentOS 7, RHEL 7 or later
- Server: VMWare, RedHat KVM or equivalent
- CPU: 2x V-CPU or more
- RAM: 2GB or more VRAM
- Disk Space: 8GB or more of available space

2.3 Offline Activation

Offline Activation is used when an end-user computer running MADe cannot access the internet or is fully isolated, and the Zentitle Relay or Deamon Server can't be used. During the offline activation process, the end-user needs help from someone with internet access (such as an Administrator or ICT user) to obtain an Activation Certificate. Once MADe is activated, MADe can run in an offline environment.

3. How Nalperion Zentitle Licensing Works

The following section outlines the activation process using Nalperion Zentitle licensing.

3.1. Network

Activation of the MADE software by default is via the Zentitle Server on the cloud. A license code is entered into the software on each of the end-user computers upon opening the application for the first time. This enables access of MADE to be opened by multiple end-user computers connected to the cloud.

The computer will require a persistent internet connection which communicates with the Zentitle Servers to activate the license. This will initially check-out the license for an interval (default interval is 8 hours). After the check-out period has lapsed, the computer will communicate with the Zentitle Servers to ensure the license is still valid and check-out for another set interval.

If internet access is no longer available, the user will be prompted to take action. In the first instance, the user is allowed to get a temporary extension of the license (default period 10 minutes) which allows continuation of work. Once this temporary license extension of 10 minutes lapses, the user will only be allowed to refresh the lease or shutdown MADE. Upon selection of shutdown MADE, the user will still be prompted to save any work as required.

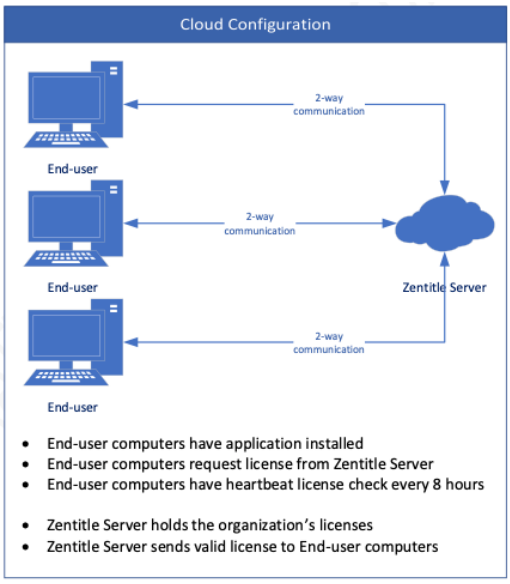


Figure 1: Cloud Configuration for Zentitle Licensing

3.2. Server activation

Offline activation via a Relay Server or Local Daemon Server is currently supported for network and node-locked licences. Offline activation for an isolated or occasionally connected computer is supported via Offline Activation for node-locked licences.

3.2.1. Relay Server

To configure the Relay Server, see **Appendix A**.

License checks are performed from the end-user computer to the Zentitle Server via the relay server. Upon loading the application, the end-user computer requests a license through the relay server which communicates to the Zentitle Cloud server and checks-out the license. A valid license is returned through the relay server which passes the access controls to the end-user. Similar to node-locked license behaviour, the license lease is checked every 8 hours through the Relay Server providing internet access is still available.

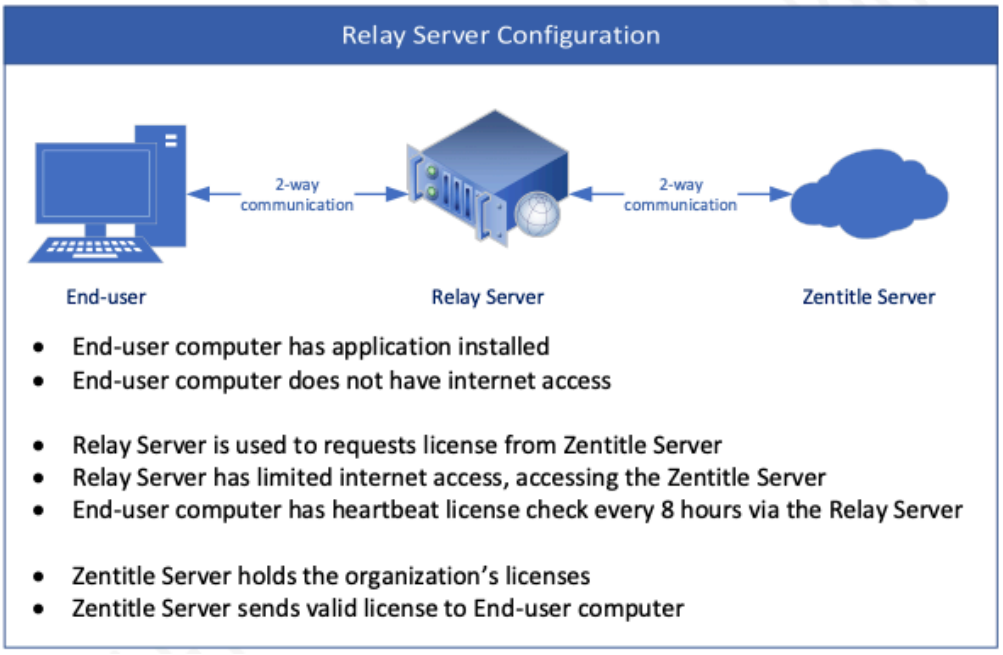


Figure 2: Relay Server Configuration for Zentitle Licensing

3.2.2. Local Daemon Server

To configure the Local Daemon Server, see **Appendix B**.

The Local Daemon Server can have limited or no connection to the Zentitle Server to obtain the license.

For Local Daemon Server installation regardless of connection to the Zentitle Server, a Master License code and activation process will be required to serve the Local Daemon Server. The Master License code is a code which is provided by PHMT; it is different to the product license code issued. The activation process can be conducted through the PHMT Offline License activation portal or online if the Local Daemon Server has access to the Zentitle Cloud service at the time of activation.

Where the connection to the Zentitle Server does not exist, additional steps are required to activate the license code. The license activation can also be conducted through the PHMT Offline activation portal.

In this configuration, the end-user computer will request a license from the Local Daemon Server to check-out the license. A valid license is returned to allow access for the end-user computer. License checks are performed by the end-user computer to the Local Daemon Server every 60 minutes. The local daemon server can only have one product license code. If adding an additional license, it will replace the existing activated license code.

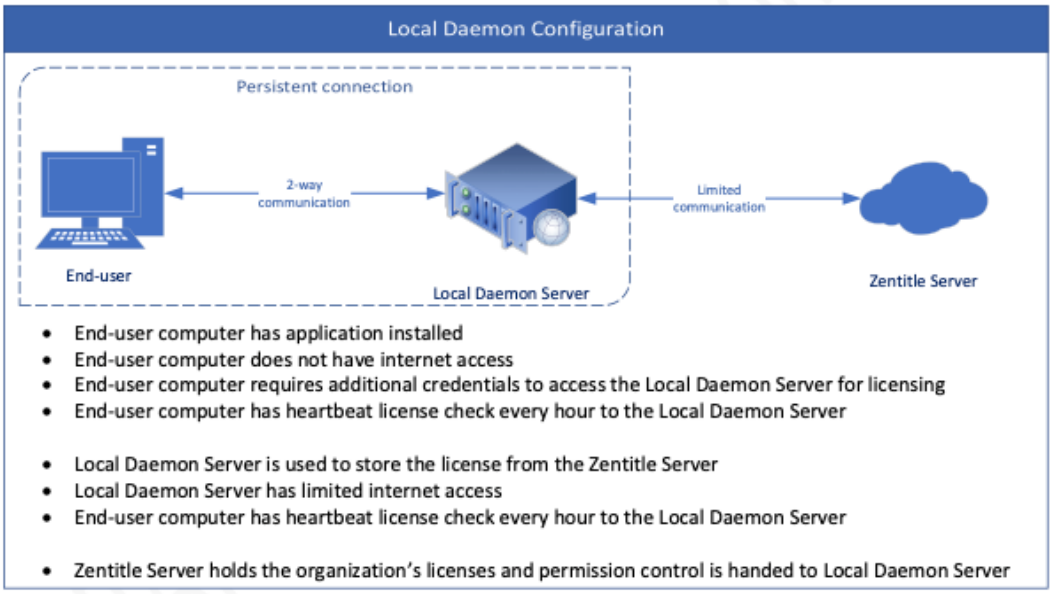


Figure 3: Local Daemon Configuration for Zentitle Licensing

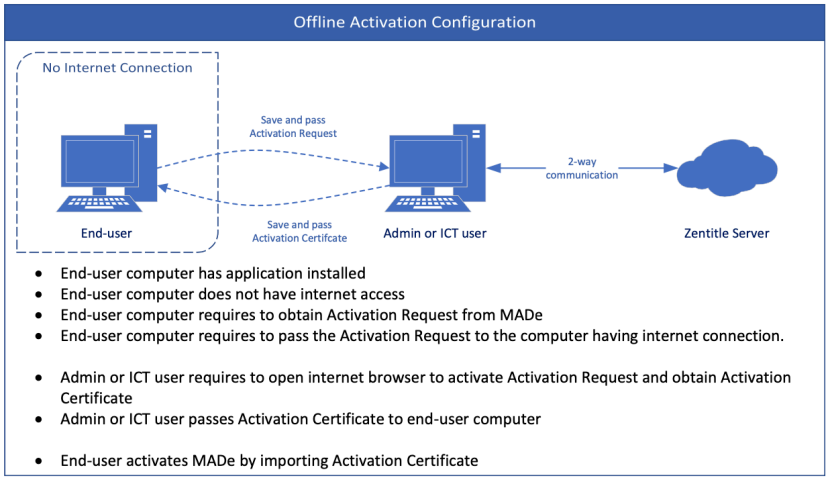
3.3 Offline Activation

3.3.1 Activation

Offline Activation currently supports node-locked licenses and is designed for use on an individual isolated computer.

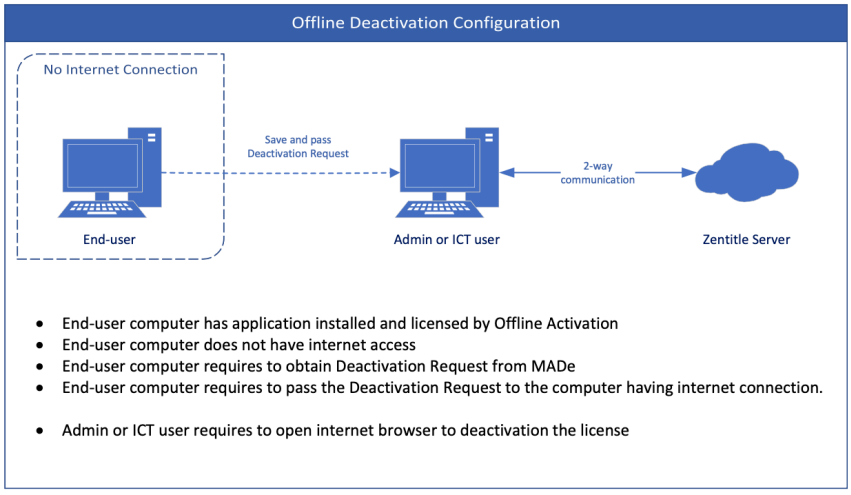
Offline Activations are performed in MADe using the MADe License Wizard by the end-user and on the PHMT License self-service portal website on a computer with internet access by an Administrator or ICT user.

In MADe, an Activation Request is generated, and a URL is provided for the PHMT License self-service portal. This information can be saved by the end-user and passed onto an Administrator or ICT user. On a computer with internet access, an Activation Certificate is generated from the Activation Request using the PHMT License self-service portal, which can be saved and passed back to the end-user. Finally, back in MADe, the Activation Certificate is used to activate the node-locked license.



3.3.2 Deactivation

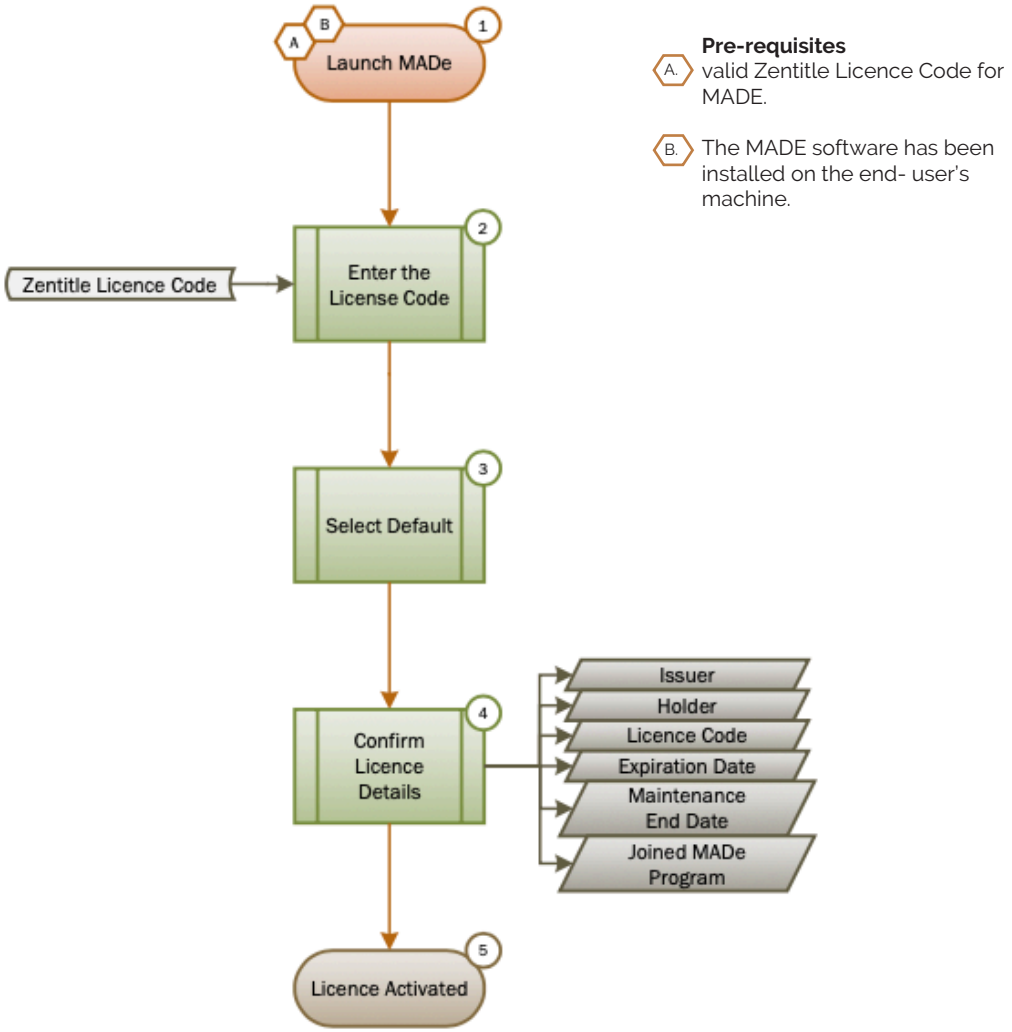
Deactivating a licence offline requires a similar process. In MADe, a Deactivation Request is generated, and a URL is provided for the PHMT License self-service portal. Once the Deactivation Request is generated, the selected licence is removed from MADe, and MADe will be closed. The Deactivation Request and URL can be saved by the end-user and passed onto an Administrator or ICT user. The Deactivation Request can be entered into the PHMT License self-service portal on a computer with internet access, freeing up the license for use on another computer.



4. Zentitle License Activation Workflow

The following section outlines the workflows for the different Zentitle License Activation scenarios.

4.1. Cloud



1. Launch the MADE software on the end-user PC. If the MADE license has not been activated, the MADE License Finder dialogue will appear.

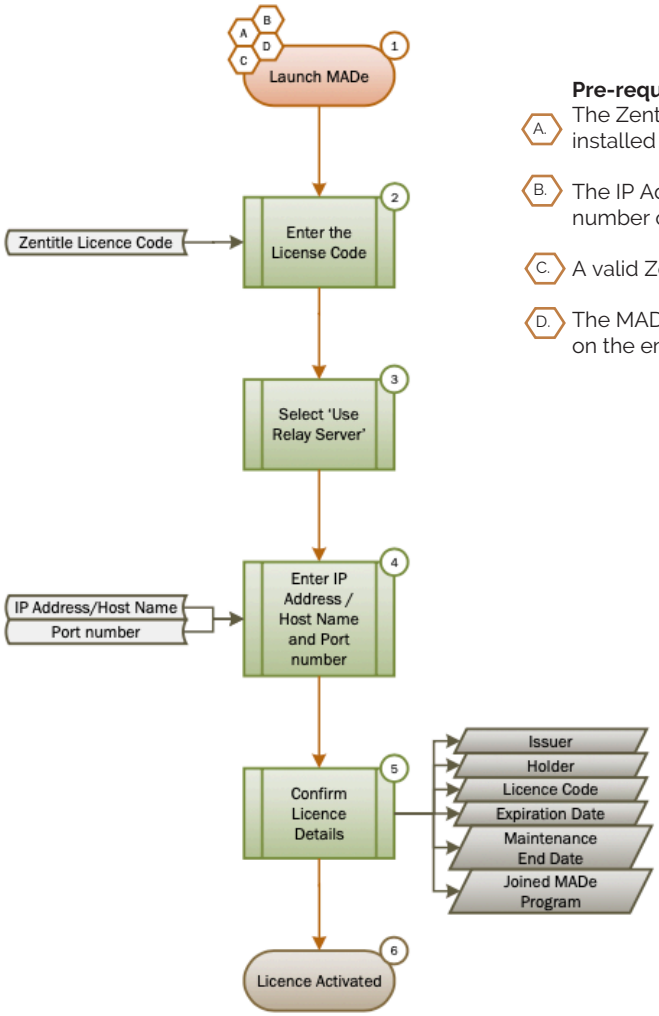
2. Enter the License Code in the 'Licence Code Activation' text field on the MADE License Finder dialogue.

3. Select the 'Default' radio buttons underneath the "Licence Code Activation" text field, then select the 'Next' button at the bottom of the MADE License Finder dialogue to continue.

4. Confirm that the license details displayed match the issued license and are all correct.
   - **Issuer:** The organization that issued the license to you
   - **Holder:** Your organization and style of license
   - **Licence Code:** The licence code provided by the issuer entered in step 2
   - **Expiration Date:** The last valid date for the license
   - **Maintenance End Date:** The last valid date for maintenance
   - **Joined MADE Program:** Yes or No based on your selection
   - Select 'Finish' to finalize the process.

5. The MADE Licence is now activated, and the MADE License Finder dialogue will close, allowing access to the MADE software.

4.2. Relay Server



1. Launch the MADE software on the end-user PC. If the MADE license has not been activated, the MADE License Finder dialogue will appear.

2. Enter the License Code in the 'Licence Code Activation' text field on the MADE License Finder dialogue.

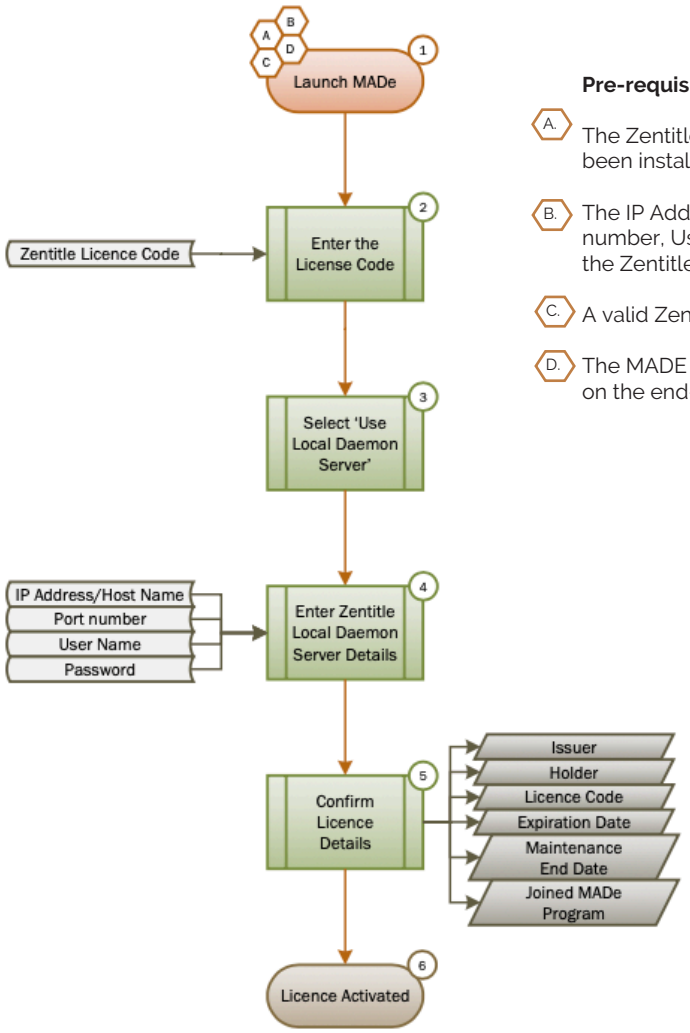
3. Select the 'Relay Server' radio buttons underneath the "Licence Code Activation" text field.

4. Enter the IP Address or Host Name and the Port number of the Relay Server, then select the 'Next' button at the bottom of the MADE License Finder dialogue to continue.

5. Confirm that the license details displayed match the issued license and are all correct.
   - **Issuer:** The organization that issued the license to you
   - **Holder:** Your organization and style of license
   - **Licence Code:** The licence code provided by the issuer entered in step 2
   - **Expiration Date:** The last valid date for the license
   - **Maintenance End Date:** The last valid date for maintenance
   - **Joined MADE Program:** Yes or No based on your selection
   - Select 'Finish' to finalize the process.

6. The MADE Licence is now activated, and the MADE License Finder dialogue will close, allowing access to the MADE software.

4.2. Local Daemon Server



1. Launch the MADE software on the end-user PC. If the MADE license has not been activated, the MADE License Finder dialogue will appear.

2. Enter the License Code in the "Licence Code Activation" text field on the MADE License Finder dialogue.

3. Select the 'Local Daemon Server' radio buttons underneath the 'Licence Code Activation' text field.

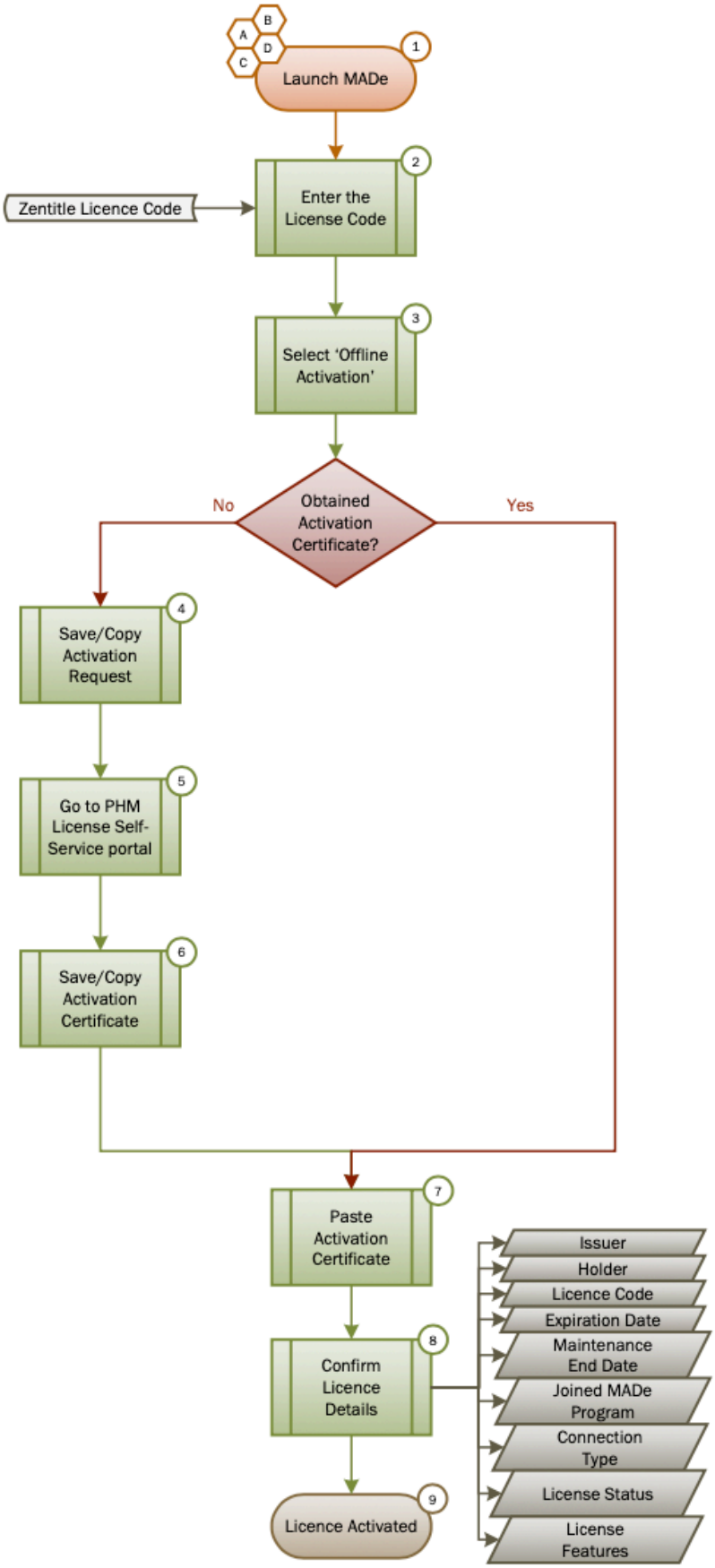
4. Enter the IP Address or Host Name, the Port number, User Name and Password of the Local Daemon Server, then select the 'Next' button at the bottom of the MADE License Finder dialogue to continue.

5. Confirm that the license details displayed match the issued license and are all correct.
   - **Issuer:** The organization that issued the license to you
   - **Holder:** Your organization and style of license
   - **Licence Code:** The licence code provided by the issuer entered in step 2
   - **Expiration Date:** The last valid date for the license
   - **Maintenance End Date:** The last valid date for maintenance
   - **Joined MADE Program:** Yes or No based on your selection
   - Select 'Finish' to finalize the process.

6. The MADE Licence is now activated, and the MADE License Finder dialogue will close, allowing access to the MADE software.

4.3. Offline Activation

4.3.1 Activation of License



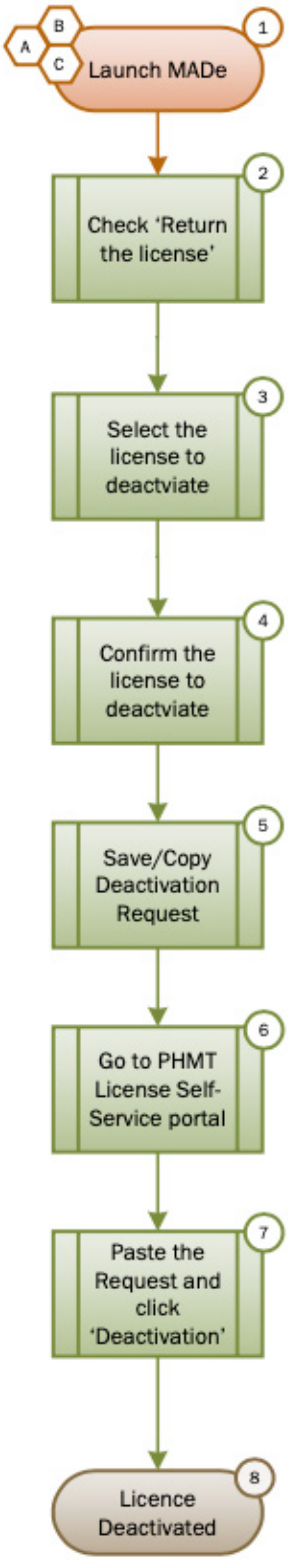
1. Launch the MADe software on the end-user PC. If the MADe license has not been activated, the MADe License Finder dialogue will appear.
2. Enter the License Code in the 'License Code Activation' text field on the MADe License Finder dialogue.
3. Select the 'Offline Activation' radio buttons underneath the 'License Code Activation' text field.
4. Save or Copy the Activation Request generated by the MADe License Wizard dialogue and PHM License self-service portal URL.
5. On a computer with internet access, open the PHMT License self-service portal URL in an internet browser, paste Activation Request into the text area and click the 'Activate' button.
6. An Activation Certificate will be generated. Save or copy the certificate and pass it back to the end-user computer.
7. Paste the Activation Certificate into the MADe License Wizard.
8. Confirm that the license details displayed match the issued license and are all correct.

   Issuer: The organization that issued the license to you
   Holder: The name of your organization
   License Code: The license code provided by the issuer entered in step 2
   Expiration Date: The last valid date for the license
   Maintenance End Date: The last valid date for maintenance
   Joined MADe Program: Based on your selection
   Connection Type: Offline Activation
   License Status: Valid License Code
   License Features: Check that the expected license features for your license are listed here.

   Select 'Finish' to finalize the process.

9. The MADe License is now activated.

4.3.2 Deactivation License



1. Launch the MADe software on the end-user PC and open the MADe License Wizard.
2. Check the “Return the license” option.
3. Select the license to deactivate.
4. Confirm the license code to deactivate.
5. Save or Copy the Deactivation Request generated by the MADe License Wizard dialogue, and the PHMT License self-service portal deactivation URL.
6. On the computer with internet access, open PHMT License self-service portal deactivation URL in an internet browser,
7. Paste the Deactivation Request into the text area and click “Deactivate”.
8. The MADe Licence is now fully deactivated and can be closed.

5. Scenarios

The following section outlines the different working scenarios and behaviour of the Zentitle licensing for the MADE software.

5.1. Network License, user works offline

In this scenario, the user would be able to use MADE for up to 8 hours before the next license heartbeat check occurs. The user will also be limited to the module they are currently in for this duration. After the 8 hours has lapsed, the user will be prompted with a dialog which indicates the license heartbeat check has failed to obtain a valid license code. The user will be prompted with 3 options:

5.1.1. Get Extension

The user will be granted a 10-minute extension to use the software. This option only appears once, after the 10-minute extension has been granted, the user must either Refresh Lease or Shutdown MADE.

5.1.2. Refresh Lease

The user can connect to the internet and select this option to obtain a valid license for the next 8 hours. If the Refresh Lease fails, the same dialog will appear.

5.1.3. Shutdown MADE

The MADE software will shutdown, prompting the user to save where unsaved changes exist.

5.2. Node-locked License, user works offline

In this scenario, the user would be able to use MADE for up to 8 hours before the next license heartbeat check occurs. The user will have access to all paid modules for this duration. After the 8 hours has lapsed, the user will be prompted with a dialog which indicates the license heartbeat check has failed to obtain a valid license code. The user will be prompted with 3 options:

5.2.1. Get Extension

The user will be granted a 10-minute extension to use the software. This option only appears once, after the 10-minute extension has been granted, the user must either Refresh Lease or Shutdown MADE.

5.2.2. Refresh Lease

The user can connect to the internet and select this option to obtain a valid license for the next 8 hours. If the Refresh Lease fails, the same dialog will appear.

5.2.3. Shutdown MADE

The MADE software will shutdown, prompting the user to save where unsaved changes exist.

5.3. Network license, multiple user access

In this scenario, multiple users can access the license, providing there are available seats. Multiple computers can enter in the same license code and have the software activated, however, if there are no available seats, the user will observe a dialog indicating no seats are available at this point in time.

E.g. A company has purchased a MADE Suite license (which includes one license for each of the 4 modules) with 6 computers connected to the network license. For this configuration, four concurrent users can access the MADE software – one in each module. The two additional computers which have MADE installed will not be able to access the software until a seat is available; when a user exits the application which returns the module seat.

For the four users with access to the MADE software, they will only be able to utilize the module they are in as there will be no available seats for other modules. When attempting to access modules with no available seats, the user will be prompted with a dialog indicating that there is no available seats to be checked out. The user will remain in their current module.

5.4. Perpetual license without active maintenance & support subscription

Perpetual licenses are locked to the version of the software which was purchased. An Annual Maintenance and Support package can be purchased which enables the license to be used with the software upgrades for the maintenance period. The annual Maintenance and Support package is priced as a percentage of the current license list price.

E.g. A company has purchased a Perpetual license on January 1st, 2022. At the time, MADE 3.8.4 was available. The Company will have access to this version of the software. Without purchasing the Annual Maintenance and Support package, the company will not have access to future versions of the software.

On January 1st 2023, the company wishes to purchase the Annual Maintenance and Support package. This will be available, however, the cost will be prorated back to the end date of the prior Support and Maintenance package. In this instance, it will be for 2 years of annual Maintenance and Support – for January 1st 2022 to December 31st 2022 as well as January 1st 2023 to December 31st 2023.

5.5. Multiple Network Licenses Purchase

In the situation where multiple licenses are purchased by a company, there will be a single license code which is applicable. The licensing and expiry dates of the newly purchased licenses will be added to the initial license code.

E.g. A company has purchased an annual MADE Suite subscription license on January 1st, 2022. On July 1st, 2022, the company purchases two additional annual MADE Suite subscription licenses. This configuration means that one MADE Suite license will expire on the December 31st, 2022, and two MADE Suite licenses will expire on the June 30th, 2023. The license code, which was issued on the January 1st, 2022 will be applicable to both purchases – the additive licenses are configured by PHMT on the cloud.

5.6. Network License, Multiple MADE instances on single computer

In this situation, multiple MADE instances can be opened on a single computer providing the license seat is available.

E.g. A company has purchased an annual MADE Suite subscription license with a network license configuration. Four users are using the software on different computers: one in each module. The user in the MADE Modeling module can open another instance of MADE in the same module, however, access to the other modules will be unavailable due to insufficient license seats. Each time a new module is selected, MADE will check to see if there is an available seat for that module. If a seat is available MADE will swap to that module and release the seat for the previous module.

5.7. Node-locked License, Multiple MADE instances

In the situation where a user has purchased a node-locked license for the MADE Suite, the user will be able to open as many instances of MADE as they wish with no limitations on modules.

E.g. A user has purchased an annual MADE Suite subscription license with a node-locked license configuration. Multiple instances of MADE can be opened in any module without restriction.

Appendix A

Relay Server
Configuration

A1.0 Introduction

This article outlines the way you can securely link out from your user's site to the Zentitle Licensing Cloud. Relaying from a DMZ within a user network to the Zentitle Licensing Cloud) without having to install our LAN Daemon, which acts as an on-premise licensing server, inside your customer's local network.

Whoever is installing the server must be familiar with adding a virtual machine to a DMZ.

This is fast, easy to install and will simply relay end-user login access calls directly to the Zentitle Servers outside the network and relay back any of the required access control information in order that the correct number of users can access the protected Software.

A2.0 Pointing MADE to the Relay Server

To use the relay server you must point the MADE client to the Relay Server rather than to Zentitle's server. This may be done when first launching MADE prior to entering a License Code to activate, when using the License Wizard follow these instructions:

1. Enter your License Code provided ready to be activated.
2. Check the "Use Proxy Server / Local License Server" option.
3. Enter the IP Address / Host name of the Relay Server.
4. Enter the Port of the Relay Server.
5. Select "Finish" to perform the license activation and validation.

A3.0 Relay Server Access and Setup Details

The Relay Server is a virtual machine (VM) created from a stripped down version of CentOS 6.5 designed to port forward from your network to the Zentitle server. The VM has most services disabled. The only ports it listens on are 16700, 16701 (the ports that are forwarded to Zentitle), 22 (ssh) and 68 (udp for dhclient).

Additionally, there is a firewall protecting the vm. By default the Network Relay Server listens on port 16700 and 16701 of eth0 and forwards to port 80 and 443 at 184.106.60.185. If these defaults will work with your network, you'll just have to set up the Network Relay Server in the virtualization software of your choice. Information on configuring the Ethernet card in the virtual machine may be found below. Information is also available below if you would like to change or add Ethernet cards or change ports.

A4.0 Setting up the Relay Server

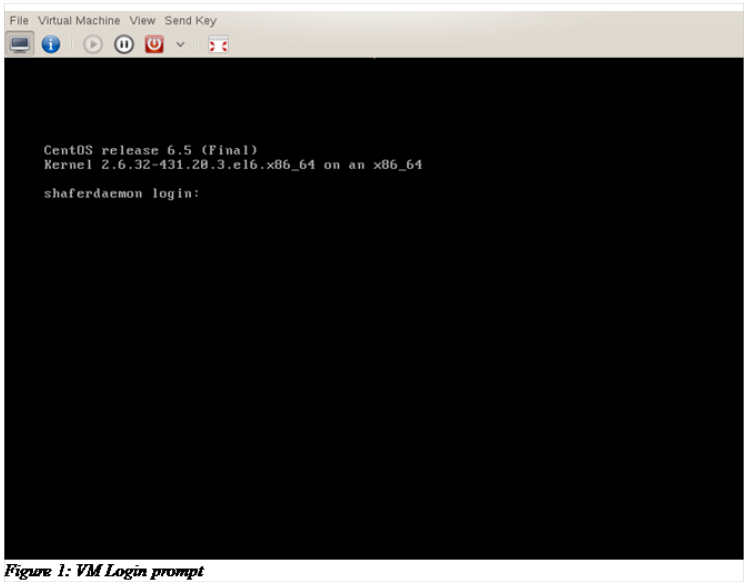


Figure 1: VM Login prompt

An image of the Relay Server's hard drive is provided in a format suitable for:

- **Qemu-kvm** [*http://www.nalpeiron.com/cust_ctr/files/NalpDQEMU.zip*]
- **VMWare** [*http://www.nalpeiron.com/cust_ctr/files/NalpDVMWare.zip*]
- **VBox** [*http://www.nalpeiron.com/cust_ctr/files/NalpDVBox.zip*]
- **HyperV** [*http://www.nalpeiron.com/cust_ctr/files/NalpDHyperV.zip*]

Download the image that corresponds to your virtualization software, unzip it and use it as the hard drive for your virtual machine. The details of this process depend on which virtualization software you are using. During setup, be sure to add at least one Ethernet card.

When this is complete boot the VM.

You should see a prompt as in Figure 1. Login with the following credentials:

Username: **root** | Password: **shaferdaemon**

For security, you should immediately change the root password.

Do this by typing "passwd" at the command line. Enter the new password twice as prompted.

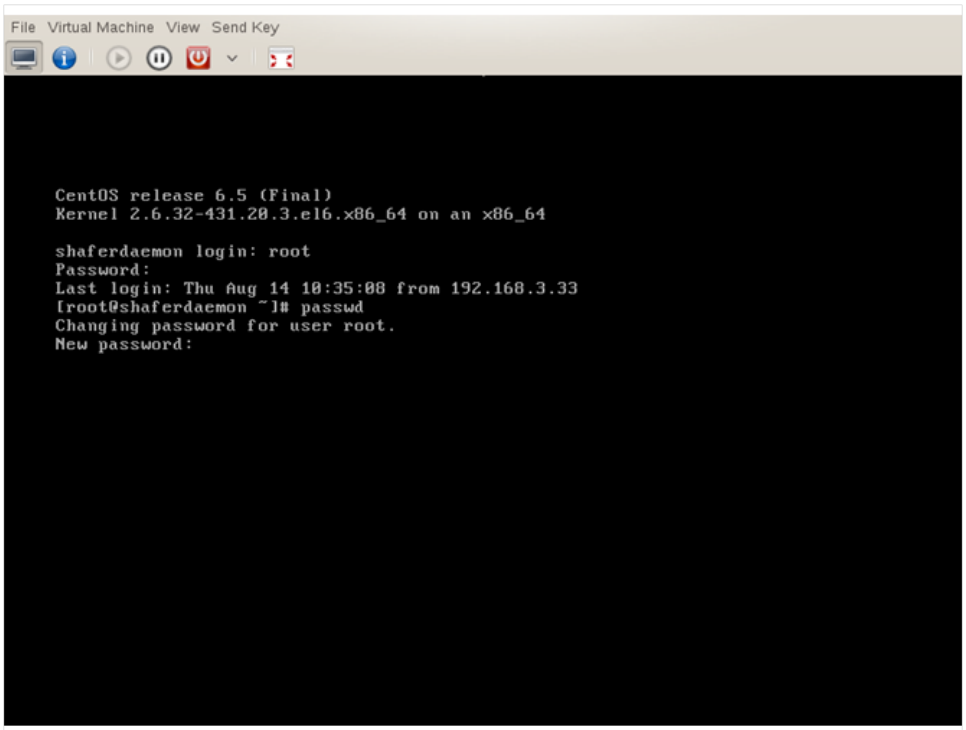


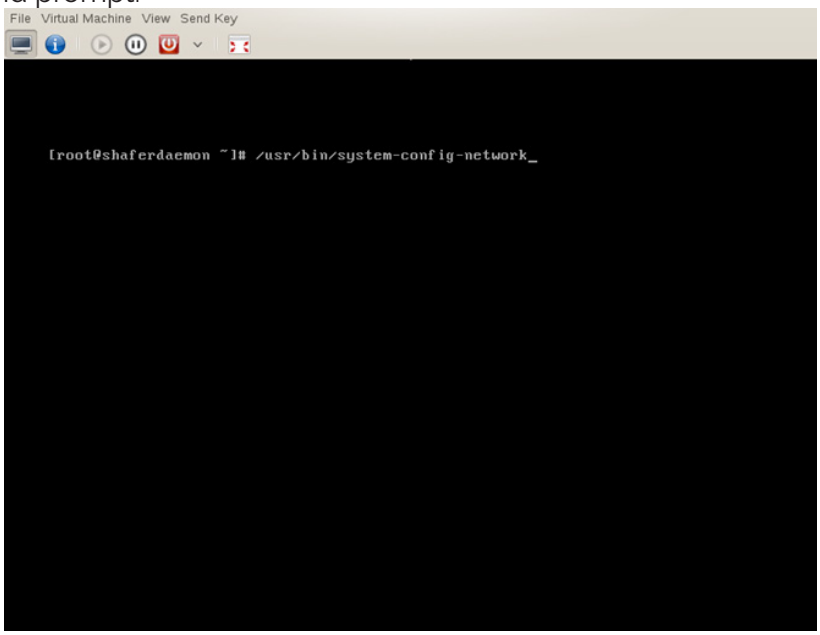
Figure 1: Change root password with passwd

The root password is now changed.

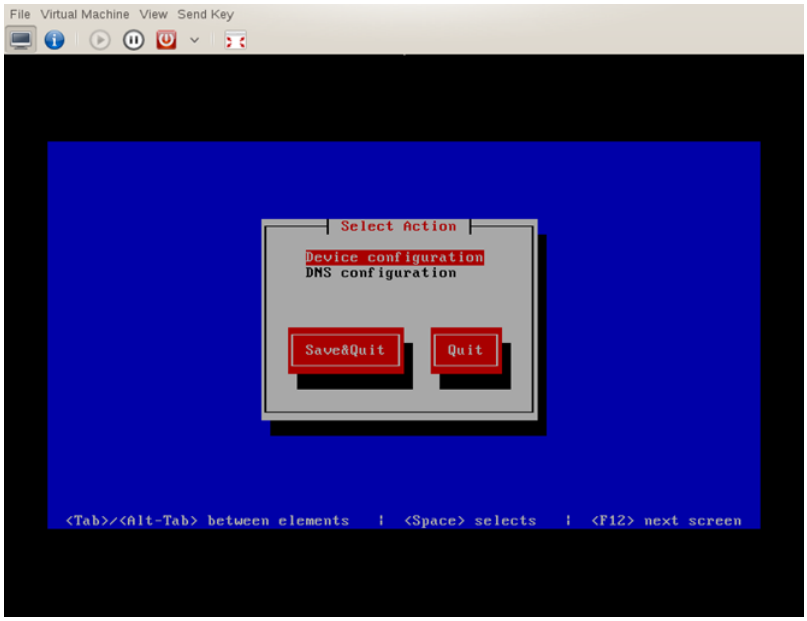
Do not lose or forget this password as it will be required to login and administer the virtual machine.

The next step will be to configure your network card.

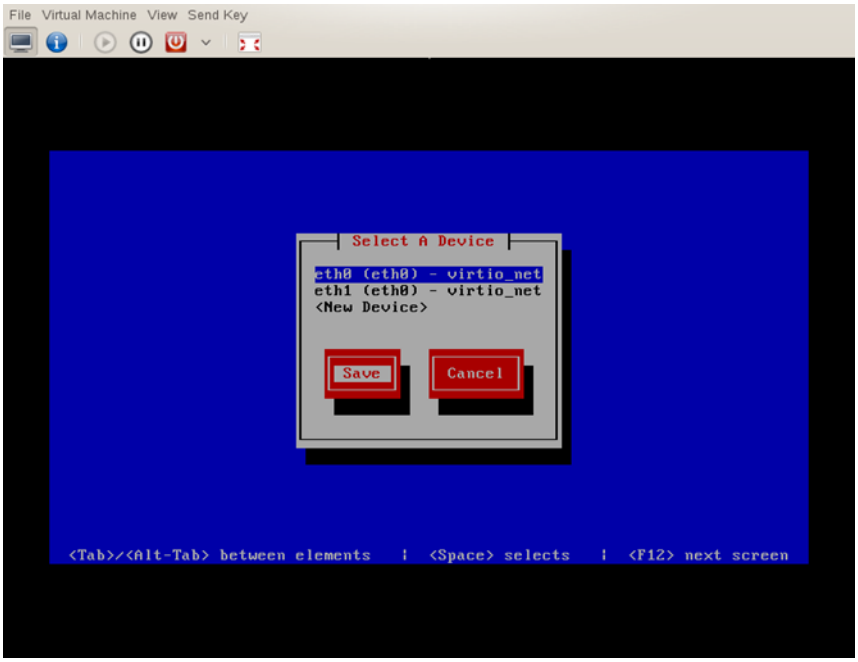
- Open the network card configuration dialog by typing "/usr/bin/system-config-network" at the command prompt.



- When the configuration interface opens, select "device configuration".

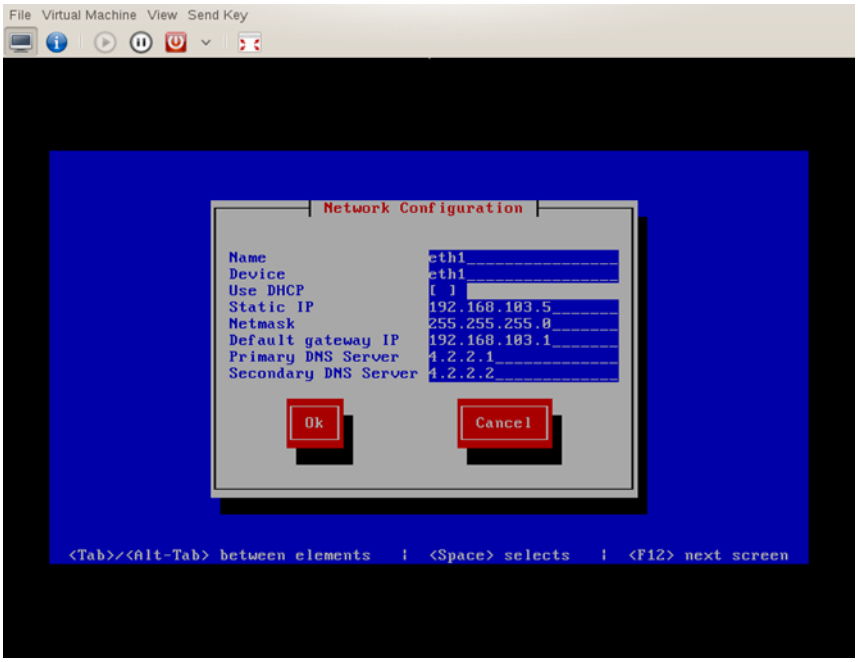


- From the device menu select the Ethernet card you wish to edit. Generally, the first card added will be eth0, the second card eth1, etc.

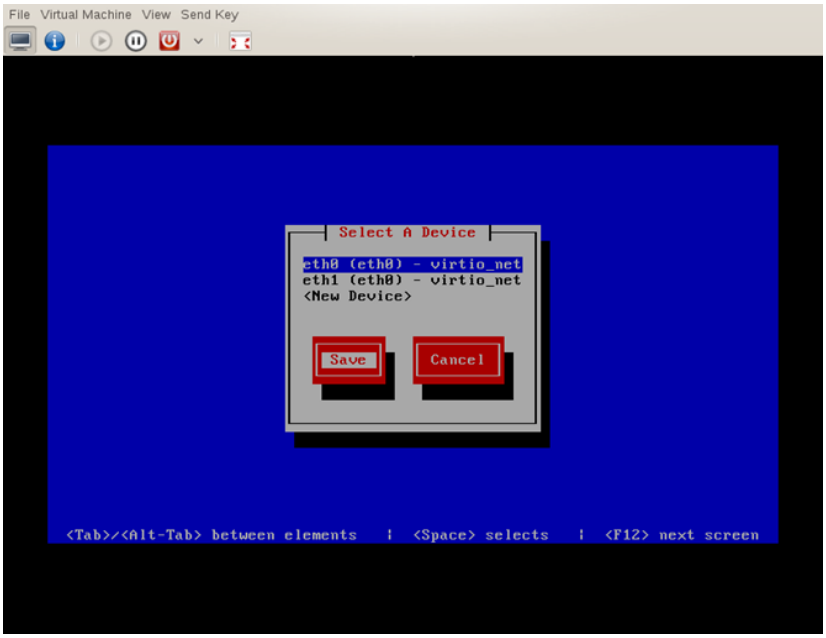


By default, the cards are set up for DHCP.

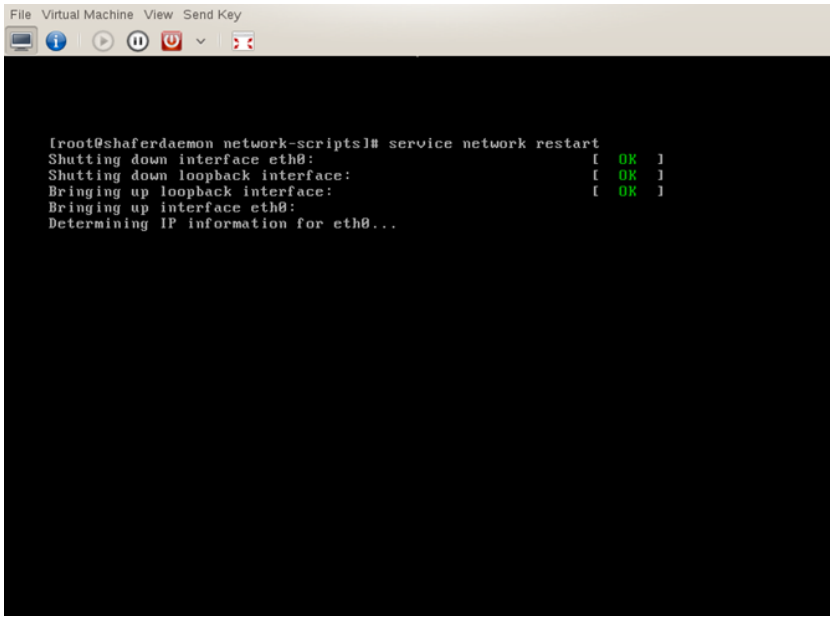
- If that is acceptable, tab down to the OK button and continue.
- If you wish to set the card manually, tab down to "Use DHCP" and use the space bar to de-select it. You will now be able to set the VMs IP address, netmask, and gateway. You may set the DNS servers if you wish.
- When you are satisfied with the settings tab to OK and press return.



- When finished configuration all devices, select “Save” and hit return. You will be returned to the command line

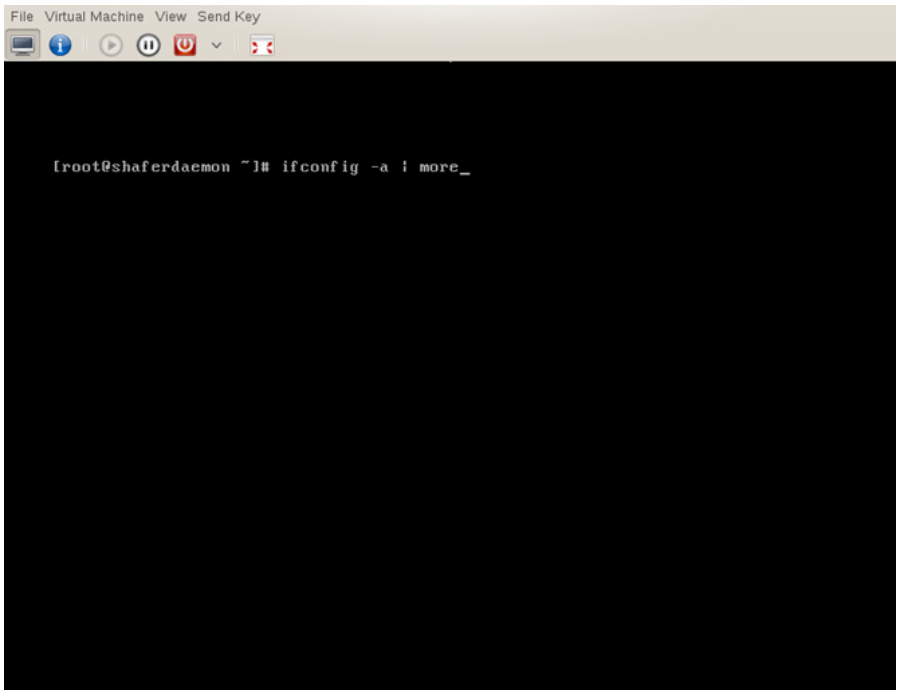


Now restart networking services so that your changes will take effect. Use the command “service network restart” to do this. You should see a “Bringing up interface ethn” line for each Ethernet device in your system.

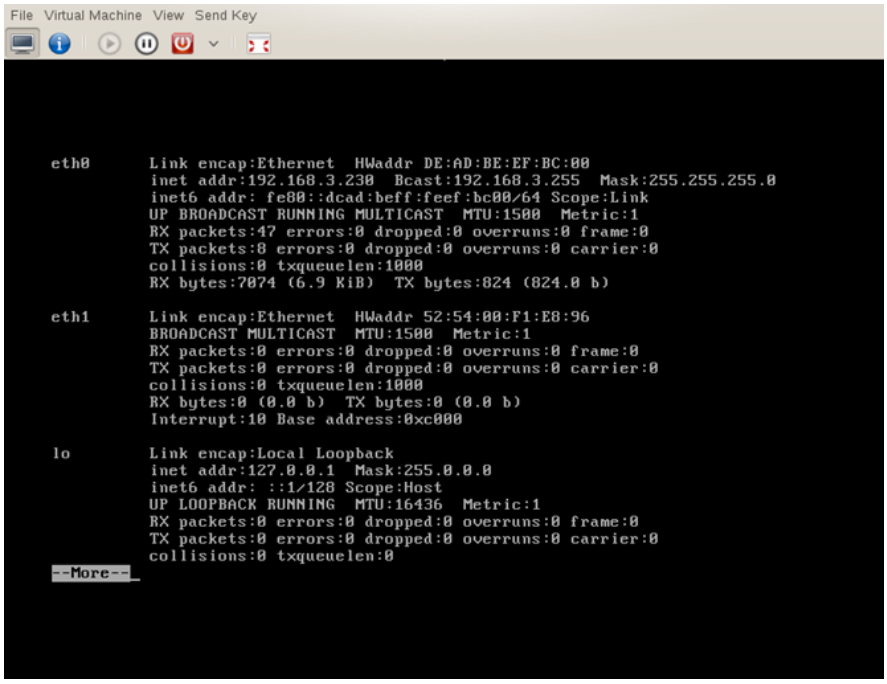


- Check to make sure that your changes were enacted as expected by using the “ifconfig -a” command.

For each Ethernet device present on your VM, you should see networking information. On the second line of the device information, you should see the IP address for the device.



In the following figure, eth0 has an Internet address of 192.168.3.230 but eth1 has no address. In this case, eth1 is not enabled and would be available for networking.

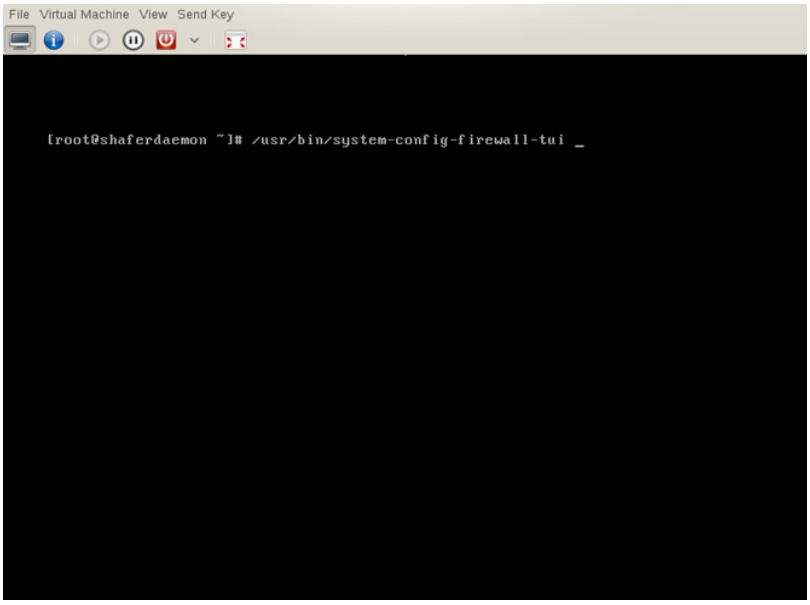


If you are satisfied with the default configuration (one Ethernet card listening on port 16700 for your network and transmitting to Zentitle) then you are finished setting up the Relay Server and can test that it's working correctly.

A5.0 Relay Server Advanced Configuration

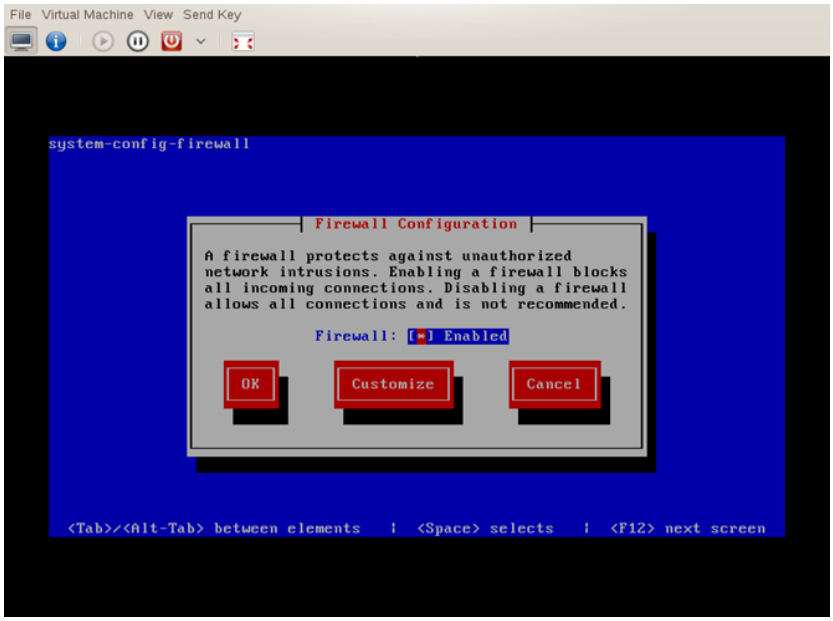
A5.1 Changing Ports and Additional Configuration

If you'd like to change ports or have one card listen on your network and a second card transmit to Zentitle then continue with these instructions.Start the firewall configuration program by typing "/usr/bin/system-config-firewall-tui" at the command prompt.



The firewall should be marked as enabled.

- To edit, tab to "Customize" and press return.

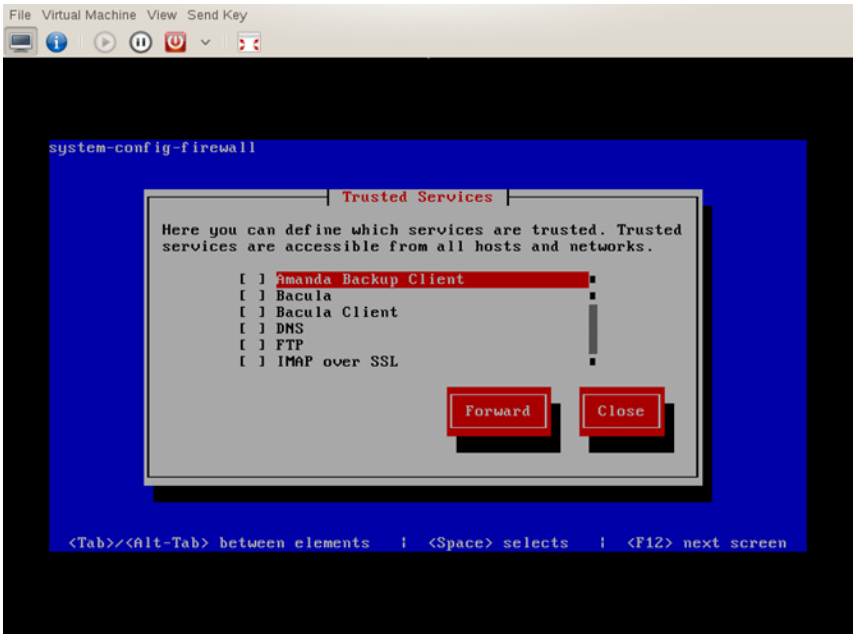


The first screen you'll see allows you to mark certain services as trusted. None of these will be marked.

We do not need trusted services for relaying.

There will be several of these pages where nothing needs to be changed.

- On each page, tab to the "Forward" button and press return.



- Stop when you reach the "Other Ports" page.

The "Other Ports" page is where we choose a port and protocol for the Network Relay Server to listen on your network.

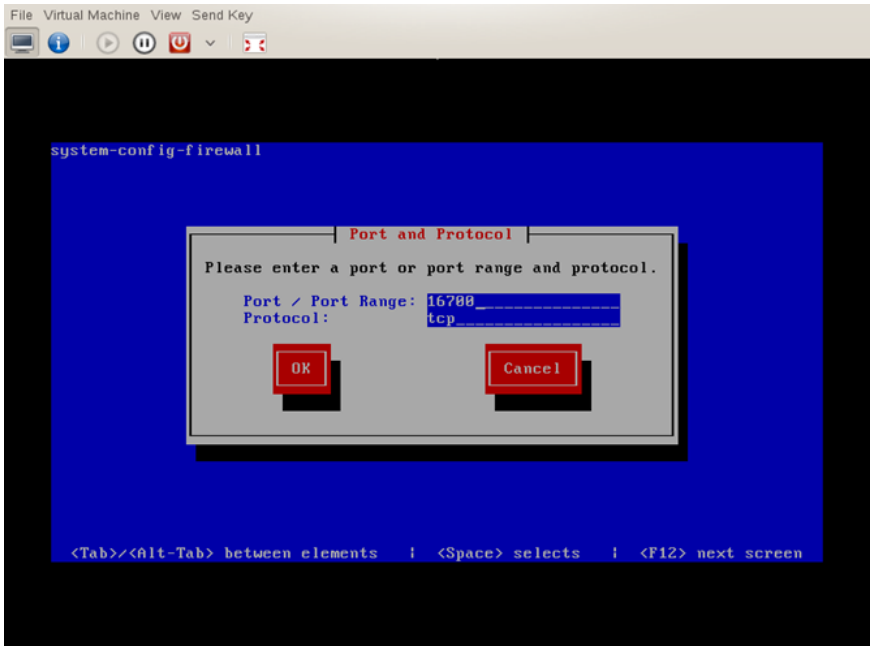
By default, the VM listens on port 16700.

You may change this if you wish.

However, the protocol, TCP, must remain unchanged.

- Tab forward to "edit" and press return.
- Tab forward to the "Port" entry and backspace over 16700 then type the port you would prefer.
- When you are finished, tab to "OK" and press return.

If you change this port, **you need to change the port that is forwarded later in this document.**

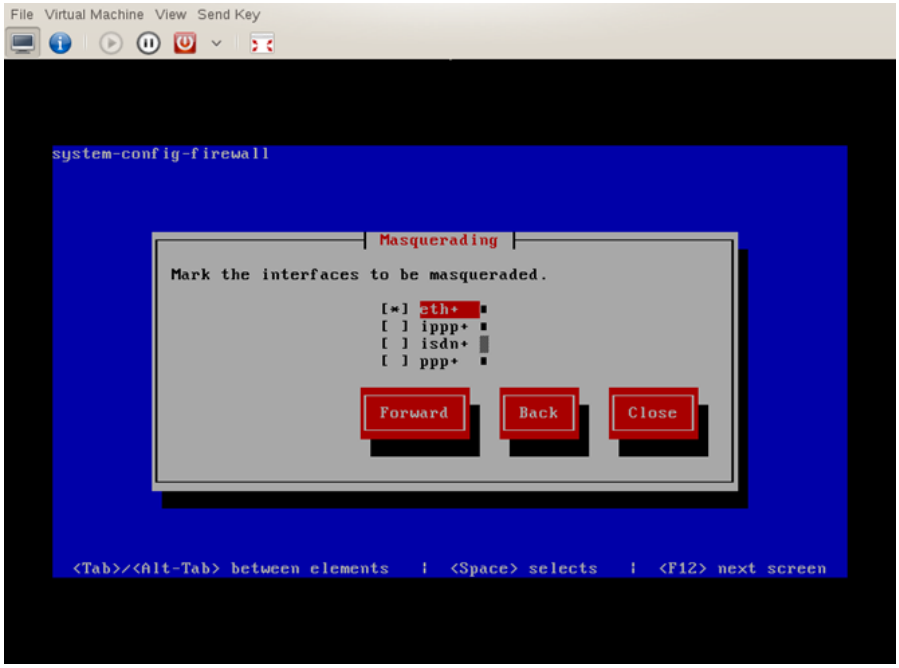


Once, you have changed the port and pressed “OK” you will return to the main page.

- Tab to the “Forward” button and press return. The next change we will make is on the “Port Forwarding” page.

As you as passing through configuration pages, you might notice the “Masquerading” page. It should have“eth+” enabled as shown below.

Do not change this. Masquerading on ethn is needed for the port forwarding to work.



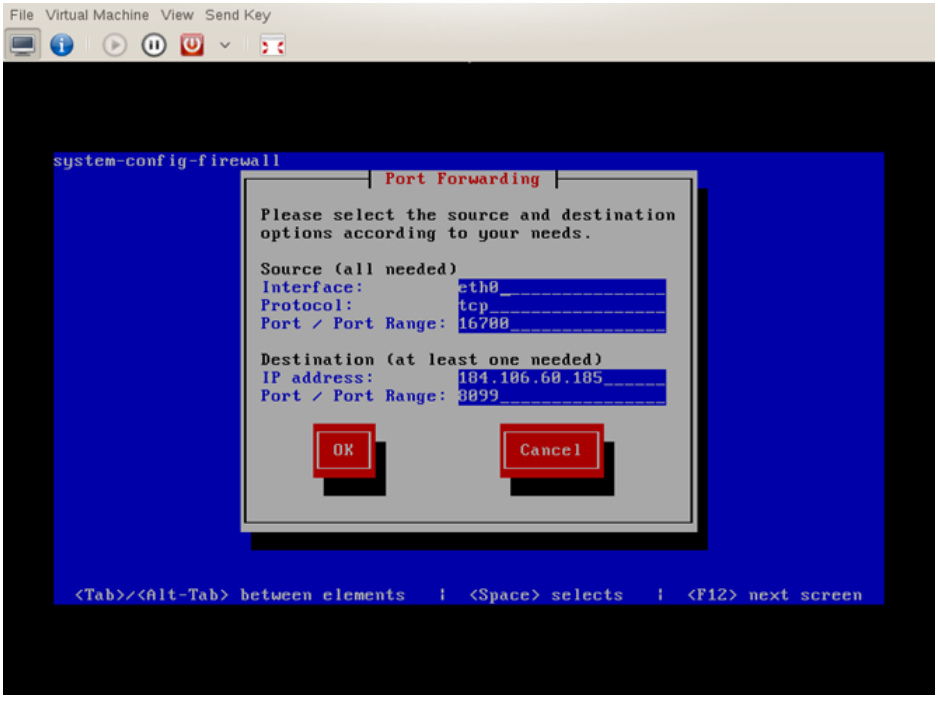
If you changed the listening port from 16700 or wish to change the transmitting Ethernet card, you'll make these changes on the "Port Forwarding" page.

- Tab to the "edit" button and press return.

By default, the port forwarding listens on eth0 port 16700 (and/or port 16701 for https).

- You may change either or both of the values.

Do not change the protocol (TCP) or the destination IP address (184.106.60.185) or the destination port (80).
NOTE the above image and those following are outdated. The correct port is port 80 and NOT port 8099 although port 8099 will continue to function for the foreseeable future.



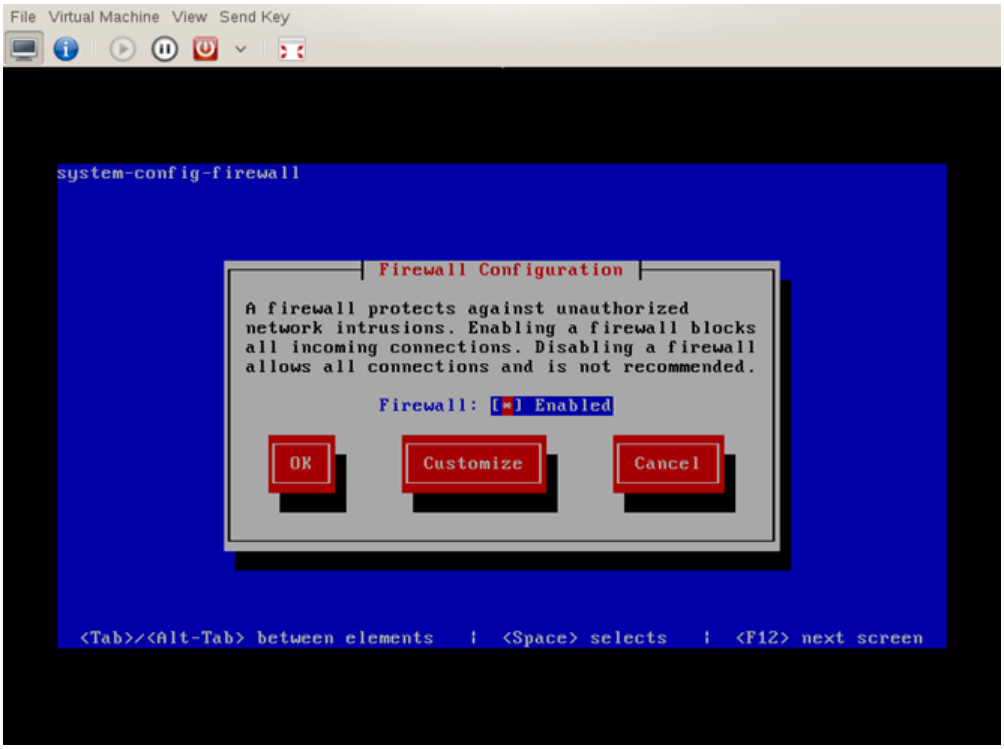
- When finished tab to "OK" and press return.

- Tab to the “Close” button and press return.

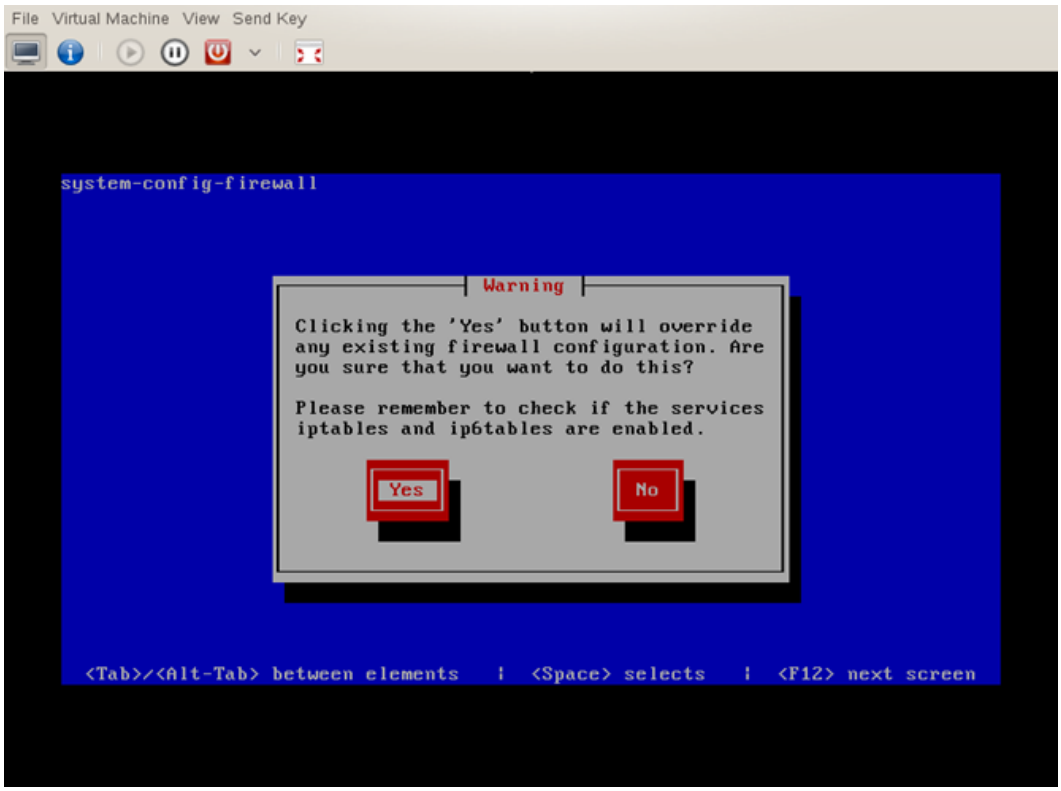
You’ve now finished making changes. You’ll be taken back to the initial firewall configuration page.

- On the initial page, tab to “OK” and press return.

You’ll next be asked if you really want to make the change.



- Tab to “YES” and press return for the changes to take place.



You've finished configuring the Network Relay Server and can now test the setup to ensure it's working correctly.

Appendix B

Local Daemon Server

Guide

B1.0 Introduction

The Zentitle LAN daemon is a local server, usually running on a virtual machine, whose purpose is to manage the licenses of client applications running on a local area network (LAN.)

This LAN may or may not be connected to the internet and so it need not be able to contact the Zentitle server. As such, it is ideally suited to license management scenarios involving dark sites or where internet access is otherwise limited or restricted.

The LAN daemon is to be distinguished from the Zentitle relay daemon. The relay daemon serves as a link to the Zentitle server. Its purpose is simply to pass data between the client machines and the Zentitle server where all license management is carried out. The LAN daemon, on the other hand, provides a local implementation of much of the license management functionality of the Zentitle server.

Although the daemon must interact with the server to enable and disable license codes, this can be carried out with offline activation/deactivation if necessary and the actual activation and deactivation of client machines is carried out solely on the daemon. As such, it is more useful in dark site situations where the LAN has no internet connection and so cannot directly contact the Zentitle licensing server.

B2.0 Software Download & Configuration

B2.1 Download Components

Below are three items that should be downloaded:

1. A virtual machine image on which to install the LAN daemon. **This is optional as you may install the LAN daemon on your own host machine (see below).** You only need to select one, which ever suits your environment.

   A) VMWare Disk Image
   [*https://phmt-assets.s3.amazonaws.com/Zentitle/daemonVMV2VMWare.zip*]

   B) KVM Disk Image
   [*https://phmt-assets.s3.amazonaws.com/Zentitle/daemonVMV2KVM.zip*]

2. A PostgreSQL database, which will be installed on the host machine.

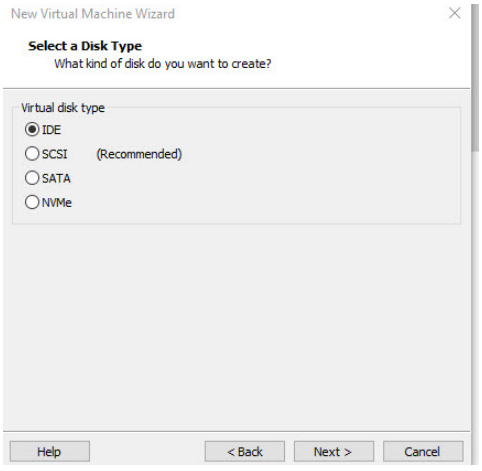
   RPM PostgreSQL Installer
   [*https://phmt-assets.s3.amazonaws.com/Zentitle/nalppgsql-2.8.1.6-3.8.1.6.x86_64.rpm*]

3. The Zentitle Daemon package, which will also be installed on the host machine.

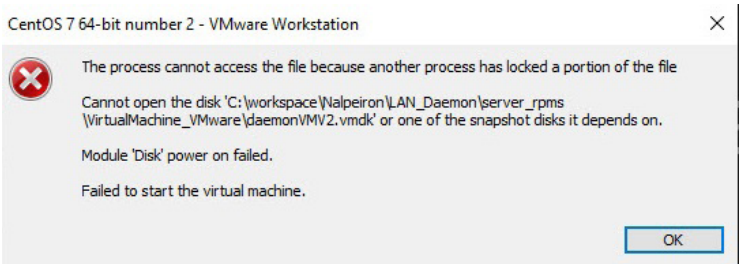
   RPM Zentitle Daemon package
   [*https://phmt-assets.s3.amazonaws.com/Zentitle/5213_7431_nalpdaemon-2.8.1.6-3.8.1.6.x86_64.rpm*]

Both the PostgreSQL database and Daemon package are both packaged as rpm files to be installed on the Virtual Machine OS.

NOTE: On the VMWARE image on a Windows 10 host machine, it is necessary when installing the image to select the IDE disk type as shown here:



If you choose an alternative disk type, you may obtain the following error message:



B2.0 Daemon Installation

B2.1 Installing the Disk Image (Optional)

On the Network Configuration page, you can choose to download either the pre-prepared KVM or VMWARE image on which to install the LAN Daemon. Alternatively, you can supply your own VM, in which case see below for requirements. The KVM image is provided in the .raw format while the VMWARE image is provided as a .vmdk virtual disk. Please consult the documentation for your chosen virtualization platform for details on how to import virtual machine images in the required format. The default login credentials for the VM are:

- **username: root**
- **password: nalpeirondaemon**

For security, you are advised to change these as soon as possible.

B2.2 Installing the Daemon Components

B2.2.1 VM Requirements

The Zentitle LAN Daemon is supported on CentOS 7 and RHEL 7 and requires that systemd be installed and working. Other dependencies will be installed by the daemon's rpms.

B2.2.2 Installing the rpms

Use "sudo" install for each command if not logged in as root (i.e., sudo yum install /path/to/rpm).

1. yum install /path/to/nalppgsql.rpm
2. yum install /path/to/nalpdaemon.rpm
3. Modify the firewall to allow connections to the daemon (port 16700) and the web interface (port 80)

Adjust firewall:

- firewall-cmd --permanent --add-port=16700/tcp
- firewall-cmd --permanent --add-port=80/tcp

4. Disable SELINUX: edit /etc/sysconfig/selinux
   change SELINUX=enforcing to SELINUX=disabled

5. Check the following values and, if needed, increase the open file limit of your system

6. $ ulimit -aH

```
core file size          (blocks, -c) unlimited
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 63684
max locked memory       (kbytes, -l) 16384
max memory size         (kbytes, -m) unlimited
open files                      (-n) 8192 <--Open file limit
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) unlimited
cpu time                (seconds, -t) unlimited
max user processes              (-u) 63684
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

7. If your open file limit is less than 8192, change this value by editing /etc/security/limits.conf and adding or changing the “nofile” lines to:

   - soft nofile 8192
   - hard nofile 8192

8. Check and, if necessary, increase the kernel's socket backlog limit, to
   $ sysctl net.core.somaxconn
   net.core.somaxconn = 128

9. Increase this value to 2048 (or higher) by editing /etc/sysctl.conf and adding or editing the "net.core.somaxconn" value:
   net.core.somaxconn = 2048

10. Reboot the Operating System now.

B2.3 Testing the Installation

Check to make sure that the daemon is running.

```
sudo systemctl status nalpdaemon
```

Check to make sure postgresql is running.

```
ps -elf | grep postgres
```

Enable daemon on reboot/restart.

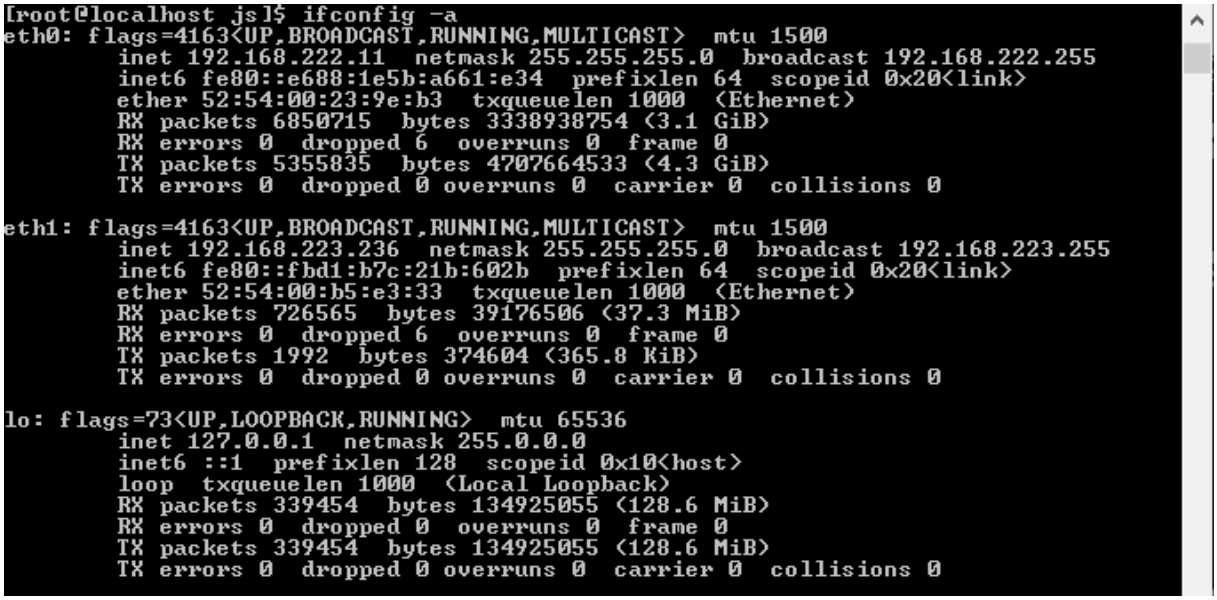
```
sudo systemctl enable nalpdaemon
```

The daemon will be installed to /var/www/html/nalpeiron.

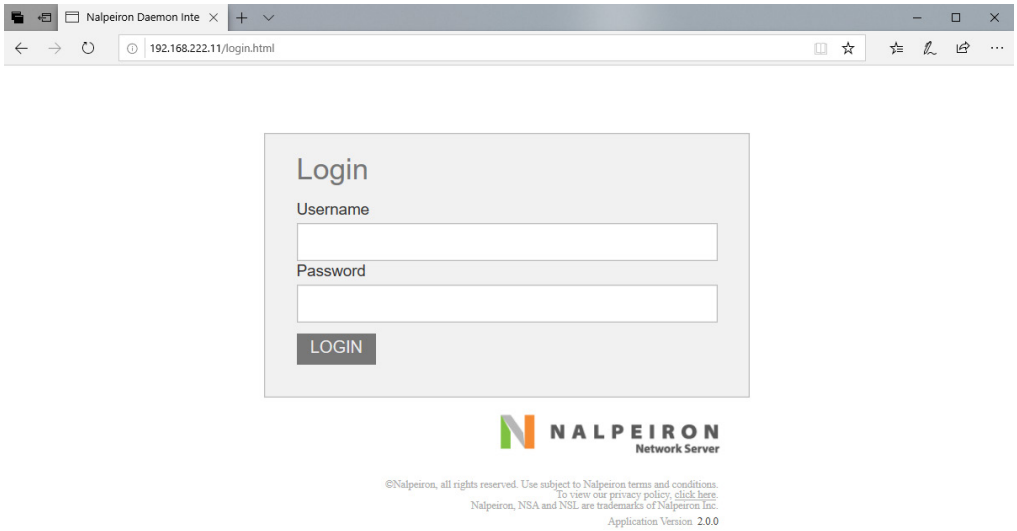
Following installation, the daemon should be accessible on your network. To obtain the daemon's IP address, type the following command into a command shell:

```
ifconfig -a
```

The daemon IP address is associated with the default network device (eth0 below) and we see that here it is 192.168.222.11.



At the daemon IP address, you should see the following login page:



The default username and password are 'admin' and 'nalpeiron' respectively. We will subsequently see how to change the admin password and how to add new users.

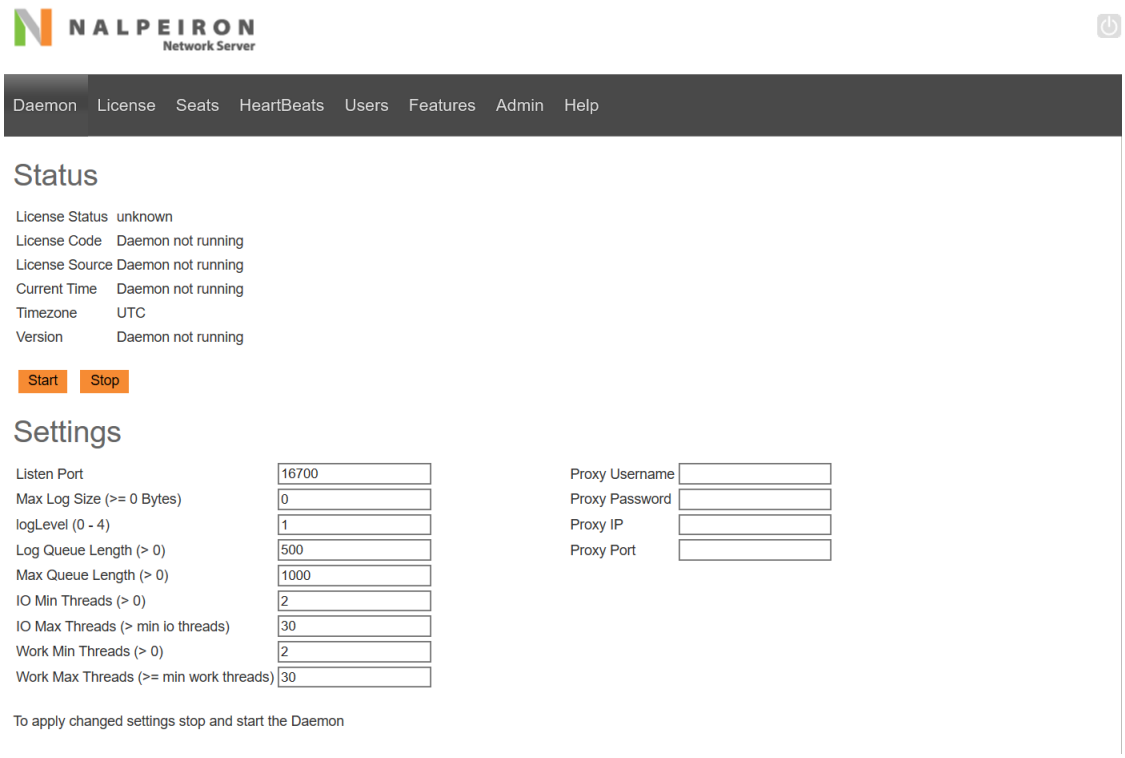
Only the admin user can log in to the daemon although all users (including the admin) can use their credentials in client applications.

NB: It may be necessary to clear your browser cache after upgrading to a newer version of the LAN daemon.

Default Credentials:

Username: **admin**
Password: **nalpeiron**

On logging in you will be presented with the daemon status and settings page as shown below.



This page provides status information and the values of several configuration settings for the daemon. The status fields are as follows:

- **License Status:** Whether the daemon is running and, if so, whether or not it is licensed.
- **License Code:** Daemon master license code (see below).
- **Computer ID:** ID of the host machine on which the daemon is running.
- **License Source:** The domain name of the Zentitle server from which the daemon master license code has been obtained.
- **Current Time:** Current time of the Zentitle Server.
- **Time zone:** Time zone of the Zentitle Server.
- **Version:** Daemon version number.

The daemon must be started by clicking the 'Start' button on this page prior to licensing. It must also be stopped, by clicking the 'Stop' button, before making any settings changes, following which it should be restarted.

The configuration settings are as follows:

- Listen Port: This is the port on which the daemon listens to the clients. The default value is set to 16700.

- Max Log Size: Maximum length of a log file on disk in bytes. When a log file reaches this size, a new log file is created up to a maximum of 5 log files. When there are 5 full log files, the oldest one is deleted and a new one is created. The default value is 0 (unlimited growth allowed).

- logLevel: Level of logging detail (0-4). Level 4 should always be used for diagnostics/ Nalpeiron support tickets. A value of 1 is sufficient for non-debug purposes.

- Log Queue Length: Maximum length of the log queue (number of entries waiting to be logged).

- Max Queue Length: Maximum size of the connection queue (i.e., number of clients waiting in line to be answered).

- IO Min/Max Threads, Work Min/Max Threads: Parameters which govern the ability of the daemon to handle IO requests and perform internal tasks. The higher the value, the more client machines can be handled although the more demanding this will be of the host machine. The daemon manages the size of its thread pool within these bounds.

- Proxy Username/Password/IP/Port: If the daemon is connecting to the internet via a proxy server, use these values to specify the IP address, port number and, if necessary, user credentials for the proxy server. If no proxy is used, these can be left empty or unspecified. The default is no proxy.

The log is written to the .log file in the /logs subdirectory of the /etc/nalpeiron/ directory, which is the daemon's working directory.

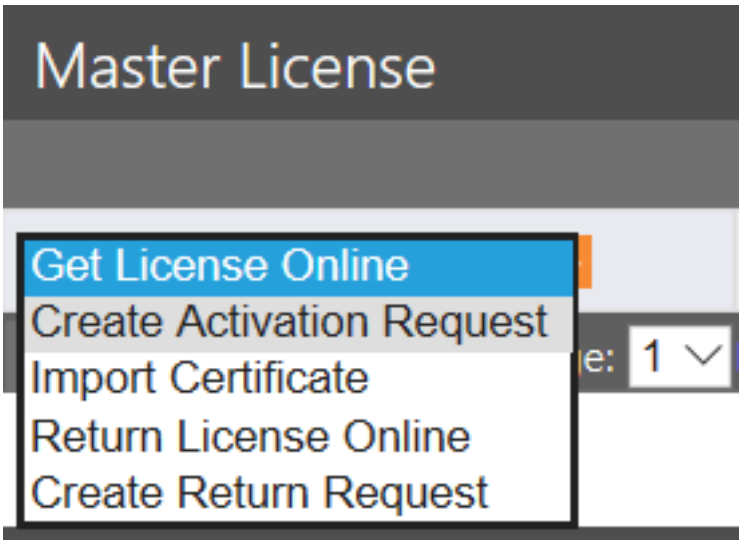
Once the daemon has been suitably configured and started, the next step is to set up the daemon licensing.

B3.0 Licensing the Network Daemon

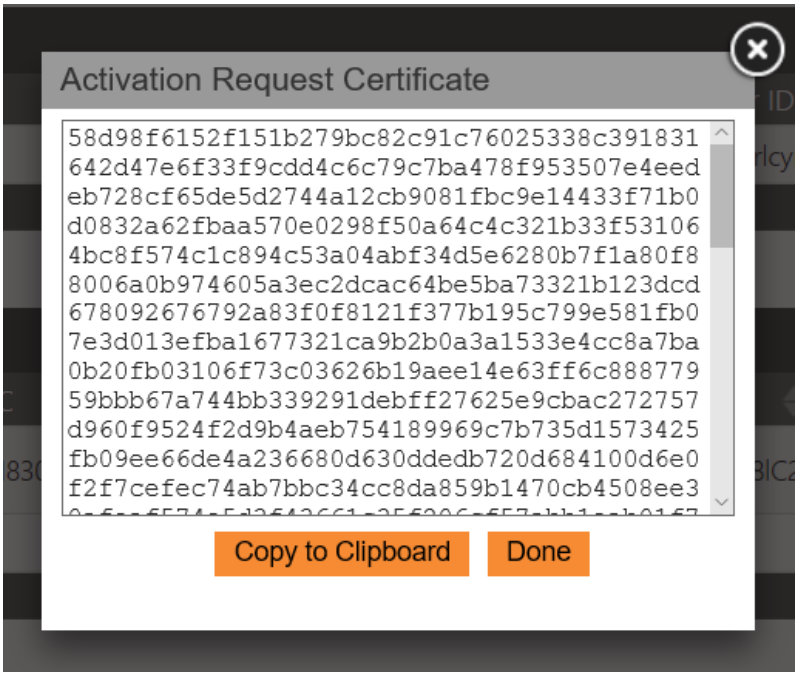
B3.1 Offline Master License Activation

The offline activation and deactivation procedures for the LAN daemon are similar to those employed for client applications. Here, the daemon is analogous to a client application.

To proceed with an offline activation, on the Master License drop-down, select the Create Activation Request item and click the orange arrow button.



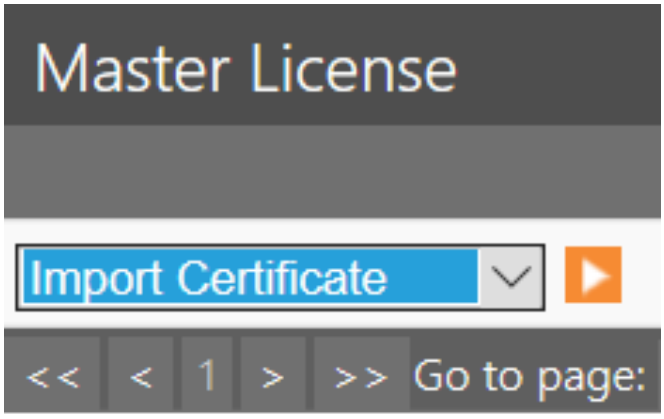
This will prompt you to enter the master license code obtained from the server as in the online case. Following this, you will be presented with an activation request certificate to be pasted into the Portal Server.



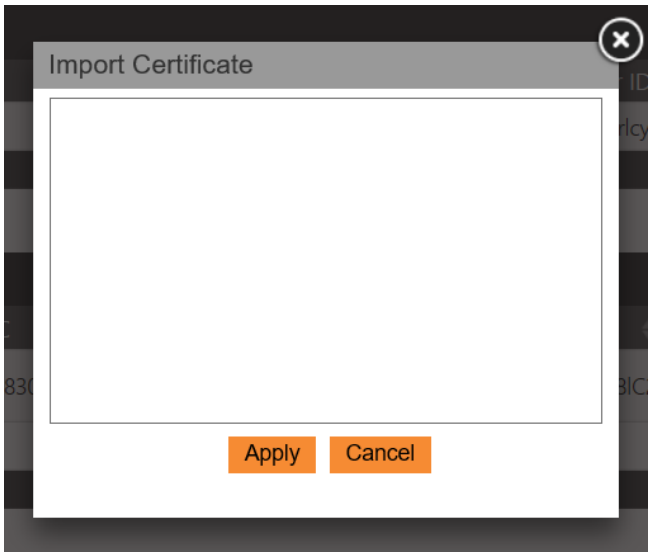
Navigate to the following website URL below, this is the license Activation/Deactivation Portal provided by PHM Technology to assist with the creation of the License and certificates.

https://www.activationportal.me/selfservice/activation.aspx?Type=1&cid=7431&pid=8841&lang=en-US

On obtaining an activation certificate from the server, go back to the Master License drop-down on the daemon, select the Import Certificate item and click the orange arrow button.



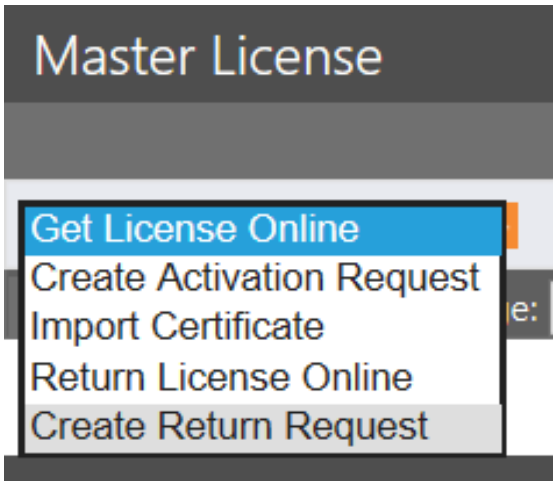
This will present you with a form in which to paste the server certificate.



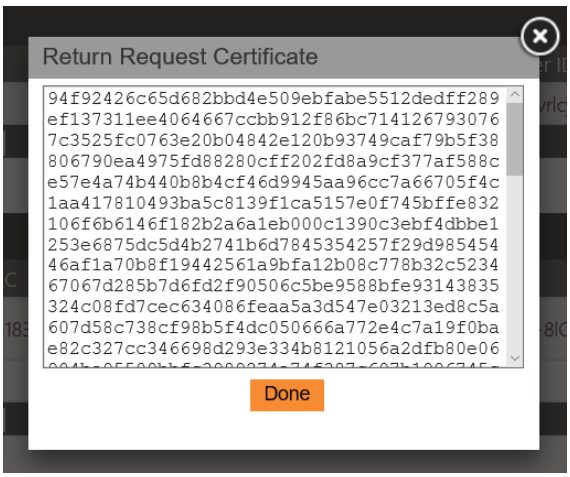
Clicking the Apply button will complete the offline activation process.

B3.2 Offline Master License Deactivation

Offline deactivation proceeds by first selecting the Create Return Request item on the master license drop-down and clicking the orange arrow.



After entering the license code, you will be presented with a Return Request certificate:

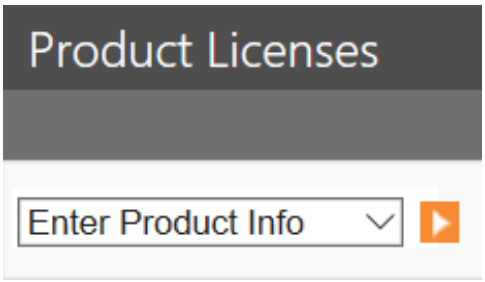


This should be pasted into the server.

This is all that is needed to deactivate the master license code. However, it can be reactivated at any time by following one of the methods described above.

B3.3 Product Setup

To set up one of your products on the daemon, on the daemon License page, go to the Product Licenses drop-down on the License page and select the Enter Product Info item.



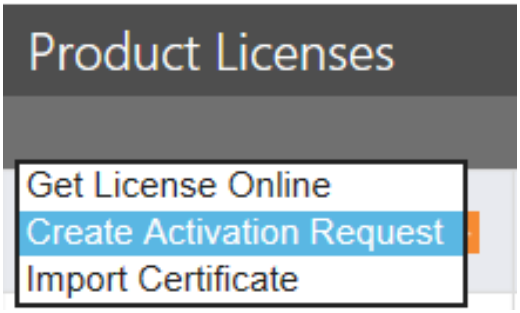
You will then be presented with a dialog to enter your Customer ID and Product ID. Enter the following information into each field respectively:

Customer ID: **5213**
Product ID: **100**

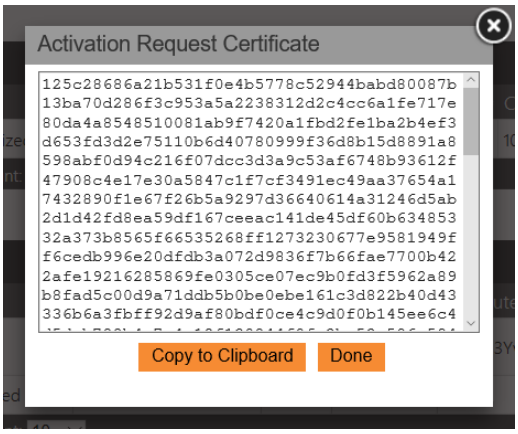
Click the Accept button to complete the product setup.

B3.4 Offline Product License Activation

For offline activation and deactivation, the steps for product licenses are similar to those of the master license. Offline activation proceeds by going to the product license drop-down and selecting Create Activation Certificate and clicking the orange arrow button as shown:



This will then prompt you for the product license code as shown above. On entering this, the activation request certificate will be generated.

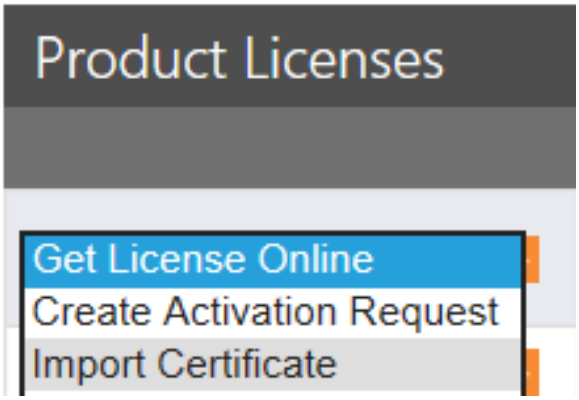


Navigate to the following website URL below, this is the license Activation/Deactivation Portal provided by PHM Technology to assist with the creation of the License and certificates.

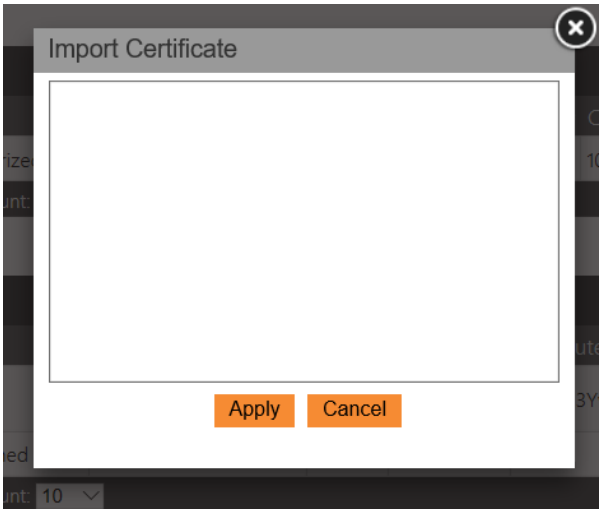
https://www.activationportal.me/selfservice/activation.aspx?Type=1&cid=7431&pid=8841&lang=en-US

This activation request certificate should be pasted into the portal and repeat the activation process.

The server will return a certificate which is used to complete the offline activation procedure on the daemon in the following way. On the product license menu on the daemon, select the Import Certificate item and click the orange button.

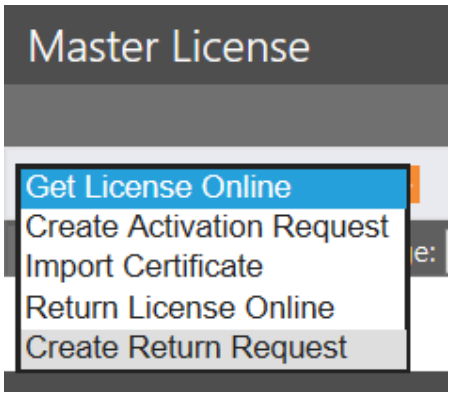


After entering the license code, you will be presented with a box in which to apply the certificate from the server. Clicking Apply will complete the offline activation procedure.



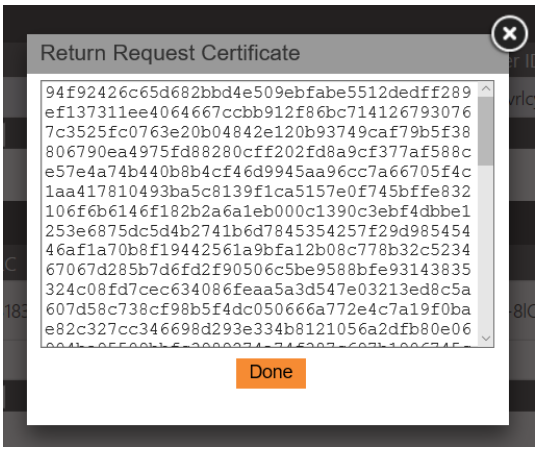
B3.4 Offline Product License Deactivation

For offline deactivation, on the Product Licenses drop-down, select the Create Return Request option.

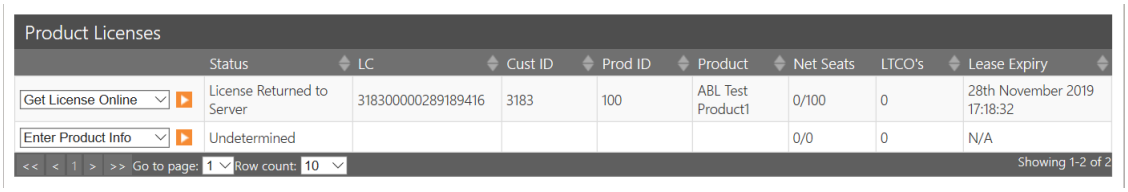


This will deactivate the product on the daemon side. It will present you with a deactivation certificate to import into the PHMT Portal to complete the process on the Zentitle server. Navigate to the following website URL to paste the certificate and complete the process.

https://www.activationportal.me/selfservice/deactivation.aspx?Type=1&cid=7431&pid=8841&lang=en-US



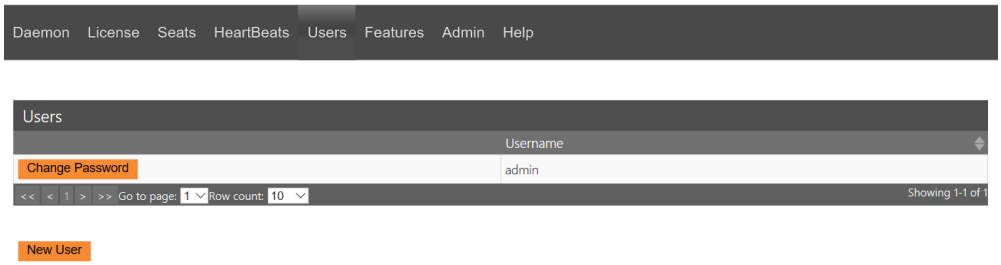
You will see in the Product Licenses section of the page that the license has been returned to the server.



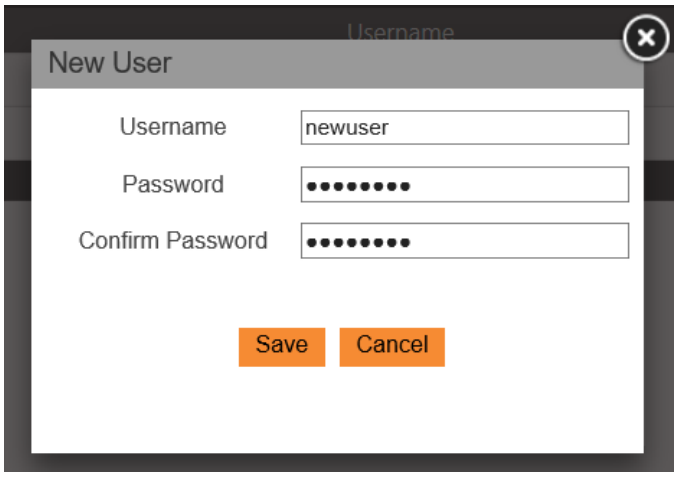
B4.0 Managing Users

On the Users page of the Zentitle daemon server, you can manage the users whose software is permitted to make use of the daemon. On installation of the daemon, there will only be one user, the admin user, who has permission to administer the daemon server and use the daemon. You may create additional users; however, they will only have the latter permission.

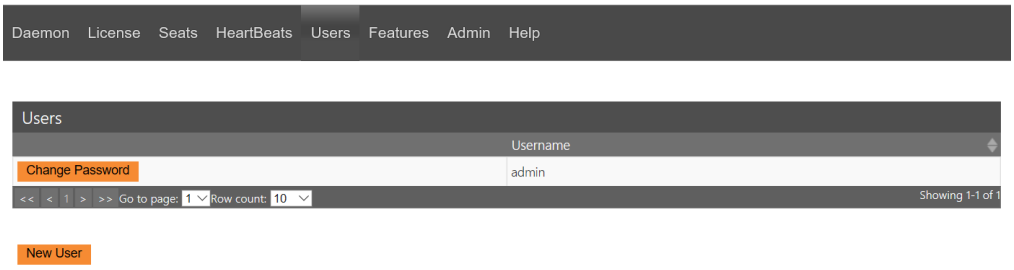
The Users page will initially have the following appearance:



Clicking the New User button will present you with a popup in which to add the credentials of your new user.



On doing so, you will see your new user added to the list.



Note that you can also delete this user by clicking the Delete User button and that the admin user cannot be deleted. The password for any user can, however, be changed. To do so click the Change password button.

END

PHM Technology
Decisions better made

9/120 Queens Parade
North Fitzroy 3068