NE-ONE™

User and Administration Guide

Revision 10

Reproduction

Warranty

All information is believed to be true and correct at time of print. Information in this document is subject to change without notice and does not represent a commitment on the part of Calnex.

Calnex makes no warranties, expressed or implied of any kind with regards to this material or its products, including the implied warranties of merchantability and fitness for a particular purpose.

Calnex shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this material or supplied products.

Please note: there are no internal serviceable parts in any equipment supplied by Calnex. Opening the hardware voids all warranties.

Trademarks

Calnex NE-ONE is a registered trademark of Calnex. Other trademarks are the property of their respective owners.

Table of Contents

Chapter 4: Installation and Configuration

Chapter 5: Ports and Services Management

Chapter 6: User Administration

Chapter 7: System Maintenance

Chapter 8: General System Procedures

Chapter 9: Creating and Running Point-to-Point Networks

Chapter 10: Creating and Running Multi-Point Networks

Chapter 13: The File Browser

Chapter 14: Using The Script Editor and Custom Code

Chapter 15: Packet Input Functions

Chapter 16: Dynamic Formulas and Network Variables

Appendix 2: Available Functions

Appendix 3: Available Link Types and Link Sub-Types

CHAPTER 1 ABOUT THIS TECHNICAL PUBLICATION

1. INTRODUCTION

This User and Administration Guide describes how to administer and use the NE-ONE, and is intended for admin user and end users.

2. ASSOCIATED DOCUMENTS

This User and Administration Guide refers to the following documents:

- *NE-ONE AWS Installation Guide*
- *NE-ONE Azure Installation Guide*

3. DOCUMENTATION CONVENTIONS

The following conventions are used in the text of this document to distinguish particular types of information:

3-1. Special emphasis in text

The following table shows the types of emphasis used to distinguish particular elements in the text of this document:

Font Convention	Identifies
Bold	Graphical user interface (GUI) elements such as buttons, tiles, panels, menu items, fields, radio buttons, check boxes, etc. Command names, variable values, field values and executables.
Italic	Document names, external references to other documents, internal references and hyper links.
`Monospace`	File names, pathnames, variable names, File contents, program output, code examples, and command line interface (CLI) examples / syntax.
`Monospace bold`	Commands and text that users are instructed to enter at the keyboard.

3-2. User interface conventions

The following conventions are used:

- All button options are represented with the word on the button in bold font.

  For example, the Next button is represented as **Next**.

  All menu options are represented with the option name in bold. For example, the Connect option is represented as **Connect**.
- When an instruction to select a menu option is given, the path to the menu option is represented with the menu options in bold typeface and each level separated by a greater than symbol (>).

  For example, to select the Open command from the File menu you will be instructed to select the **File > Open** command.

3-3. Entering and typing

Depending on the situation, you may be instructed to type or enter a command or string of text. When you are required to press the return key after typing a command or string of text, the actual command or string of text is prefixed by enter or entering. For example, in a command line interface (CLI) you are instructed as follows:

Change to the `temp` directory by entering:

```
cd temp
```

In some cases you are not required to press the return key after typing a command or string of text, for example:

- field entries in a graphical user interface (GUI)
- typing a menu option in a CLI which does not require you to press the return key.

In these cases you are instructed to type the appropriate command or string of text. For example, to specify your name in a GUI field you are instructed as follows:

Type your first name in the **First Name** field.

3-4. Mouse Buttons

It is assumed that the left mouse button is the primary one.

3-5. Definition of Notices and Notes

! Notice:

Used for instructions to the user to prevent damage to property.

Note:

Used to draw attention to information that is important for the user to know.

4. CONTACT INFORMATION

If you need to contact Calnex regarding the installation or use of the NE-ONE, please do so using the following channels:

Postal Address	Calnex Solutions plc Oracle Campus Linlithgow West Lothian EH49 7LR United Kingdom
Telephone (Calnex EMEA and other regions)	+44 (0)1799 252 200
Telephone (Calnex Americas)	+1 888-448-4366
Global support email	support@ne-one.com
Website	http://www.ne-one.com

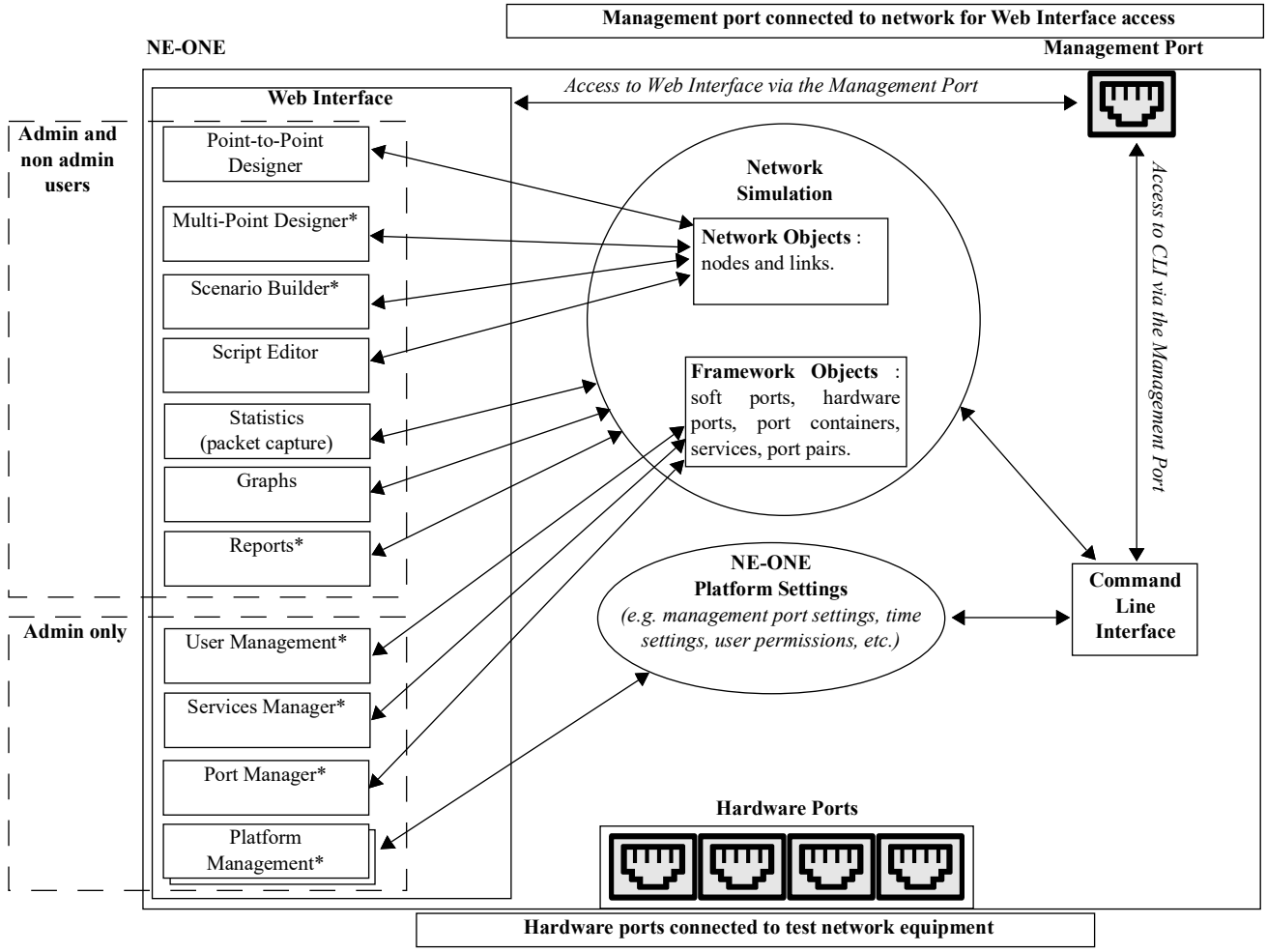
CHAPTER 2 NE-ONE OVERVIEW

1. INTRODUCTION

The NE-ONE is a flexible and easy to use network simulator letting you create Software Defined Test Networks (SDTNs) that simulate a wide range of network conditions, which can be used for testing real world applications. The NE-ONE lets you fully test your real world applications over the SDTN before deploying them in a real world network, ensuring that they are network ready for deployment into the real world. This is all done without investment in a huge array of network equipment. The NE-ONE lets you see how your applications perform both subjectively and objectively using the large number of provided graphing and reporting tools.

Illustration 1 shows a high-level functional overview of the NE-ONE. The NE-ONE has a powerful and intuitive Web Interface with different pages, allowing admin users to administer all aspects of the NE-ONE, and allowing non-admin users to create and run SDTNs for testing purposes. For more information on the user types and the roles they perform, see *User Types and Roles on page 27*.

ILLUSTRATION 1 - HIGH-LEVEL FUNCTIONAL OVERVIEW OF THE NE-ONE



Note:

Traffic cannot pass between the management port and hardware ports.

The asterisk (*) in *Illustration 1* indicates that some or all of the Web Interface is associated with a premium feature. For more information, see *Standard vs Premium Features on page 20*.

Note:

The NE-ONE also has a powerful and flexible command line interface (CLI), which can perform all the functional tasks (and more) than that of the Web Interface. This document describes only the use of the Web Interface. It is beyond the scope of this document to discuss the concepts and usage of the NE-ONE CLI.

The NE-ONE is an Appliance based solution that can be connected into an Ethernet network, supporting up to 10 Gbit/s.

The NE-ONE is supplied with two or more hardware ports and is delivered and rapidly deployed as one of the following:

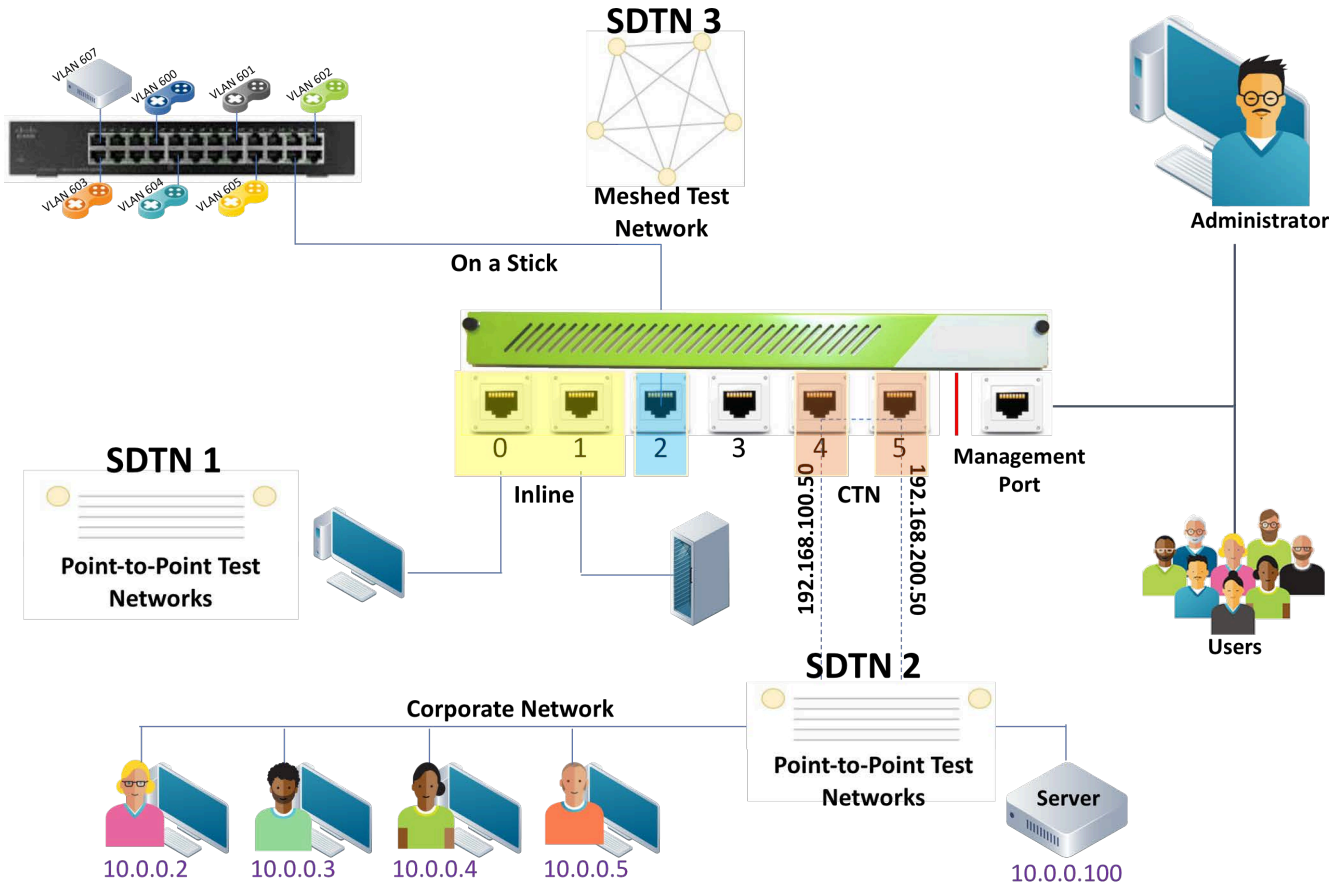
- Physical Desktop unit (which also includes an LCD panel (see *Chapter 17*, *The LCD Panel*) for quick access to certain configuration and network/scenario related operations)
- Physical a 1U rack mount system

Note:

Larger custom 2U or 5U rack mount systems (depending on exact options and ports) are available on special order. For more information, contact you Calnex sales representative.

- Virtual Appliance (supports VMWare and OpenStack).
- Cloud Appliance (supports Microsoft Azure and Amazon Web Services (AWS)).

ILLUSTRATION 2 - EXAMPLE OF RUNNING THREE SOFTWARE DESIGNED TEST NETWORKS



Some NE-ONE models support the ability for multiple users to simultaneously run independent SDTNs across different ports and port pairs, which is highly cost effective when compared to using separate dedicated appliances. *Illustration 2* shows an example of an NE-ONE with six hardware ports being used to simultaneously implement and run three different SDTNs. It is beyond the scope of this chapter to describe this implementation in detail. More detailed information of this example implementation can be found in *Implementation of SDTNs with the NE-ONE*

on page 55 in *Chapter 4*, *Installation and Configuration*.

Note:

SDTN3 in *Illustration 2* is a Fully Meshed network topology that is only available if the Multi-Point Designer premium feature activated. For more information on the different Premium features that are available, see *Standard vs Premium Features on page 20*.

Once connected, the user can easily configure a wide range of parameters, and can change these in real-time to mimic real network conditions. Timed scenarios of SDTN events can be recorded and re-run automatically. For example, timed scenarios could be created to simulate good, busy, and heavily congested network conditions so that applications can be benchmarked against each other.

Note:

Timed scenarios are only possible if the Automatic Scenario Builder premium feature activated. For more information on the different Premium features that are available, see *Standard vs Premium Features on page 20*.

1-1. Standard vs Premium Features

All entry level NE-ONEs have a standard feature set with basic user management and built-in authentication, letting you create simple Point-to-Point networks (using pre-defined port pairs), create manual scenarios, and generate standard reports.

The NE-ONE also has a payable premium feature set (summarized in *Table 1*) that can be customized according to your network simulation needs. The license on the NE-ONE determines which (if any) of the premium features are activated. For more information on the premium features and customizing your network simulation needs, contact your sales representative or Calnex sales.

TABLE 1 - NE-ONE PREMIUM FEATURES

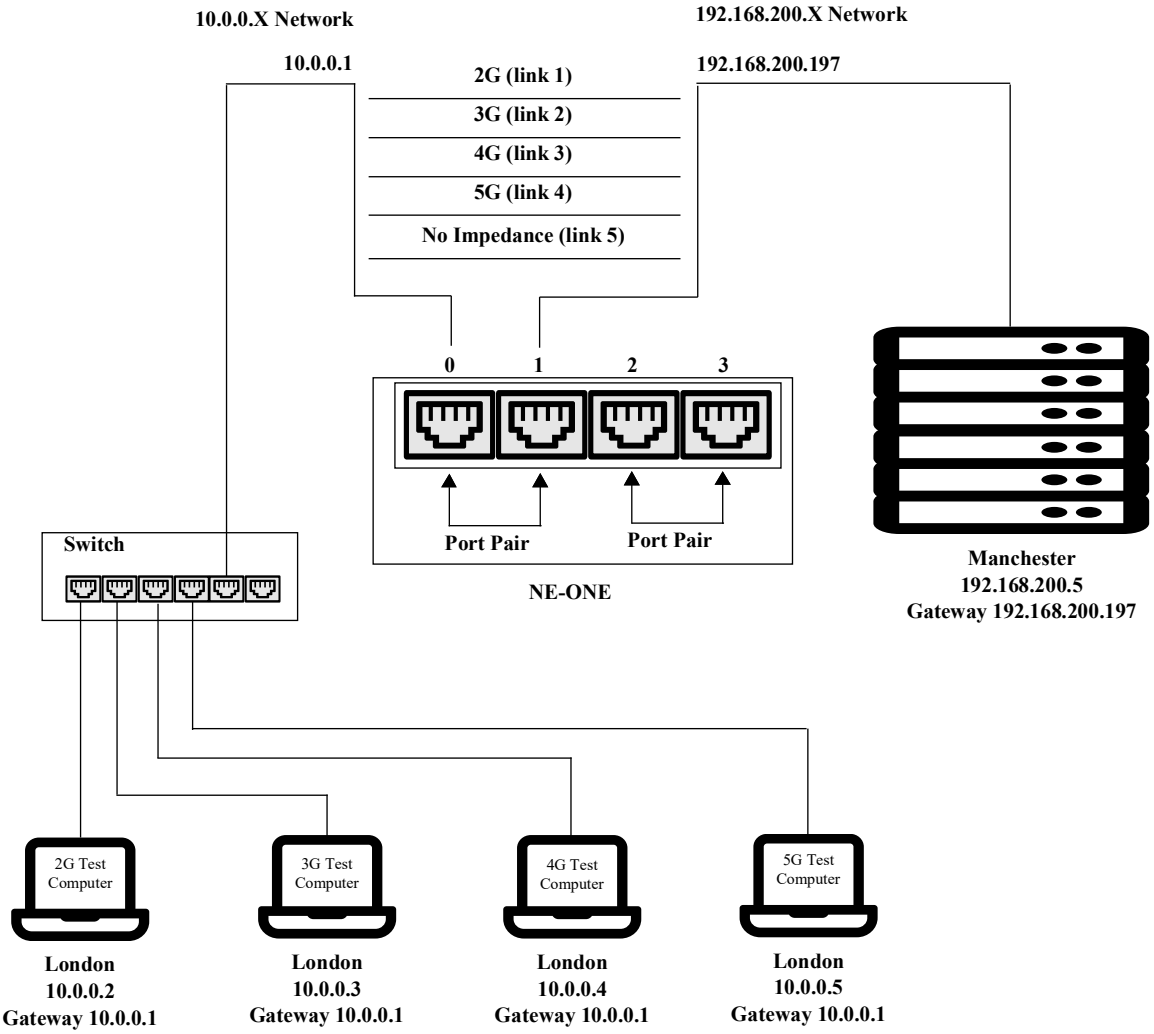
Premium Feature	Description
Automatic Scenario Builder	All NE-ONEs come with a simplistic Manual Scenario Builder (see *Illustration 7 on page 26*) that lets you quickly create a simple network experience by graphically combining two or more networks together, that can then be manually selected and run. Compared to the more sophisticated Automatic Scenario Builder, the Manual Scenario Builder has a simpler interface with only a Workspace area (i.e. no Timeline area). The more sophisticated Automatic Scenario Builder feature (see *Illustration 8 on page 27*) lets you to create a network experience over time by graphically combining two or more networks together, which can be automatically played on a Timeline. To provide a more realistic test scenario, the networks can be optionally joined together using one of three transitions.
Port Manager	An NE-ONE without the Port Manager feature comes with pre-defined port pairs allocated to the hardware ports, and the port pairs can be assigned to different users. An NE-ONE the Port Manager feature provides a diverse range of flexibility regarding the management of ports, letting you: • Create soft ports. Soft ports are very useful for port sharing in a multi user environment, and if you need a lot ports to plug test devices into, but your data rates are modest so that you can share a hardware port with a lot of test devices. For an example using soft ports in such an environment, see *Illustration 4 on page 23*. • Create and manage pre-defined port pairs. • Assign not only port pairs, but also individual ports to different users.
Service Manager	All NE-ONEs come with some in-built services such as Port Addressing and Default Transmission for simple network testing environments. The Service Manager feature lets you to create and manage additional services for more complex network testing environments, such as: • using DHCP helper services • using background port to port transmission via either the Background service or Background Expression Routed service If the Service Management feature is activated on the NE-ONE, you can create and use these services to create more complex test networks with DHCP helpers and/or background port to port transmission (either with or without complex expression routing).

Premium Feature	Description
Advanced User Permissions	All NE-ONEs come with a ability to create and manage users, and determine whether the users are admin or non-admin users. The Advanced User Permissions feature additionally lets you, define the maximum number of networks and objects available for the user, and define whether or not a user can login to the Web Interface.
Advanced Functions	All NE-ONEs come with a standard library of realistic network impairment functions letting you easily mimic what happens in real-world networks, and test your applications. Each impairment function has multiple parameters letting you customize its behavior for your specific testing needs. The Advanced Functions feature provides you with larger list of network impairment functions compared to the standard library. **Note:** The latest library of functions can be found on the Calnex website at: https://ne-one.com/ne-one-family-impairments-sheet/
Advanced Authentication (*)	All NE-ONEs come with a built-in authentication, where the authentication of users is built-in and handled locally on the NE-ONE. The Advanced Authentication feature additionally lets you configure the NE-ONE to use either LDAP or RADUIS authentication methods so that the NE-ONE can be fully integrated into the enterprise's centralized authentication system.
Application Reporting	All NE-ONEs come with a standard reporting (i.e. a Configuration Report and a Test Report) which are useful for simple reporting needs. The Application Reporting feature provides two additional report types (i.e. a general Application Report and detailed Application Performance Report) to let you easily identify whether your applications are network ready for real world implementation, giving you accurate predictions on how an application will perform over a range of latencies and bandwidths.
Multi-Point Designer	All NE-ONEs come with a Point-to-Point Designer, which lets you create Point-to-Point network topologies. The Multi-Point Designer feature lets you create more sophisticated Multi-Point network topologies using either a free-form designer or fully meshed, hub and spoke, and cloud (star) topology templates.
Defense Pack	The Defense Pack feature provides an additional Defense node category (with defense related node icons) and a TDMA Mesh (Labs) function in the Multi-Point designer. These let you create and run networks using Time Division Multiple Access (TDMA).
* - If you have the Advanced Authentication feature and use RADIUS authentication, you must also have the Advanced User Permissions feature.	

1-2. Simple Test Networks Using the Standard Features

Illustration 3 shows an example of how the NE-ONE can used to simulate a simple Point-to-Point network using the standard (i.e. non-premium) features of the NE-ONE. This example is fully described in more detail in *Creating Point-to-Point Networks (Single) on page 292* within *Chapter 9*, *Creating and Running Point-to-Point Networks*. In this case, the standard Point-to-Point Designer feature which is available on all NE-ONEs can be used to quickly create the Point-to-Point network.

ILLUSTRATION 3 - EXAMPLE POINT-TO-POINT NETWORK - 5 LINKS WITH PORT ADDRESSING



1-3. Sophisticated Test Networks Using the Port Manager and Multi-Point Designer Features

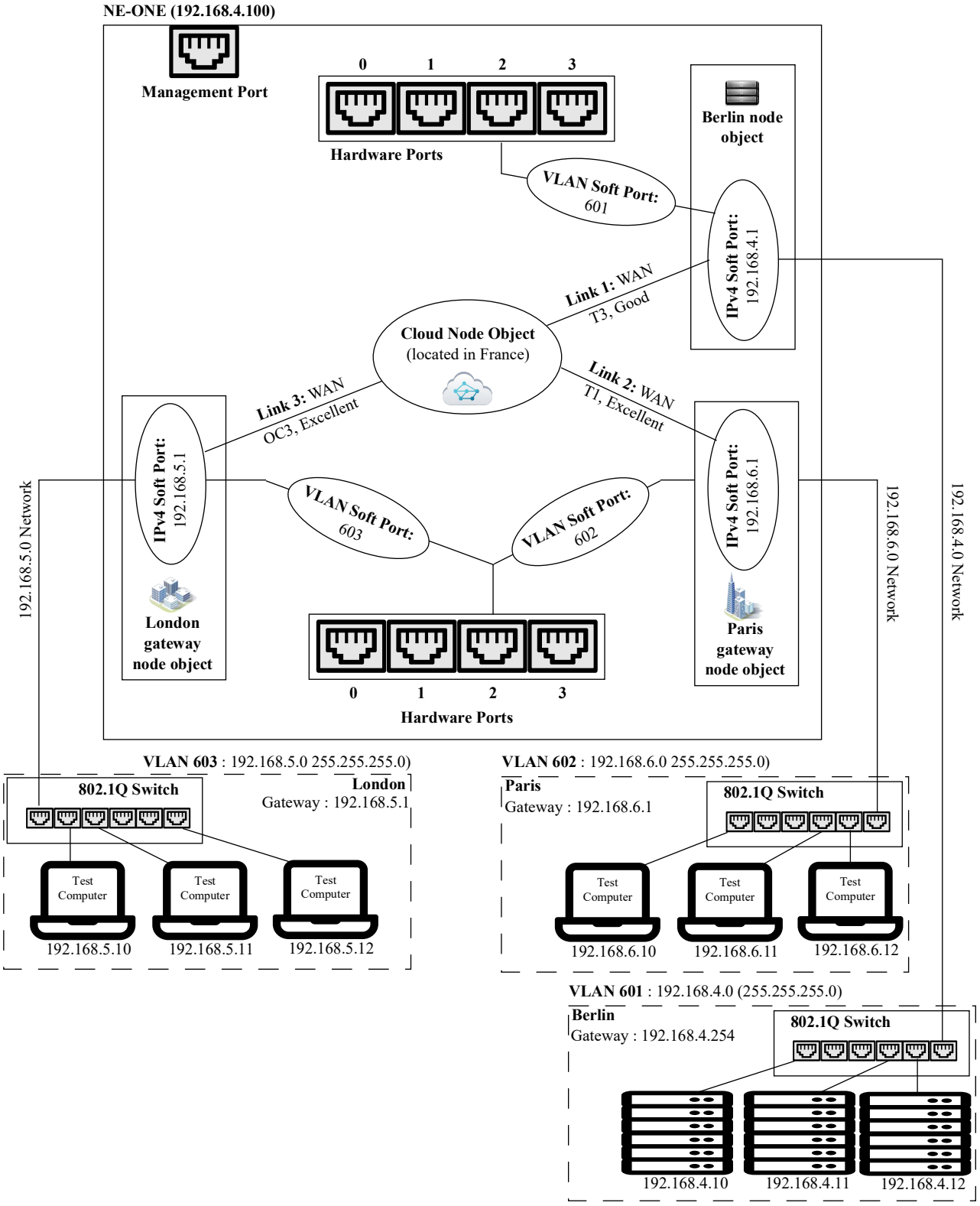
Illustration 4 shows an example of how the NE-ONE can used to simulate a cloud network for testing between different test networks with different VLANs on different networks.

It illustrates how simulations of sophisticated network environments can easily be created on the NE-ONE with the use of:

- soft ports that are only available with the Port Manager feature
- a cloud (star) topology that is only available with the Multi-Point Designer feature

This type of sophisticated network environment can only be created if the premium Port Manager and Multi-Point Designer features are activated on the NE-ONE.

ILLUSTRATION 4 - EXAMPLE OF A SIMULATED CLOUD NETWORK (WITH VLAN AND IPV4 SOFT PORTS)



In *Illustration 4*, we can see that with the use of VLAN and IPv4 soft ports, node routing functions, and cloud functions, that only one hardware port (in this case hardware port 2) is needed to connect to three test networks on three different VLANs via a simulated cloud network.

In reality, the three VLAN networks are connected to only one hardware port via a 802.1Q switch, and the simulated cloud network on the NE-ONE seamlessly filters and routes the traffic via the NE-ONE's VLAN and IPv4 soft ports, node route functions and cloud functions.

Thus, with the use of the NE-ONE's soft ports and node functions, you can easily and quickly simulate extremely large network testing environments.

2. NETWORK TYPES AND SCENARIOS

2-1. Point-to-Point vs Multi-Point Network Designers

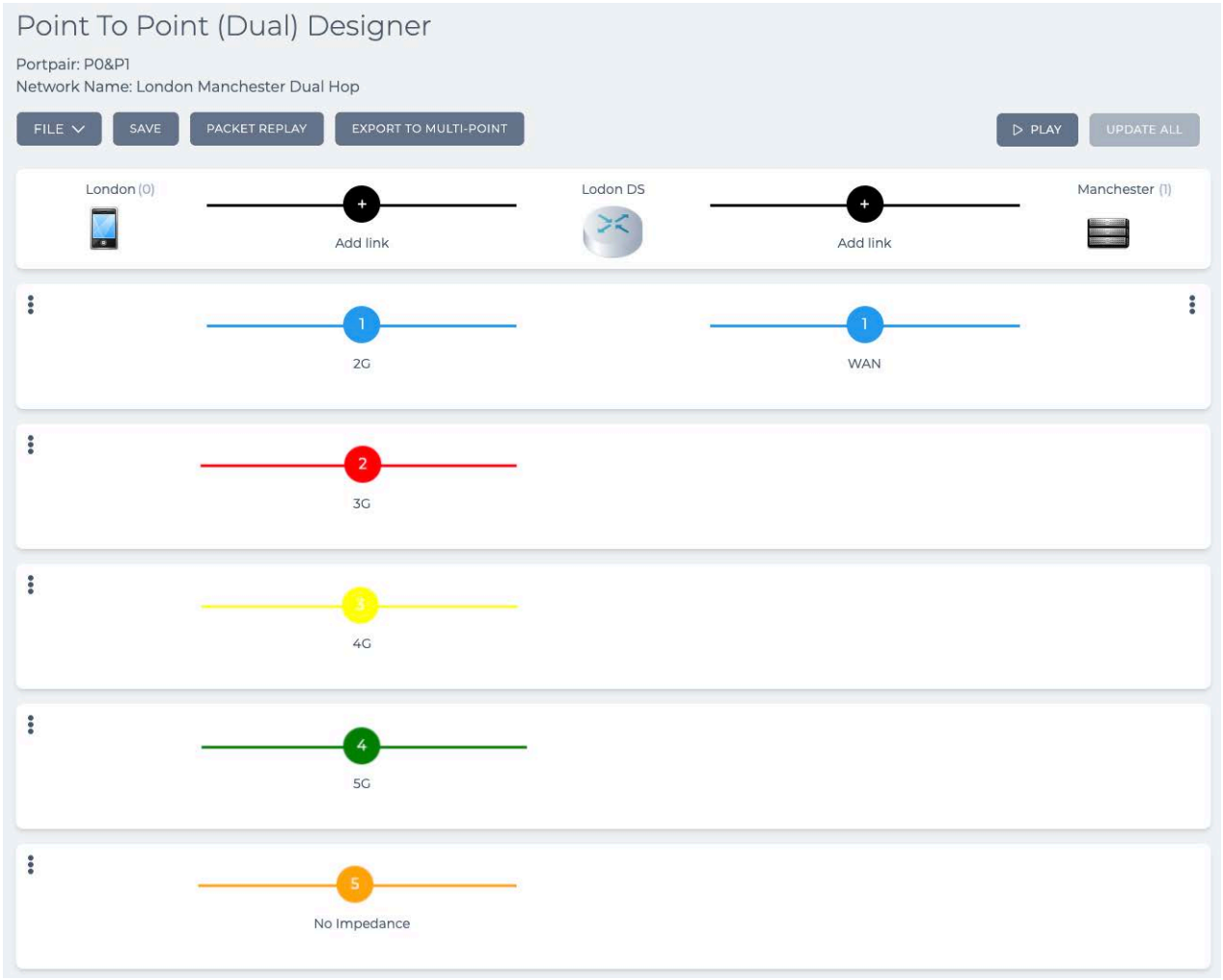
For ease of network creation, the NE-ONE distinguishes between two network topology types that can be categorized, as either Point-to-Point (including Point to Point (single) and Point to Point (dual hop)), and Multi-Point (including: Fully Meshed Hub and Spoke, Cloud (star), and Free Form).

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

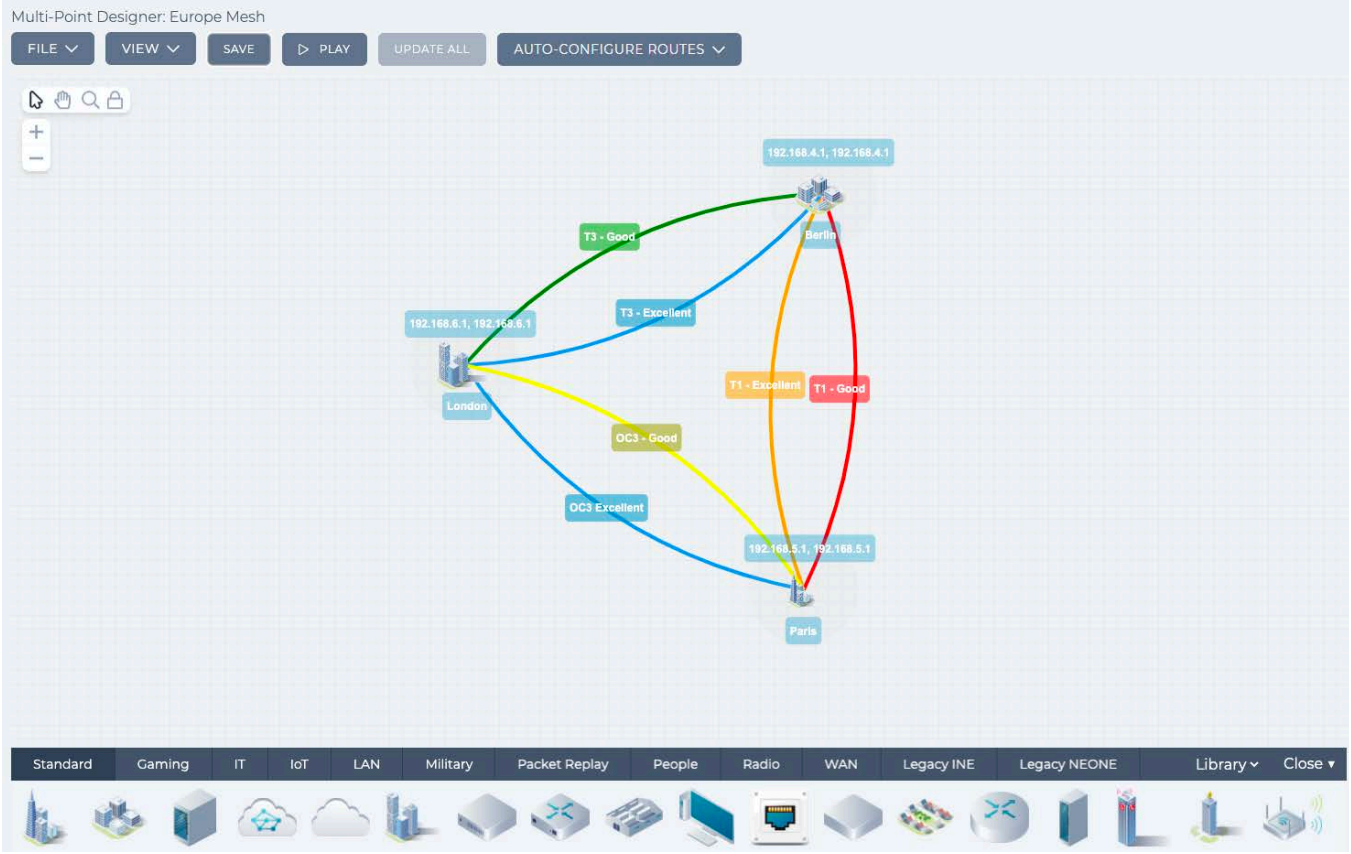
Point-to-Point networks can be rapidly created via the Point-to-Point Designer (*Illustration 5*), and assigned to port pairs, where the traffic routing is already implicitly applied to the nodes in the Point-to-Point network. All NE-ONE models support multiple links and dual hop/last mile capability.

ILLUSTRATION 5 - EXAMPLE POINT-TO-POINT DESIGNER WITH A IN A DUAL HOP NETWORK



For more complex network types, with more than two nodes, and more complex routing requirements, Multi-Point networks can be rapidly created via the Multi-Point Designer (*Illustration 6*), and complex routing can explicitly and quickly be defined. The Multi-Point Designer uses a leading edge, graphical Workspace, that lets you seamlessly create complex Multi-Point networks.

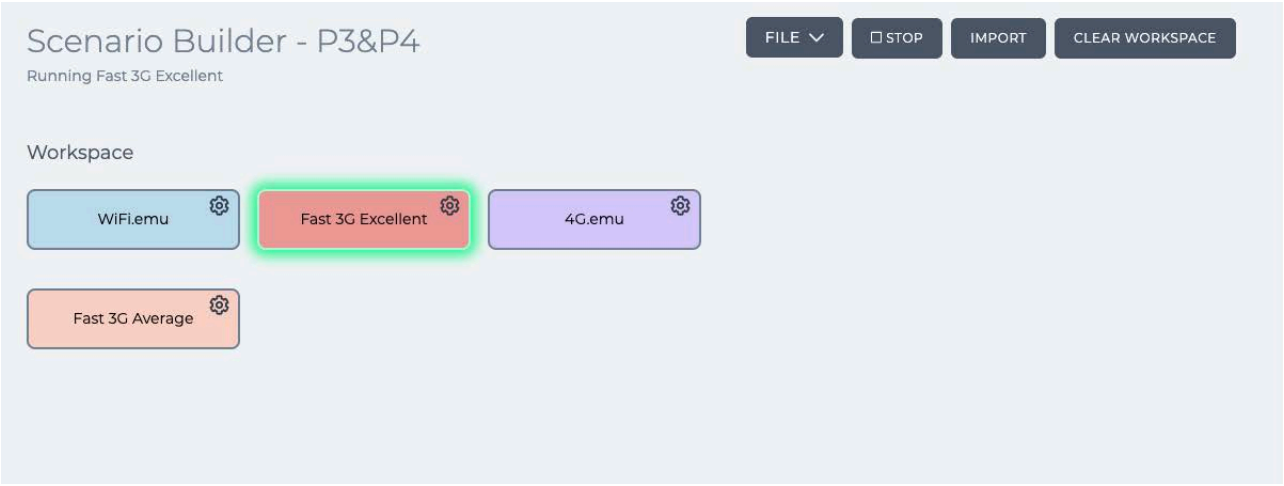
ILLUSTRATION 6 - EXAMPLE MULTI-POINT DESIGNER WITH A FULLY MESHED 3 NODE NETWORK



2-2. Manual Scenario Builder vs Automatic Scenario Builder

In addition to the Point-to-Point and Multi-Point network types, the NE-ONE's entry-level Manual Scenario Builder feature (*Illustration 7*) lets you create Point-to-Point and Multi-Point network types whose link characteristics change only with manual user intervention, and without different transition types between the change in link characteristics. These manually changing networks are know as Manual Scenarios.

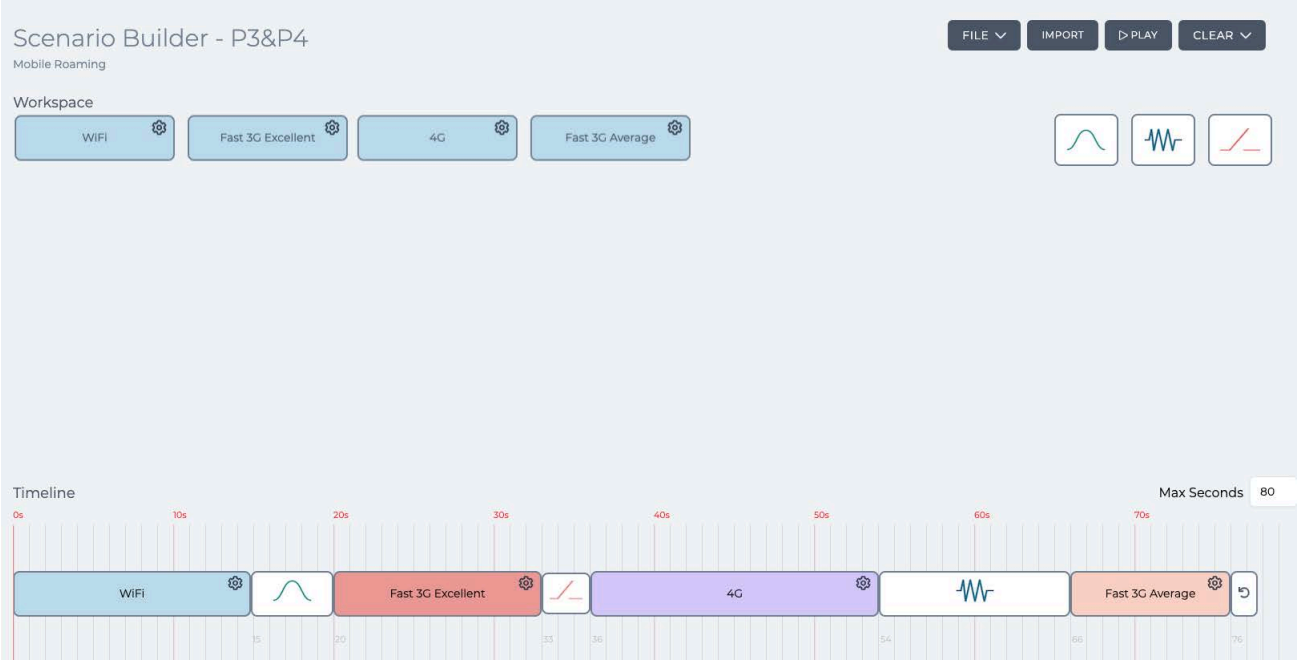
ILLUSTRATION 7 - MANUAL SCENARIO BUILDER (STANDARD FEATURE)



In addition to the Point-to-Point and Multi-Point network types, the NE-ONE's Automatic Scenario Builder feature

(*Illustration 8*) lets you create Point-to-Point and Multi-Point network types whose link characteristics dynamically change with time, and with different transition types between the change in link characteristics. These dynamically changing networks are know as Automatic Scenarios.

ILLUSTRATION 8 - AUTOMATIC SCENARIO BUILDER (PREMIUM FEATURE)



3. USER TYPES AND ROLES

The NE-ONE supports two type of user role:

- Admin user - with all rights, responsible for the following tasks:
  - Configuring and installing the NE-ONE in the company/corporate network (via the **Platform Management** pages).
  - Creating soft ports and port pairs (via the **Port Manager** pages) (if the Port Manager feature is activated).
  - Creating network services (via the **Service Manager** page) (if the Service Manager feature is activated). Thus allowing the NE-ONE to:
    - be integrated into an existing company/corporate network, and take on the routing functions if necessary,
    - act as a DHCP relay.
  - Creating users and assigning port pairs and individual ports to non-admin users (via the **User Management** pages).
  - Optionally creating and running Point-to-Point or Multi-Point networks (via the **Point-to-Point Designer** and **Multi-Point Designer** pages, respectively). Creation of Multi-Point networks is only possible if the Multi-Point Designer feature is activated.
  - Optionally creating and running scenarios (via the **Scenario Builder** page).
- Non-admin user - with limited rights (configured by an admin user), responsible for the following tasks:
  - Creating and running Point-to-Point or Multi-Point networks (via the **Point-to-Point Designer** and **Multi-Point Designer** pages, respectively). Creation of Multi-Point networks is only possible if the Multi-Point Designer feature is activated.
  - Optionally creating and running scenarios (via the **Scenario Builder** page).

- Creating reports (via the **Reports** page).
- Creating graphs (via the **Graphs** page).
- View statistics of Packet Processing Objects (PPOs) on running network simulations (via the **Statistics** pages).
- Creating packet capture files (`*.pcap`) for analysis in tools such as Wireshark.
- Monitoring live packet data for *in-situ* debug analysis of network applications in real-time.

CHAPTER 3 NE-ONE WEB INTERFACE OVERVIEW

1. ACCESSING THE WEB INTERFACE

The NE-ONE has an intuitive Web Interface, which is securely accessible using a web browser. *Table 2* summarizes the recommended web browsers that are compatible and available for use with the NE-ONE.

TABLE 2 - RECOMMENDED AND COMPATIBLE WEB BROWSERS

Web Browser**	Windows	MacOS
Safari ***	No*	Yes
Windows Edge	Yes	Not Applicable
Google Chrome	Yes	Yes
Mozilla Firefox	Yes	Yes

* - The last version (5.1.7) of Safari for Microsoft Windows is no longer maintained by Apple and is now obsolete.
** - In order for the Web Interface to function, JavaScript must be enabled on your web browser.
*** - Safari does not support named destination markers in PDF files. The context sensitive help of the Web Interface uses named destination markers within the embedded PDF file of this *User and Administration Guide*. If you want to benefit from the context sensitive help functionality, you must use either Google Chrome, Mozilla Firefox, or Windows Edge.

Your network administrator will have configured the NE-ONE so that its Web Interface is accessible on your network, and will provide you with the following access details:

- IP address and/or hostname
- Username
- Password

Note:
If your organization uses LDAP (Lightweight Directory Access Protocol) or RADIUS (Remote Dial-In User Service) authentication, the admin user will have configured the NE-ONE to use LDAP or RADIUS as its authentication method. If this is the case, simply use the same username and password that you use to login to your organization's network.

Note:
LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

Note:
Out of the box, the NE-ONE contains default factory settings that are not configured with users or your network. If you are the network/IT administrator (i.e. an admin user of the NE-ONE), the first time you use the NE-ONE you will need to know how to access the Web Interface. A leaflet is provided in the box describing how to access the NE-ONE for the first time so that it can be configured to be accessible on your network.

1-1. First time Web Interface access (accepting the default self-signed SSL certificate)

The NE-ONE's web server that hosts the Web Interface uses HTTPS (Secure Hypertext Transfer Protocol) and SSL (Secure Socket Layer) protocol.

When you try to access the NE-ONE's Web Interface over the SSL protocol, it has to identify itself with an SSL certificate to the web browser. In order for web browsers to trust the SSL certificate presented by the web server, the SSL certificate must be issued by a trusted Certificate Authority (CA). An SSL certificate that is issued by a trusted CA is called a root SSL certificate, whereas an SSL certificate that is not issued by a trusted CA will be self-signed, and is called a self-signed SSL certificate.

The default SSL certificate supplied by Calnex on the NE-ONE's web server is a self-signed one, meaning that it has not been issued by a trusted CA. Instead, the NE-ONE has signed the SSL certificate as being valid. This works fine for encrypting data, but presents you with a "privacy" or "security risk" error/warning message in your web browser the first you try to access the secure content of the Web Interface.

Note:

The NE-ONE allows an admin user to install another SSL certificate to replace the default self-signed SSL certificate supplied by Calnex. If your organization uses a root SSL certificate issued by a trusted CA, the admin user will have configured the NE-ONE with that root SSL certificate (according to *Installing and Updating Root SSL Certificates on page 84*), and you will not need to configure your web browser to accept the default self-signed SSL certificate according to the steps below.

If the NE-ONE's web server is using the default Calnex self-signed SSL certificate then the first time you access the Web Interface, you will need to configure your web browser to trust that certificate. The way in which you configure your web browser to trust the default Calnex self-signed SSL certificate varies according to the web browser and operating system that you use.

Use the appropriate section below to configure your web browser to trust the default Calnex self-signed SSL certificate:

- *Section 1-1-1, Accepting the self-signed SSL certificate on MacOS with the Safari web browser on page 30*
- *Section 1-1-2, Accepting the self-signed SSL certificate on MacOS or Windows with the Google Chrome web browser on page 32*
- *Section 1-1-3, Accepting the self-signed SSL certificate on MacOS or Windows with the Mozilla Firefox web browser on page 34*
- *Section 1-1-4, Accepting the self-signed SSL certificate on Windows with the Microsoft Edge web browser on page 35*

1-1-1. Accepting the self-signed SSL certificate on MacOS with the Safari web browser

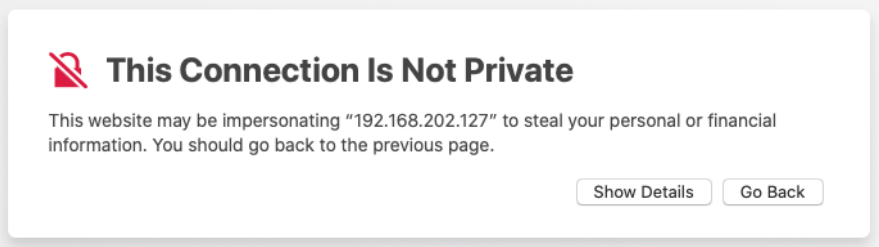
To access the Web Interface for the first time and configure the Safari web browser in MacOS to accept the self-signed SSL certificate, do the following:

1. Launch Safari, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

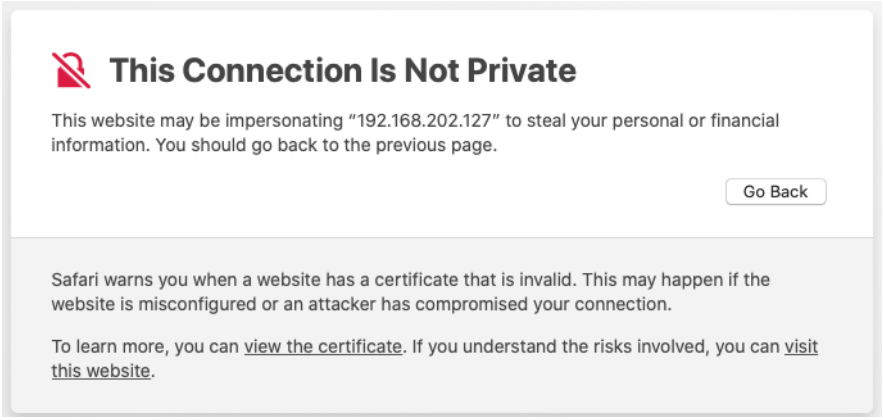
   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **This Connection Is Not Private** dialog box appears.

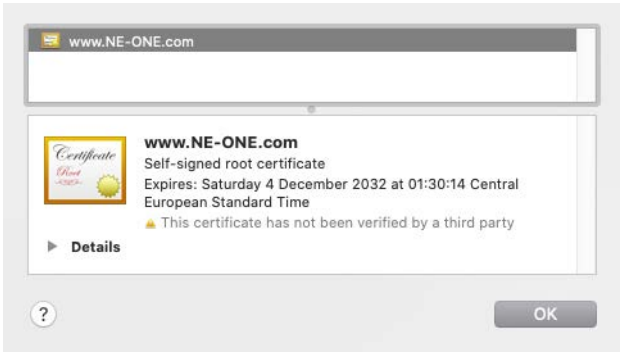


2. From the **This Connection Is Not Private** dialog box that appears, click **Show Details**.

The **This Connection Is Not Private** dialog box expands with more details.



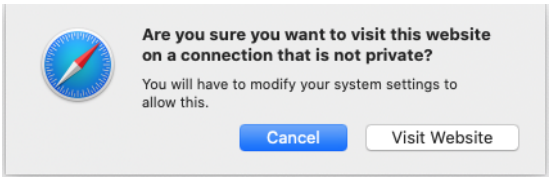
3. If you want to know when the self-signed SSL certificate expires, click the **view the certificate** link.
   A dialog box appears summarizing the details of the self-signed certificate.



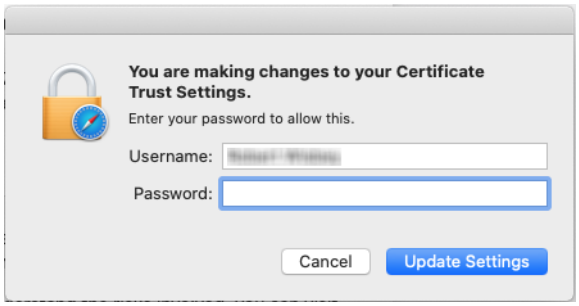
   Click **OK** to close the dialog box.

Note:
You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page on page 42*).

4. Click the **visit this website** link.
   A dialog box appears prompting you to confirm if you are sure you want to visit the website on a connection that is not private.



5. From the dialog box that appears, click **Visit Website**.
   A dialog box appears prompting you to specify your MacOS login credentials.



6. Type your MacOS username and password in the **Username** and **Password** fields, respectively. Then click **Update Settings**.

   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page on page 42*).

7. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-2. Accepting the self-signed SSL certificate on MacOS or Windows with the Google Chrome web browser

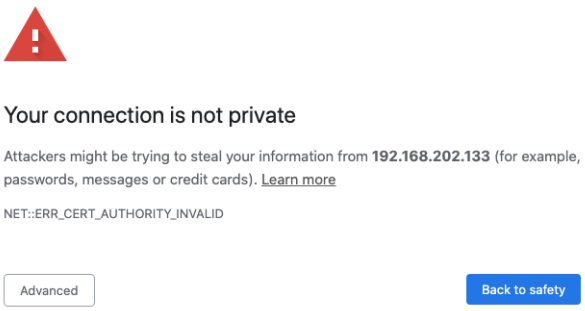
To access the Web Interface for the first time, and configure the Google Chrome web browser in MacOS or Windows to accept the self-signed SSL certificate, do the following:

1. Launch Google Chrome, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **Your connection is not private** page appears.

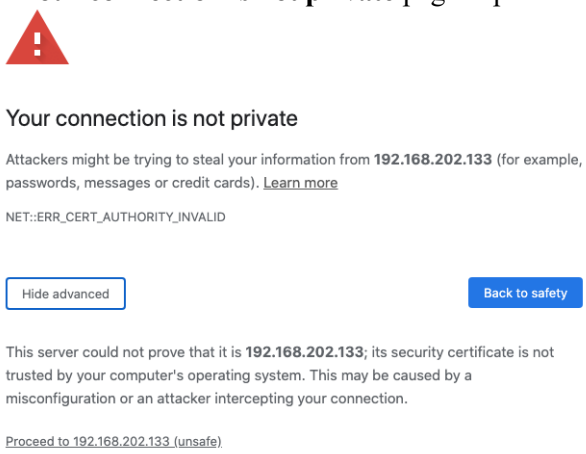


Note:

The Windows version of Google Chrome's **Your connection is not private** page contains an additional check box to help improve web security by sending URLs of some pages visited. This check box is irrelevant to this procedure.

2. From the **Your connection is not private** page that appears, click **Advanced**.

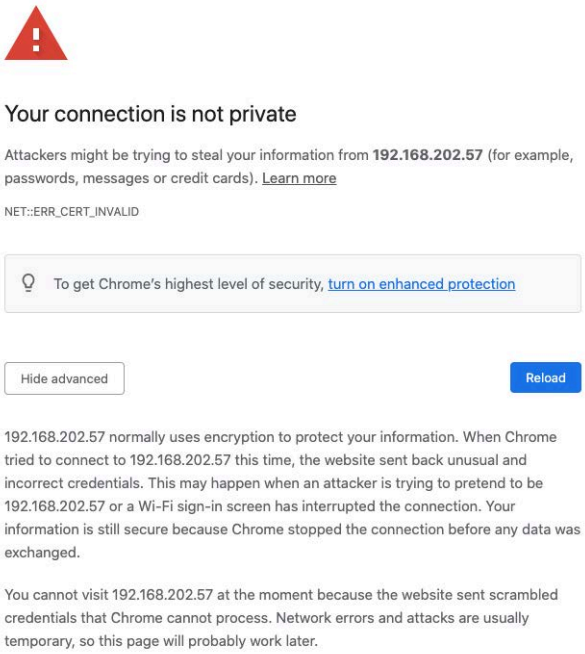
   The **Your connection is not private** page expands with more details.



3. Click the **Proceed to <IP address or hostname> (unsafe)** link.

Note:

Depending on your Chrome browser and computer's Operating System environment the **Proceed to <IP address or hostname> (unsafe)** link may not appear in the **Your connection is not private** page, and appears as follows. In this case, click within the Chrome browser on this page, and enter the following string: **`thisisunsafe`** (i.e this is unsafe, without the spaces).



The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page on page 42*).

4. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-3. Accepting the self-signed SSL certificate on MacOS or Windows with the Mozilla Firefox web browser

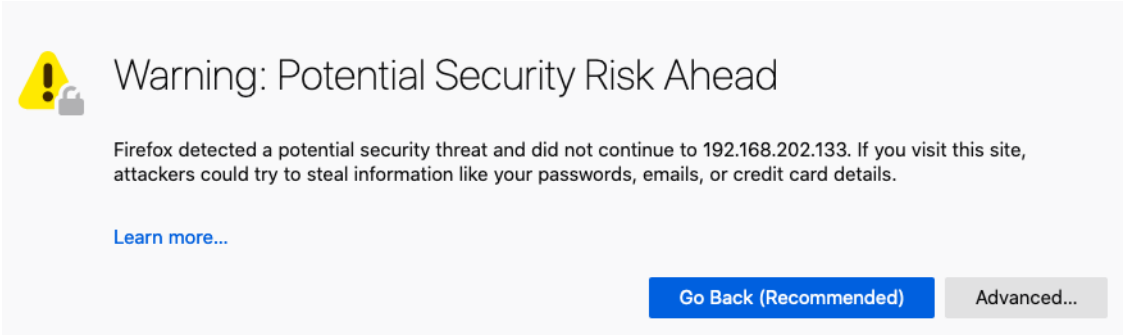
To access the Web Interface for the first time and configure the Mozilla Firefox web browser in MacOS or Windows to accept the self-signed SSL certificate, do the following:

1. Launch Mozilla Firefox, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

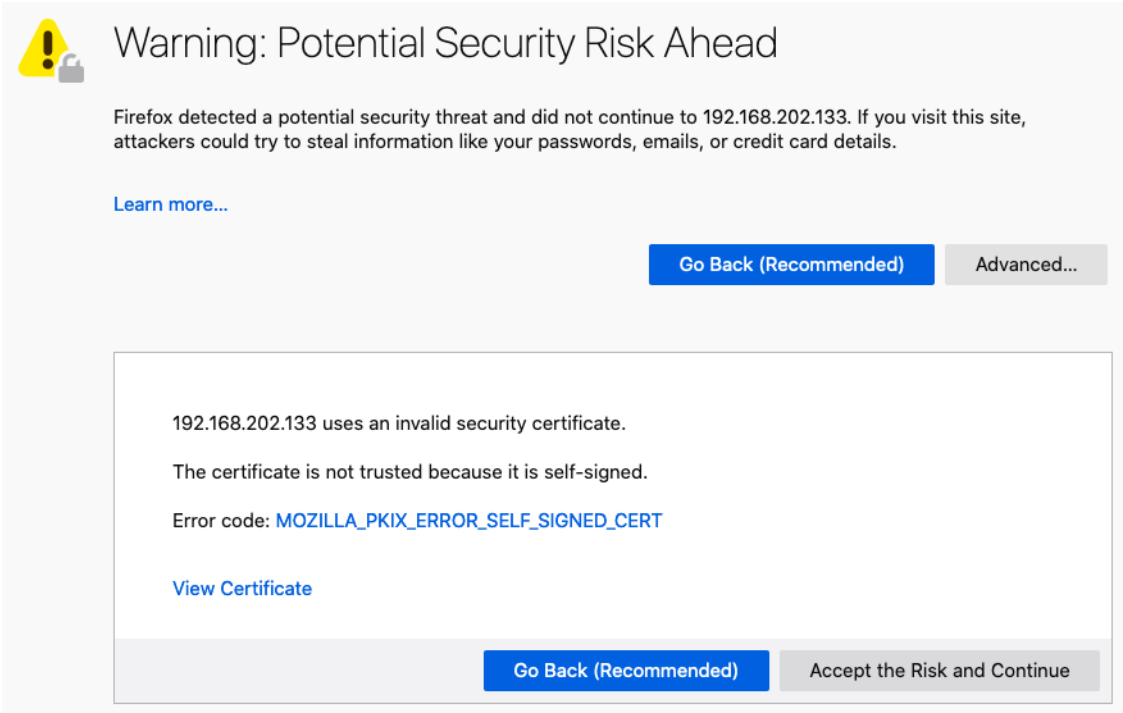
   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **Warning: Potential Security Risk Ahead** page appears.



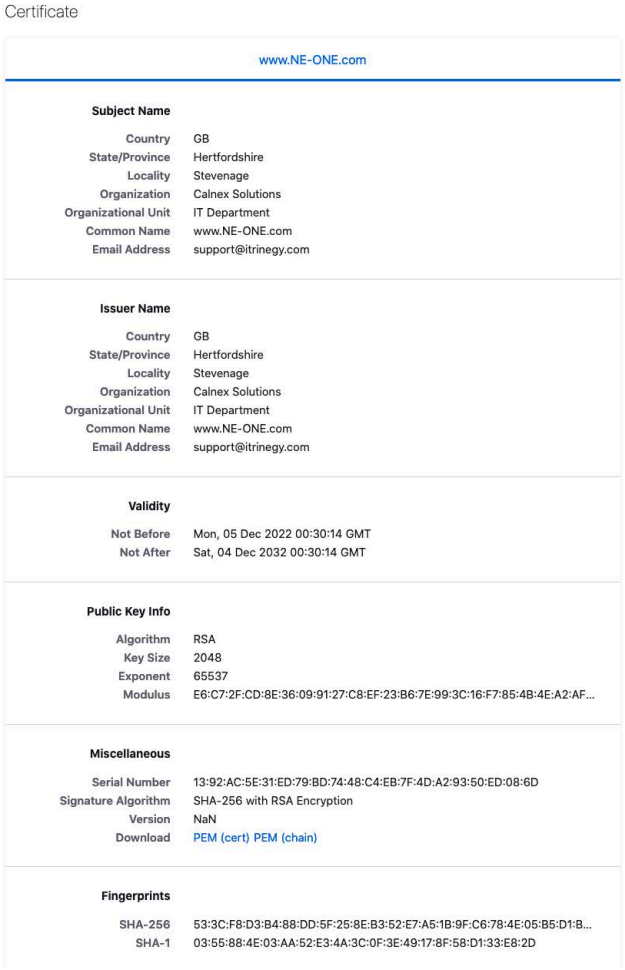
2. From the **Warning: Potential Security Risk Ahead** page that appears, click **Advanced...** .

   The **Warning: Potential Security Risk Ahead** page expands with more details.



3. If you want to know when the self-signed SSL certificate expires, click the **View Certificate** link.

A new **Certificate for www.NE-ONE.com** tab appears summarizing the details of the self-signed certificate.



Click **X** to close the **Certificate for www.NE-ONE.com** tab.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page on page 42*).

4. Click **Accept the Risk and Continue**.

   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

5. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-4. Accepting the self-signed SSL certificate on Windows with the Microsoft Edge web browser

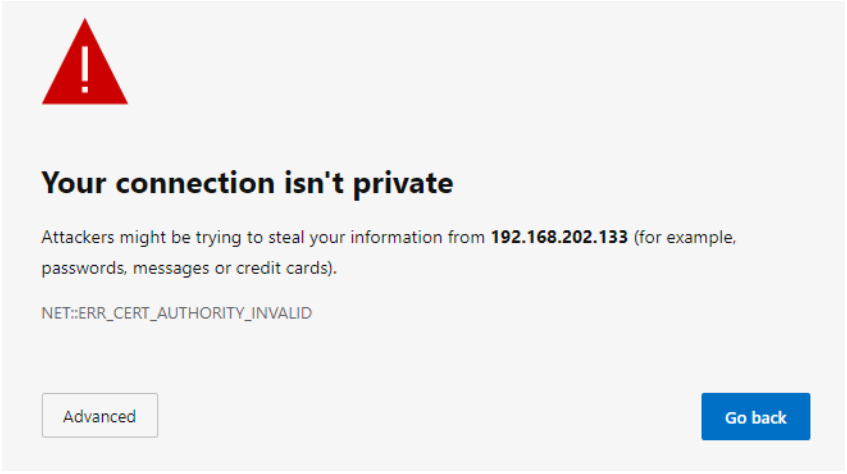
To access the Web Interface for the first time and configure the Microsoft Edge web browser in Windows to accept the self signed SSL certificate, do the following:

1. Launch Microsoft Edge, and specify the following URL in the address bar:

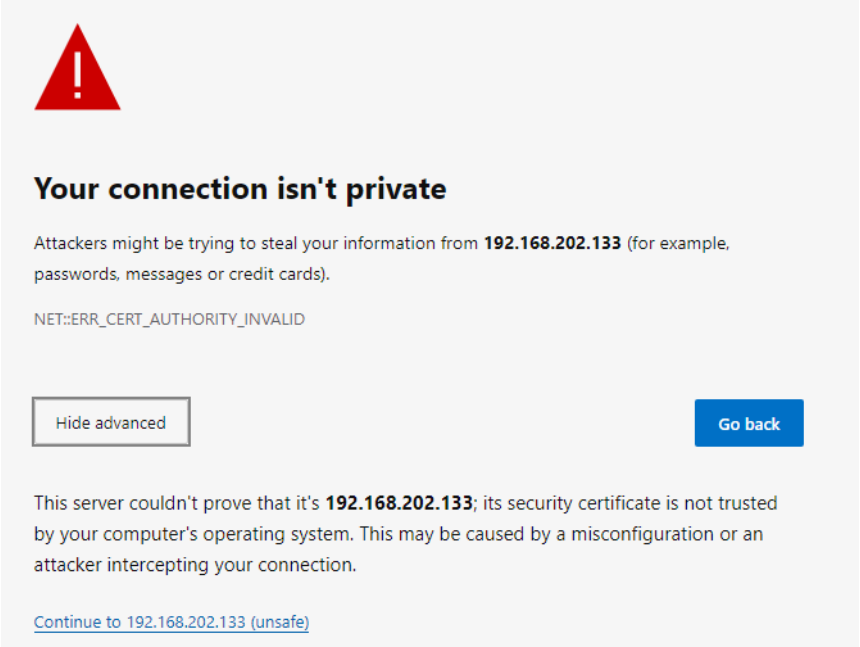
   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

A **Your connection isn't private** page appears.



2. From the **Your connection isn't private** page that appears, click **Advanced**.
   The **Your connection isn't private** page expands with more details.



3. Click the **Continue to <IP address or hostname> (unsafe)** link.
   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:
You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page on page 42*).

4. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-2. Accessing the Web Interface

Once you have configured your preferred web browser to accept the NE-ONE's self-signed SSL certificate (see *First time Web Interface access (accepting the default self-signed SSL certificate) on page 29*) or if the NE-ONE is configured with your organization's root SSL certificate, you can access the Web Interface directly, without needing to take additional configuration steps. Use the following steps to access and log in to the Web Interface:

1. Launch your preferred web browser, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A login page appears.

Note:

The login page above is the generic one supplied with the NE-ONE. The appearance of the login page may vary it if has been personalized by an admin user according to *Personalizing the Login Page on page 73* in *Chapter 4*, *Installation and Configuration*.

2. From the login page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

   Upon successfully logging in, you are presented with the Web Interface (see *Web Interface Layout on page 38*).

Note:

If you are logging in as the built-in local (built-in) admin user for the first time or after the admin user password has been reset, you will be promoted to change the default password before being presented with the Web Interface. For more information, see *Changing the Default Admin Password on page 64* in *Chapter 4*, *Installation and Configuration*.

Note:

If you are logging in for the first time you must accept the Calnex terms and conditions before using the NE-ONE's Web Interface.

Note:

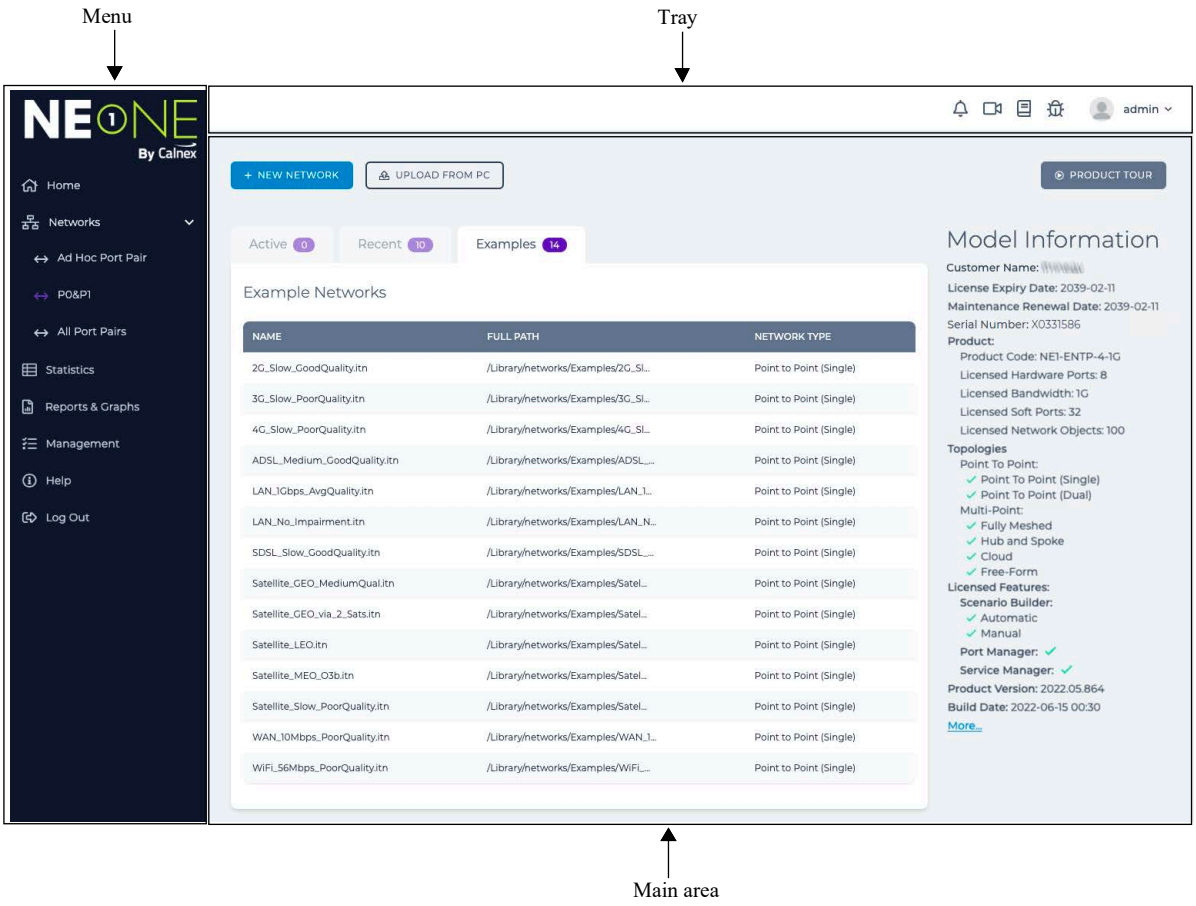
If your organization has an Audit and Compliance policy your admin user will have applied a customized User Acceptance Document according to *Applying a Compliance and Audit Acceptance Agreement on page 75* in *Chapter 4*, *Installation and Configuration*. In this case, each time you login to the NE-ONE you must accept the terms and conditions of your organization's User Acceptance Document before using the NE-ONE's Web Interface.

2. WEB INTERFACE LAYOUT

Illustration 1 shows the layout of the Web Interface, which comprises the following three elements:

- Menu — contains different menu items that give you access to all functions to manage the NE-ONE. Clicking on a menu item updates the main area of the Web Interface with a corresponding page. For more information, see *The Web Interface Menu on page 39*.
- Tray — contains network/scenario status icons, notification icons, on-line help icons, and user drop-down menu. For more information, see *The Web Interface Tray on page 40*.
- Main area — updates with different pages according to the menu item you selected, or according to other actions you have taken within the different pages.

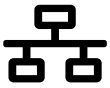
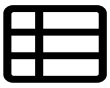
ILLUSTRATION 1 - NE-ONE WEB INTERFACE LAYOUT



2-1. The Web Interface Menu

The Menu provides a quick way to access all the functions on the NE-ONE. *Table 3* summarizes each of the Menu items.

TABLE 3 - MENU ITEMS

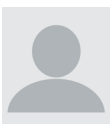
Menu Item	Menu Icon	Description
Home		Opens the **Home** page from where you can create new networks, edit existing networks and scenarios, and view your NE-ONE model information. For more information, see *Home Page on page 42*.
Networks		Opens the **Network** page, from where you can create, and edit (if they already exist) networks and scenarios. For more information, see *Networks Page on page 44*.
		If port pairs have been created by an administrator and assigned to another user (see *Creating Port Pairs on page 170* and *Configuring and Editing User Permissions (for Built-in and LDAP authentication) on page 217*), they are listed as sub-items underneath the **Networks** menu item if the user has starred (favorited) the port pair (see *Creating "Starred" Port Pair Favorites on page 256*). Clicking on a port pair opens the **Network Port Pair** page, from where you can do the following for the selected port pair: • create, and edit (if they already exist) networks and scenarios • edit the port settings (i.e. port addressing and default transmission) For more information, see *Network Port Pair Page on page 45*.
Statistics		Opens the **Statistics** page (see *Illustration 171 on page 567*), which is the central location listing the statistics of the following objects from where you launch packet capture or data graphing for an object: • network objects (i.e. links and nodes) associated with any currently active (running) networks • framework objects (i.e. hardware port, soft port, port container, or service) For more information, see *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing on page 565*.
Reports & Graphs		Opens the **Reports And Graphs** page (see *Illustration 178 on page 594*), from where you can do the following: • create graphs (see *The Graphs Page on page 594*) • generate reports (see *The Reporting Page on page 606*) • view historical statistics (see *The Historical Statistics Pages on page 603*) For more information, see *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing on page 565*.
Management		Opens the **Management** page, from where you can drill down further in order to manage all aspects of the NE-ONE. The management functions that are available vary according to your user profile type (admin or user). For more information, see *Management Page on page 48*.
Help		Opens the **Help** page, from where you view the embedded online documentation and videos, request support, and view the EULA agreement.
Log Out		Logs you out of the Web Interface and returns you to the **Login to your account** page.

2-2. The Web Interface Tray

The Web Interface Tray (see *Illustration 2* and *Table 4*) provides quick access to user centric functions, system notifications, context sensitive on-line help, and a quick access and status area for running and open (i.e. work-in-progress) networks/scenarios.

ILLUSTRATION 2 - THE WEB INTERFACE TRAY

TABLE 4 - WEB INTERFACE TRAY ICONS AND ELEMENTS

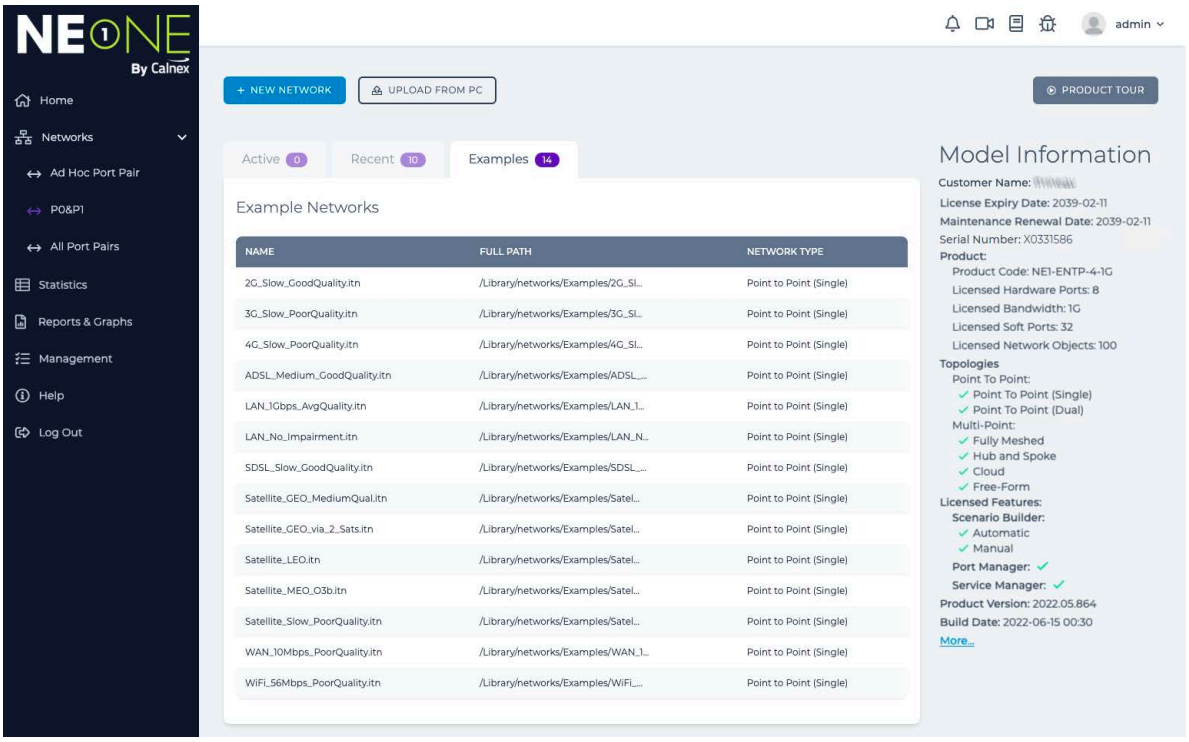
Tray icon or element	Description
	Only visible if a network or scenario is open, stopped and currently being created or edited. Clicking on this icon opens the currently work-in-progress network/scenario in the Main area, letting you continue to edit it and once finalized, run (play) it. Placing your mouse on this icon results in mouse over text appearing with the name of the network/ scenario. Right mouse clicking on this icon reveals a **Close** pop-up menu, which upon selecting will close the network/scenario.
	Only visible if a network or scenario is currently running. Clicking on this icon opens the currently running network/scenario in the Main area, letting you stop running (playing) it for editing or launch graphs. Placing your mouse on this icon results in mouse over text appearing with the name of the network/ scenario. Right mouse clicking on this icon reveals a **Close** pop-up menu, which upon selecting will close the network/scenario. The running network/scenario will continue running, and be listed in the **Active** tab of the **Home** page. **Note :** A running network or scenario is attached to the user who initially ran it. This icon only visible during the current login session for the user who run a network or scenario. This icon not visible if: • the user's Web Interface session closes and the same user logs back in • the same user logs out and logs back in to the Web Interface later on • if a different user logs in to the Web Interface
	The **View More** drop-down menu icon. Only visible if more than a total of six networks/scenarios are open, letting you select the additional (from the seventh onwards) open networks/scenarios.
	Displays the username of the currently logged in user. Contains the following menu items: • **Change Password** — opens a **User Profile** page allowing the logged in user to update their password. For more information, see *Changing Your User Password via the Tray User Menu on page 254* in *Chapter 8*, *General System Procedures* **Note :** The **Change Password** menu item is only visible if the NE-ONE uses the built-in authentication method. If the NE-ONE is configured with LDAP or RADIUS authentication, the **Change Password** menu item will not be visible as the user passwords will be managed by the organization's Directory Access servers. • **Change Language** — opens a **Choose language** dialog box allowing the logged in user to set the language displayed in the Web Interface. For more information, see *Setting the Web Interface Language via the Tray User Menu on page 254* in *Chapter 8*, *General System Procedures*. • **Log Out** — allows the existing logged in user to log out of the Web Interface.

Tray icon or element	Description
	Opens a context sensitive help video (in a separate browser tab) that describes the use of the page that is currently open.
	Opens in a separate browser tab, context sensitive help documentation from the embedded PDF file of the *User and Administration Guide*, describing the use of the Web Interface page that is currently open. **Note :** Safari does not support named destination markers in PDF files. The context sensitive help of the Web Interface uses named destination markers within the embedded PDF file of this *User and Administration Guide*. If you want to benefit from the context sensitive help functionality, you must use either Google Chrome, Mozilla Firefox, or Windows Edge.
	Opens a **Report a Bug** page letting you submit a bug report to the technical support team at Calnex.
	Opens the **System Notifications** page, from where you can view a chronological list of system level events, categorized by event type. For more information, see *Viewing System Notifications on page 257* in *Chapter 8*, *General System Procedures*. **Note :** The **System Notifications** page can also be opened via the **Management** page.
	Opens the **Live Packet Monitoring** page, from where you can monitor live packet data for any Packet Processing Objects (PPOs) that you have chosen to be added (pinned) to this page. For, more information, see *The Live Packets Dialog Box and the Live Packet Monitoring Page on page 581* in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note :** By default, initially no PPOs are being monitored, and this icon is not visible. Once one or more PPOs have been added (pinned) to the **Live Packet Monitoring** page, this icon becomes visible in the Tray.

3. HOME PAGE

The **Home** page (see *Illustration 3*) appears immediately after logging in to the Web Interface, or after clicking **Home** from the Menu.

ILLUSTRATION 3 - HOME PAGE



The **Home** page lets you quickly:

- create new networks based on existing network templates via the **Examples** tab
- view and if necessary edit recently created networks via the **Recent** tab
- view currently active networks via the **Active** tab.

Note:

Initially when the NE-ONE contains no user created networks, the **Recent** tab and **Active** tab are empty, and upon logging in, the **Home** page defaults to showing the **Examples** tab. This lets you quickly create new networks based on the network templates supplied with the NE-ONE. As networks are open (i.e. created or edited) and run, they are listed in **Recent** tab and **Active** tab, respectively. Once a user created network exists on the NE-ONE, upon logging in the **Home** page defaults to showing the **Recent** tab.

Note:

Existing networks can also be opened, edited, and launched via the File Browser. For more information, see *Opening and Playing Networks and Scenarios via the File Browser on page 642* in *Chapter 13*, *The File Browser*.

The **Home** page also lets you:

- launch the **Network** page by clicking on the **+ NEW NETWORK** button
- launch a useful product tour video by clicking on the **PRODUCT TOUR** button
- upload a network file or scenario file from your local PC to your `/Private/networks` directory by clicking on the **LOAD FROM PC** button

The **Model Information** section of the **Home** page also immediately provides you with the following useful

product licensing and system build information:

- NE-ONE product code, which has the following format:

  NE1-<Edition>-<Licensed Hardware Ports>-<Maximum Bandwidth>

  where:

  - <Edition> is the NE-ONE edition type (this will vary according to the feature set that was sold to you by your sales representative).
  - <Licensed Hardware Ports> is the number of licensed Hardware ports available for use.
  - <Maximum Bandwidth> is the maximum bandwidth permitted on the fastest port of the group of licensed Hardware ports. For example, if an NE-ONE has two 1 Gigabit/s Hardware ports and two 10 Gigabit/s Hardware ports, the maximum permitted bandwidth displayed is 10G.
- Maximum number of licensed Network Objects (i.e. packet processing objects).
- Maximum number of licensed links.

  Note:

  If your NE-ONE is licensed with an unlimited number of links, the line showing the number of licensed links is not present.
- Number of licensed Hardware ports.
- Number of licensed Soft ports.

  Note:

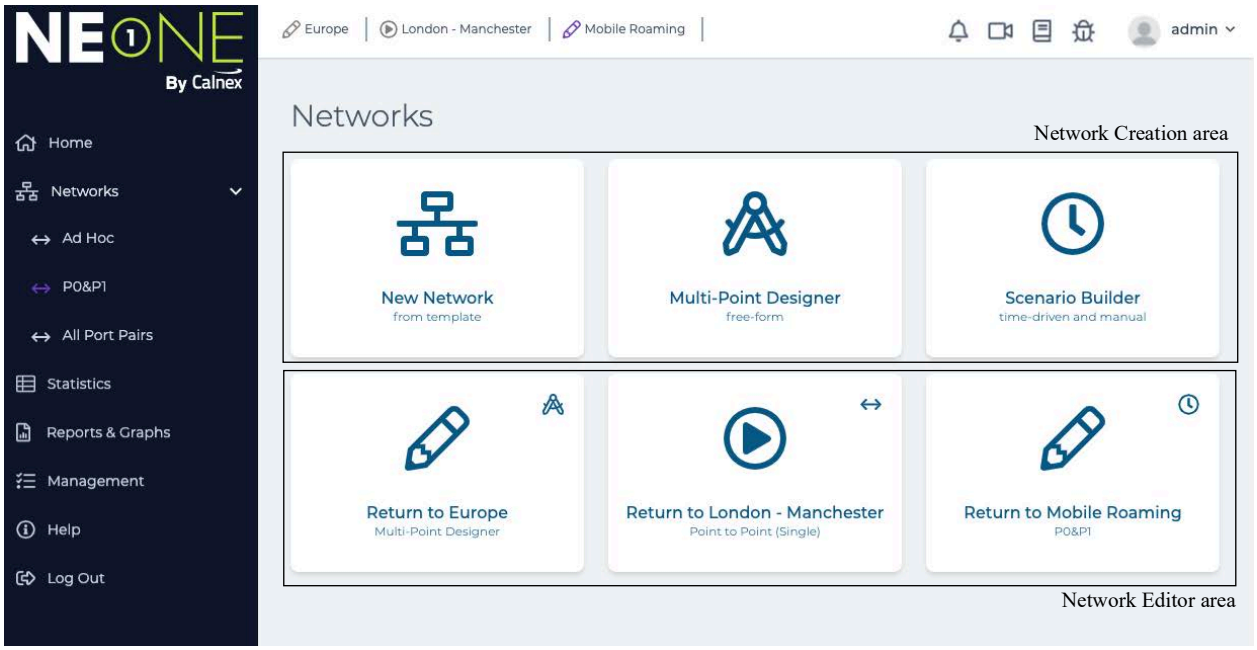
  If your NE-ONE is not licensed to use the Port Manager feature, the line showing the number of licensed Soft ports is not present.
- License expiry date (once the license has expired, the Web Interface remains accessible).
- The maximum bandwidth permitted on the fastest port of the group of licensed Hardware ports. For example, if an NE-ONE has two 1 Gigabit/s Hardware ports and two 10 Gigabit/s Hardware ports, the maximum permitted bandwidth displayed is 10G.
- The product version, which has the following format: **<Year>.<Month>.<Incremental Build Number>**.
- Maintenance renewal date — once the maintenance renewal date has passed the NE-ONE remains fully functional. However, for unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date.
- Serial number - the serial number of the NE-ONE.
- The Scenario Builder feature licensing information, indicating whether or not the Manual and Automatic Scenario Builder features are licensed.
- The system build date of the following format: **<Year>:<Month>:<Day> <Hour>:<Minute>**.
- Port Manager licensing information, indicating whether or not the Port Manager feature is licensed.
- Service Manager licensing information, indicating whether or not the Service Manager feature is licensed.
- A **More...** link, which takes you to **License** page letting you manage the license on the NE-ONE. For more information, see *Viewing and Applying License Files on page 86*.

4. NETWORKS PAGE

The **Networks** page (see *Illustration 4*) appears after clicking **Networks** from the Menu, and contains the following two areas:

- Network Creation area
- Network Editor area

ILLUSTRATION 4 - NETWORKS PAGE



The network creation area of the **Networks** page lets you do one of the following:

- Launch the Network Wizard using predefined network topology templates.

  Clicking on the **New Network** tile opens the Network Wizard page which lets you create a network based on one of the different network topology templates.

  - For more information, see *The Network Wizard Page (From a Point-to-Point Perspective) on page 266*, in *Chapter 9*, *Creating and Running Point-to-Point Networks*.
  - For more information, see *The Network Wizard Page (from a Multi-Point Perspective) on page 336*, in *Chapter 10*, *Creating and Running Multi-Point Networks*.

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

- Launch the Free Form **Multi-Point Designer** page.

  Clicking on the **Multi-Point Designer** tile opens a **Network Name** dialog box that prompts you to specify a new network name. Once you have specified and confirmed the new network name, the main area of the Web Interface updates with **Multi-Point Designer** page (in Free Form), from where you can create networks of any network topology.

- Launch the Scenario Builder.

  Clicking on the **Scenario Builder** tile opens the Scenario Builder page, which lets you either load, run, and stop an existing scenario, or create a new time based scenario (combination of networks with transitions).

The network editor area of the **Networks** page lists all the networks and scenarios that are open (i.e. either stopped for editing/creation ( )) or playing ( ). Each open network and scenario is represented by a tile, which has the following layout:

- the bottom of the tile displays the name of the network/scenario
- the middle of the tile displays a status icon for the open network/scenario, as follows:
  - represents stopped for editing/creation
  - represents currently playing
- the top right of the tile displays an icon representing the network or scenario type, as follows:
  - represents a Point-to-Point type network
  - represents a Multi-Point type network
  - represents a scenario

Note:

Initially when the NE-ONE has no open or playing networks or scenarios, the Network Editor area is empty. As networks or scenarios are opened (edited or being created) or running, they are listed in the Network Editor area of the Web Interface.

Clicking on the tile of an existing network or scenario within the Network Editor area opens it in the Main area of the Web Interface, letting you manage (i.e. edit, play, or stop) the selected network/scenario.

5. NETWORK PORT PAIR PAGE

The **Network Port Pair** page (see *Illustration 5*) appears after either:

- clicking a pre-defined port pair ( ) from within the expanded **Networks** item in the Menu, or
- selecting **Management** > **Port Pairs**, and clicking on a port pair tile in the **Port Pairs** page (*Illustration 41 on page 169*) that appears.

Note:

Initially when the NE-ONE contains no pre-defined port pairs, the **Networks** item in the Menu contains no pre-defined port pairs, but only the **Ad Hoc** port pair item and **All Port Pairs** item. The **Ad Hoc** port pair item lets you create a temporary on-the-fly port pair for a networks. The **All Port Pairs** item opens the **Port Pairs** page where existing pre-defined port pairs can be managed. Once an administrator has created, named, colored a port pair, and assigned the port pair to another user, that port pair will appear under the **Networks** item in the Menu if the user has starred (favorited) it.

5-1. Network Port Page Areas

The **Network Port Pair** page contains the following two areas:

- Port Pair Network Creation area
- Port Pair Network Editor area

The Port Pair Network Creation area of the **Network Port Pair** page lets you do one of the following for the selected port pair:

- Launch the Port Pair Network Wizard using one of the point to point templates.

  Clicking on the **New Network** tile opens the Port Pair Network Wizard page (see *The Port Pair Network Wizard Page on page 268*, in *Chapter 9*, *Creating and Running Point-to-Point Networks*), which lets you create either a Point to Point (Single) or Point to Point (Dual) network for the selected port pair.
- Launch the Scenario Builder.

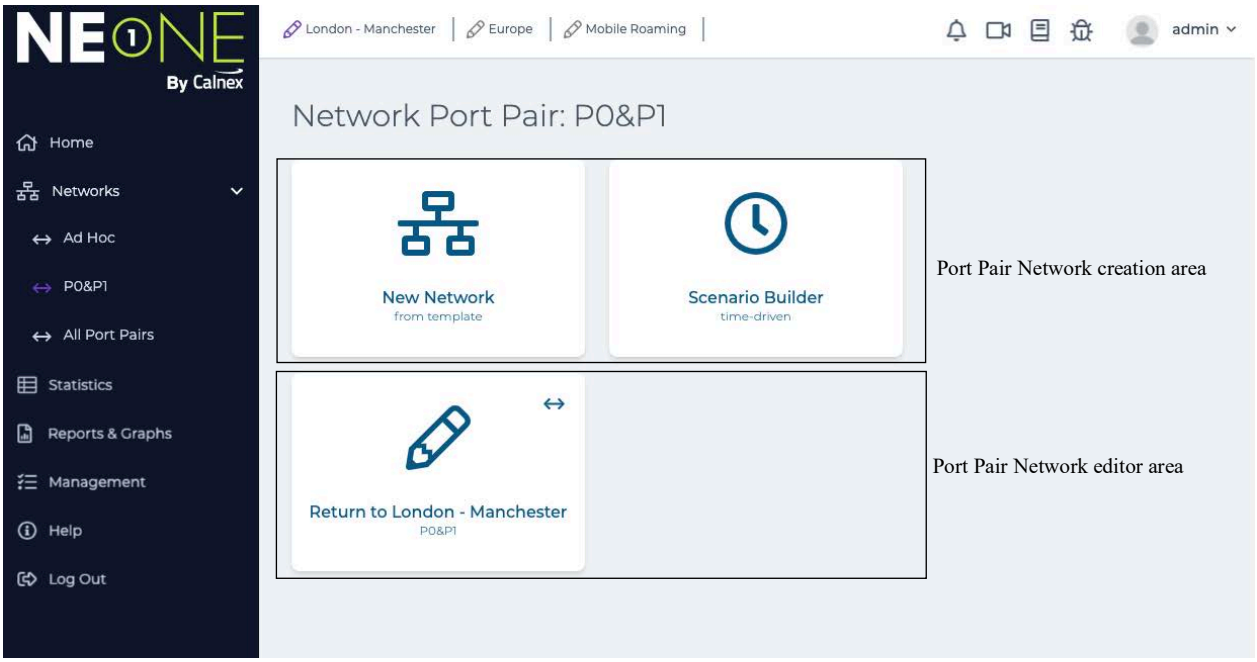
Clicking on the **Scenario Builder** tile opens the **Scenario Builder** page, which lets you either load, run, and stop an existing scenario, or create a new time based scenario for the selected port pair.

- Configure the port addressing and default transmission settings.

  Clicking on the **Port Settings** tile opens the **Port Setting** page, which lets you configure the port addressing and default transmission settings for the selected port pair. For more information, see *Port Pair Settings on page 174* in *Chapter 5*, *Ports and Services Management*.

  Note: Since an Ad Hoc port pair is a temporary 'on-the-fly' port pair for a network, port settings cannot be configured for an Ad Hoc port pair. Port settings can only be configured for pre-defined port pairs.

ILLUSTRATION 5 - NETWORK PORT PAIR PAGE



The Point Pair Network Editor area of the **Network Port Pair** page lists existing networks and scenarios for the selected port pair.

Note:

Initially when the NE-ONE contains no networks or scenarios associated with the selected port pair, the port pair network editor area is empty. As networks or scenarios are created for a selected port pair, they are listed in the Port Pair Network Editor area of the **Network Port Pair** page.

Clicking on an existing network or scenario within the Port Pair Network Editor area opens it in the main area of the Web Interface, letting you manage (i.e. edit, play, or stop) of the selected network/scenario for the selected port pair.

5-2. Networks Menu Port Pair Items

The **Networks** menu contains sub-menu items related to port pairs.

Depending on whether or not the Port Manager feature is activated on the NE-ONE, pre-defined port pairs will either already exist or not already exist, as follows:

- If the Port Manager feature is deactivated on the NE-ONE, then by default a set of pre-defined hardware port pairs will already be available and pre-configured, and will appear under the **Networks** item.
- If the Port Manager feature is activated on the NE-ONE, then by default, the NE-ONE is not configured with any point pairs. Port pairs can be created between the different port types using the Port Manager.

  In this case, initially when the NE-ONE (with Port Manager feature activated) contains no pre-defined port pairs, the **Networks** menu contains only the two following sub-menu items:

  - ↔**Ad Hoc** port pair item. Clicking this launches a pair of **Choose Left Port** and **Choose Right Port** dialog boxes letting you select the left and right ports for creating a temporary on-the-fly port pair, which will be used for a new Point-to-Point type network. Once the temporary port pair is created, you are taken to the **Network Port Pair** page for that temporary port pair, from where you can create a new Point-to-Point network.
    Note: as long as you save them, any Point-to-Point type network created via a temporary port pair is not lost (i.e. they are not temporary like the port pair they were initially assigned to when you created the network). Saved Point-to-Point type networks can be launched later on either another temporary Ad Hoc port pair, or a pre-defined port pair.
  - ↔ **All Port Pairs** item opens the **Port Pairs** page where existing pre-defined port pairs can be managed. For more information on managing port pairs, see *Managing Port Pairs on page 168* in *Chapter 5*, *Ports and Services Management*.

  Once an administrator has created, named, colored a port pair, and assigned the port pair to another user, that port pair will appear under the **Networks** item in the Menu if the user has starred (favorited) it.

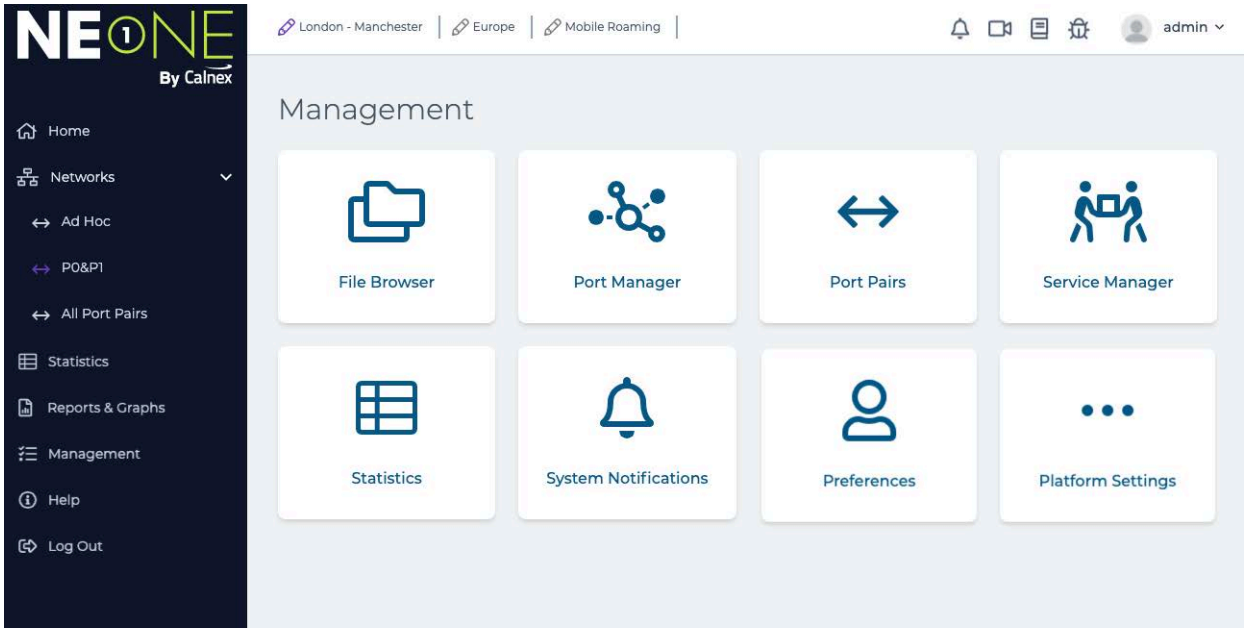
6. MANAGEMENT PAGE

The **Management** page (see *Illustration 6*) appears after clicking **Management** from the Menu, and contains a set of management tiles that let you manage all aspects of the NE-ONE.

Note:

The management tiles that are visible vary according to the user type (i.e. admin or non-admin) logged in to the Web Interface.

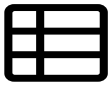
ILLUSTRATION 6 - MANAGEMENT PAGE



Clicking on a management tile (see *Table 5*) opens an appropriate page in the Main area of the Web Interface.

TABLE 5 - MANAGEMENT TILES

Management Tile	Tile Icon	Description
File Browser		Opens the **File Browser** page (see *Illustration 218 on page 633*) from where you can navigate the local filing system NE-ONE in order to perform various tasks such as: • opening a network or scenario file • opening a network or scenario file in script editor • share a network or scenario with another user A full description of the File Browser is beyond the scope of this chapter. For more information, see *Chapter 13*, *The File Browser on page 633*.
Port Manager*		Only available to admin type users. Opens a **Port Manager** page (see *Illustration 17 on page 107*), allowing an admin user to create soft ports. For more information see, *Managing Ports on page 107*, in *Chapter 5*, *Ports and Services Management*.
Port Pairs		Only available to admin type users. Opens a **Port Pairs** page (see *Illustration 41 on page 169*), allowing an admin user to create port pairs, modify existing port pairs and define whether a pre-defined port pair appears under the **Networks** item in the Menu. For more information see, *Managing Port Pairs on page 168* in *Chapter 5*, *Ports and Services Management*.

Management Tile	Tile Icon	Description
Service Manager*		Only available to admin type users. Opens a **Services** page (*Illustration 52 on page 188*), allowing an admin user to create and modify services which run background tasks (performing default transmission of data between ports or relaying of DHCP requests on a DHCP helper service). Once created and enabled, the service runs as a background task on the NE-ONE. For more information see, *Managing Services on page 188* in *Chapter 5*, *Ports and Services Management*.
Statistics		Opens the **Statistics** page (see *Illustration 171 on page 567*), which is the central location listing the statistics of the following objects from where you launch packet capture or data graphing for an object: • network objects (i.e. links and nodes) associated with any currently active (running) networks • framework objects (i.e. hardware port, soft port, port container, or service) For more information, see *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing on page 565*.
System Notifications		Opens the **System Notifications** page, from where you can view a chronological list of system level events, categorized by event type. For more information, see *Viewing System Notifications on page 257* in *Chapter 8*, *General System Procedures*.
Preferences		Opens the **Preferences** page (see *Illustration 70 on page 259*), from where you can access different user preferences. Allows the currently logged in user change their password, change the Web Interface language, and show/hide unlicensed features. For more information, see *User Related Preferences via the User Preferences Page on page 259* in *Chapter 8*, *General System Procedures*.
Platform Settings		Only available to admin type users. Opens the **Platform Settings** page (see *Illustration 7*), which contains a set of platform settings tiles (see *Table 6*) that allow an admin user to manage platform specific aspects of the NE-ONE.
*- The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.		

7. PLATFORM SETTINGS PAGE

The **Platform Settings** page (see *Illustration 7*) appears after clicking **Management > Platform Settings** from the Menu, and contains a set of tiles that let you manage all the platform specific aspects of the NE-ONE.

Note:

The **Platform Settings** page is only visible for admin type users logged in to the Web Interface.

ILLUSTRATION 7 - PLATFORM SETTINGS PAGE

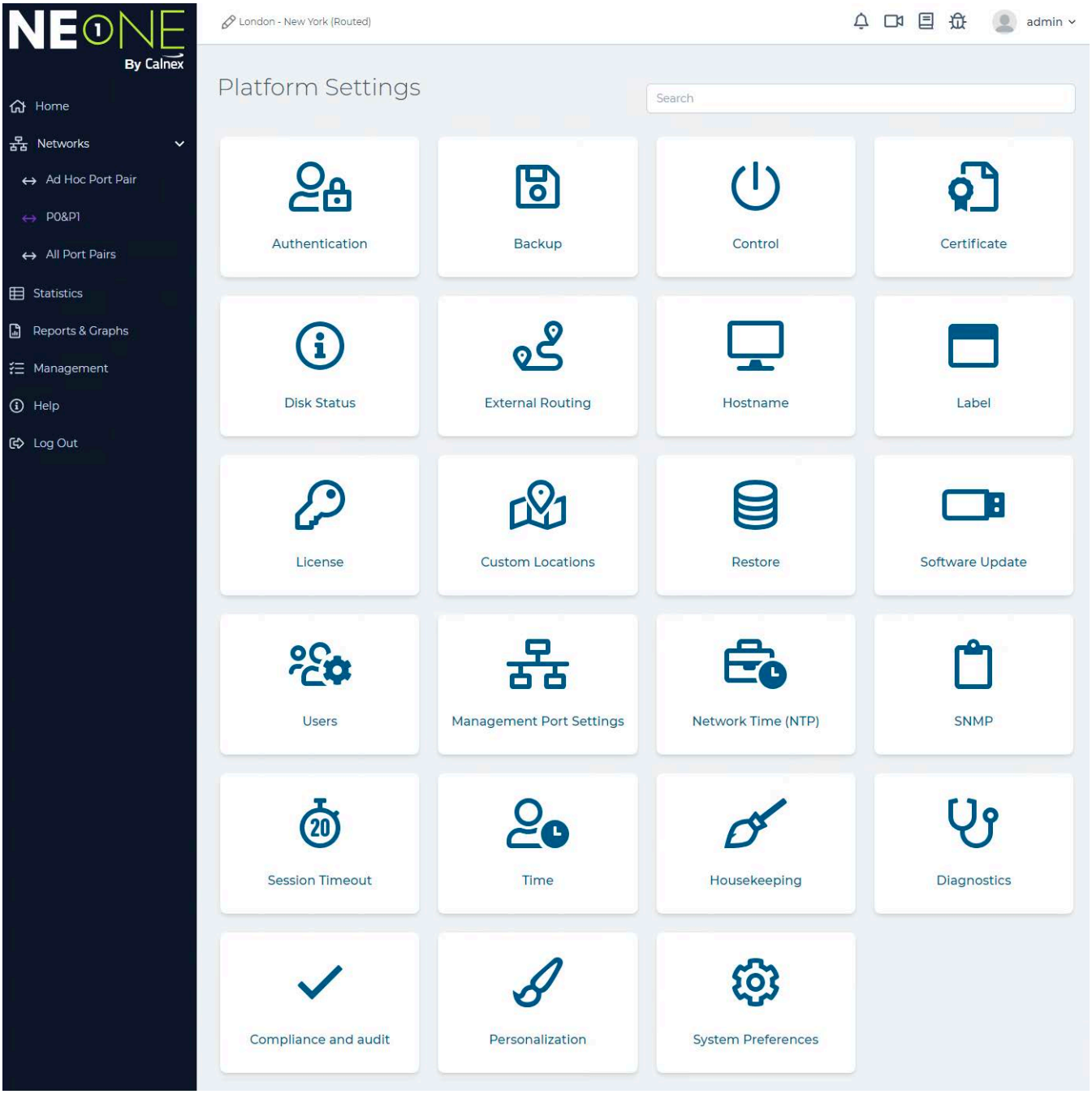
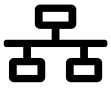


TABLE 6 - PLATFORM SETTINGS TILES

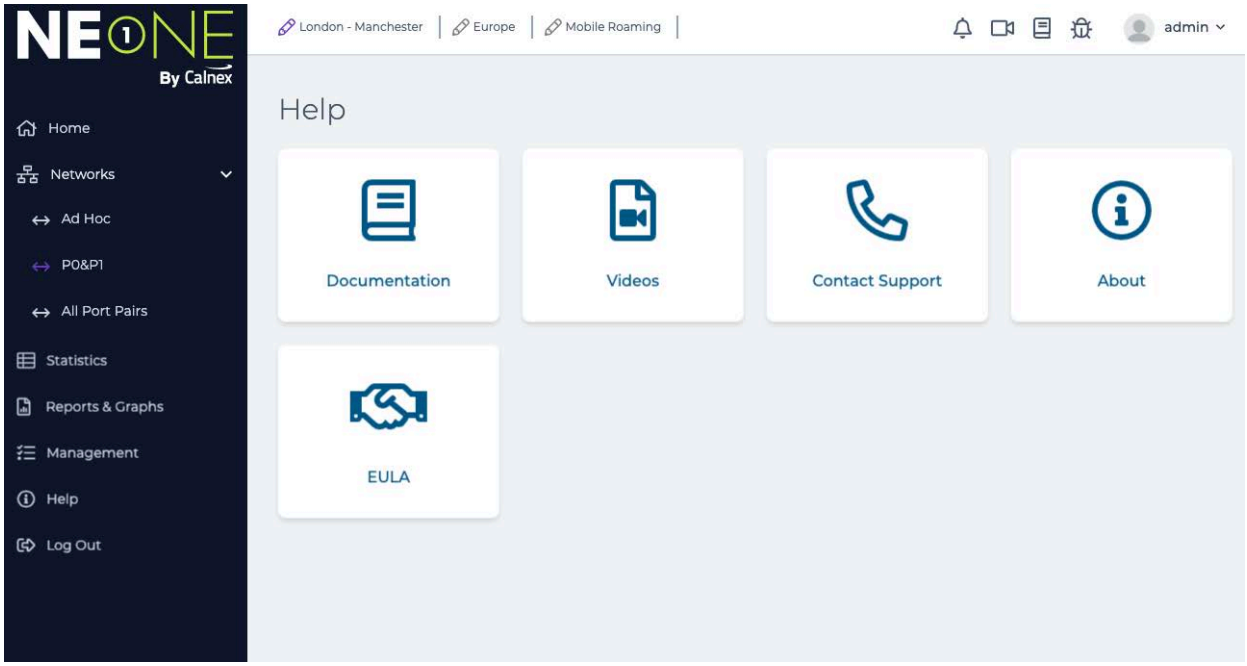
Platform Settings Tile	Tile Icon	Description
Authentication		Opens an **Authentication** page, allowing an admin user to optionally configure the NE-ONE to use either an LDAP or RADIUS server as its user authentication method if the Advanced Authentication feature is activated. For more information, see *Configuring the Authentication Method on page 79* in *Chapter 4*, *Installation and Configuration*.
Backup		Opens a **Backup** page, allowing an admin user to view the existing backup history (if it exists), download the historical backup files (if they exist), and create/download a current backup of the NE-ONE user accounts, log files, and settings. For more information, see *Backing up the System on page 239 Chapter 7*, *System Maintenance*.
Control		Opens a **Control** page, allowing an admin user to shut down or reboot the NE-ONE. For more information, see *Controlling the System on page 238 Chapter 7*, *System Maintenance*.
Certificate		Opens a **Certificates** page, allowing an admin user to: • view the status of the SSL certificate currently installed on the NE-ONE • update the NE-ONE with a new SSL certificate and private key For more information, see *Installing and Updating Root SSL Certificates on page 84* in *Chapter 4*, *Installation and Configuration*.
Disk Status		Opens a **Disk Status** page, allowing an admin user to view the disk status of NE-ONE. For more information, see *Monitoring System Disk Usage on page 244 Chapter 7*, *System Maintenance*.
External Routing		Opens an **External Routing** page, allowing an admin user to optionally configure external routing on the NE-ONE (if the NE-ONE is implemented within a network environment that uses dynamic routing). For more information, see *Configuring External Routing on page 94* in *Chapter 4*, *Installation and Configuration*.
Hostname		Opens a **Hostname** page, allowing an admin user to set the hostname of the NE-ONE. For more information, see *Configuring the Hostname on page 69* in *Chapter 4*, *Installation and Configuration*.
Label		Opens a **Label** page, allowing an admin user to optionally change the label (defined by the title tag) that appears in a web browser for the NE-ONE's Web Interface. For more information, see *Configuring the Web Interface Label on page 70* in *Chapter 4*, *Installation and Configuration*.
License		Opens a **License** page, allowing an admin user to view the existing license information, and update the license on the NE-ONE. For more information, see *Viewing and Applying License Files on page 86* in *Chapter 4*, *Installation and Configuration*.
Custom Locations		Allows an admin user to create a custom location with longitude and latitude coordinates. Once a custom location is created, it can be used for setting the location of a node within a network. For more information, see *Custom Locations on page 87* in *Chapter 4*, *Installation and Configuration*.
Restore		Opens a **Restore** page, allowing an admin user to restore a backup from either an uploaded backup file, or restore a backup file from a list of backups that were previously created and/or uploaded locally on the NE-ONE. For more information, see *Restoring a System Backup on page 242 Chapter 7*, *System Maintenance*.

Platform Settings Tile	Tile Icon	Description
Software Update		Opens a **Software Update** page, allowing an admin user to view the existing software update history, and update the software on the NE-ONE. For more information, see *Viewing and Updating the System Software on page 230* in *Chapter 7*, *System Maintenance*.
Users		Opens a **Users** page, allowing an admin user to manage the user accounts on the NE-ONE. For more information, see *Chapter 6*, *User Administration*.
Management Port Settings		Opens a **Management Port Settings** page, allowing an admin user to set the networking configuration (i.e. IP Address, Netmask, and Gateway) of the NE-ONE's management port. For more information, see *Configuring the Management Port Settings on page 62* in *Chapter 4*, *Installation and Configuration*.
Network Time (NTP)		Opens a **Network Time** page, allowing an admin user to optionally configure the NE-ONE to use a network time protocol (NTP) servers for its time instead of a manually set time. For more information, see *Network Time Protocol (NTP) Configuration on page 67* in *Chapter 4*, *Installation and Configuration*.
SNMP		Opens a **Network SNMP** page, allowing an admin user to optionally configure the NE-ONE to work with the Simple Network Management Protocol network management system. For more information, see *Configuring SNMP on page 78* in *Chapter 4*, *Installation and Configuration*.
Session Timeout		Opens a **Session Timeout** page, allowing an admin user to define the NE-ONE's user session timeout value in seconds and configure whether user sessions can timeout when networks/scenarios are running. For more information, see *Session Timeout Configuration on page 85* in *Chapter 4*, *Installation and Configuration*.
Time		Opens a **Time** page, allowing an admin user to define the NE-ONE's date, time and time zone. For more information, see *Time Configuration on page 67* in *Chapter 4*, *Installation and Configuration*.
Housekeeping		Opens a **Housekeeping** page, allowing an admin user to configure the housekeeping properties of the NE-ONE. For more information, see *Configuring Housekeeping on page 71* in *Chapter 4*, *Installation and Configuration*.
Diagnostics		Opens a **Diagnostics** page, allowing an admin user to run a system diagnostics that creates a binary diagnostics file, which can be sent to Calnex support or your support representative. For more information, see *Running Diagnostics on page 245* in *Chapter 7*, *System Maintenance*.
Compliance and Audit		Opens a **Compliance and Audit** page, allowing an admin user to optionally apply a compliance and audit conditions that users will have to accept before using the NE-ONE. For more information, see *Applying a Compliance and Audit Acceptance Agreement on page 75* in *Chapter 4*, *Installation and Configuration*.
Personalization		Opens a **Personalization** page, allowing an admin user to optionally personalize the appearance of the login page of the NE-ONE. For more information, see *Personalizing the Login Page on page 73* in *Chapter 4*, *Installation and Configuration*.
System Preferences		Opens a **System Preferences** page, allowing an admin user to configure certain system preferences of the NE-ONE. For more information, see *Configuring the System Preferences on page 77* in *Chapter 4*, *Installation and Configuration*.

8. HELP PAGE

The **Help** page (see *Illustration 8*) appears after clicking **Help** from the Menu, and contains a set of help tiles that let you view support related aspects of the NE-ONE.

ILLUSTRATION 8 - HELP PAGE



Clicking on a help tile (see *Table 7*) opens an appropriate page in the Main area of the Web Interface.

TABLE 7 - HELP TILES

Management Tile	Tile Icon	Description
Documentation		Opens the embedded user manual (in a separate browser tab), starting on the first page.
Videos		Opens the **Videos** page containing a list of all the help videos. Clicking on a video will open it in another web browser tab.
Contact Support		Opens a temporary dialogue box (that closes after several seconds) with the contact details of the Calnex support team.
About		Opens the **About** page, which provides the model information (same as that of the that displayed in the Home page), and general attributions information about the NE-ONE.
EULA		Opens the **EULA** page, which contains the end user license agreements associated with the NE-ONE.

CHAPTER 4 INSTALLATION AND CONFIGURATION

1. INTRODUCTION

This chapter is applicable to admin users, and describes the installation and configuration procedures that you use to initially install and configure the NE-ONE in your network.

1-1. Implementation of SDTNs with the NE-ONE

Before proceeding to the steps in the sub-sections below, it is useful to discuss some examples of the different ways in which the Software Defined Test Networks (SDTNs) on the NE-ONE can be implemented within a network.

ILLUSTRATION 9 - EXAMPLE OF THREE SOFTWARE DESIGNED TEST NETWORKS

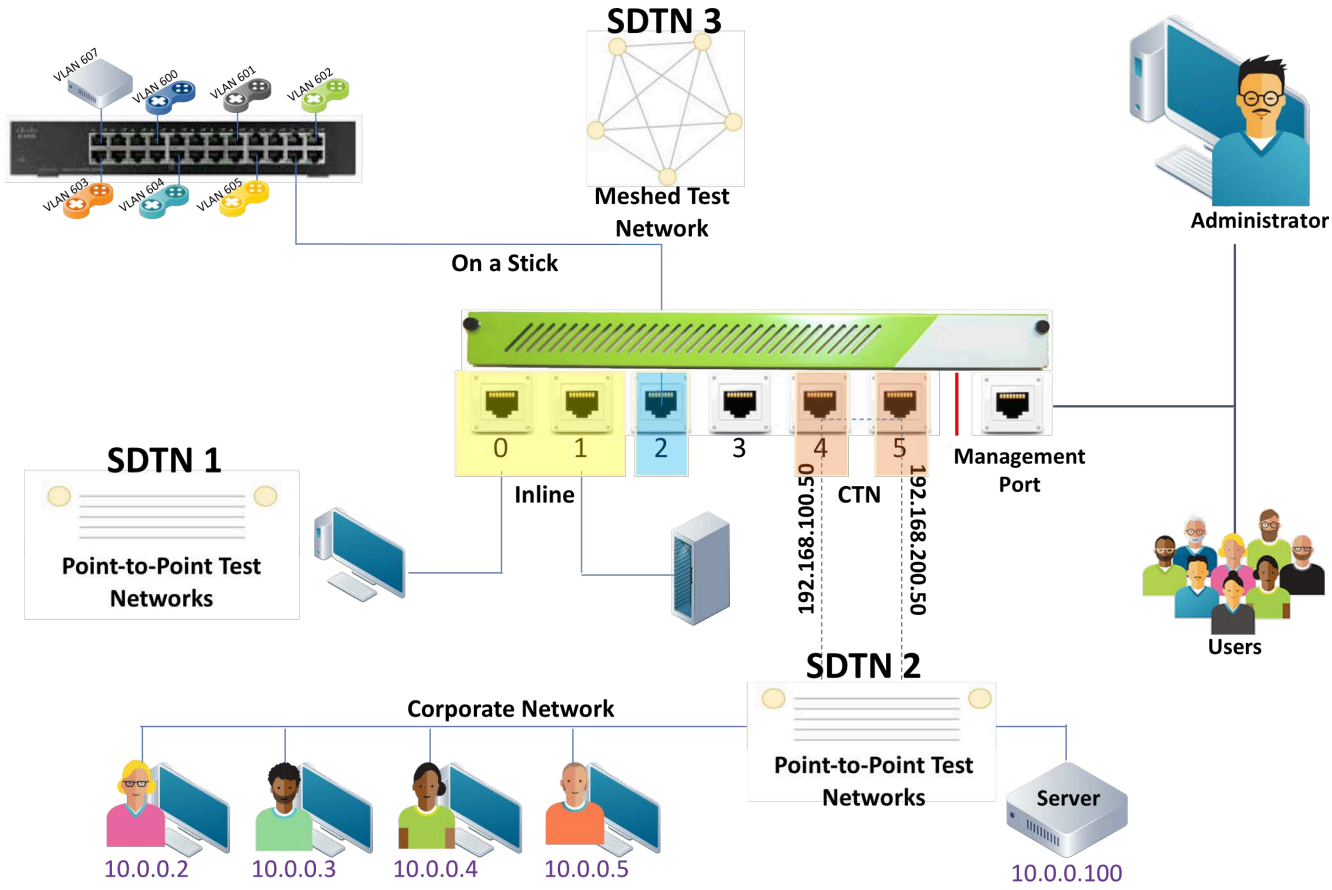


Illustration 9 shows an example of an NE-ONE being used to implement the following SDTNs:

- Inline (SDTN1)
  - Uses two out-of-band ports which can be bridge (Layer 2) or route (Layer 3).
  - Ethernet switches can be connected to the out-of-band ports so that multiple devices can use the Point-To-Point test network at the same time.
  - The Point-To-Point test network is setup with the appropriate impairments are created and configured using the Point-To-Point Designer. See *Creating Point-to-Point Networks (Single) on page 292* in *Chapter 9*, *Creating and Running Point-to-Point Networks* as an example. In this example, port addressing is enabled on hardware ports 0 and 1 as the client test computers are on one network (i.e. 10.0.0.X) while the test server is on another network (e.g. 192.168.200.X).
  - There is no limit on the number of devices or users that can use the test network.

  - In this example, this configuration has no dynamic routing, and does not require external routes to be configured on the NE-ONE. However, if required, you can configure dynamic routing if needed, in which case external routing would need to be configured using the **External Routing** page (see *Configuring External Routing on page 94*).

- CTN - Continuous Test Network (SDTN2).

  The concept of the CTN is to let "client" users access the same server via either the production network (corporate network without any impairments) or the test network (via impairments that are defined in the NE-ONE).

  - Two out-of-band ports of the NE-ONE are attached to the corporate network.
  - The Network Administrator sets up two pools of IP addresses (typically, by using an alternate sub-net) for both the users and the server.

    One pool is assigned to the "production" environment (for DevOps use for example), where the packets are routed so they do not pass through the NE-ONE.

    The other pool is assigned to the "alternate" test network, where the packets are routed to pass through the NE-ONE instead.
  - The Network Administrator also sets up the core routers so that the "alternate" IP addresses are routed through the NE-ONE, while the "production" IP addresses are not routed through the NE-ONE.
  - The NE-ONE Administrator (normally a different person to the Network Administrator) configures client to server mappings on the NE-ONE by creating Static NAT soft ports. The Static NAT soft ports are configured to translate the "alternate" IP addresses to "production" IP addresses. For more information, see *Creating a Static NAT Soft Port on page 147* in *Chapter 5*, *Ports and Services Management*.
  - When the user wants to access the server via the "alternate" test network, they specify the "alternate" NE-ONE IP Address instead of the normal "production" server IP address. In this case, the core routers redirect the users packets to the NE-ONE where impairments are introduced, and the Static NAT soft ports on the NE-ONE will translate the alternate address to production address, forwarding/receiving packets to/from the server.
  - When the user wants to access the server directly via the "production" network, they specify the normal "production" server IP address. In this case, the core routers will route the users packets to avoid passing through the NE-ONE and remain entirely within the corporate network without any impairments.

- On-a-stick (SDTN3)
  - Uses one out-of-band port for sending and receiving data between the NE-ONE and the VLAN switch.
  - The out-of-band port on the NE-ONE is connected to the trunk port on the VLAN switch, and each test device is on a separate VLAN connected to the VLAN switch.
  - The NE-ONE Administrator creates a VLAN soft ports for each VLAN so that each user has their own test network. For example, see *Creating a VLAN Soft Port on page 116* in *Chapter 5*, *Ports and Services Management*.
  - The NE-ONE Administrator also creates a set of IPv4 soft ports under each VLAN soft port so that each user has their own test network, and can define their own SDTN. For example, see *Creating an IPv4 Soft Port on page 123* in *Chapter 5*, *Ports and Services Management*. Each IPv4 soft port .
  - If necessary, routing can be setup between each VLAN so that devices/users can communicate with each other.

    If the routing between the VLAN and devices is configured to use static routing, external routes do not need to be configured on the NE-ONE.

    If the routing between the VLAN and devices is configured to use dynamic routing, external routes need to be configured on the NE-ONE using the **External Routing** page (see *Configuring External Routing on page 94*).

- The test networks with the appropriate impairments can then be created and configured by the users via either the Point-to-Point Designer or Multi-Point Designer. The users will create their own SDTNs within each VLAN using the IPv4 soft ports that were assigned to them, and applying those IPv4 soft ports to each of the nodes in their SDTNs. In the example of *Illustration 9*, a Fully Meshed Multi-Point network is created by one user.

All three SDTNs can run at the same time with different test networks and different impairments.

Note:
The implementation of the Inline SDTN (SDTN1) is possible with all NE-ONEs. The implementation of the On-a-stick (SDTN3) and Continuous Test Network (SDTN2) SDTNs are only possible with NE-ONEs that have the Port Manager feature enabled, since in these examples soft ports are required.

2. PREREQUISITES

Before installing the NE-ONE in your network, do the following:

1. Obtain the appropriate license from Calnex (*support@calnexsol.com*).

   Note:
   If you do not initially have a license, the NE-ONE will operate with limited functionality so that it can be licensed.

2. Check with Calnex if there are software updates available for the NE-ONE.
3. Check with your network administrator if the NE-ONE can have a manually assigned static IP address, or whether it needs to dynamically obtain an IP address from your network's DHCP server. In the case the NE-ONE uses a static IP address, get the following network parameters from the network administrator:
   - IP Address
   - Network Mask
   - Default Gateway
   - Primary DNS Server
   - Secondary DNS Server

   Note:
   Ask the network administrator for the fully qualified domain name (FQDN) they will apply to the NE-ONE on the organization's domain name servers (DNS).
   If you choose to use a dynamic IP address, the IP address of the NE-ONE risks changing with time. In this case it is recommended that you communicate the FQDN of the NE-ONE to your users in order for them to access the Web Interface.

4. Check with your network administrator if the hostname to be used for the NE-ONE.

   Note:
   If you do not specify a hostname for the NE-ONE, it will use NE-ONE.

   Note:
   If the organization's network contains more than one NE-ONE, Calnex recommends that a unique hostname is defined on each of the NE-ONEs.

5. Check with your network administrator if the organization uses either the LDAP or RADIUS authentication method, and if it does, obtain the following:
   - Primary LDAP/RADIUS Server FQDN or IP address
   - Secondary Primary LDAP/RADIUS Server FQDN or IP address

Note:

LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

6. Check with your network administrator if the organization uses Simple Network Management Protocol (SNMP) for its network management, and if does, obtain the community string, location, and contact.

Note:

At the current release, the NE-ONE does not support SNMP V3 username and password implementation.

7. Check with your network administrator if the organization uses a Root SSL Certificate (i.e. an SSL Certificate signed by a trusted Certificate Authority. If it does, obtain the Root SSL Certificate and Private Key from the organization's network administrator.

Note:

If the organization does not use a Root SSL Certificate, the NE-ONE will use the default supplied self-signed Calnex SSL Certificate. In this case, when users connect to the NE-ONE Web Interface for the first time, they will need to perform a few steps to accept the self-signed Calnex SSL Certificate. For more information, see *First time Web Interface access (accepting the default self-signed SSL certificate) on page 29*.

8. Check with your network administrator if the organization is using dynamic routing (adaptive routing) or static routing (non-adaptive routing). If the organization is using dynamic routing (adaptive routing), the network administrator will have chosen a routing protocol of preference (BGP, OSPF, OSPFv6, RIP, or RIPng) for the network. Ask the network administrator which routing protocol is implemented within the network, and the external routing tables that you need to define on the NE-ONE in order for the NE-ONE to inter-operate with the routing protocol that is implemented within the network.

Note:

At the time of publication, the NE-ONE currently supports BGP, OSPF, OSPFv6, RIP, and RIPng routing protocols. If your organization uses another routing protocol such as Interior Gateway Routing Protocol (IGRP) or Intermediate System to Intermediate System (IS-IS), contact your Calnex representative for more information on how and when those other routing protocols will be implemented on the NE-ONE.

9. If the NE-ONE is running on a virtual environment (i.e. VMWare or Openstack) or a cloud computing environment (i.e. Amazon Web Services (AWS) or Microsoft Azure), ensure that the environment has been set up for the NE-ONE.

   For more information on setting up the AWS cloud computing service to support the NE-ONE, refer to the *NE-ONE AWS Installation Guide*.

   For more information on setting up the Microsoft Azure cloud computing service to support the NE-ONE, refer to the *NE-ONE Azure Installation Guide*.

3. INSTALLATION WORK FLOW

When you install a new NE-ONE use the installation work flow summarized in *Illustration 10* and *Illustration 11*.

Note:

The sections referenced by the installation work flow are generically written as individual procedures, and describe the full set of steps to take to navigate within the Web Interface. However, when you are already within the **Management** pages and **Platform Settings** pages of the Web Interface, you can click on the **BACK** button to return up one level. For more information on general Web Interface navigation principles, refer to *Chapter 3, NE-ONE Web Interface Overview*.

Note:

Some parts of the installation work flow in *Illustration 10* and *Illustration 11* may not be applicable, and depend on the features that are licensed with your edition of NE-ONE.

LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

The Port Manager feature is a premium feature. Depending on your license, the Port Manager feature may be either activated or deactivated.

The Service Manager feature is a premium feature. Depending on your license, the Service Management feature may be either activated or deactivated.

In *Illustration 10* and *Illustration 11* below, these features are indicated by thicker, dashed rectangles.

ILLUSTRATION 10 - INSTALLATION AND CONFIGURATION WORK FLOW

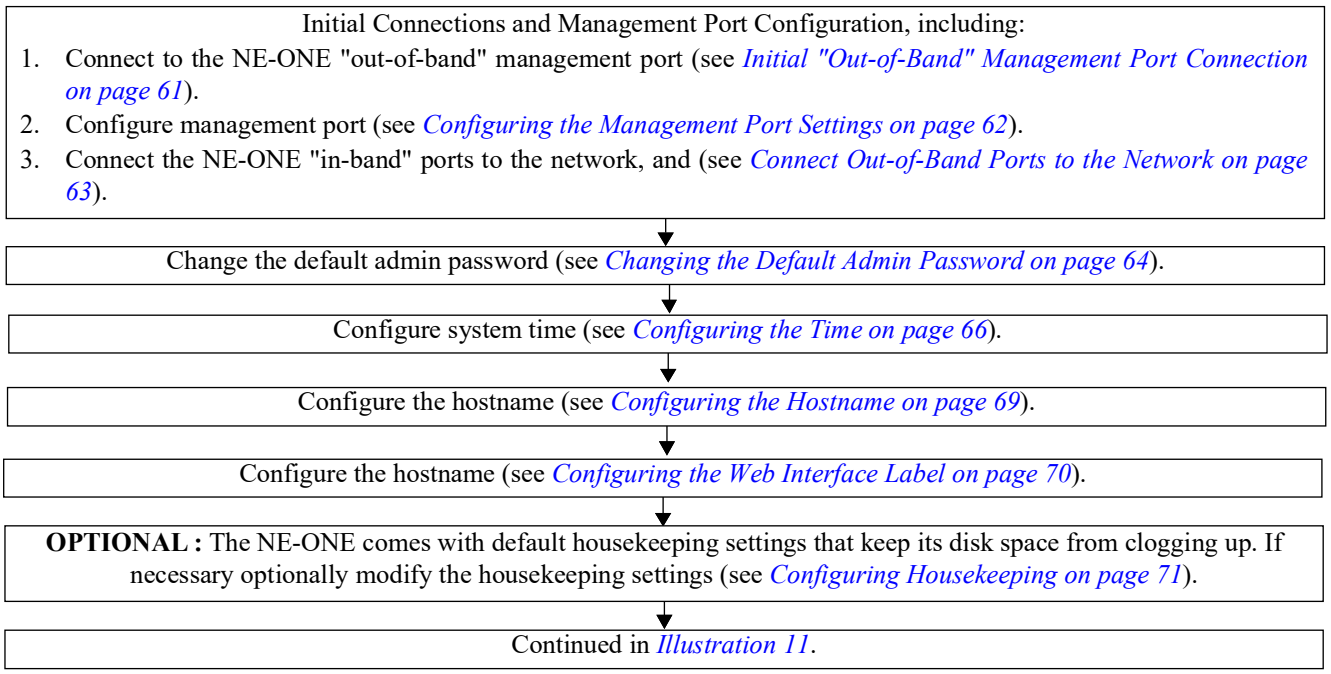
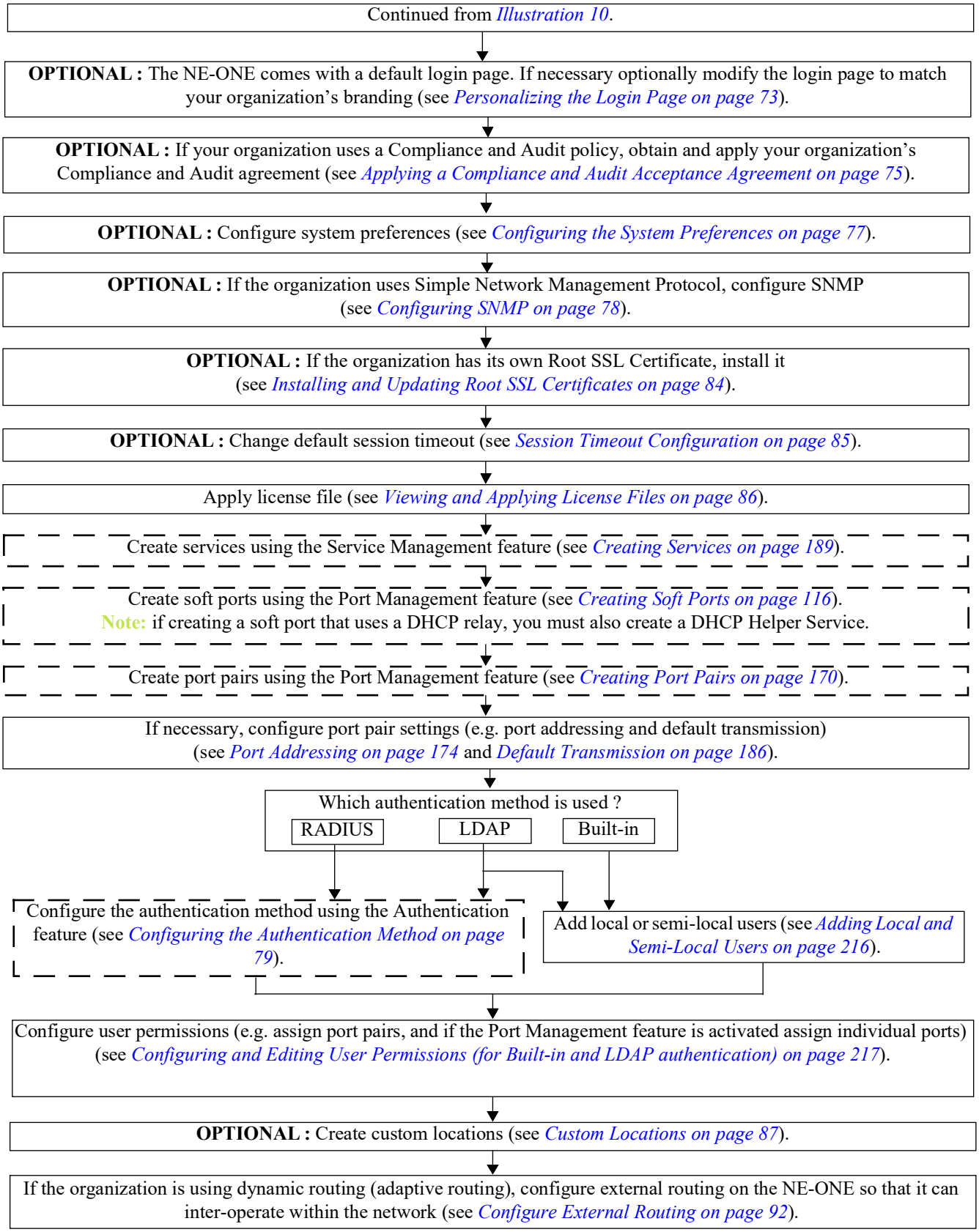


ILLUSTRATION 11 - INSTALLATION AND CONFIGURATION WORK FLOW (CONTINUED)



4. INITIAL CONNECTIONS AND MANAGEMENT PORT CONFIGURATION

Use this section when you install the NE-ONE for the first time within your network, or if you want to change how the NE-ONE is connected and configured within your network.

4-1. Initial "Out-of-Band" Management Port Connection

A *Setup Guide* is provided in the NE-ONE's packaging describing the initial steps you take to connect with the NE-ONE's "out-of-band" management port, and to access the Web Interface. Follow the steps described with the provided *Setup Guide*. The steps described with the provided *Setup Guide* vary according to the type of NE-ONE you have (see*Table 8*).

TABLE 8 - NE-ONE TYPE AND CORRESPONDING SETUP GUIDE INFORMATION

NE-ONE Type	Summary of type of information in provided Setup Guide
Physical : Desktop	• Because there is a visual method to view a dynamically assigned IP address on the NE-ONE via an LCD panel, the management port IP address obtained automatically via DHCP (if DHCP server exists and reachable in the network). • Connect NE-ONE's management port located on the rear panel to the network. • Use the NE-ONE's LCD panel to view and determine the dynamically assigned IP address of the management port. For more information, see *Show IP Address on page 852* in the *Network Settings* section of *Chapter 17*, *The LCD Panel*. • If no IP address is dynamically assigned (because the network's DHCP server was not reachable) or you want to manually change the dynamically assigned IP address, use the front panel buttons to manually configure a static IP address for the management port. For more information, see *DHCP on page 852* and *Static IP Address on page 853* in the *Network Settings* section of *Chapter 17*, *The LCD Panel*. • Connect to the Web Interface via **https://<Management Port IP address>**
Physical : Rack mount (half rack or 1U)	• Because there's no visual method to view a dynamically assigned IP address, the default management port IP address configured on the NE-ONE is 192.168.0.10 (netmask 255.255.255.0). • Connect NE-ONE's management port located on the rear panel to the a laptop PC who's NIC is configured within the 192.168.0.0 network with netmask 255.255.255.255. • Connect to the Web Interface via **https://192.168.0.10**
Virtual Appliance (VMWare or OpenStack) Cloud Appliance (AWS or Microsoft Azure)	• The network interfaces of the NE-ONE will have been defined within the cloud computing environment. • The management port IP address is created and defined by the cloud computing environment. • Use cloud computing environment's interface to view and determine the IP address of the NE-ONE's management port. For more information on determining the IP address of the NE-ONE's management port within the AWS cloud computing service, refer to the *NE-ONE AWS Installation Guide*. For more information on determining the IP address of the NE-ONE's management port within the Microsoft Azure cloud computing service, refer to the *NE-ONE Azure Installation Guide*. • Connect to the Web Interface via **https://<Management Port IP address>**

Note:

Initially the NE-ONE contains a self-signed Calnex SSL Certificate. When connecting to the Web Interface for the first time, you need to accept the self-signed Calnex SSL Certificate according to *First time Web Interface access (accepting the default self-signed SSL certificate) on page 29*.

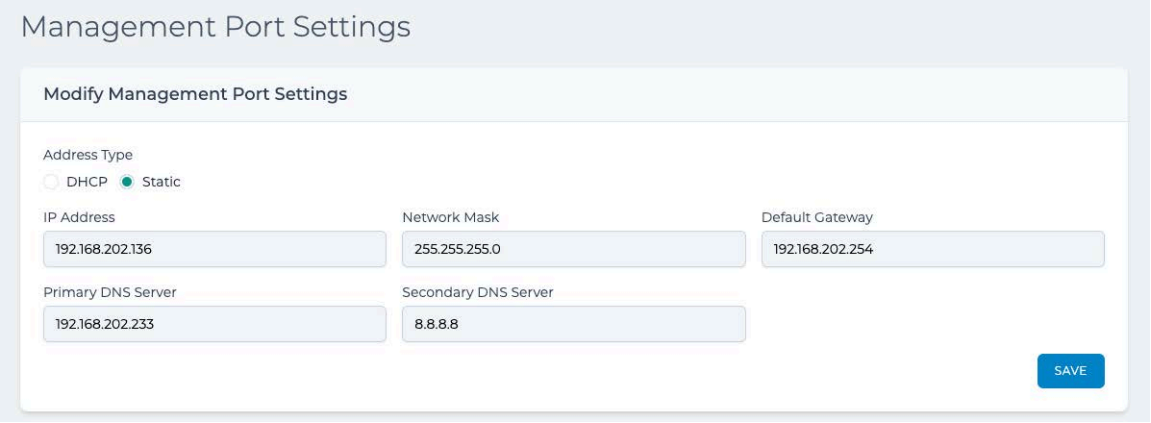
4-2. Configuring the Management Port Settings

Use this section when you install the NE-ONE for the first time, or if you want to change the existing network settings of the NE-ONE's management port.

As summarized in *Table 8 on page 61*, depending on the type of NE-ONE you have, the NE-ONE is delivered with its management port to either obtain its network configuration automatically via a DHCP server (for Physical Desktop and Virtual Appliance NE-ONEs) or have a static network configuration (for the Physical Rack mount NE-ONEs).

Use the following steps to configure the network configuration of the NE-ONE's management port:

1. From the Web Interface, click **Management > Platform Settings > Management Port Settings**.



2. From the **Management Port Settings** page that appears, do the following:
   a. Enable the appropriate **Address Type** radio button:
      Enable the **DHCP** radio button if the NE-ONE is to get its network configuration from a DHCP server on the organization's network.
      Enable the **Static** radio button if the NE-ONE is to have a manually configured static IP address, network mask, default gateway, and DNS servers.
   b. If you enabled the **Static** radio button, additionally do the following:
      In the **IP Address** field, type the IP address for the NE-ONE (given to you by the network administrator).
      In the **Netmask** field, type the netmask used by the NE-ONE (given to you by the network administrator).
      In the **Default Gateway** field, type the IP address of the Default Gateway used by the NE-ONE (given to you by the network administrator).
      In the **DNS Server 1** field, type the IP address of the primary DNS server used by the NE-ONE (given to you by the network administrator).
      In the **DNS Server 2** field, type the IP address of the primary DNS server used by the NE-ONE (given to you by the network administrator).
   c. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

4-3. Connect Out-of-Band Ports to the Network

The NE-ONE needs to be connected "between" your user(s) and server(s) systems (or indeed any systems which you want to test in "impaired" networks) either directly or via switches and routers.

The simplest configuration of all is to connect the test user (client) to the NE-ONE and the NE-ONE to the server. This is often possible in a "lab" type environment (but rarely in a corporate network). With this configuration, there is no risk of other network activities impacting on the data flow. Such a configuration is shown by SDTN1 in *Illustration 9 on page 55*, where the NE-ONE is directly connected in-line between the test user's client PC on hardware port 0 and the server on hardware port 1.

However, if your test users (clients) and server(s) are connected via switches, hubs and (possibly) routers (as is most usual), and cannot be connected directly, you can connect the NE-ONE at some other suitable point between the test users (clients) and the servers. One possible such configuration is shown by SDTN2 in *Illustration 9 on page 55*, where the NE-ONE is indirectly connected in-line between multiple test user client PCs via a hub/switch/router on hardware port 3 and the server via a hub/switch/router on hardware port 4. In this configuration, if dynamic routing is being used by the routers, you must also configure external routing on the NE-ONE according to *Configure External Routing on page 92*.

A third possibility is that the NE-ONE is not physically connected between the client and server (or other devices) in the test, but rather network routing is set up to direct traffic from systems or networks under test to the NE-ONE, which can then be itself configured to route traffic to the target networks (having first "impaired" or "restricted" the traffic as required). Using this principle, the NE-ONE can be inserted into any desired configuration. The example configurations of SDTN1 and SDTN2 in *Illustration 9 on page 55* show just two possibilities. There are of course many other configuration possibilities such as inserting the NE-ONE in the uplink/downlink between two switches, placing it in a VLAN trunk and even using it as an "SDTN on a stick" as shown by the SDTN3 configuration *Illustration 9 on page 55*. The advantage of this type of configuration is that you only use up one hardware port of the NE-ONE. In this configuration, if dynamic routing is being used by the routers, you must also configure external routing on the NE-ONE according to *Configure External Routing on page 92*.

If you are using a physical (desktop or rack mount) NE-ONE, connect the out-of-band ports of the NE-ONE to your network as required using an Ethernet cable. In the example of *Illustration 9 on page 55*, the NE-ONE ports are connected as follows:

- Hardware port 0 is connected to a test user's client PC
- Hardware port 1 is connected to a server
- Hardware port 2 is connected to a port on a Cisco switch which is configured with different VLANs.
- Hardware port 3 is connected within the corporate network
- Hardware port 4 is connected within the corporate network

Note:

At this stage the NE-ONE's in-band ports do not need to be connected to your network. You can connect them later on at any point during the configuration work flow summarized in *Illustration 11 on page 60*.

If you are using an NE-ONE Virtual Appliance, use the virtual appliance management tools to configure (map) the out-of-band ports of the NE-ONE Virtual Appliance to virtual hardware ports in your virtual environment, then connect the physical NIC of the server hosting the NE-ONE Virtual Appliance to the network.

Note:

It is beyond the scope of this *User and Administration Guide* to describe how the NE-ONE Virtual Appliance's out-of-band ports are configured (mapped). The *Setup Guide* and other instructions provided in the NE-ONE Virtual Appliance's packaging describe how to configure the NE-ONE Virtual Appliance's out-of-band ports.

Note:
If you are using an NE-ONE Virtual Appliance, the physical NIC of the server hosting the NE-ONE Virtual Appliance will probably already be connected to the network.

Note:
By convention, the example test networks described in this *User and Administration Guide* it's assumed that for two-port in-line configurations that test users (clients) are connected to the NE-ONE's hardware port 0 and the servers to the NE-ONE's hardware port 1, but this is not mandatory. Additionally, if you have the Port Manager feature activated on the NE-ONE, which lets you configure port pairs for your test users, you could for example leave hardware port 0 assigned to an "SDTN on a stick" configuration, and create a port pair on hardware ports 1 and 2 for a two-port in-line configurations. The Port Manager feature gives you the flexibility in letting you define how you want to allocate single ports and port pairs.

5. CHANGING THE DEFAULT ADMIN PASSWORD

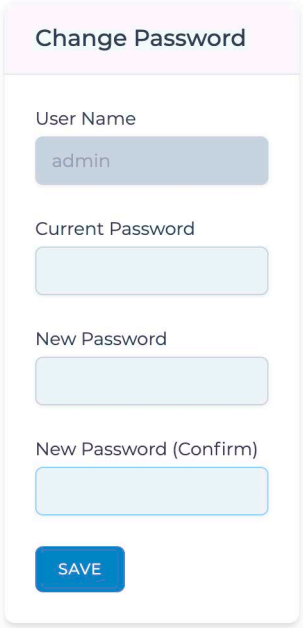
The default password for the local (built-in) admin user on the NE-ONE is admin. Upon connecting to the Web Interface for the first time, you will be prompted to change the password for the admin user to another password other than admin. Once you have changed the default admin password you will be able to access the Web Interface pages.

Use the steps below to change the default admin user password.

1. Launch your preferred web browser, and specify the following URL in the address bar:
   `https://<IP address or hostname>`
   where `<IP Address or hostame>` is the IP Address or hostname of the NE-ONE Management Port.
   A login page appears.

2. From the login page that appears, type **`admin`** in the **Username** field and type **`admin`** in the **Password** field, then click **LOGIN**.

Upon successfully logging in, the following dialog box appears, prompting you to change the admin password.



3. In the **Current Password** field, type **`admin`**.
4. In the **New Password** and **New Password (Confirm)** fields, type the new password for the admin user.
5. Click **SAVE**.
   A **Changed!** dialog box appears confirming that the admin password has been successfully changed.
6. From the **Changed!** dialog box that appears, click **OK**.
   You are automatically logged out of the Web Interface, and are returned to the **Login to your account** page.
7. From the login page that appears, type **`admin`** in the **Username** field and type the new password that you had created in the **Password** field, then click **LOGIN**.
   Upon successfully logging in, you are presented with the Web Interface (see *Web Interface Layout on page 38*).

6. CONFIGURING THE TIME

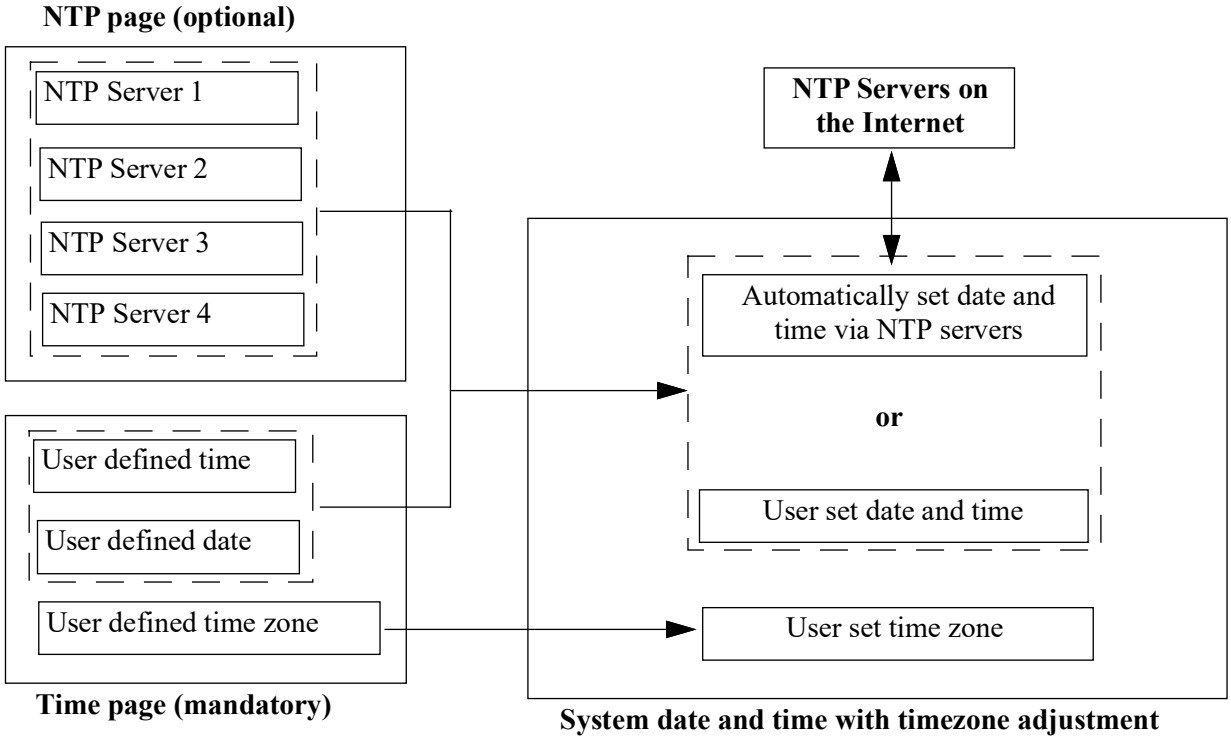
Use this section when you install the NE-ONE for the first time, or if you want to change the existing time settings of the NE-ONE.

The time configuration is separated into two separate areas on the Web Interface, as follows:

- a mandatory **Time** page where you must select the time zone, and manually specify a time and date (see *Time Configuration on page 67*)
- an optional **Network Time Protocol (NTP)** page, where you can optionally define NTP servers that can be used to override the manual date and time setting (see *Network Time Protocol (NTP) Configuration on page 67*)

Illustration 12 illustrates the way in which the time configuration is implemented on the NE-ONE.

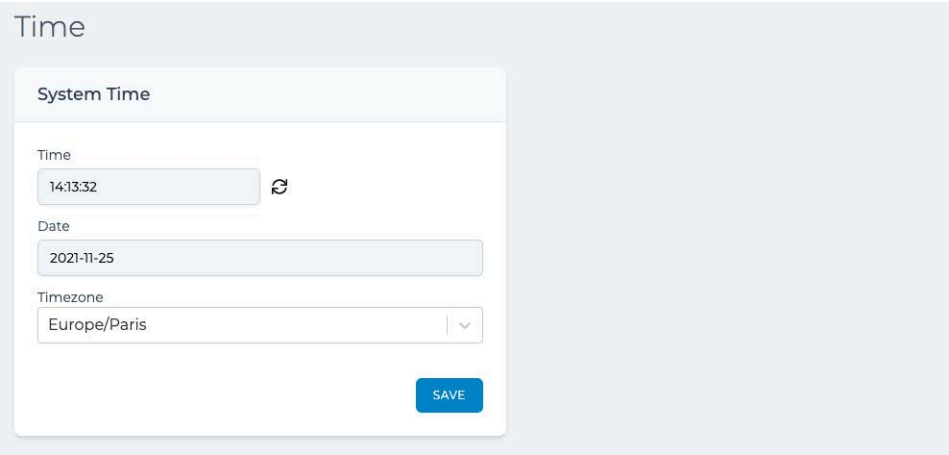
ILLUSTRATION 12 - TIME CONFIGURATION



6-1. Time Configuration

Use the following steps to set the time zone, and manually specify a time and date:

1. From the Web Interface, click **Management > Platform Settings > Time**.



2. From the **Time** page that appears, do the following:
   a. Select the appropriate timezone from the **Timezone** drop-down field.
   b. In the **Time** field, type the current time.
      The time must be in 24 hour format, as follows : `HH:MM:SS`.
   c. In the **Date** field, type the current date.
      The date format must use the following international format : `YYYY-MM-DD`.

Note:
A refresh time icon exists next to the **Time** field. Clicking on the refresh time icon updates the **Time** field with the current time and **Date** field with the current date based on the local system time and date, and is not linked to the time and date optionally obtained via NTP servers (if configured).

   d. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

6-2. Network Time Protocol (NTP) Configuration

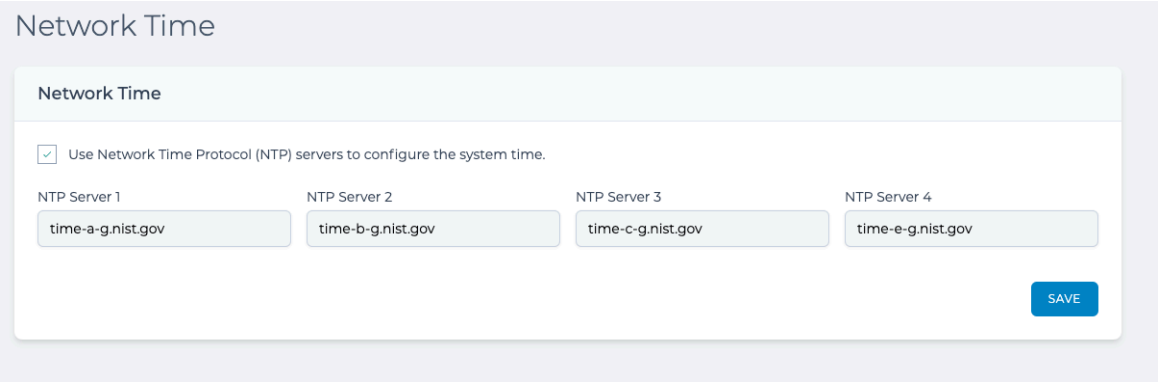
The NE-ONE lets you use the network time protocol (NTP) to set the time instead of manually configuring the time and date. For redundancy purposes, you can specify up to four different NTP servers.

Note:
If you enable NTP, the manual date and time settings defined in the **Time** page (see *Time Configuration on page 67*) are overridden, but you must still configure the timezone.

Note:
For redundancy purposes, Calnex recommends that you specify four NTP servers.

Use the following steps if you want to use NTP for setting the NE-ONE's date and time:

1. From the Web Interface, click **Management > Platform Settings > Network Time (NTP)**.



2. From the **Network Time** page that appears, do the following:
   a. Enable the **Use Network Time Protocol (NTP) servers to configure system time** check box.
      The **Time Server 1**, **Time Server 2**, **Time Server 3**, and **Time Server 4** fields are no longer grayed out.
   b. In the **Time Server 1** field, type the address of the primary NTP server.
   c. In the **Time Server 2** field, type the address of a second backup NTP server.
   d. In the **Time Server 3** field, type the address of a third backup NTP server.
   e. In the **Time Server 4** field, type the address of a fourth backup NTP server.
   f. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

7. CONFIGURING THE HOSTNAME

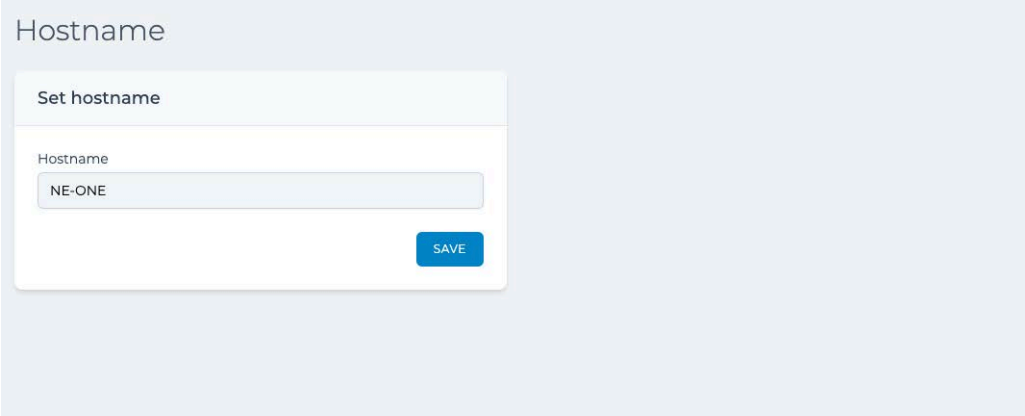
Use this section when you install the NE-ONE for the first time, or if you want to change the existing hostname of the NE-ONE. By default, the hostname assigned to the NE-ONE is NE-ONE.

Note:

If the organization's network contains more than one NE-ONE, Calnex recommends that a unique hostname is defined on each of the NE-ONEs.

Use the following steps to change the hostname of the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Hostname**.



2. From the **Hostname** page that appears, do the following:
   a. In the **Hostname** field, type the hostname that you want to assign to the NE-ONE.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

8. CONFIGURING THE WEB INTERFACE LABEL

Use this section when you install the NE-ONE for the first time, or if you want to change the existing label assigned to the NE-ONE's Web Interface.

The NE-ONE's Web Interface has a label (defined by the title tag) that appears in a web browser (see *Illustration 13*).

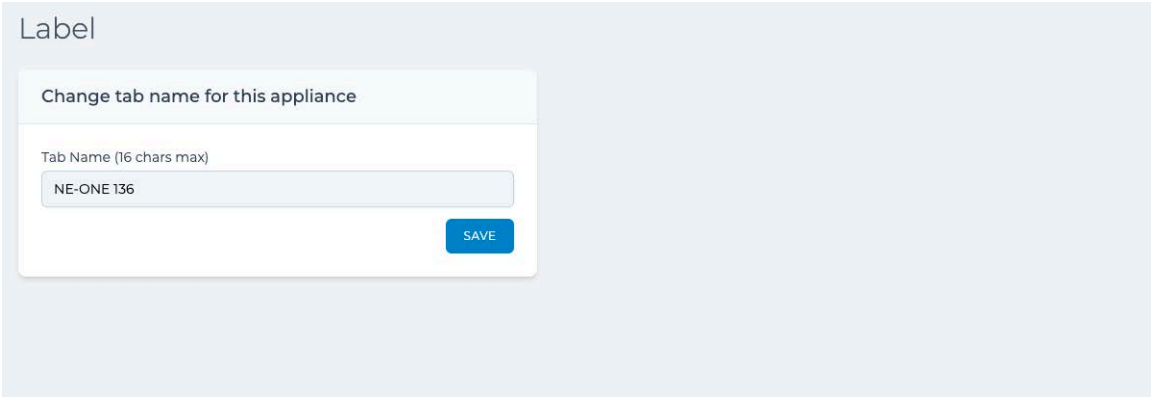
ILLUSTRATION 13 - MULTIPLE WEB INTERFACES OPEN IN A WEB BROWSER

The label is useful for situations where users have multiple NE-ONE Web Interfaces open in a web browser, and they want to quickly identify and switch between them via the web browser tabs. The label parameter lets you define a unique label for each NE-ONE so that a user can easily identify between them if they have more than one Web Interface open in their web browser.

By default, the label assigned to the NE-ONE's Web Interface is NE-ONE.

Use the following steps to change the label assigned to the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Label**.



2. From the **Label** page that appears, do the following:
   a. In the **Tab Name** field, type the label that you want to assign to the NE-ONE. The label can contain up to 16 alphanumeric characters.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

9. CONFIGURING HOUSEKEEPING

By default the NE-ONE is delivered with a housekeeping agent active so that it does not run out of disk space.

The housekeeping agent is initially configured as follows:

- housekeeping starts deleting files when the used storage reaches the high watermark level of 30%
- housekeeping stops deleting files when the used storage reaches the low watermark level of 20%
- the files older than 20 days are deleted in the following order (from top to bottom) until the low watermark level is reached:
  - Upgrade kits
  - System statistics
  - Network statistics
  - Operating system logs
  - User logs
  - Debug files

For example, if the used storage reaches 30% (i.e. high watermark level) and deleting some upgrade kits results in the used storage reaching 20% (i.e. the low watermark level), the housekeeping agent stops deleting files (i.e. System statistics, network statistics, etc. are not deleted).

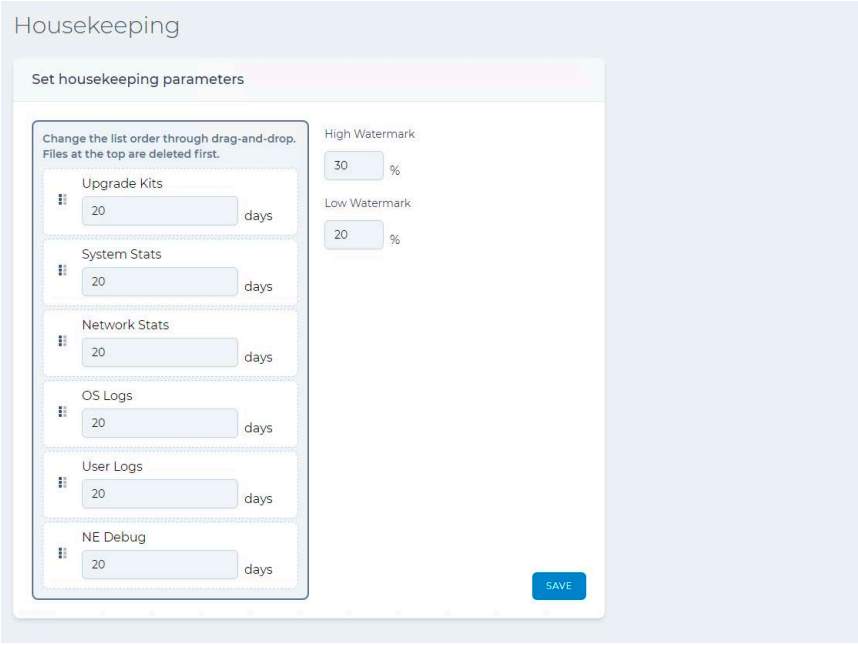
If desired, you can modify the housekeeping agent's high watermark level, low watermark level, the order in which the files are deleted, and the ages of the files that are deleted.

Note:

Setting the days value to -1 for a file type prevents that file type from being deleted. Therefore, if you set the days value to -1 for all file types, the housekeeping agent is effectively disabled.

If you want to modify the default housekeeping configuration, do the following:

1. From the Web Interface, click **Management > Platform Settings > Housekeeping**.
   A **Housekeeping** page appears.



2. From the **Housekeeping** page that appears, do the following:
   a. Optionally change the **High Watermark %** value (i.e. the percentage of the used storage at which the

system will start deleting files). The default value is 30%.

b. Optionally change the **Low Watermark %** value (i.e. the percentage of the used storage at which the system will stop deleting files). The default value is 20%.

c. In the days field for each of the file types, optionally modify the age at which the housekeeping agent will start deleting those file types. The default age threshold deletion date for each file type is 20 days.

d. Optionally re-order the order in which the file types are deleted. To do this, do the following:

- Place the mouse over the icon on the left hand side of the file type. The mouse icon changes to a cross.
- Click the mouse button to grab and select the file type.
- Drag the file type above or below another file type to the required position.
- Un-click the mouse button let go of the selected file type.
- Repeat these sub-steps above until the desired file type deletion order is achieved.

e. Click **SAVE**.

3. From the **Success** confirmation dialog that appears, click **OK**.

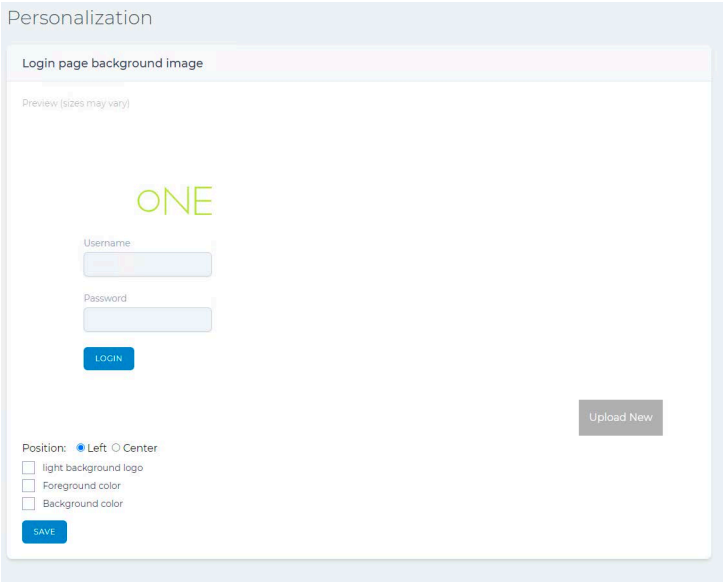
10. PERSONALIZING THE LOGIN PAGE

The NE-ONE login page can be personalized so that it matches your organizations branding. The personalization page lets you choose:

- the position of the login fields (left or center)
- whether the NE-ONE logo is dark (white NE and green ONE) or light (green NE and black ONE)
- the foreground color (i.e. the color of the login area)
  - if the login position is set to left, the chosen foreground color appears as a strip on the left hand side of the login page
  - if the login position is set to center, the chosen foreground color appears as a rectangle around the login fields
  - if no foreground color is chosen (i.e. transparent), the defined background color (bottom layer) or background image (middle layer) will be visible
- the background color (i.e. the color of the background (middle layer))
  - if no background color is chosen (i.e. transparent), the defined background image (middle layer) will be visible
  - if no background color is chosen and a background image is chosen, defined background image (middle layer) will be visible because it is above the background (bottom layer)
- an image
  - if the login position is set to left, the chosen image appears and is scaled within the area to the right hand side of the left hand side strip
  - if the login position is set to center, the chosen background appears and is scaled across the entire login page
  - if a background image is chosen, it replaces the chosen background color (i.e. the background image is the middle layer above the background layer, and below the layer of the foreground layer)

To personalize the login page, do the following:

1. From the Web Interface, click **Management** > **Platform Settings** > **Personalization**.
   A **Personalization** page appears.



2. Select the **Position** radio button (i.e. **Left** or **Center**) to set the position of the login fields. By default, **Left** is selected.

3. If required, ticked the light background check box.
   - If ticked, the NE-ONE logo is light (green NE and black ONE).
   - If ticked, the NE-ONE logo is dark (white NE and green ONE).
4. Optionally change foreground color (i.e. the color of the login area). To do this, tick the **Foreground color** and from the color palette that appears, select the desired color.
5. Optionally change background color. To do this, tick the **Background color** and from the color palette that appears, select the desired color.
6. Optionally upload a custom image. To do this, do the following:
   a. Click the **Upload New** button, and from the **Open** dialog box that appears navigate to and select an appropriate image, then click **Open**.

      The selected image gets uploaded to the NE-ONE and appears in the image gallery area of the **Personalization** page. It can now be chosen from the gallery by clicking on it.

      If necessary, repeat this step to upload additional images to add them to the image gallery area.
   b. Click on the uploaded image within the image gallery area to select the image. The selected image is indicated by a tick and appears in the preview area on the **Personalization** page.

      The example below shows an uploaded image selected with a gray foreground and a left login position.

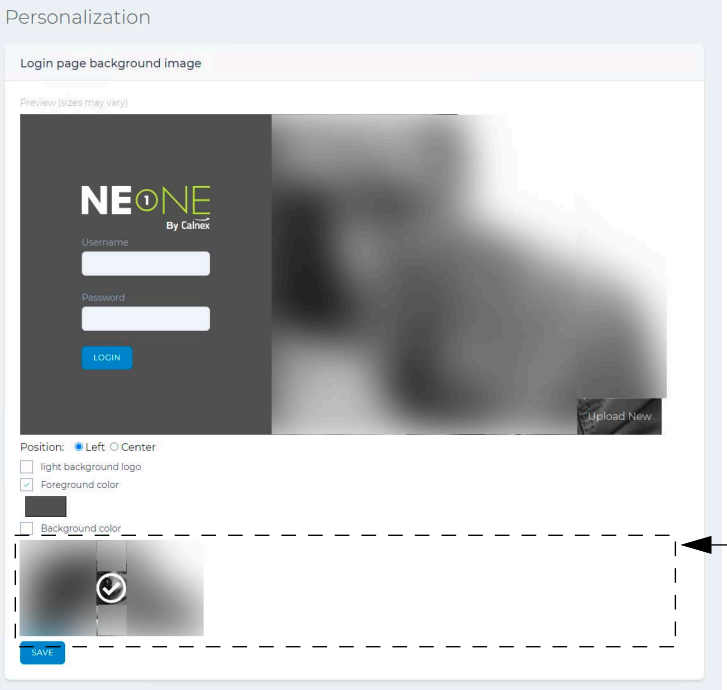


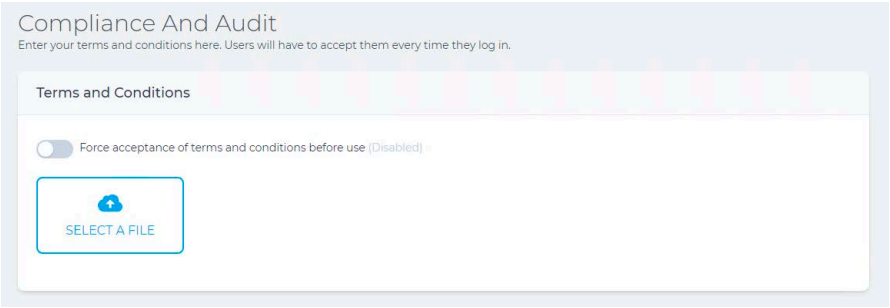
Image Gallery Area
Uploaded images can be selected by clicking on them in the image gallery area.

7. Click **SAVE**.
8. From the **Successfully updated login** page dialog, click **OK**.

11. APPLYING A COMPLIANCE AND AUDIT ACCEPTANCE AGREEMENT

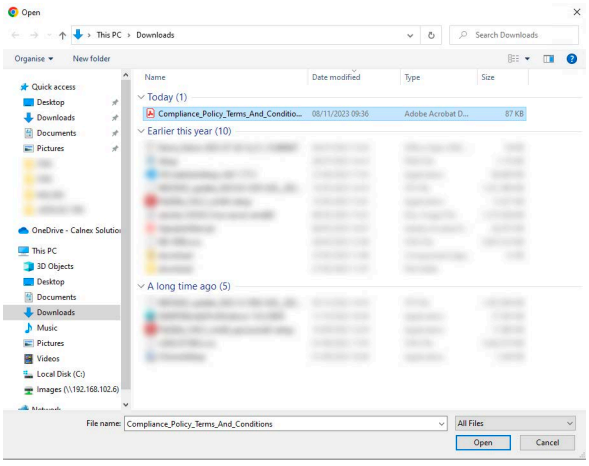
If your organization has a compliance and audit policy, you can upload a User Acceptance Document (in PDF format) to the NE-ONE and configure the NE-ONE so that it forces all users to agree to that policy each time they log in. To do this, use the following steps:

1. Obtain the User Acceptance Document (in PDF format) from the appropriate department in your organization. Copy it to an appropriate location on your PC (in our example, the Downloads folder).
2. From the Web Interface, click **Management > Platform Settings > Compliance and Audit**.
   A **Compliance And Audit** page appears.



Note:
If a User Acceptance Document has previously been uploaded, an additional **DOWNLOAD CURRENT** button exists.

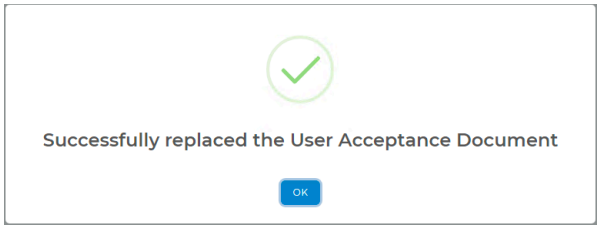
3. Click the **Select a File** button. From the **Open** dialog box that appears navigate to and select the User Acceptance Document PDF file that you copied to your PC and click **Open**.



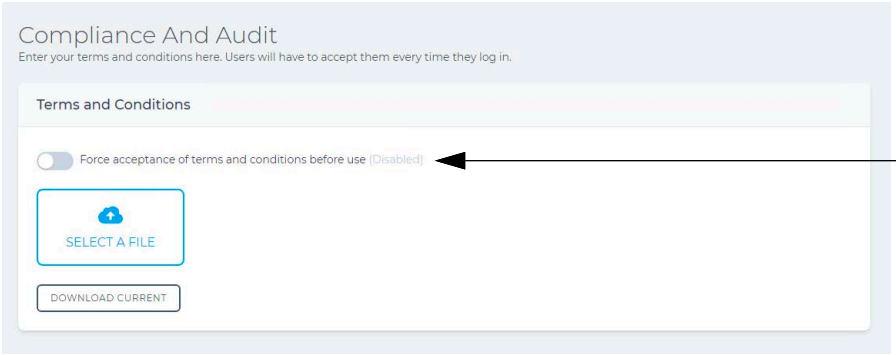
The **Compliance And Audit** page updates with the selected file.

4. Click the **UPLOAD FILE** button.

A **Successfully replaced the User Acceptance Document** dialog box appears.

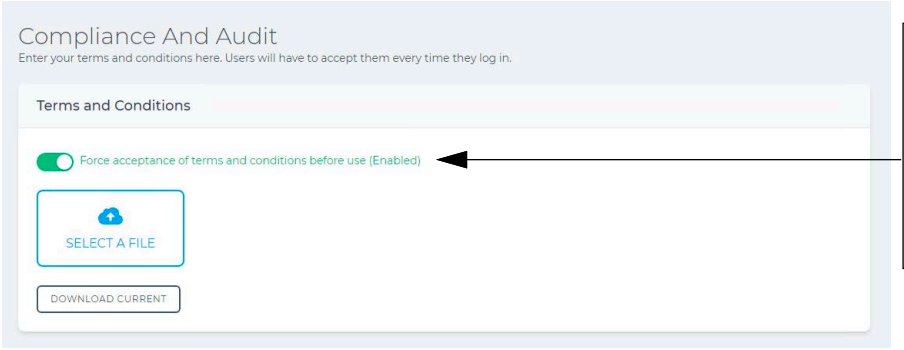


5. From the **Successfully replaced the User Acceptance Document** dialog box that appears, click **OK**.
   The **Compliance And Audit** page updates containing a **DOWNLOAD CURRENT** button, indicating that a User Acceptance Document exists on the NE-ONE.



With the toggle button disabled, the users are not prompted to agree with the terms and conditions of the uploaded User Acceptance Document each time they log in.

6. Enable the **Force acceptance of terms and conditions** toggle button.



With the toggle button enabled, the users are prompted to agree with the terms and conditions of the uploaded User Acceptance Document each time they log in.

Note:

Clicking the **DOWNLOAD CURRENT** button lets you download the currently uploaded User Acceptance Document.

12. CONFIGURING THE SYSTEM PREFERENCES

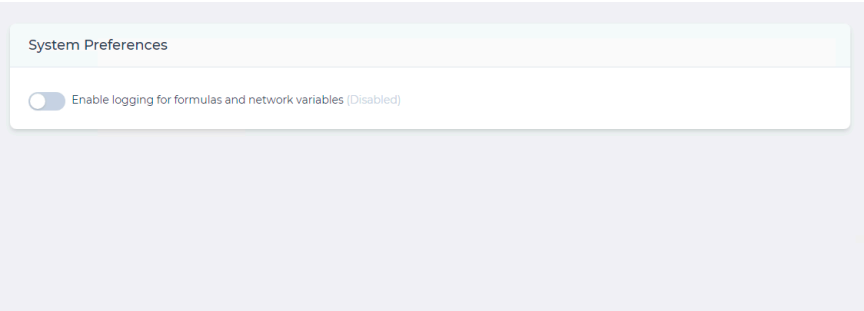
Use this section when you install the NE-ONE for the first time, or if you want to change the existing system preferences settings of the NE-ONE.

Note:

At the current release the **System Preferences** page has one setting for enabling/disabling logging for formulas and network variables. By default, logging for formulas and network variables is disabled. Logging for formulas and network variables is useful when using formulas and network variables on your networks. When logging is enabled, the log information is written to the `system.log` file in the `/Support` directory. For more information on the use for formulas and network variables, see *Chapter 16*, *Dynamic Formulas and Network Variables*.

Use the following steps to change the system preferences of the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > System Preferences**.



2. From the **System Preferences** page that appears, do the following:
   - If you want logging for formulas and network variables enabled, click on the **Enable logging for formulas and network variables** toggle switch so that the status is enabled.
   - If you want logging for formulas and network variables disabled, click on the **Enable logging for formulas and network variables** toggle switch so that the status is disabled.

13. CONFIGURING SNMP

If the organization uses Simple Network Management Protocol (SNMP) as a method of network management, then use this section when you install the NE-ONE for the first time, or at a later date if the organization's SNMP configuration changes.

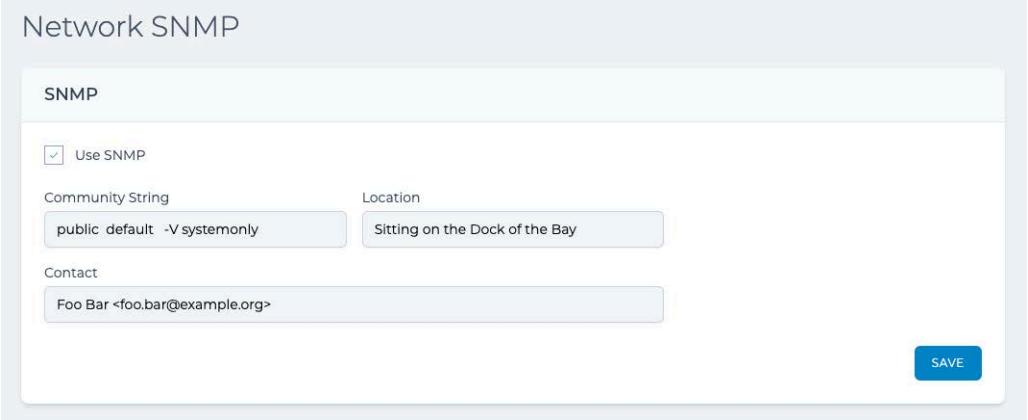
By default, the NE-ONE is not configured to use SNMP (i.e. the SNMP service is not enabled and not configured). If the organization uses SNMP, their network administrator will provide you with the following the Community String, location and contact.

Note:

At the current release, the NE-ONE does not support SNMP V3 username and password implementation.

Use the following steps to change the SNMP configuration of the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > SNMP**.



2. From the **Network SNMP** page that appears, do the following:
   a. If you want the SNMP service to be active, check the **Use SNMP** check box. If you do not want the SNMP service to be active, uncheck the **Use SNMP** check box.
   b. If the SNMP service is enabled, define the following values:

      In the **Device Location** field, type an appropriate location corresponding to where the NE-ONE is located in the organization. The **Device Location** field accepts alphanumeric characters and spaces.

      In the **Community String** field, type an appropriate community string (e.g. `public default -V systemonly`). The **Device Location** field accepts alphanumeric characters and spaces.

      In the **Contact** field type the name and email address of the contact person responsible for managing the NE-ONE. The email address must be surrounded by angled brackets. For example, it the contact person is called Foo Bar with the e-mail address foo.bar@example.org, you would type `Foo Bar <foo.bar@example.org>`.
   c. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

14. CONFIGURING THE AUTHENTICATION METHOD

Use this section when you install the NE-ONE for the first time, or at a later date if the organization's authentication method has changed and you need to change the existing authentication method used by the NE-ONE.

By default, the NE-ONE is configured to use built-in authentication, with locally (built-in) defined users. In this case, the authentication and users are managed locally on the NE-ONE.

In addition to local (built-in) authentication, the NE-ONE also supports LDAP and RADIUS authentication methods.

Note:

LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

If the NE-ONE uses local (built-in) authentication or LDAP authentication, you must also add local users (see *Adding Local and Semi-Local Users on page 216*).

Table 9 summarizes the differences between how the Built-in, LDAP and RADIUS authentication methods are implemented on the NE-ONE.

Note:

In order to access the NE-ONE for the first time, a built-in admin user exists, which cannot be removed even if LDAP or RADIUS authentication is configured. This is normal so that the built-in admin user can be used for initial access, and if necessary future access in cases where the organization's LDAP or RADIUS server may be down.

TABLE 9 - DIFFERENCES BETWEEN BUILT-IN, LDAP, AND AUTHENTICATION METHODS

	Built-in	LDAP	RADIUS
User type	Local	Semi-local	Non-local
Creation of users	On the NE-ONE's **Users** Web Interface page.	Users (usernames and passwords) exist on the LDAP server. These users must also be created on the NE-ONE's **Users** Web Interface page, but no password is specified as it is managed by the LDAP server.	Users (usernames and passwords) exist on the RADIUS server.
Configuration of user permissions (i.e. assigned ports, number of networks, number of objects, number of links)	On the NE-ONE's **Edit User Details** Web Interface page.		On the RADIUS server: • by importing the `dictionary.itrinegy` file into the RADIUS sever • by adding appropriate `iTrinegy-NEONE` attributes to the user
Web Interface user authentication method	Locally on the NE-ONE, via the local database.	Remotely on the LDAP server: • login request from NE-ONE sent to LDAP server • if username does not exist on LDAP server the login request is rejected • if username exists on LDAP server, but the specified password is wrong the login request is rejected • if username exists on LDAP server, and the specified password is correct the login request is accepted	Remotely on the RADIUS server: • login request from NE-ONE sent to RADIUS server • if username does not exist on RADIUS server the login request is rejected • if username exists on RADIUS server, but the specified password is wrong the login request is rejected • if username exists on RADIUS server, and the specified password is correct the login request is accepted • if the successfully logged in user has connected to the NE-ONE for the first time, a `/Private` directory is created for that user
Presentation of the user permissions to the logged in user on the Web Interface	Determined locally on the NE-ONE, via the local database, and what an admin type user had configured for the user within the **Edit User Details** Web Interface page.		Determined remotely on the RADIUS server according to the different `iTrinegy-NEONE` attributes that were assigned to the user.

14-1. Configuring Built-in Authentication

By default, the NE-ONE is configured to use built-in authentication, with locally (built-in) defined users. You would only use the steps below in the rare situation where you had previously configured LDAP or RAIDUS

authentication, but want to revert back to using built-in authentication.

1. From the Web Interface, click **Management > Platform Settings > Authentication**.
2. From the **Authentication** page that appears, select **Built-in** in the **Authentication Method** drop-down field.
3. Click **SAVE**.
4. From the **Success** confirmation dialog that appears, click **OK**.

Note:
If you were previously using the LDAP authentication method, you will need to edit each of the existing users on the NE-ONE to configure their passwords as previously the NE-ONE was getting their passwords from the LDAP server. For more information, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication) on page 217*.

Note:
If you were previously using the RADIUS authentication method, the `/Private` directories for each of those users will already exist on the NE-ONE. You will need to create the users (according to *Adding Local and Semi-Local Users on page 216*) and define permissions (according to *Configuring and Editing User Permissions (for Built-in and LDAP authentication) on page 217*). In this rare case, if you require additional help to know how to find the usernames that have been created on the NE-ONE, contact your Calnex support representative, or Calnex support.

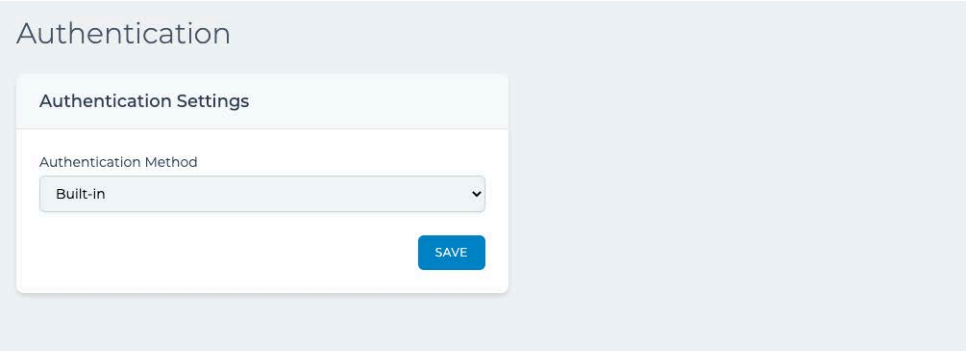
14-2. Configuring LDAP Authentication

If the organization uses either the LDAP authentication method, their network administrator will provide you with the following:

- Primary LDAP Server FQDN or IP address
- Secondary Primary LDAP Server FQDN or IP address

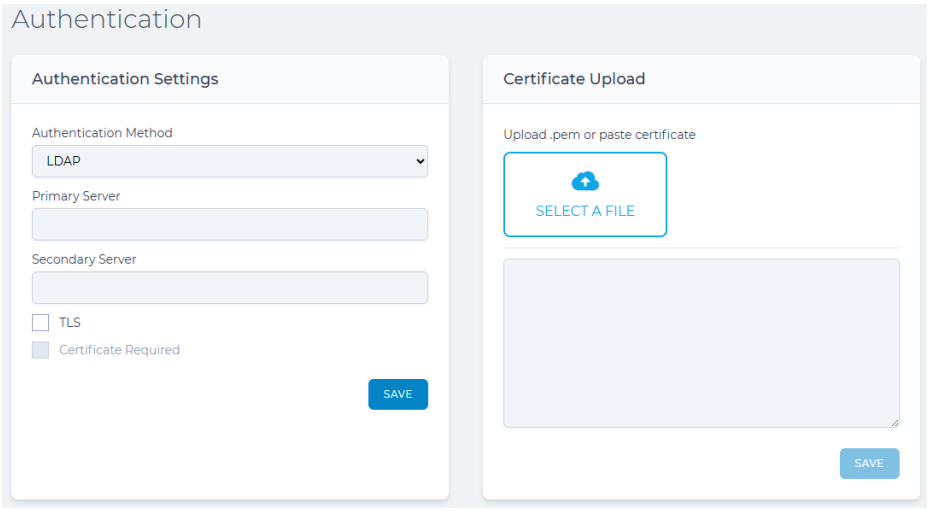
Use the following steps to configure the NE-ONE to use the LDAP authentication method:

1. From the Web Interface, click **Management > Platform Settings > Authentication**.



2. From the **Authentication** page that appears, select **LDAP** in the **Authentication Method** drop-down field.
   The **Authentication Settings** tile of the **Authentication** page updates with fields corresponding to configuring

the LDAP servers.



3. In the **Primary Server** field, type the FQDN or IP address of the organization's Primary LDAP Server.
4. In the **Secondary Server** field, type the FQDN or IP address of the organization's Secondary LDAP Server.
5. If you want to enable secure authentication over LDAP, tick the TLS option. If the LDAP server requires certificate verification, check the "Certificate Required" box and upload the .pem file that belongs to the LDAP server. After uploading the certificate file, it will be displayed on the left. Make sure both "SAVE" buttons are clicked.
6. Click **SAVE**.
7. From the **Success** confirmation dialog that appears, click **OK**.

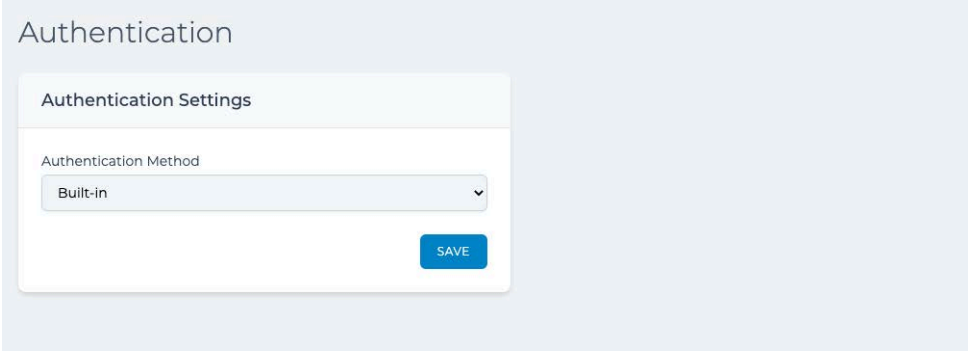
14-3. Configuring RADIUS Authentication

If the organization uses the RADIUS authentication method, obtain the following information from the network administrator:

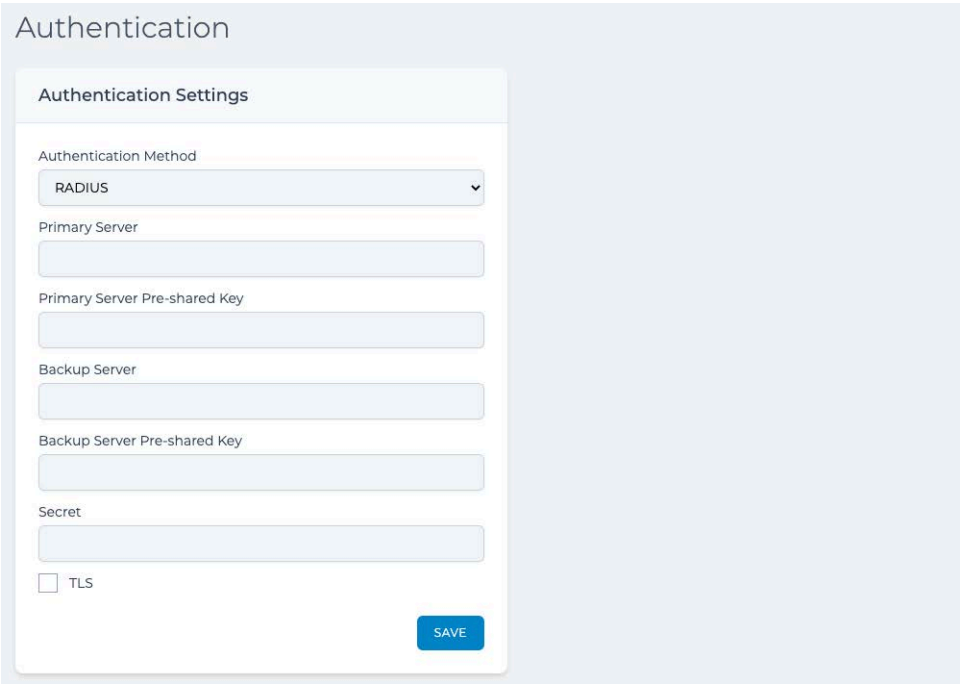
- Primary RADIUS server FQDN or IP address.
- Primary RADIUS server pre-shared key (PSK).
- Backup RADIUS server FQDN or IP address.
- Backup RADIUS server PSK.
- The shared secret used by the Primary and Backup RADIUS servers.
- Determine whether or not the RADIUS servers are using RADIUS over TLS with the PSKs (i.e. the RADIUS servers are using secure communication via the Transport Layer Security (TLS) protocol with the PSKs).

Use the following steps to configure the NE-ONE to use the LDAP authentication method:

1. From the Web Interface, click **Management > Platform Settings > Authentication**.



2. From the **Authentication** page that appears, select **RADIUS** in the **Authentication Method** drop-down field. The **Authentication Settings** tile of the **Authentication** page updates with fields corresponding to configuring the RADIUS servers.



3. In the **Primary Server** field, type the FQDN or IP address of the organization's Primary Radius Server.
4. In the **Primary Server Pre-shared Key** field, type the PSK of the organization's Primary Server.
5. In the **Backup Server** field, type the FQDN or IP address of the organization's Backup Radius Server.
6. In the **Backup Server Pre-shared Key** field, type the PSK of the organization's Backup Server.
7. In the **Secret** field, type the shared secret that is used to send its encrypted access-request to the RADIUS servers.
8. If the RADIUS servers are using secure communication via the TLS protocol (using the PSK), check the **TLS** check box. If the RADIUS servers are not using secure communication via the TLS protocol (using PSK), un-check the **TLS** check box.
9. Click **SAVE**.
10. From the **Success** confirmation dialog that appears, click **OK**.

15. INSTALLING AND UPDATING ROOT SSL CERTIFICATES

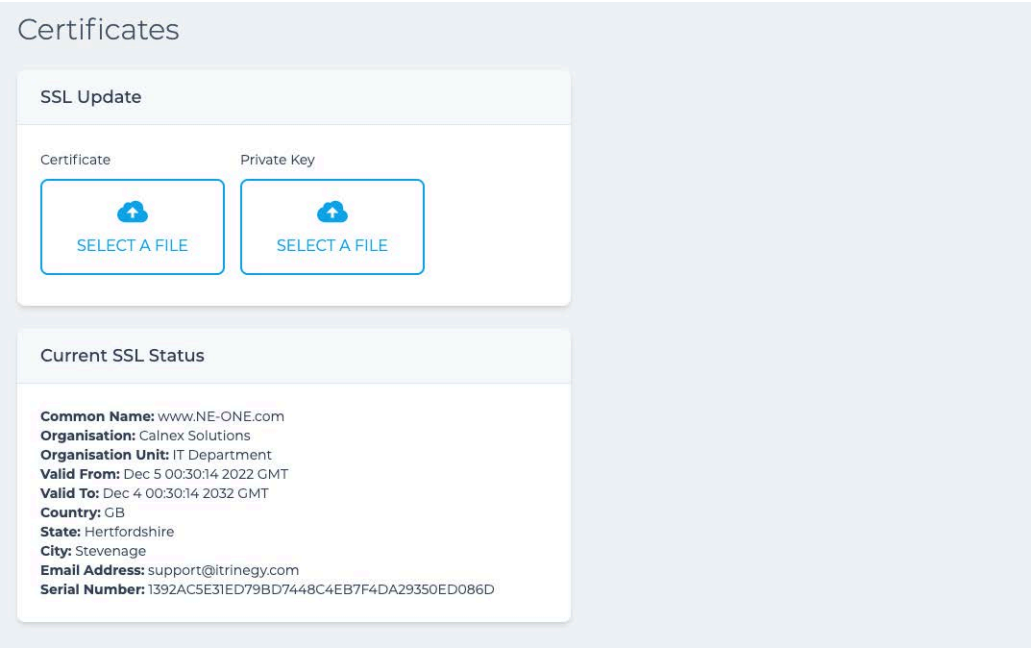
If the organization uses a Root SSL Certificate, then use this section when you install the NE-ONE for the first time, or at a later date when the organization's current Root SSL Certificate is due to expire.

Note:

If the organization does not use a Root SSL Certificate, the NE-ONE will use the default supplied self-signed Calnex SSL Certificate. In this case, when users connect to the NE-ONE Web Interface for the first time, they will need to perform a few steps to accept the self-signed Calnex SSL Certificate. For more information, see *First time Web Interface access (accepting the default self-signed SSL certificate) on page 29*.

Use the following steps to install a Root SSL Certificate and Private Key on the NE-ONE:

1. Obtain the latest Root SSL Certificate and Private Key from the organization's network administrator, and copy them to your preferred location on your computer's filing system.
2. From the Web Interface, click **Management > Platform Settings > Certificate**.



Note:

The **Current SSL Status** section of the **Certificates** page contains the SSL certificate expiry date (indicated by **Valid To:**). This information is useful to ensure that you have the time to plan and acquire a new Root SSL certificate from a trusted CA before the current Root SSL certificate runs out.

3. From the **Certificates** page that appears, do the following:
   a. Click the **Certificate SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the SSL Root Certificate to upload.
   b. Click the **Private Key SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the Private Key to upload.
4. From the **Success** confirmation dialog that appears, click **OK**.

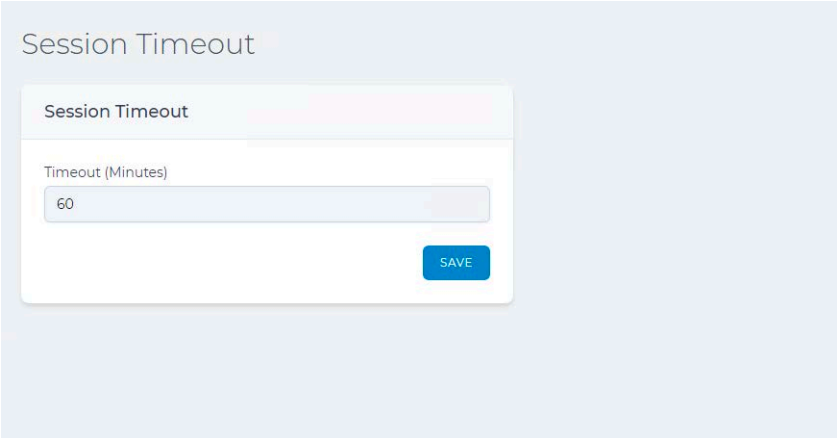
16. SESSION TIMEOUT CONFIGURATION

Use this section when you install the NE-ONE for the first time, or if you want to change the existing session timeout configuration of the NE-ONE.

The session timeout configuration defines how long an inactive Web Interface session remains open before automatically logging out. By default the session timeout configuration is set to 60 minutes.

Use the following steps if you want to change the existing session timeout configuration of the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Session Timeout**.



2. From the **Session Timeout** page that appears, do the following:
   a. In the **Timeout (Minutes)** field, type the value in minutes (or use the up/down arrows) to define the session timeout.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

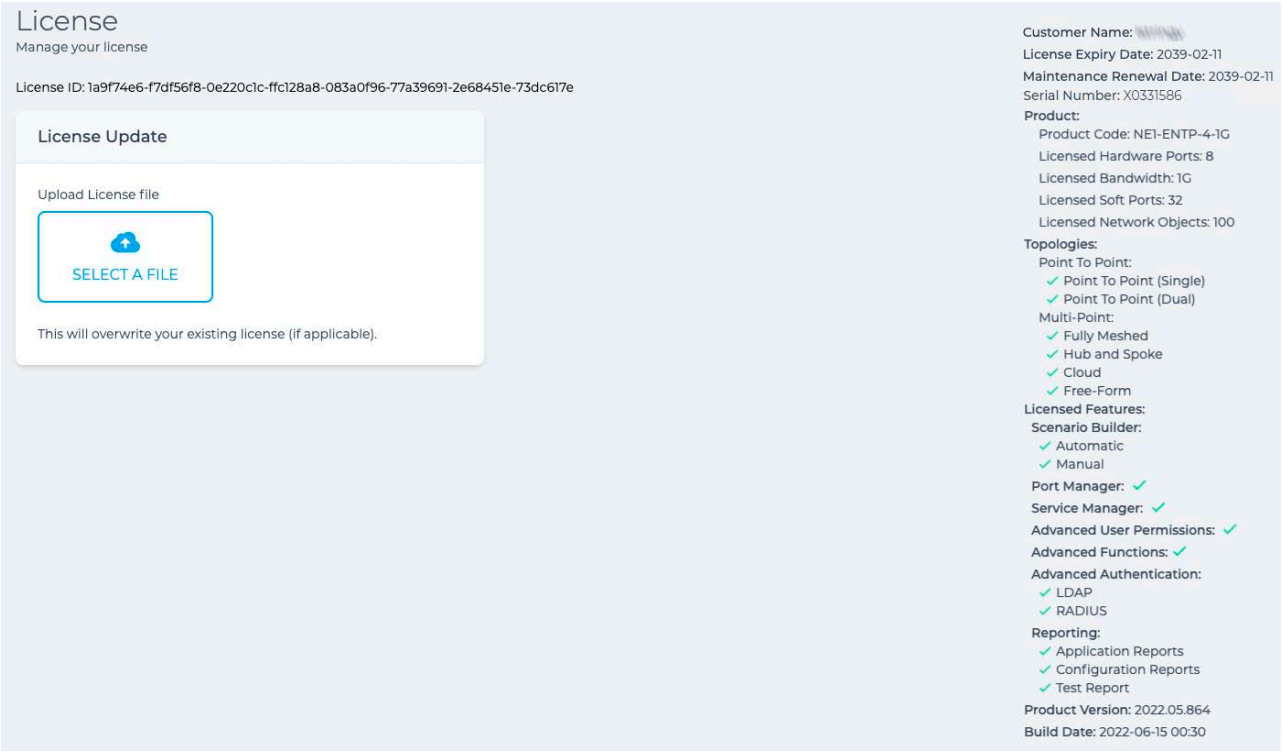
17. VIEWING AND APPLYING LICENSE FILES

Use this section when you install the NE-ONE for the first time, or if you want to view and/or update the existing license file that is installed on the NE-ONE.

By default, the NE-ONE is supplied with a temporary license file with limited functionality. In order to make the NE-ONE fully functional, you must obtain a license file from Calnex and apply it on the NE-ONE.

Use the following steps to view and install a license file on the NE-ONE:

1. Obtain the license file from the Calnex customer support site:
   a. Go to *https://calnex-support.com*, and login with your Calnex provided customer username and password.
   b. In the Calnex customer support site, navigate to the licenses area, and download the license associated with your NE-ONE to your computer's local filing system.
2. From the Web Interface, click **Management > Platform Settings > License**.



3. From the **License** page that appears, do the following:
   a. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the license to upload.
4. From the **Success** confirmation dialog that appears, click **OK**.

18. CUSTOM LOCATIONS

By default, the NE-ONE is delivered with the majority of locations within the world. The locations are used when configuring a node's location from within the **Edit node** panel of either the Point-to-Point Designer (see *Illustration 77 on page 276*) or Mutli-Point Designer (see *Illustration 91 on page 348*).

If compared to those included with the NE-ONE, your non-admin users require additional locations for the nodes that they create within their networks, follow the steps described in *section 18-1*, *Creating Custom Locations*.

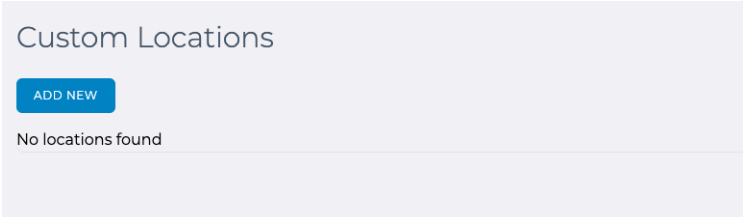
18-1. Creating Custom Locations

Use the steps below to create a custom location.

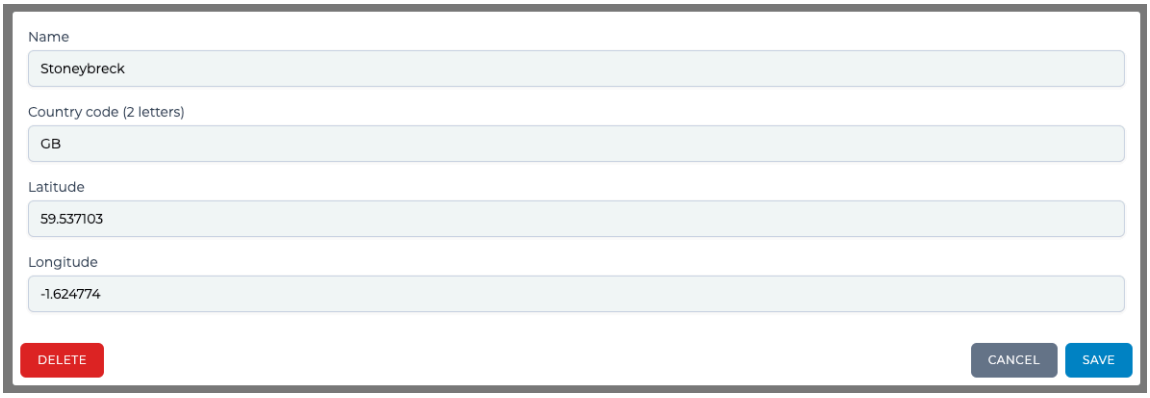
Note:

The example below shows adding the small island of Stonybreck in the sea, just north of Scotland.

1. From the Web Interface, click **Management > Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist (if any) on the NE-ONE.

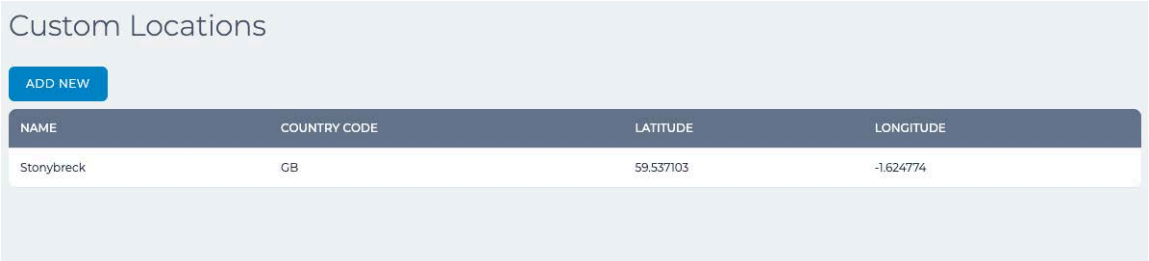


2. From the **Custom Locations** page that appears, click the **ADD NEW** button.
   A dialog box appears letting you define the parameters of the custom location.



3. From the dialog box that appears, do the following:
   a. In the **Name** field, type the name of the location.
   b. In the **Country code (2 letters)** field, type the two letter ISO3166-1 alpha-2 Country Code corresponding to the country in which the location exists.
   c. In the **Latitude** field, type the latitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   d. In the **Longitude** field, type the longitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   e. Click **SAVE**.
4. From the **Successfully added location** confirmation dialog that appears, click **OK**.
   The **Successfully added location** confirmation dialog box closes, and the **Custom Locations** page updates

with the newly added custom location.



Once a custom location has been created, if necessary, it can be edited or deleted. For more on editing and deleting a custom location, see *section 18-2*, *Editing Custom Locations* and *section 18-3*, *Deleting Custom Locations*, respectively.

Notice:

Once you have created all of your custom locations, instead of having to re-create them all again on a different NE-ONE, they can be quickly imported to a different NE-ONE. For more information, see *section 18-4*, *Importing Already Created Custom Locations to Other NE-ONEs*.

18-2. Editing Custom Locations

Once one or more custom locations have been created, they are listed in the **Custom Locations** page, from where their parameters (i.e. country code and latitude/longitude coordinates) can be edited if necessary. If you want to edit an existing custom location, use the steps below.

Note:

You cannot edit the name of an existing custom location. If you created a location with the wrong name, delete it according to *section 18-3*, *Deleting Custom Locations*, then re-create it with the correct name according to *section 18-1*, *Creating Custom Locations*.

1. From the Web Interface, click **Management > Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist on the NE-ONE.

2. From the **Custom Locations** page that appears, click the custom location that you want to edit.
   A dialog box appears letting you edit the existing parameters of the custom location.

3. From the dialog box that appears, do the following:
   a. If necessary, in the **Country code (2 letters)** field, modify the two letter ISO3166-1 alpha-2 Country Code corresponding to the country in which the location exists.
   b. If necessary, in the **Latitude** field, modify the latitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   c. If necessary, in the **Longitude** field, modify the longitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   d. Click **SAVE**.
4. From the **Successfully edited location** confirmation dialog that appears, click **OK**.
   The **Successfully added location** confirmation dialog box closes, and you are returned to the **Custom Locations** page.

18-3. Deleting Custom Locations

Once one or more custom locations have been created, they are listed in the **Custom Locations** page, from where they can be edited if necessary. Typically, you would not want to delete a custom location, unless you had incorrectly named it during its initial creation. If you want to delete an existing custom location, use the steps below.

1. From the Web Interface, click **Management > Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist on the NE-ONE.

2. From the **Custom Locations** page that appears, click the custom location that you want to delete.
   A dialog box appears letting you delete the custom location.

3. From the dialog box that appears, click **DELETE**.
   The custom location is immediately deleted, and **Deleted location successfully** confirmation dialog appears.
4. From the **Deleted location successfully** confirmation dialog that appears, click **OK**.
   The **Deleted location successfully** confirmation dialog box closes, and you are returned to the **Custom Locations** page.

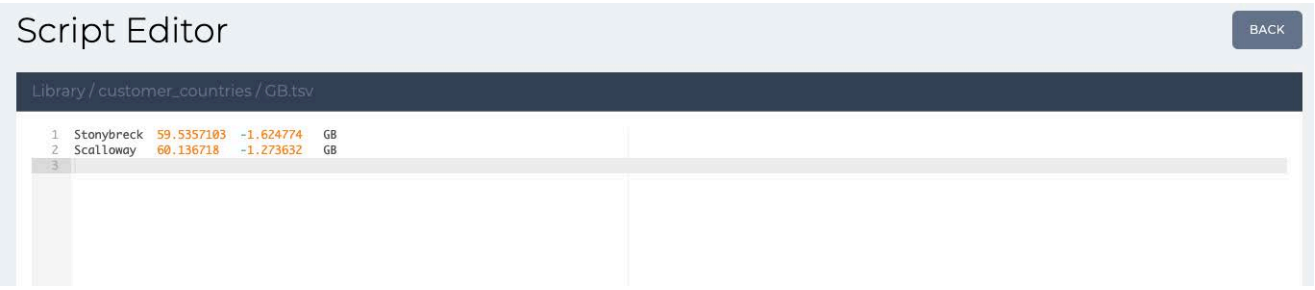
18-4. Importing Already Created Custom Locations to Other NE-ONEs

When you create a custom location, a `<country code>.tsv` file gets created in the `/Library/customer_countries` directory, where `<country code>` is the two letter ISO3166-1 alpha-2 Country Code. Each time you add a custom location belonging to the same `<country code>`, its parameters get appended to the `<country code>.tsv` file on a new line. Each custom location in the `<country code>.tsv` file is a separate line, in tab delimited form of the following format:

`<location name> <latitude> <longitude> <country code>`

Illustration 14 shows an example of two custom locations called Stonybreck and Scalloway belonging to the same GB country code that get created in a `GB.tsv` file. In this example, when you create the first custom location (e.g. Stonybrock) belonging to the GB country code, a `GB.tsv` file gets created within the directory `/Library/customer_countries`. If you add additional custom locations within the same GB country code (e.g. Scalloway), they get appended to the `GB.tsv` file.

ILLUSTRATION 14 - EXAMPLE TSV FILE FOR TWO CUSTOM LOCATIONS WITHIN COUNTRY CODE GB

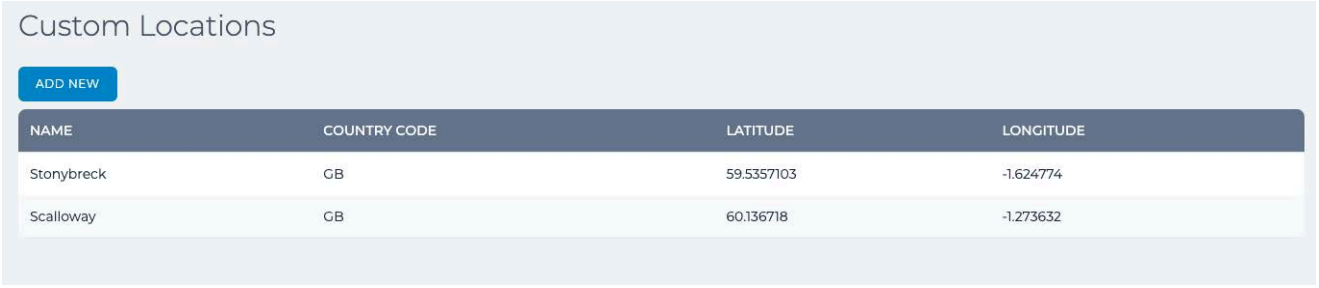


Note:

You can view *.tsv files in the script editor for viewing, but the possibility to modify the file and save it is intentionally dis-activated.

Illustration 15 shows how the same two locations (e.g. Stonybreck and Scalloway) belonging to the same GB country code are represented in the **Custom Locations** page.

ILLUSTRATION 15 - EXAMPLE CUSTOM LOCATIONS PAGE FOR TWO CUSTOM LOCATIONS WITHIN COUNTRY CODE GB



If you have created many custom locations belonging to different country codes and have multiple NE-ONEs in your environment, rather than taking time re-create them on the other NE-ONEs you can download each of the finalized `<country code>.tsv` files from the "master" NE-ONE where you created them, and upload them to the "other" NE-ONEs in your environment. To do this, use the following steps below:

1. Login to the "master" NE-ONE as an admin user, and create all of your custom locations for each county code according to *section 18-1*, *Creating Custom Locations*.
2. Once you are happy with the finalized set of locations for each country code on the "master" NE-ONE, do the following:
   a. From the Web Interface, click **Management > Platform Settings > File Browser**.

The **File Browser** page opens with the path of your `/Private` directory.

b. Navigate to the `/Library/customer_countries` directory.

c. For each of the `<country code>.tsv` files that exist, right mouse click on them, and select **Download selected File**.

Each of the `<country code>.tsv` files are downloaded to your computer's local filing system, and are now ready for uploading to all the "other" NE-ONEs in your environment.

3. For each of the "other" NE-ONEs in your environment that you want to import the `<country code>.tsv` files, do the following:

a. Login as an admin user on the "other" NE-ONE.

b. From the Web Interface, click **Management > Platform Settings > File Browser**.

The **File Browser** page opens with the path of your `/Private` directory.

c. Navigate to the `/Library/customer_countries` directory.

d. Right mouse click and select **Upload new File**.

A dialog box appears prompting you to select a file to upload.

e. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the appropriate `<country code>.tsv` file to upload. Then click **OK**.

f. Repeat sub-steps d to e until all the `<country code>.tsv` files are uploaded to the "other" NE-ONE.

The custom locations from the "master" NE-ONE are now available on the "other" NE-ONE.

19. CONFIGURE EXTERNAL ROUTING

Use this section when you install the NE-ONE for the first time within your network if it uses dynamic routing (adaptive routing), or at a later time if the network has changed to use dynamic routing (adaptive routing).

Note:

At the time of publication, the NE-ONE currently supports BGP, OSPF, OSPFv6, RIP, and RIPng routing protocols. If your organization uses another routing protocol such as Interior Gateway Routing Protocol (IGRP) or Intermediate System to Intermediate System (IS-IS), contact your Calnex representative for more information on how and when those other routing protocols will be implemented on the NE-ONE.

In order for the NE-ONE to inter-operate with networks using dynamic routing (adaptive routing), external routing must be configured on NE-ONE for the routing protocols used within the network.

External routing on the NE-ONE is configured for example in production or DevOps environments, when connecting to the edge of the corporate network. External routing on the NE-ONE would not be configured in a pure test environment.

Table 10 provides a high level comparison between the different routing protocols supported by the NE-ONE, and when they are typically used. If you require assistance defining your external routing requirements, contact your Calnex support representative for further support.

TABLE 10 - HIGH LEVEL COMPARISON BETWEEN ROUTING PROTOCOLS SUPPORTED ON THE NE-ONE

Comparison Criteria		RIP RIPng	BGP	OSPF OSPFv6
Algorithm used		Bellman Ford	Best Path Selection	Dijkstra algorithm
Routing Protocol Method		Distance Vector Routing (DVR) protocol that uses the distance or hops count to determine the transmission path.	Path Vector Routing (PVR) protocol that provides routing information for autonomous systems on the Internet via its AS-Path	Link State Routing (LSR) protocol and it analyzes different sources like the speed, cost and path congestion while identifying the shortest path.
Organization size used within		Small	Large (exterior gateway protocol, typically only at edge locations)	Large (interior gateway protocol)
Typical use within the large organization (between BGP and OSPF)	Internet redundancy	Not applicable for comparison	Most often used	Never or rarely used
	LAN environments		Never or rarely used	Most often used
	WAN environments		Most often used	Occasionally used
	Data center		Never or rarely used	Most often used
	IaaS environments		Most often used	Occasionally used
Maximum hops allowed	Maximum hops allowed	15	255	No restriction on the hop count.
Networks classified as	Networks classified as	Areas and tables.	Peers.	Areas, sub areas, autonomous systems and backbone areas.
Default administrative distance	Default administrative distance	120	20	110

Comparison Criteria		RIP RIPng	BGP	OSPF OSPFv6
Protocol (port) used	Protocol used	UDP (520)	TCP (179)	IP (89)
By default, for path selection calculates the metric in terms of	By default, for path selection calculates the metric in terms of	Hop Count (only next hop in calculation)	Hop Count (determines best path as calculation, includes the 'path' of ASes that are used to reach the destination)	Bandwidth

19-1. External Routing Prerequisites

Check with your network administrator if the organization is using dynamic routing (adaptive routing) or static routing (non-adaptive routing).

- If the organization is static routing (non-adaptive routing), no further action is required (i.e. external routing on the NE-ONE does not need to be configured).
- If the organization is using dynamic routing (adaptive routing), the network administrator will have chosen a routing protocol of preference (BGP, OSPF, OSPFv6, RIP, or RIPng) for the network and will have defined routing tables on the routers within the network. In this case external routing on the NE-ONE needs to be configured.
  - Ask the network administrator which routing protocol is implemented within the network, and the external routing tables that you need to define on the NE-ONE in order for the NE-ONE to inter-operate with the routing protocol that is implemented within the network.

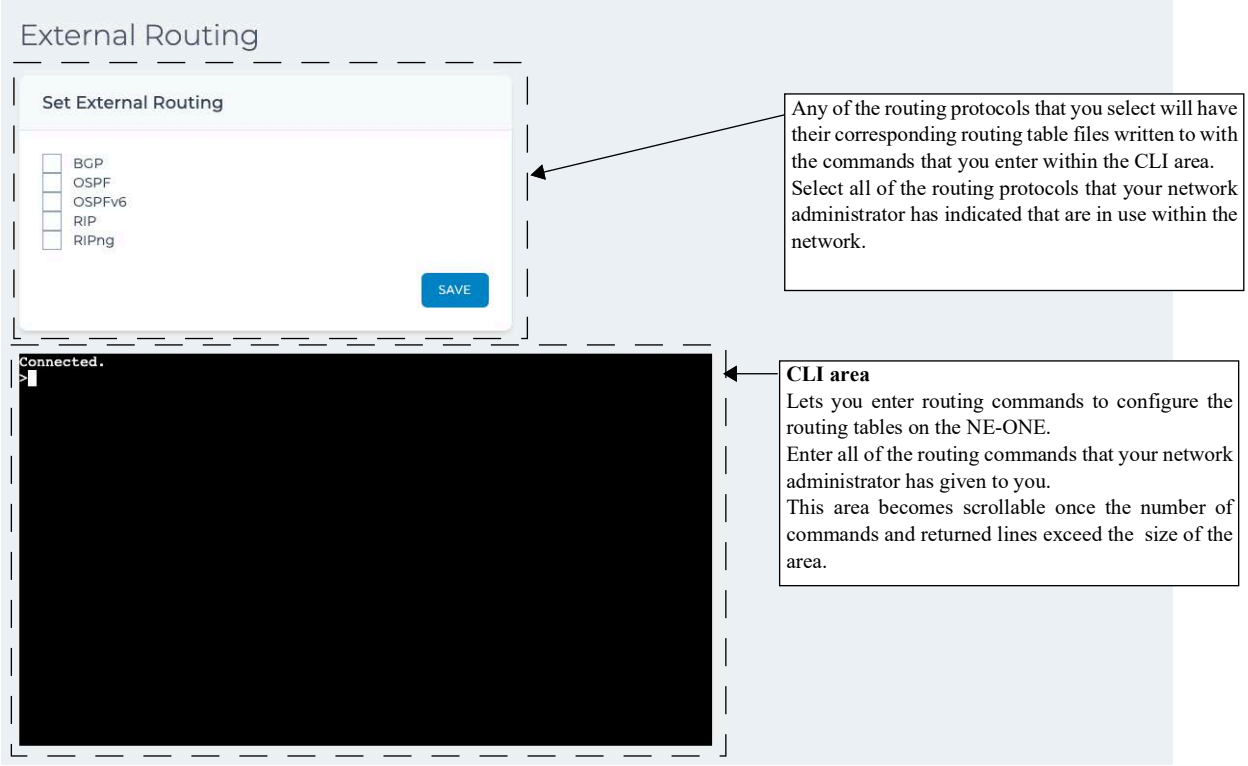
    The network administrator will indicate which routing protocol is implemented within the network and the routing commands that you need to specify in order to build the routing tables on the NE-ONE. Once you have this information from the network administrator, proceed to *Configuring External Routing on page 94*.

19-2. Configuring External Routing

If the NE-ONE is implemented in a network where dynamic routing (adaptive routing) is used then the NE-ONE must be configured to use external routing based upon the routing information that you obtained from your network administrator.

The **External Routing** page (see *Illustration 16*) lets you set up external routing on the NE-ONE so that it can inter-operate within networks that use dynamic routing (adaptive routing).

ILLUSTRATION 16 - THE EXTERNAL ROUTING PAGE



The **External Routing** page contains the following:

- A **Set External Routing** tile with check boxes allowing to select one or more of the following routing protocols:
  - **BGP** - Border Gateway Protocol
  - **OSPF** - Open Shortest Path First
  - **OSPFv6** - Open Shortest Path First for IPv6 (used only for Cisco devices to define the configuration done with the `ipv6 router ospf` command).
  - **RIP** - Routing Information Protocol
  - **RIPng** - Routing Information Protocol (next generation for IPv6)
- A command line interface (CLI) area lets you enter routing commands letting you set up your routing table and routing rules according to your routing requirements. Any of the routing commands that you enter in the CLI area will get written to the routing table file(s) of the selected routing protocol(s).

  The command line interface (CLI) area initially appears with the top-level command prompt, >.

  To enter a particular routing mode's command line in the command line window, the appropriate check box in the **Set External Routing** tile must be checked, and you must enter the appropriate command of the format **`ip-routing <routing protocol>`**, where **`<routing protocol>`** is either **`bgp`**, **`ospf`**, **`ospfv6`**, **`rip`**, or **`ripng`**. For example:

- To enter the BGP routing mode, enter **`ip-routing bgp`**

  A `bgp#` prompt will appear. Any commands you enter from the `bgp#` prompt will be applied to the BGP routing table.
- To enter the OSPF routing mode, enter **`ip-routing ospf`**

  An `opsf#` prompt will appear. Any commands you enter from the `ospf#` prompt will be applied to the OSPF routing table.
- To enter the OSPFv6 routing mode, enter **`ip-routing ospfv6`**

  An `opsfv6#` prompt will appear. Any commands you enter from the `ospfv6#` prompt will be applied to the OSPFv6 routing table.
- To enter the RIP routing mode, enter **`ip-routing rip`**

  A `rip#` prompt will appear. Any commands you enter from the `rip#` prompt will be applied to the RIP routing table.
- To enter the RIPng routing mode, enter **`ip-routing ripng`**

  A `ripv6#` prompt will appear. Any commands you enter from the `ripng#` prompt will be applied to the RIPv6 routing table.

To exit a particular routing mode, enter **`exit`**. The command prompt returns to the top level command prompt, >.

Entering **`?`** at any time returns the help pages associated to where you are within the command line hierarchy.

Entering **`ippe-interfaces`** at the top-level command prompt results in returning the list of configurable interfaces on the NE-ONE.

Pressing the **Tab** key at any time auto-completes and proposes any applicable commands that correspond to where you are within the command line hierarchy.

Continuously pressing the **Up Arrow** cursor key any time cycles through the previously entered commands.

Use the following steps to configure the external routing tables on the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > External Routing**.
2. From the **External Routing** page (see *Illustration 16*) that appears, do the following:
   a. In the **Set External Routing** tile, tick the appropriate check boxes corresponding to the routing protocols that you want the NE-ONE to use.

      During the *External Routing Prerequisites on page 93*, your network administrator will have communicated to you which routing protocols are implemented in the network, and which routing protocols that they want you to implement on the NE-ONE.
   b. Click **SAVE**.

      The NE-ONE will write the commands entered into the routing files of routing protocols that you selected in the **Set External Routing** tile.
3. In the CLI area, do the following for each of the routing protocols that you want to configure.
   a. Enter an appropriate routing mode, by entering the appropriate command of the format:

      `ip-routing <routing protocol>`

      where **`<routing protocol>`** is either **`bgp`**, **`ospf`**, **`ospfv6`**, **`rip`**, or **`ripng`**.

      The command line prompt changes according to the routing mode that you entered. For example, if you had entered **`ip-routing ospf`**, an `ospf#` prompt appears.
   b. Enter all the appropriate routing commands to set up your routing tables as required.

      During the *External Routing Prerequisites on page 93*, your network administrator will have communicated to you which routing commands to specify in order to build the routing tables on the NE-ONE.

c. Once you have finished setting up the appropriate routing, enter **`wr f`** to in order write all of the routing commands that you had entered into the routing table file for the current routing protocol.

d. Exit the routing mode, by entering:

`exit`

The command prompt returns to the top level command prompt, >.

e. Repeat the sub-steps a to d for each of the routing protocols that you want to configure.

19-3. OSPF Routing Example

It is beyond the scope of this *User and Administration Guide* to go into detail about all routing examples. Your Network Administrator will provide you with the actual routing commands to enter. However, the example below shows the steps you take to illustrate the general usage of the **External Routing** page command line area.

In the example below, of the two interfaces (ippe1 and ippe2) that exist on the NE-ONE, the interface **ippe1** is configured using the OSPF routing protocol, and has a not-so-stubby (NSSA) type area with a decimal ID of 1 (i.e. **area 1**) assigned to it with the class 2 **10.0.0.0/24** network.

1. From the Web Interface, click **Management > Platform Settings > External Routing**.
2. From the **External Routing** page (see *Illustration 16*) that appears, do the following:
   a. In the **Set External Routing** tile, tick the **OSPF** check box.
   b. Click **SAVE**.
   The NE-ONE will write the commands you enter into the OSPF daemon file `ippe/config/external_routing/ospdf.conf`.
3. Query the available interfaces on the NE-ONE, by entering:
   `ippe-interfaces`
   The command line returns the available interfaces. For our example above, the following available interfaces are returned.
   ```
   ippe1    1
   ippe2    2
   ```
   Make a mental note of the interface that you want to configure. In our example, we will configure the interface called **ippe1** later on.
4. Go into the OSPF routing mode, by entering:
   `ip-routing ospf`
   The command line prompt changes to `ospf#`, indicating that you are currently in the OSPF routing mode.
5. Go into configure terminal mode, by entering:
   `conf t`

   Note:
   You can also use **`configure terminal`**, however, the shorthand command **`conf t`** is quicker to type.

   The command line prompt changes to `ospf(config)#`, indicating that you are currently in the OSPF configure terminal mode.
6. Go into configure router mode, by entering:
   `router ospf`
   The command line prompt changes to `ospf(config-router)#`, indicating that you are currently in the OSPF router configuration mode.
7. Create an OSPF area with decimal value 1 to be a not-so-stubby (NSSA) type area, by entering:
   `area 1 nssa`
8. Assign the class 2 network of 10.0.0.0/24 to the **area 1** that you just created, by entering:

`network 10.0.0.0/24 area 1`

The OSPF area 1 has now been configured, and is ready to be assigned to interface ippe1.

9. Exit the OSPF router configuration mode, and return up one level in the command line, by entering:

   `exit`

   The command line prompt changes to `ospf(config)#`, indicating that you are back in the OSPF configure terminal mode.

10. Select the interface called **ippe1** to be configured, by entering:

    `interface ippe1`

    The command line prompt changes to `ospf(config-if)#`, indicating that you are currently in the OSPF interface configuration mode.

11. Assign the OSPF router **area 1** to the interface ippe1, by entering:

    `ip ospf area 1`

    The interface ippe1 is now configured to use the OSPF area 1 that you had created in steps 7 to 8 above.

    At this stage the OSPF routing commands that you entered have not yet been saved (i.e. written) to file on the NE-ONE.

12. Write the OSPF routing configuration that you had made to file by entering:

    `wr f`

    Note:

    You can also use **`write file`**, however, the shorthand command **`wr f`** is quicker to type.

    Note:

    You can use **`write file`** or **`wr f`** at any time (i.e. any position within the command line hierarchy). Any of the routing commands that you have entered will be saved to file. If you have a large number of routing commands to enter, it is useful to progressively write them to file by using the **`write file`** or **`wr f`** command.

    The routing commands you had entered are now written into the OSPF daemon file `ippe/config/external_routing/ospfd.conf`. The changes take effect immediately (i.e. the NE-ONE does not need to be rebooted).

13. Exit the OSPF interface configuration mode, and return up one level in the command line, by entering:

    `exit`

    The command line prompt changes to `ospf(config)#`, indicating that you are back in the OSPF configure terminal mode.

14. Exit terminal mode, by entering:

    `exit`

    The command line prompt changes to `ospf#`, indicating that you are back in the OSPF routing mode.

15. Exit OSPF routing mode, by entering:

    `exit`

    The command line prompt changes to >, indicating that you are back to the top level of the command line.

This page is intentionally left blank.

CHAPTER 5 PORTS AND SERVICES MANAGEMENT

1. INTRODUCTION

This chapter is applicable to admin users, and describes managing ports and services on the NE-ONE.

Typically an admin user uses the procedures in this chapter at installation time and/or at a later date in order to set up soft ports, port pairs, and services on the NE-ONE, and to configure port addressing of port pairs.

Note:

If the NE-ONE is to be used in a network implementation where dynamic routing is required between soft ports used within the user's SDTNs and the test network environment, the admin user must also configure external routing (see *Configure External Routing on page 92*) according to their routing needs **after** the creation of the required soft ports that is undertaken within this chapter.

Once set up, soft ports, and port pairs are available to users for use within the Web Interface when they create Point-to-Point or Multi-Point networks.

! Notice:

Before creating users, Calnex recommends that you create and configure all the soft ports and port pairs that will be needed on the NE-ONE. This is because the **Edit User Details** page (see *Illustration 61 on page 214*) which is used when creating a user includes a dynamic list of soft ports and port pairs, which can change as more soft ports are added or deleted. If you create additional soft ports or port pairs after creating a user, those new soft ports/port pairs are not enabled by default for those users, and you would have to reconfigure the user's permissions in order to add the new soft ports/port pairs.

Note:

Not all, but the majority of the information in this chapter is related to use with the Port Manager feature and Service Manager feature (see *Table 12*). Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

TABLE 11 - SUMMARY OF FEATURE SPECIFIC INFORMATION

Section within chapter	Specific to the Port Manager feature ?	Specific to the Service Manager feature ?
Section 1-1, *Ports Management*	YES	N/A
Section 1-2, *Port Pairs*	NO	N/A
Section 1-3, *Available Port Management Capabilities*	NO	N/A
Section 1-4, *Service Management*	N/A	YES
Section 2, *Managing Ports*	YES	N/A
Section 3, *Managing Port Pairs*, containing: *Section 3-1*, *Creating Port Pairs* *Section 3-2*, *Editing Port Pairs* *Section 3-3*, *Deleting Port Pairs* *Section 3-4*, *Port Pair Settings*	 YES YES YES NO	 N/A N/A N/A N/A
Section 4, *Managing Services*	N/A	YES

Table 12 summarizes the tasks an admin user can undertake within this chapter.

TABLE 12 - HIGH LEVEL STEERING GUIDE

Step	Task	Specific to the Port Manager feature ?	Specific to the Service Manager feature ?
1	Configure all the necessary soft ports and port pairs, according to *Managing Ports on page 107* and *Managing Port Pairs on page 168*, respectively.	YES	N/A
2	If necessary, configure Port Addressing according to *Configuring Port Addressing on page 178* in *Chapter 5*, *Ports and Services Management*	NO	N/A
3	If necessary, configure services according to *Managing Services on page 188* within *Chapter 5*, *Ports and Services Management*	N/A	YES
4	If necessary, configure a DHCP relay according to *DHCP Server / DHCP Relay on page 183* in *Chapter 5*, *Ports and Services Management*	N/A	YES

1-1. Ports Management

1-1-1. Soft Ports

The NE-ONE has a minimum of two hardware ports. Depending on your NE-ONE model, you can have up to eight hardware ports, numbered 0 to 7.

In addition to the hardware ports, if the Port Manager feature is activated, the NE-ONE additionally lets you create soft ports.

Soft ports are very useful for:

- port sharing in a multi user environment, or
- if you need a lot ports to plug test devices into, but your data rates are modest so that you can share a hardware port with a lot of test devices.

If you have many users, you can create many soft ports, and assign certain soft ports to certain users according to their testing needs. For more information on assigning soft ports to users, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication) on page 217* in *Chapter 6*, *User Administration*.

Soft ports are also very useful for generating traffic, creating ping targets, and for dumping packets.

Different types of soft ports are created via soft port functions. Each of the soft port functions, and their typical use cases are described in *Available Soft Port Functions on page 100*.

1-1-1-1. Available Soft Port Functions

Table 13 lists the types of soft port functions available to the NE-ONE.

Note:

For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. As new soft port functions get developed, having an active maintenance contract lets you add those new soft port functions via software updates.

TABLE 13 - AVAILABLE SOFT PORT TYPES

Soft Port Function	Description
Soft Port : VLAN (for more information, see *Creating a VLAN Soft Port on page 116*).	This function lets you select traffic from the parent port by VLAN Id. Unlike the more generic *Soft Port : Filter* described below this port is also intelligent with the ability to detag and retag (i.e. change the tag) VLAN Ids in packets on output. Thus the port you define has just some of the data that came into the parent port. This function uses hashing to provide extremely fast mapping of the 802.1q VLAN tags to the relevant soft port. This is especially useful in cases where parent ports (typically hardware ports) are divided into larger numbers (i.e. >10) of VLAN child ports. Multiple VLAN Ports can be defined for a parent port letting you carve up a VLAN Trunk – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user or multi port environment.
Soft Port : IPv4 (for more information, see *Creating an IPv4 Soft Port on page 123*).	This function lets you create a child port of a parent port that has an IPv4 address (as well as a Netmask, Gateway, DHCP Relay and Multicast – or not – capability), and supports Dynamic NAT. Unlike the more generic *Soft Port : Filter* port described below, this port is also intelligent with the ability to Respond to ARP requests, Make ARP requests and Respond to Pings (ICMP Echo) both externally and internally. Thus the port you define has just some of the data that came into the parent port. Multiple IPv4 soft ports can be defined for a parent port allowing the parent to appear to have many IPv4 addresses on the same hardware port for routing. This feature is very useful for port sharing in a multi user or multi port environment and also for having the NE-ONE route either between ports or on a "stick" (out of the same port). **Note:** DHCP Relay is performed together with the DHCP Relay Service (see *Managing Services on page 188*). Using the DHCP Relay service, up to 10 DHCP servers are supported.
Soft Port : IP (for more information, see *Creating an IP Soft Port on page 131*).	This function lets you create a child port of a parent port that has both an IPv4 address and an IPv6 address (as well as a Netmask, Gateway, DHCP Relay and number of significant bits of the network portion for IPv6 addresses). Unlike the more generic *Soft Port : Filter* soft port function described above this port is also intelligent with the ability to Respond to ARP requests, Make ARP requests, Make Neighborhood solicitations and respond to Neighborhood solicitations and Respond to Pings (ICMP Echo – IPv4 and IPv6) both externally and internally. You can also define the MAC address or the port or let one be constructed for you. Thus the port you define has just some of the data that came into the parent port. Multiple IP Ports can be defined for a parent port allowing the parent to appear to have many IPv4 and IPv6 addresses on the same hardware port for routing. This feature is very useful for port sharing in a multi user or multi port environment and also for having the NE-ONE route either between ports or on a "stick" (out of the same port). **Note:** DHCP Relay is performed together with the DHCP Relay Service (see *Managing Services on page 188*). Using the DHCP Relay service, up to 10 DHCP servers are supported.

Soft Port Function	Description
Soft Port : Filter (for more information, see *Creating a Filter Soft Port on page 133*).	This function lets you select traffic from the parent port by source and/or destination IP address and/or TCP/UDP port and/or VLAN Id. Thus the port you define has just some of the data that came into the parent port. Multiple filter ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment. For example, you may want to filter by an end user's IP address in a large multi-user environment. In this case, you could create a VLAN parent soft port, which accommodates an IPv4 child soft port which acts as a network gateway for a set of end users. Then within the IPv4 child soft port you could create hardware filter soft ports filtering on each end user's source IP address.
Soft Port : Expression Filter (for more information, see *Creating an Expression Filter Soft Port on page 141*).	This function lets you select traffic from the parent port by using the "Wireshark like" expression syntax. This allows many more possibilities than the *Soft Port : Filter* soft port function on which it is based - other than this its function is similar. Thus the port you define has just some of the data that came into the parent port. Multiple Expression Filter Ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment.
Soft Port : Static NAT (for more information, see *Creating a Static NAT Soft Port on page 147*).	This soft port function is Network Address Translation (NAT) function designed to perform static NATing and de-NATing of source and destination IPv4 addresses. This function has the following parameters: • Source IP Address - as a packet enters the soft port from the outside, if it matches this source address its source IPv4 address will changed to Inside Source IP Address (see below) • Dest IP Address - as a packet enters the soft port from the outside, if it matches this destination address its destination IPv4 address will changed to Inside DestIP Address (see below) • Inside Source IP Address - as a packet leaves the soft port from the inside, if it matches this source address its source IPv4 address will changed to Source IPAddress (see above) • Inside Dest IP Address - as a packet leaves the soft port from the inside, if it matches this destination address its destination IPv4 address will changed to Dest IP Address (see above) The idea behind this soft port is to allow, for example, a server with a real destination address of 10.10.10.10 (say) to be accessed by client 192.168.10.10 (say) as address 10.10.11.10 (say). The server would believe that the client had address 192.168.11.10 (say). This would mean that the server would remain accessible by its normal address 10.10.10.10 but if a user specified 10.10.11.10 then the core routers would direct that traffic to the NE-ONE which would NAT the destination addresses to be the real server and the source address to be a spoofed client. On the way back the NAT would be reversed to allow the server to respond indirectly to the real client.

Soft Port Function	Description
Generate : Hardware Traffic Generation (for more information, see *Creating a Hardware Traffic Generation Soft Port on page 154*).	This function creates a multi stream traffic generation port. In general (in order to not waste the use of a top level hardware port) because it is a traffic generating object it will not be set up as a child port. Instead it will be a top level port. Streams consist of: • VLAN Id (optional) – 0 = No VLAN Tag • Stream Type – TCP or UDP Ethernet Source Address Ethernet Destination Address Source TCP/UDP Port Destination TCP/UDP Port TTL • IP (V4 or V6) Source Address • IP (V4 or V6) Destination Address • Packet Data – partial contents Packet Size (without CRC) Packets per second (rate) • Bits per second (rate) • Stream enabled i.e. is generating One of Packets per second or Bits per second must be non zero. Multiple Generating Ports can be defined. This feature is very useful for: • Loading links with traffic which may compete with real traffic and create bottlenecks for testing. • Generate external traffic. **Note:** For simplicity, consolidation, and ease of use within the Web Interface, the Generate : Hardware Traffic Generation function is grouped with the other soft port functions. However, in terms of networking, the Generate : Hardware Traffic Generation function does not create a parent port that accepts traffic from other ports - it is simply a traffic generation object.
Soft Port : Dynamic Routing IPv4 (for more information, see *Creating a Static NAT Soft Port on page 147*).	The Dynamic Routing IPv4 Soft Port provides an enhanced child port creation feature for a parent port configured with an IPv4 address, Netmask, DHCP Relay, and optional Multicast support. Unlike the standard IPv4 Soft Port, this type is specifically designed to support dynamic routing environments and does not require a Gateway configuration. Upon creation, Dynamic Routing IPv4 Soft Ports automatically deploy virtual routers beneath the parent hardware port using FRR (FR Routing). These virtual routers enable NE-ONE to seamlessly participate in external OSPF and BGP networks. Each Dynamic Routing IPv4 Soft Port is initialized with OSPF enabled by default, facilitating immediate integration into dynamic routing topologies. Dynamic Routing IPv4 Soft Ports maintain intelligent networking behavior, including the ability to send and respond to ARP requests and respond to ICMP Echo (Ping), both internally and externally. Multiple Dynamic Routing IPv4 Soft Ports can coexist on a single parent port, allowing flexible and scalable simulation of complex, multi-address, and multi-router environments. **Note:** DHCP Relay functionality remains supported via the DHCP Relay Service (see *Managing Services on page 188*). Up to 10 DHCP servers can be relayed concurrently.

1-1-1-2. Soft Port Rules

Soft ports adhere to the following rules:

- You can define more than one soft port child for a parent port.
- You can also define multiple levels of soft ports, such that you can define more than one child soft port within a parent soft port.

  The normal use of this is to create parent VLAN soft ports and child IPv4 / IP soft ports of these parent VLAN soft ports. Furthermore, if necessary you can create child Filter soft ports within the IPv4 / IP soft ports for further filtering in an extremely large multi-user environment.

VLAN soft ports are discussed in *Creating a VLAN Soft Port on page 116*. IPv4 soft ports and IP soft ports are discussed in *Creating an IPv4 Soft Port on page 123*, and *Creating an IP Soft Port on page 131*, respectively. Filter soft ports are discussed in *Creating a Filter Soft Port on page 133*.

- Once you have created a soft port (child) of a parent port, the original parent port is no longer available for a network, only the child soft ports are available.
- Soft ports are semi-permanent (i.e. they will be recreated on a reboot) and exist outside any particular network. A soft port that you define may be used by other users (provided their security permits it) on the NE-ONE, but a soft (or hardware port) may only be used in one running network at a time.
- You cannot create a soft port on a port that is already part of a port pair.
- You can create top level soft ports at the same level as hardware ports. Typically you create top level soft ports when not needing (or not wanting to waste using a top level hardware port) in situations such as
  - generating traffic (with the use of the *Generate : Hardware Traffic Generation* function)
  - creating ping targets (with the use of either the *Soft Port : IPv4* or *Soft Port : IP* function)
  - creating a port for packet dumping (with the use of the *Soft Port : VLAN* function)
- Child soft ports of parent hardware ports are always subject to the fact that their parent port can only handle a certain total I/O – 1 Gbps for Gigabit Ports, and 10 Gbps for 10 Gigabit ports.

1-2. Port Pairs

Port pairs are extremely useful as they allow NE-ONE users to rapidly create Point-to-Point type network based on pre-defined port pairs. Port pairs, thus avoid the need for the user to additionally select the ports during the Point-to-Point network creation process.

Depending on whether or not the Port Manager feature is activated on the NE-ONE, pre-defined port pairs will either already exist or not already exist, as follows:

- If the Port Manager feature is deactivated on the NE-ONE, then by default a set of pre-defined hardware port pairs will already be available and pre-configured.
- If the Port Manager feature is activated on the NE-ONE, then by default, the NE-ONE is not configured with any point pairs. Port pairs can be created between the different port types using the Port Manager, as follows:
  - between two hardware ports
  - between two soft ports
  - between a hardware port and a soft port

Note:

The NE-ONE is flexible in its use letting you create port pairs between a hardware port and a soft port. However, even if this is possible, it usually makes no networking sense to create a port pair between a hardware port and a soft port.

Additionally, port pairs also allow Point-to-Point networks to be created to run over port pairs configured with specific port addressing criteria (e.g. to operate like a network router or to bridge two sub-networks). For more information on configuring a specific port addressing criteria for a port pair, see *Port Addressing on page 174*.

1-3. Available Port Management Capabilities

Table 14 below summarizes the different port management capabilities that are available on the NE-ONE according to weather or not the Port Management feature is activated.

TABLE 14 - PORT MANAGEMENT CAPABILITIES

Port Management Capabilities	Port Manager Feature Activated	Port Manager Feature Deactivated	For more information, see
See and use the Port Manager	Yes	No	*The Port Manager Page on page 107*
Create soft ports	Yes	No	*Creating Soft Ports on page 116*
Edit soft ports	Yes	No	*Editing Soft Ports on page 163*
Delete soft ports	Yes	No	*Deleting Soft Ports on page 163*
Create port pairs	Yes	No	*Creating Port Pairs on page 170*
Edit port pair	Yes	No	*Editing Port Pairs on page 172*
Delete port pair	Yes	No	*Deleting Port Pairs on page 173*
Configure specific port addressing	Yes	Yes	*Port Addressing on page 174*
Configure default transmission	Yes	Yes	*Default Transmission on page 186*

1-4. Service Management

An NE-ONE without the Service Manager feature already comes with some in-built services such as Port Addressing (see *Port Addressing on page 174*) and Default Transmission (see *Default Transmission on page 186*) for simple network testing environments.

The Service Manager feature of the NE-ONE lets you create and manage additional services for more complex network testing environments, such as:

- using DHCP helper services
- using background port to port transmission via either the Background service or Background Expression Routed service

If the Service Management feature is activated on the NE-ONE, you can create and use these services to create more complex test networks with DHCP helpers and/or background port to port transmission (either with or without complex expression routing).

Services are an additional capability that in many ways function like soft ports (see *Available Soft Port Functions on page 100*), in that they are independent of running networks. Unlike soft ports they are not directly associated with any particular hardware.

1-4-1. Available Services Functions

The NE-ONE currently has the following service functions available that you can use to create and assign to ports:

- DHCP Helper
- Background Expression Routed
- Background

Note:

For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. As new service functions get developed, having an active maintenance contract lets you add those new service functions via software updates.

Table 15 describes the differences between the service functions available to the NE-ONE, and indicate what service function/type you would use according to your networking needs.

TABLE 15 - HIGH LEVEL COMPARISON BETWEEN SERVICES

Service Function	Service Type	Services to be run	Ports (Hardware /Soft)	Implementation Remarks
Service:DHCP_Helper	Helper (see *section 1-4-1-1*)	Multiple	IPv4 and IP soft ports	For use with one or multiple DHCP servers (up to 10) in the network
Service:Background_Expression_Routed	Background (see *section 1-4-1-2*)	Single	Hardware or soft ports	Best for port pairs
Service:Background		Single		Best for meshes between three or more ports

1-4-1-1. The DHCP Helper Service

The DHCP Helper service lets you create and run up to 10 DHCP Helper services. This service is intrinsically linked with the DHCP Relay function of IP and IPv4 soft ports, and so is described there in *Creating an IPv4 Soft Port on page 123* and *Creating an IP Soft Port on page 131*. When creating an IP soft port or IPv4 soft port you can specify which of the 10 DHCP Helper services you want to use.

1-4-1-2. The Background Services

Background services allow port to port transmission when no network is running. The difference between the two Background services is that Background is the best to use for connecting ports in pairs and Background Expression Routed is the one to use for creating meshes between three or more ports.

The services Service:Background Expression Routed and Service:Background allow the creation of background services that connect ports together, and passes packets between those ports when no network is running on those ports.

When a network requests some of the ports managed (controlled) by these background services they are released for use by the network. The background service continues to run managing any other ports that are not in use in any running network.

When a network stops running, the background service is notified and resumes management of the ports. It is possible to have many background services, if required.

The ports used in the background can be either hardware ports or soft ports (or both). There are many possible configurations of background service, which are discussed in the examples within *Section 4-2*, *Creating Services on page 189*.

2. MANAGING PORTS

This section is only applicable to the NE-ONE with the Port Manager feature activated. Depending on your license, the Port Manager feature may be activated or deactivated.

There are two types of **Port Manager** page:

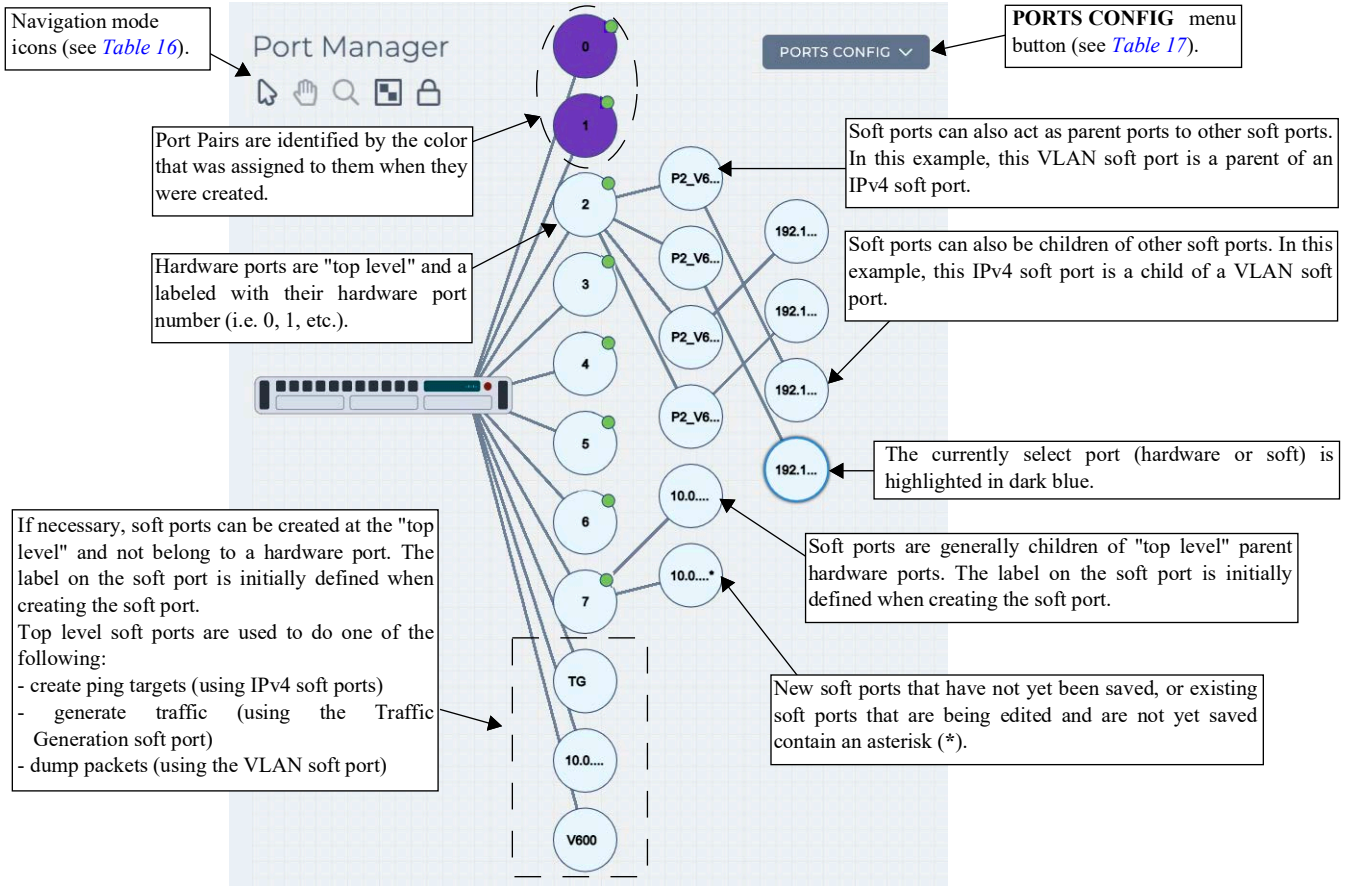
- **Port Manager** page - this is the original **Port Manager** page where all the ports are displayed (i.e. they cannot be hidden). This is used in the majority of cases when there are not many soft ports defined. For more information, see *The Port Manager Page*.
- **Port Manager (List View)** page - this is a new **Port Manager (List View)** page where all the ports are displayed, but the lower level soft ports can be by expanding and collapsing the parent ports. This is used in the cases when there are many soft ports defined. For more information, see *The Port Manager (List View) Page on page 112*.

To launch the **Port Manager** page (see *Illustration 17*) or the **Port Manager (List View)** page (see *Illustration 19 on page 112*), select **Management > Port Manager**. The type of **Port Manager** page that appears depends on the Use List Port Manager setting defined in the **General Preferences** page. For more information, see *Configuring the Type of Port Manager Page to Display on page 263* in *Chapter 8*, *General System Procedures*.

2-1. The Port Manager Page

To launch the **Port Manager** page (see *Illustration 17*) select **Management > Port Manager**.

ILLUSTRATION 17 - PORT MANAGER PAGE (WITH EDIT PORT PANEL HIDDEN)



The **Port Manager** page (see *Illustration 17*) provides a visual editor letting you manage all soft port related

functions on the NE-ONE, such as:

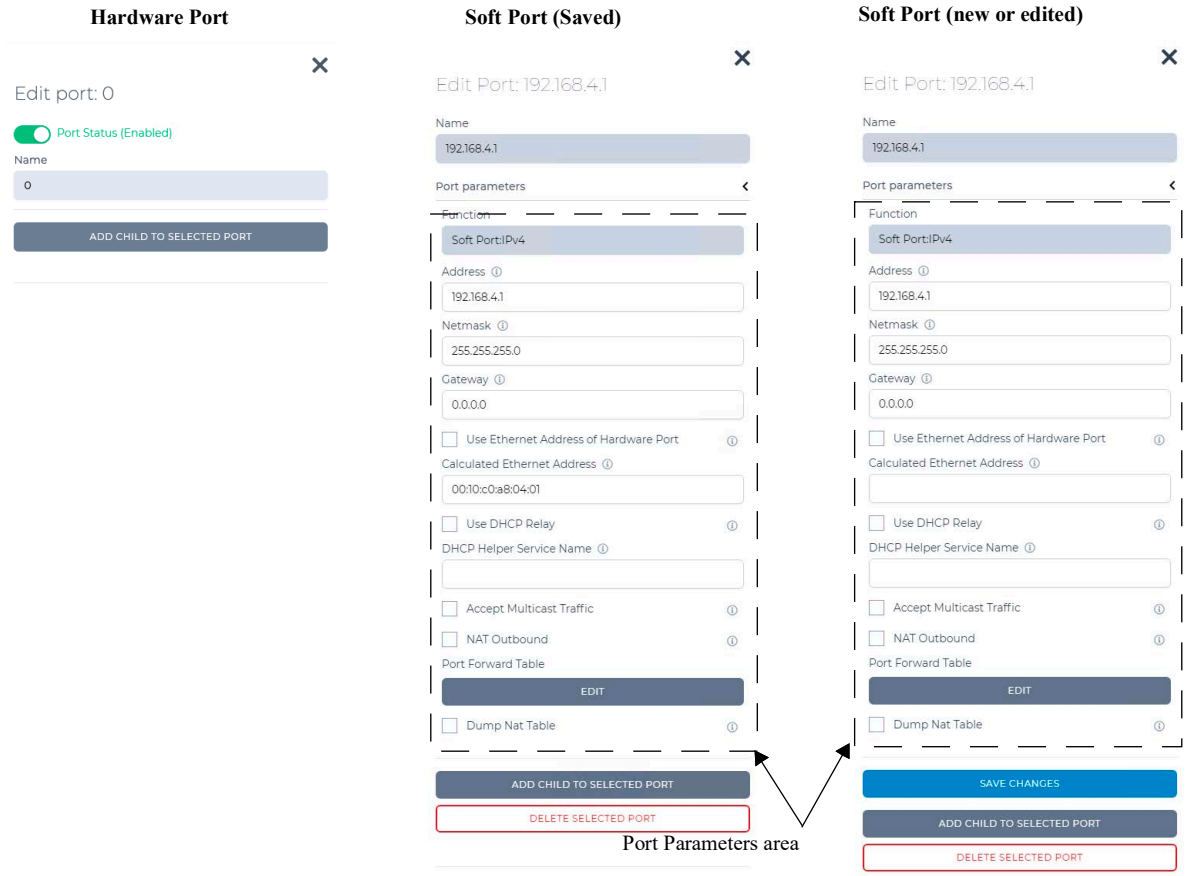
- creating soft ports (i.e. adding a child soft port to an existing parent (hardware or soft) port)
- editing soft ports (i.e. editing the parameters of an existing soft port's function)
- deleting soft ports (i.e. deleting an existing soft port from its parent port)

Note:

The **Port Manager** page shows any pre-defined port pairs that exist. Creation and management of port pairs are done from within the **Port Pairs** page. For more information, see *Managing Port Pairs on page 168*.

Ports (hardware or soft) are represented by circles in the **Port Manager** page. Clicking on a port (hardware or soft) reveals an **Edit Port** side panel (see *Illustration 18*) on the right hand side of the **Port Manager** page. The circles representing a port may have a lock icon attached to them, representing that a network is currently running on that port. If a circle representing a port has a lock icon attached to it, the port cannot be edited until the currently running network is stopped.

ILLUSTRATION 18 - COMPARISON OF EDIT PORT SIDE PANEL - HARDWARE VS SOFT PORT



The elements (i.e. buttons, fields, and check boxes) available on the **Edit Port** side panel depend on the type of port selected. Hardware ports cannot be deleted, whereas soft ports can be deleted (if they are not parents to other lower level children soft ports).

- If a hardware port is selected, the **Edit Port** side panel provides an **ADD CHILD TO SELECTED PORT** button and a **Port Status (Enabled)** toggle button.
  - Clicking on the **ADD CHILD TO SELECTED PORT** button invokes the Soft Port Creation Wizard, from where you can create a new soft port (i.e. choose the soft port function, and define all the parameters of that soft port function). The created soft port will be a child of the parent port from where it was created.