Anywhere

INTELLIGENT CONNECTIVITY

Anywhere Node Manager User Manual

For Operation and Maintenance

A-NM v1.0

Anywhere Networks

Feb , 2019

Table of Content

1. About this document

This section lists the audience, purpose and summary of information in this document.

1.1. Audience

This document is intended for qualified installers and administrators of A-OS devices.

1.2. Purpose

This document has the information necessary to install, configure, troubleshoot, and maintain the Anywhere Node Manager (A-NM) in networks that use A-OS devices.

1.3. Summary of information

This document contains information about the A-NM. The following table lists the chapter names and summaries.

Chapter Name	Summary
Introduction	Lists features and benefits of the A-NM
Software Installation	Lists the system and environmental requirements, third party software installation procedures, and the A-NM installation procedures
Using A-NM	Contains information about the A-NM, procedures to manage, configure and maintain A-OS devices
Troubleshooting	Lists problems and suggested solutions
Appendix	Lists A-OS devices factory defaults

1.4. Conventions

Certain information has special meaning for the reader. This information appears with an icon that indicates a particular condition, such as a note or warning.

Notes contain optional advice and information particular to a special case or application.

Warnings! contain information that you should obey to avoid minor injury, inconvenience, and damage to equipment. This image appears before each warning statement.

1.5. Document feedback

If you find an error or content missing from this document, we want to hear about it. You can send your feedback about any of our documents to info@anywherenetworks.com.

2. Introduction

Anywhere Node Manager (A-NM) is mainly used for the staging, configuration and troubleshooting of A-OS devices. This tool-kit lets engineers, system administrators and installers easily configure and manage A-OS devices.

2.1. A-OS Wireless Mesh Network

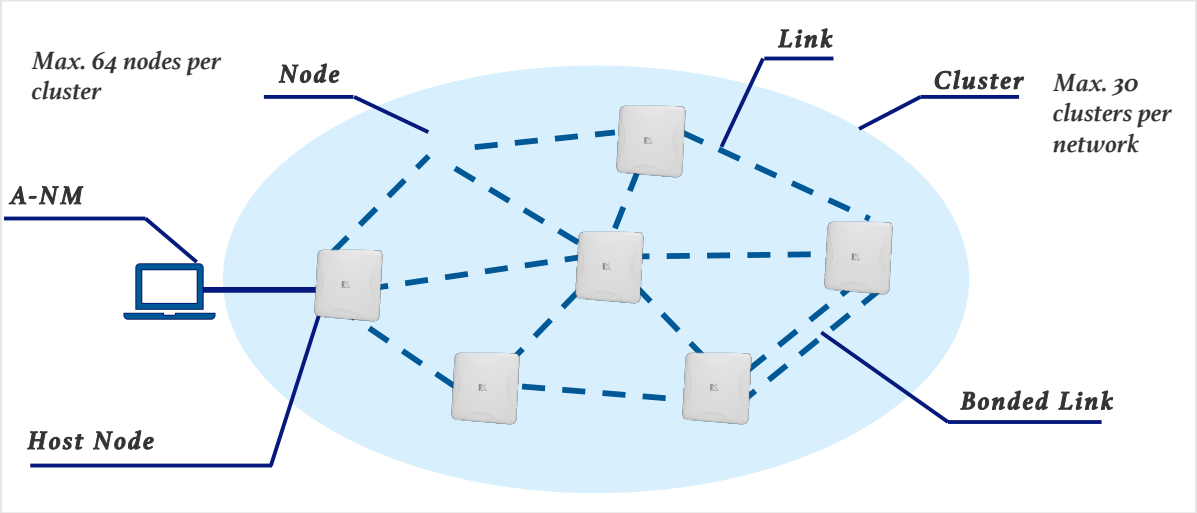


Figure 2.1A – A-OS Wireless Mesh Network

The A-OS mesh network consists of the following components.

- Cluster
  - A collection of max. 64 connected nodes. A cluster maximizes the utilization of the network by determining the optimal path for each data traffic flow. A cluster provides a Layer 2 network environment just like an ethernet switch that distributes its ports into different nodes / locations.
- Node
  - An A-OS device within a cluster. A-OS devices can automatically discover and connect to other nodes in range with the same Cluster ID and Encryption Key.
- Link
  - The wireless connection between two nodes. A-OS Mesh Networks can protect data sent over a link with AES 128-bit encryption.
- Bonded Link

    - Links formed between the same nodes using two or three pairs of radio units (A-OS devices have two or three radio units each depending on model).
- Host Node
    - The only node that communicates with the A-NM, responsible for data collection and management message delivery to the other nodes.

2.2. Mesh Network Management

The A-NM organizes cluster settings as different profiles. Users can save customized settings as ***Projects***. Every project includes the ***management IP***, ***management secret***, and the list of ***managed devices*** of the cluster. For enhanced security, users can make ***management secret*** input mandatory for every login.

Management IP is the IP address used for the management of a single cluster. The ***Management IP*** is used when building a management connection to a cluster in the A-NM and it is reachable at all nodes within the cluster, which means that any node within the cluster can be used as the physical connection point to the A-NM.

Management secret is the communication key between the A-NM and nodes. All nodes in a cluster and the A-NM MUST share the same ***management secret***. Otherwise, the nodes cannot be managed by the A-NM.

Projects help users store connection information for accessing managed devices. ***Projects*** are only stored at the A-NM but not on the devices. Different A-NM instances (i.e. on different computers with different users) can have the same device registered but may have different knowledge of it.

Managed Devices are a list of verified devices created by the user. Cluster-wide settings will only apply to the recognized devices on the list. A node can belong to a cluster, and at the same time *not* be managed in the project. This may be the case when a new node has recently been added to the cluster. Any cluster-wide configurations done in a project will only affect its managed devices.

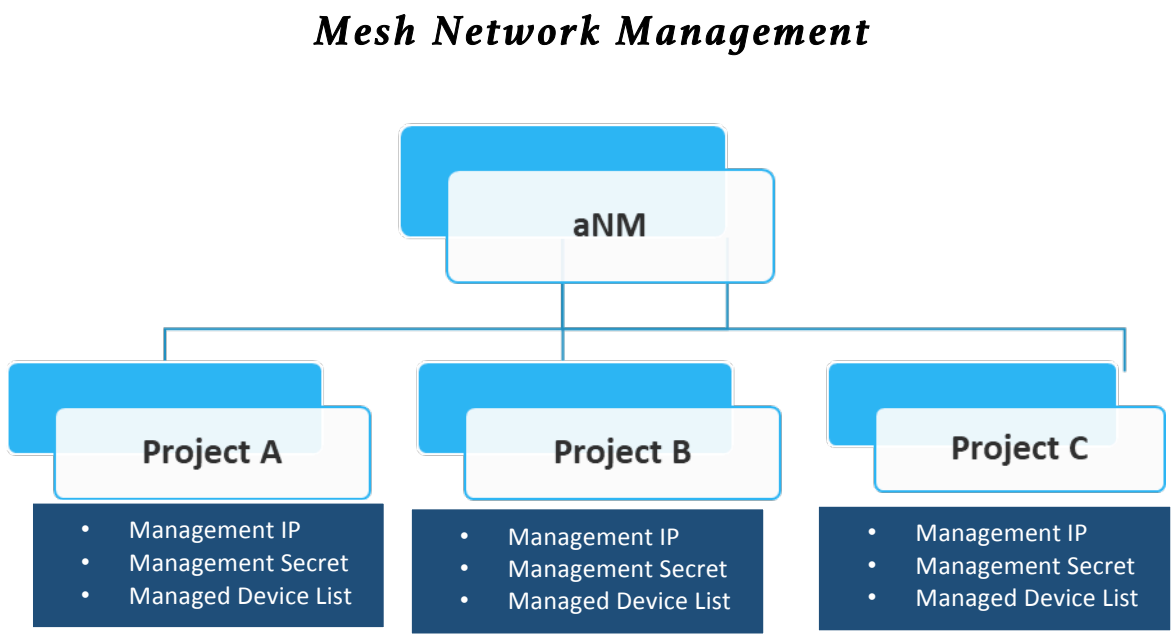


Figure 2.2A – Mesh Network Management structure

2.3. Real-time Statistics

The A-NM captures runtime status of the mesh network that is useful for troubleshooting purposes. The wireless mesh topology can be visualized on a single page. Real-time status of nodes and links is available by hovering the pointer over the node and link icons. Node information includes ***device info***, ***device status***, and ***performance statistics***.

2.4. Configuration and Maintenance

The settings in the A-NM are grouped into Cluster-wide and Node-based settings.

Cluster-wide settings include ***Cluster ID***, ***Management IP, Management Netmask, Encryption Key, Management Secret*** and **Country**. They can only be applied to all the managed devices at the same time. Advanced functions include scalable and secure ***Firmware Upgrades***, ***System Restart***, and ***Configuration Backup & Restore***.

Node-based settings include ***Hostname*** and ***Radio Settings***. Advanced functions include ***Firmware Upgrade***, ***System Restart***, ***Factory Reset*** and ***Backup & Restore***.

3. Software Installation

3.1. System Requirements

Component	Minimum Requirements
Hardware	
Operating System	Windows 7,8,10 64-bit only
CPU	Intel Core i3 or higher
RAM	4 GB or more
Storage	250 GB or more (At least 25 GB of available hard-disk space)
Network Connection	10/100/1 Gig RJ45 Ethernet
Software	
Docker CE	Docker Toolbox v18.06.0-ce
VirtualBox	v5.2.16
Google Chrome	Version 69.0.347.100 or above
Other	
Port forwarding	21, 80, 12381, 16000 - 16064, 39980 - 40000

Note: Please note that management IP behind **NAT** is not supported.

Warning! Make sure that your device fulfills the minimum requirements, or you may not be able to successfully use the A-NM.

Warning! If your computer has already installed Docker for Windows, please follows the procedures listed in the section of ***A-NM Installation Issues (see page 91)***.

3.2. Google Chrome Installation

1) Download Google Chrome at **https://www.google.com/chrome/**.
2) Click **DOWNLOAD CHROME**.

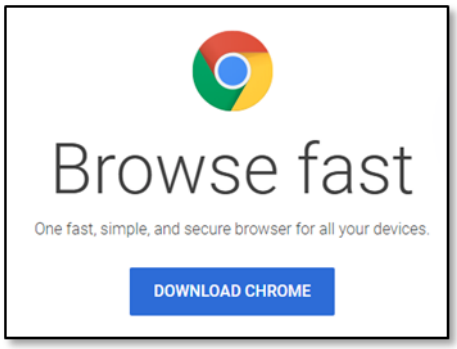


Figure 3.2A – Download chrome

3) Follow the instruction to install Google Chrome.

3.3. Docker Toolbox Installation

The installation package includes Docker CE and Virtual Box.

1) Download DockerToolbox v18.06.0-ce at **https://github.com/docker/toolbox/releases**.

Figure 3.3A – DockerToolBox Installer

2) Launch **DockerToolbox.exe.**
3) Click **Next.**

Figure 3.3B – Welcome page of DockerToolBox Installer

4) Click **Next.**

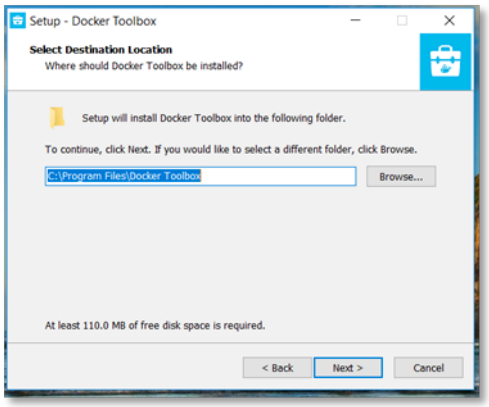


Figure 3.3C – Select install location in the DockerToolBox Installer

5) Ensure that the **Docker Compose for Windows** and **VirtualBox** are checked and click **Next.**

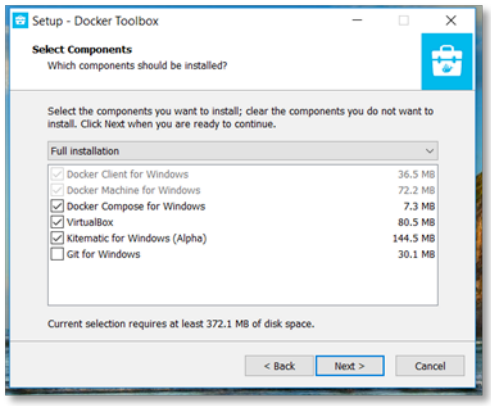


Figure 3.3D – Select components to install in the DockerToolBox Installer

6) Ensure that the **Add docker binaries to PATH** is checked and click **Next**.

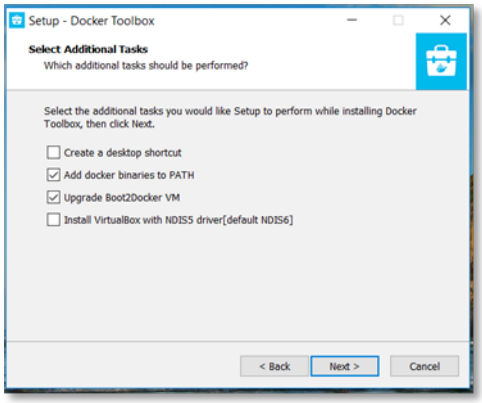


Figure 3.3E – Select additional tasks in the DockerToolBox Installer

7) Click **Install**.

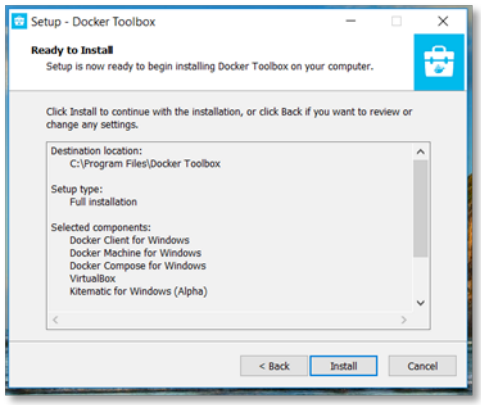


Figure 3.3F – Ready to install DockerToolBox

8) Wait for the installation process to complete and click **Finish**.

Figure 3.3G – Finish the installation of DockerToolBox

3.4. A-NM Installation

3.4.1. Prerequisites

- The computer meets the **system requirements (see page 11)**
- **Docker Toolbox** is installed **(see page 12)**
    - **Must** include Docker Compose for Windows
    - **Must** include VirtualBox
    - **Must** add docker binaries to PATH (Windows system PATH)
- **Google Chrome** is installed **(see page 12)**

3.4.2. A-NM Software Installation

1) Download the A-NM setup file.

A-NM Launcher-vXXX Setup.exe

Where xxx is the version number

Figure 3.4.2A – A-NM setup file

2) Launch **A-NM Launcher-vXXX Setup.exe**.

3) Click **Next**.

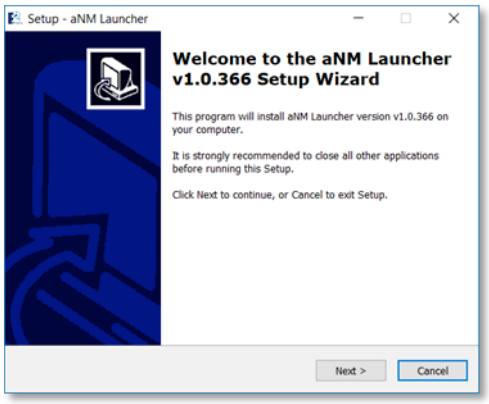


Figure 3.4.2B - Welcome page of A-NM Installer

4) Click **Next**.

Note: You can change your own installation directory.

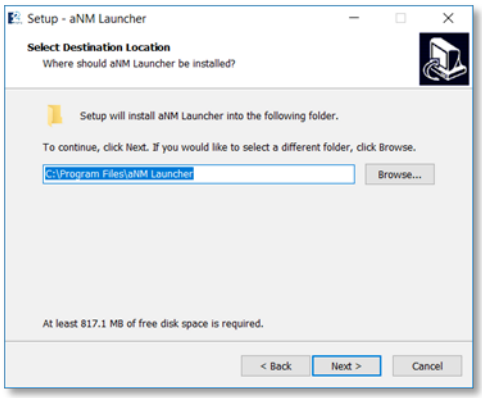


Figure 3.4.2C - Select install location at A-NM Installer

5) Check **Create a desktop shortcut** and click **Next**.

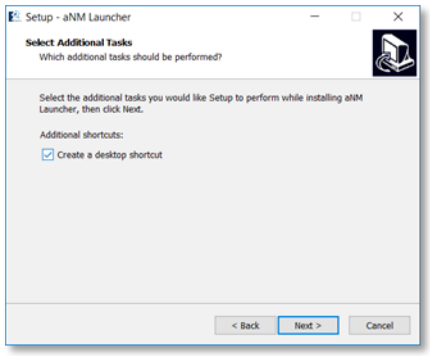


Figure 3.4.2D - Select additional tasks at A-NM Installer

6) Click **Install** and wait for the installation process to complete.

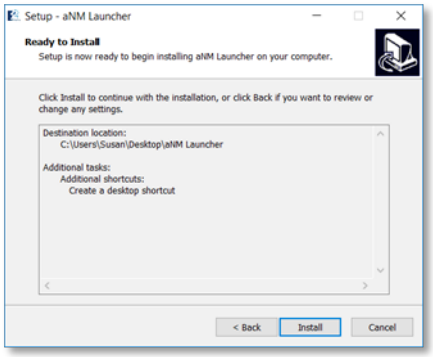


Figure 3.4.2E – Start to install A-NM

7) Ensure that **Launch A-NM Launcher** is checked and click **Finish**.

Note: Please initialize the A-NM after installing the software.

Note: The A-NM can also be launched from **Start > All Programs**

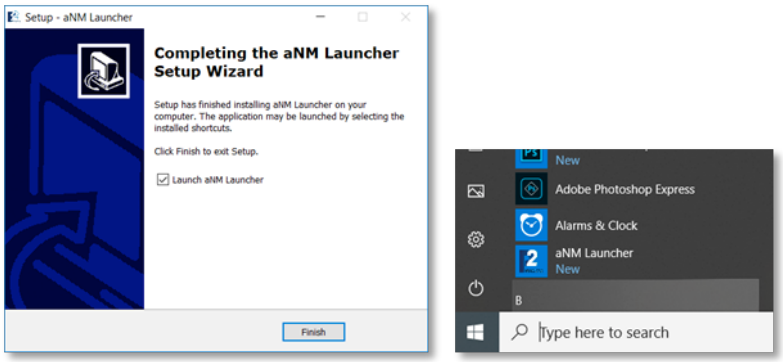


Figure 3.4.2F – Finish the installation of A-NM

3.5. A-NM Uninstallation

1) Click the **Start** menu.
2) Enter **Control Panel** and select Control Panel from the results.

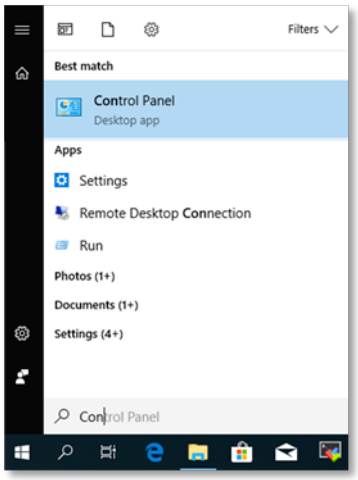


Figure 3.5A – Control Panel at Start Menu

3) Click **Programs**.

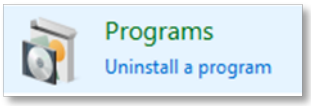


Figure 3.5B – Programs option at Control Panel

4) Click **Programs and Features**.

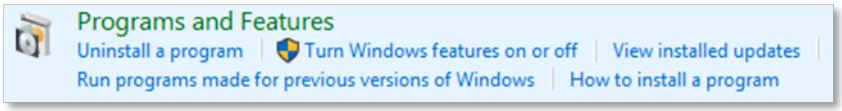


Figure 3.5C – Programs and Features at Programs option

5) Select the **A-NM Launcher** and click **Uninstall**.

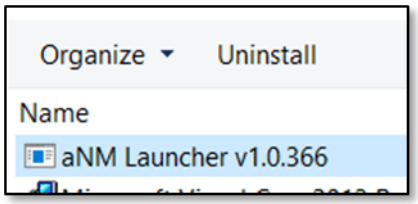


Figure 3.5D – A-NM at Programs and Features

6) Click **Yes** and wait for the uninstallation process.

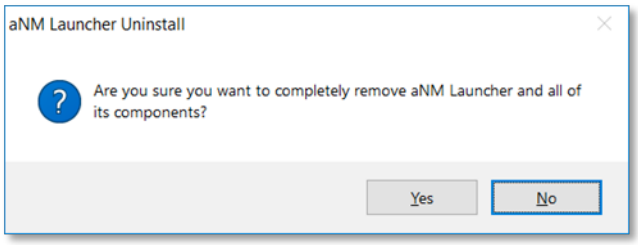


Figure 3.5E – Confirmation box of uninstallation

7) Click **OK** to complete the uninstallation process.

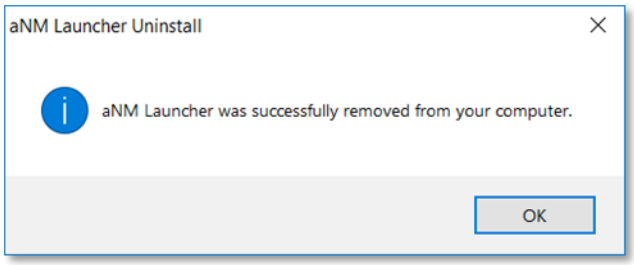


Figure 3.5F – Finish the uninstallation of A-NM

4. Getting Started

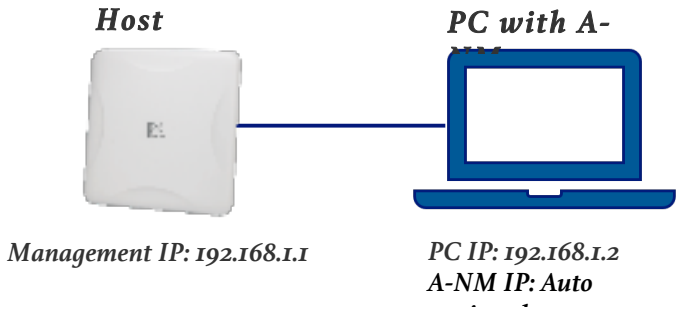


Figure 4A – Access a cluster

Note: The A-NM IP is assigned by docker and cannot be changed.

Note: The auto assigned IP range of the A-NM is 192.168.99.X/24. Please make sure that any ***Management IP*** is out of this range.

The IP address shown in the Launcher is the A-NM IP which is an unchangeable IP address assigned by the software, it is only used to access the A-NM with a Chrome browser.

In order to access the cluster, the IP address of your PC must be set with the A-NM to have the same subnet as the cluster. This is done as follows:

1) Power on A-OS device and connect the device to the computer with A-NM running on it.
2) Configure the network adapter setting on your PC.
   - Windows 7
     - Start > Control Panel > Network and Sharing Center > Change Adapter Settings
   - Windows 8/10
     - Start > Settings > Network & Internet > Ethernet > Network and Sharing Center > Change Adapter Settings
3) Right click on **Local Area Connection**.
   - Local Area Connection > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties
4) Select **Use the following IP address** and fill-in IP address and subnet mask:
   - IP address: 192.168.1.2
   - Subnet mask: 255.255.255.0

Note: It is possible to use a different IP address, e.g. 192.168.1.3 or 192.168.1.4.

5) Click **OK** to save your changes.

5. Using A-NM

5.1. Start A-NM

The A-NM runs with a launcher, which monitors the status of the server.

1) A-NM Launcher will be launched automatically after the installation or double-click the **A-NM Launcher icon.**

Figure 5.1A – A-NM Launcher icon

2) Wait until the status change from **Loading** to **On**, this process will take around **5 minutes** for the first launch to initialize the A-NM.

Note: Initialization only takes place for the first use of the A-NM. It takes 2-3 minutes for the launch after that.

Note: The waiting time depends on the hardware specifications of your server.

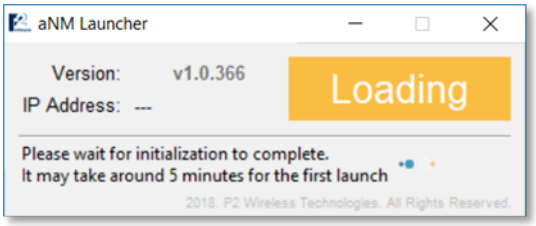


Figure 5.1B – Initialization state of A-NM Launcher

3) Click  to launch the A-NM.

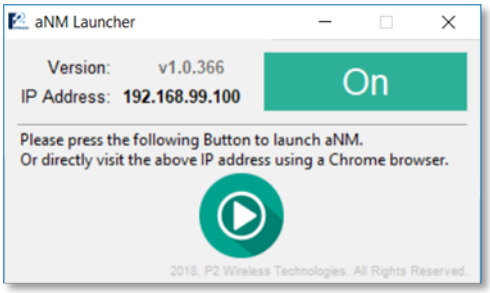
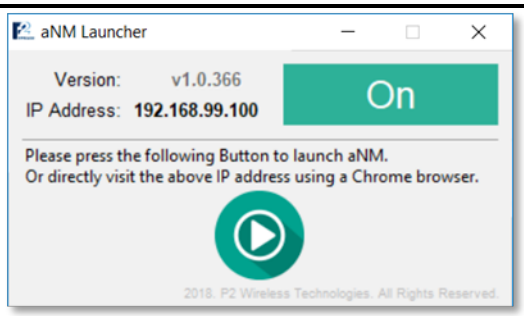
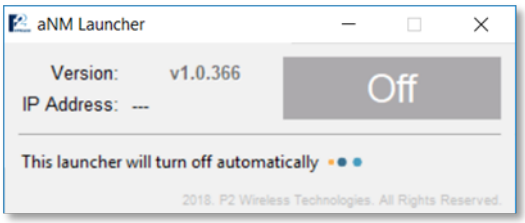
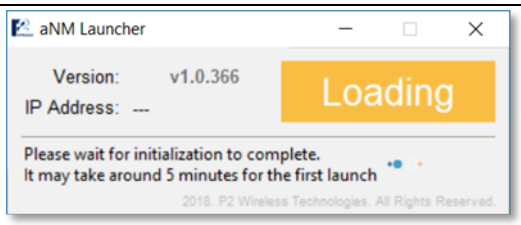
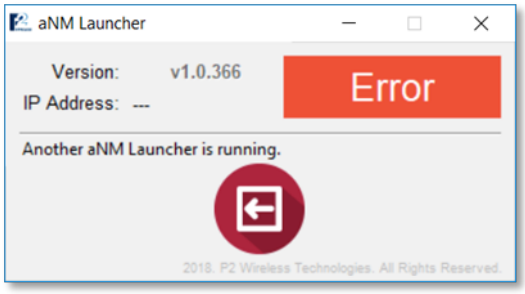


Figure 5.1C – On state of A-NM Launcher

Screen Capture	Status	Description
 Figure 5.1D – On status of the Launcher	**On**	Server is on, and ready to use
 Figure 5.1E – Off status of the Launcher	**Off**	Server is off, and launcher will be closed automatically
 Figure 5.1F – Loading status of the Launcher	**Loading**	Server is initializing

 Figure 5.1G – Error status of the Launcher	**Error**	Issue occurred during initialization

4) A window with A-NM will launch.

Note: It is also possible to access the A-NM using the Chrome browser by typing the A-NM IP address.
Note: Chrome browser is recommended for the best user experience.

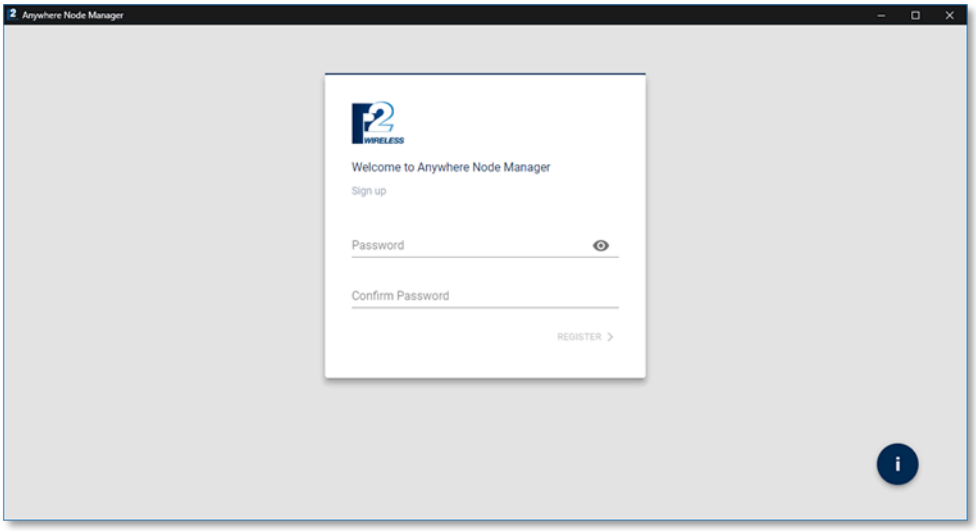


Figure 5.1H – Sign up page of the A-NM

5.2. Stop A-NM

The A-NM can be stopped without disrupting the network.

Note: It is recommended to stop the A-NM after completed configuration to avoid unauthorized access.

1) Click  to close A-NM Launcher.
2) Click **Yes** to switch off the A-NM.

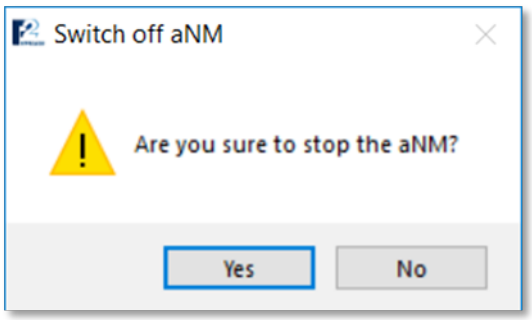


Figure 5.2A – Close the Launcher

5.3. Upgrade A-NM

Keep the A-NM up-to-date to ensure you get the latest bug-fixes and feature enhancements.

1) Download a **new** A-NM setup file.

A-NM Launcher-vXXX Setup.exe

Where xxx is the version number

Figure 5.3A – A-NM setup file

2) Launch **A-NM Launcher-vXXX Setup.exe**

Warning! Make sure that the A-NM is stopped before installation of the upgrade, or you may risk a system failure.

3) Click **Yes** to Confirm the upgrade process.

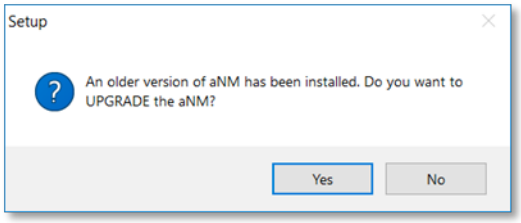


Figure 5.3B – Warning message box of upgrade the A-NM

4) Refer to **A-NM software installation session (see page 15).**

5.4. Sign up

Create sign in password after the installation and you will be redirected to the sign in page after that.

Note: This password should consist of 8 to 32 alphanumeric characters.

Warning! If you forget the password, you must uninstall and reinstall the A-NM again and all saved information will be lost.

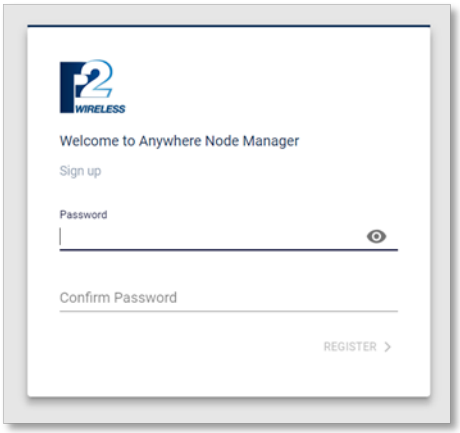


Figure 5.4A – Create sign in password

To sign up A-NM

1) **Start the A-NM (see page 20)**.
2) Create a new password at the sign up page.
3) Click **Register.**
4) Click **CONTINUE** to go to the sign in page.

5.5. Sign in

After the password registration you will be redirected to the sign in page.

Please use the registered password to sign in and start to use the A-NM.

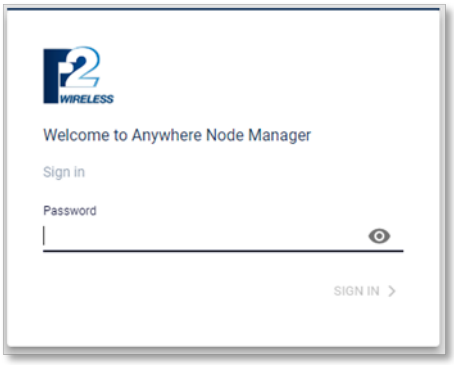


Figure 5.5A – Sign in A-NM

To sign in A-NM

1) Enter the **registered password** in the password field.
2) Click **SIGN IN**.

5.6. Mesh Network Management

Anywhere Node Manager (A-NM) is mainly used for the staging, configuration and troubleshooting of A-OS devices. It connects to a cluster through an IP address and management secret. The user can then manage clusters as ***Projects***. Every project includes the ***management IP***, ***management secret***, and the list of ***managed devices*** of the cluster. These data are stored in the A-NM, so that the user doesn't have to provide the access information every time and will be able to identify and keep track of the managed devices. For enhanced security, users can make management secret input mandatory for every login.

Note: A-OS devices do not contain Project data.

Projects help the user store connection information for accessing managed devices. ***Projects*** are only stored in the A-NM, not on the devices. Different A-NMs may have different project definitions containing the same cluster.

Management IP is the IP address used for the management of a single cluster. The Management IP is used when building a management connection to a cluster in the A-NM. The Management IP is available at all nodes within the cluster, which means that any node within the cluster can be used as the physical connection point.

Management secret is the communication key between the A-NM and nodes. All nodes in a cluster MUST share the same ***management secret***. Otherwise, the nodes cannot be managed by the A-NM.

Managed Devices are a list of verified devices created by the user. Cluster-wide settings will only apply to the recognized devices on the list.

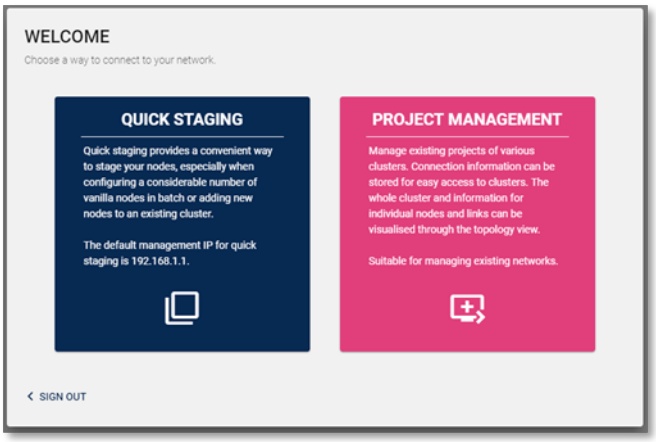


Figure 5.6A – Mesh Network Management Interface

There are two ways to connect to a cluster for the management:

- Quick Staging
  - Designed for quick access of vanilla device(s) or a cluster
  - Project data won't be saved in the A-NM until it is stored as a ***Project***
  - Use the default management IP address (192.168.1.1) for the connection
- Project Management
  - Designed for the management or troubleshooting of the devices or cluster.
  - User has to provide these authentication details:
    - Project Name
    - Management IP
    - Management secret
  - Access and management information (including ***Project Name*** and ***Management IP***) will be automatically saved under the Project.
  - A single A-NM can be used to manage multiple clusters by switching between projects.

Note: Only one cluster can be managed at a time with a single A-NM and the status polling will only happen after the sign in to a ***Project.***

5.6.1. Quick Staging

Quick Staging is a temporary project, designed for quick access of vanilla devices or a cluster. It is usually used for configuring A-OS devices straight out of the box. The project data won't be saved in the A-NM until it is manually stored as a ***Project***.

Quick Staging default project profile to access the mesh network:

Management IP	192.168.1.1

Management Secret	password

Warning! Make sure that the devices are in the same subnet with A-NM and they are reachable.

To start quick staging

1) Configure the **IP address** of your computer to 192.168.1.x/24 (Same subnet as the ***Management IP***)
2) Power up the new A-OS devices and they will auto-form a cluster within 2 to 3 minutes.
3) Connect the computer with A-NM to one of the A-OS device.
4) **Sign in to the A-NM (see page 25)**.
5) Click **QUICK STAGING** to connect the cluster with default setting.

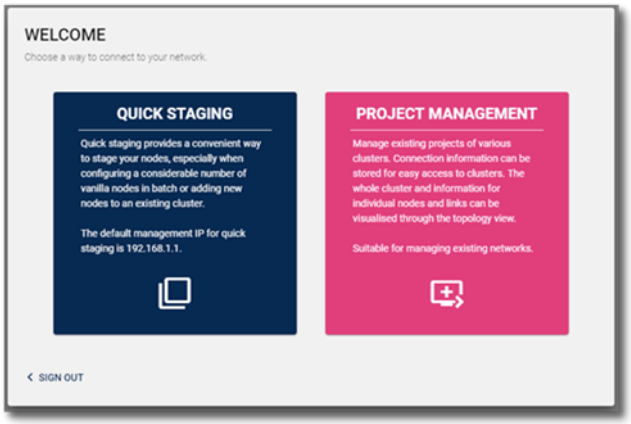


Figure 5.6.1A – Select ***Quick Staging***

6) A ***Guideline*** will be shown to briefly introduce the usage of Quick Staging**.** Read the ***Guideline*** and click **COMPLETE** after that.

Note: You can click **Do not show again** to hide the ***Guideline***.

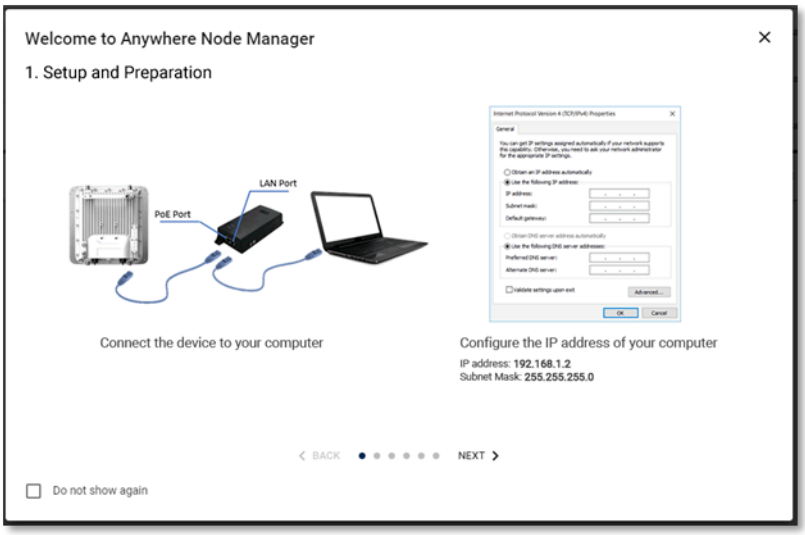


Figure 5.6.1B – ***Guideline*** at ***Quick Staging***

7) You will be redirected to the ***Managed Device List*** page. Click **OK** to view the device list. As all the discovered devices are in the unmanaged state by default, you must define your devices as **Managed Device** to further manage them. Otherwise, you cannot make any changes to the devices. For details on **how to add devices to the *Managed Device List*, please refer to page 37**.

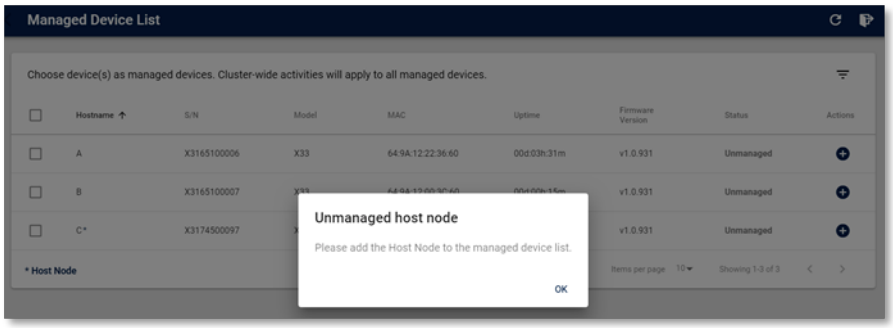


Figure 5.6.1C – Device list at ***Quick Staging***

8) Click to close the ***Managed Device List*** *after that*.

Note: You can now fine-tune the mesh network by configuring the nodes, for example changing the hostname, changing the radio channel and adjusting the transmit power.

Warning! The default access information (i.e. ***Cluster ID, Management IP*** and ***Management Secret***) should be updated to prevent unauthorized access to the network.

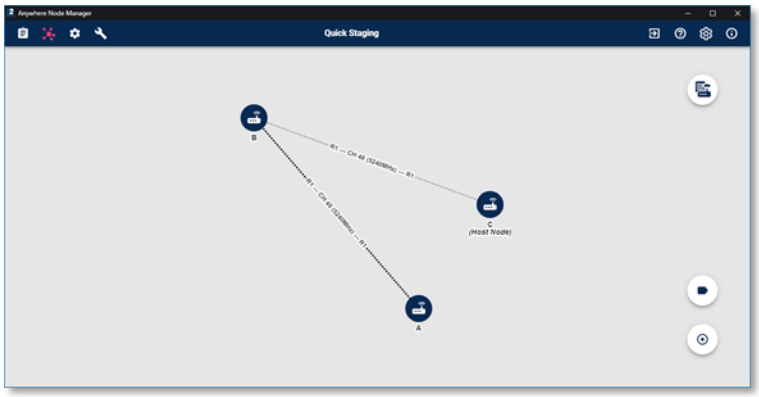


Figure 5.6.1D – Cluster topology with managed device at ***Quick Staging***

9) Click  to open the ***Project*** *menu*.

10) Click **Save Quick Stage Project As** to save the project information.

    Note: Project data will not be saved in the A-NM until it is stored as a ***Project***.

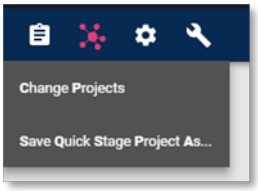


Figure 5.6.1E – Click to save the project

11) Enter a **Project Name** to define the project.

Figure 5.6.1F – Save the ***Quick Stage*** project as a new project

12) Click **SAVE**.

After saving the project, you can simply select the project to connect to the cluster without inputting the Management IP very time.

5.6.2. Project Management

The ***Project Management*** is designed to manage the project data of different clusters. As the A-NM connects to a cluster through an IP address and management secret, ***Projects*** will help user to store the connection information for accessing the cluster.

You can create project, edit project, remove project and access project using the ***Project Management.***

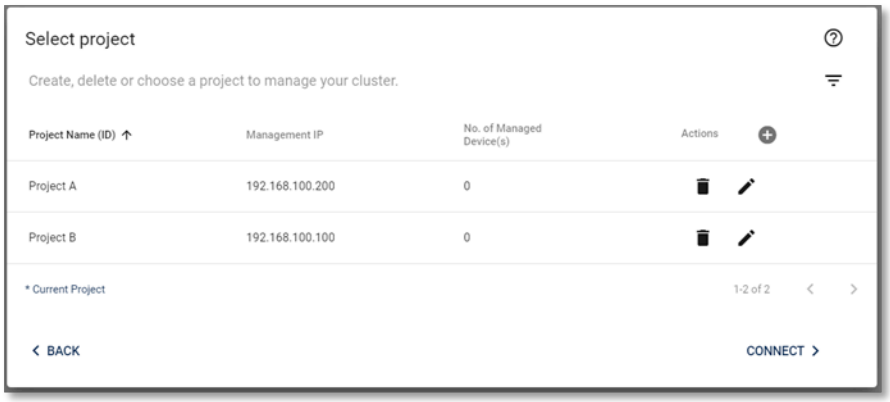


Figure 5.6.2A – ***Project Management*** user interface

To create a project

1) **Sign in to the A-NM (see page 25)**.

2) Click ***Project Management***.

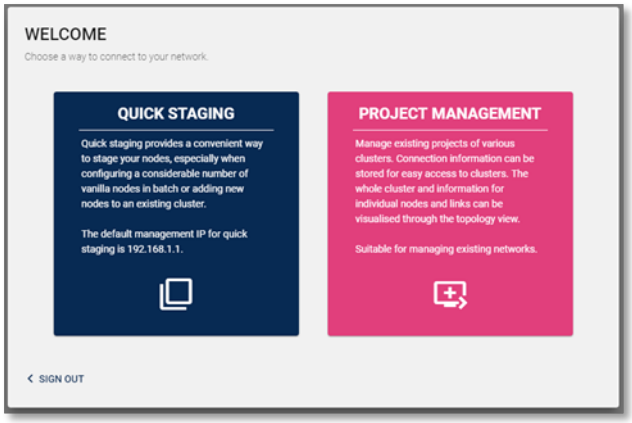


Figure 5.6.2B – Select ***Project Management***

3) Read the ***Guideline*** of the ***Project Management*** and click **NEXT** after that.

   Note: You can click **Do not show again** to hide the ***Guideline***.

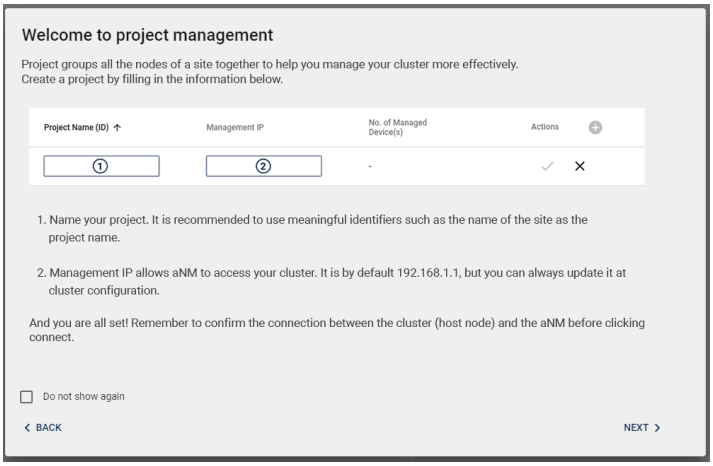


Figure 5.6.2C – ***Guideline*** of ***Project Management***

4) Click  (Next to Actions) at the project list to create a new entry.

Figure 5.6.2D – Create new project

5) Enter a new **Project Name** and **Management IP** of the cluster.

   Note: The name has to be unique. It can be up to 32 characters long with hyphen, underscore and space. The IP shall be in IPv4 format.

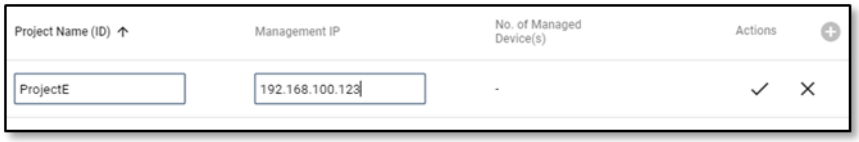


Figure 5.6.2E – Input parameters for the new project

6) Click ✓ to confirm or click ✕ to cancel.

To edit project information

1) [Sign in to the A-NM (see page 25)].
2) Click ***Project Management***.
3) Read the ***Guideline*** of the ***Project Management*** and click **NEXT** after that.

   Note: You can click **Do not show again** to hide the ***Guideline***.
4) Click the icon of the project.

   Note: You can click to reopen the ***Guideline***.

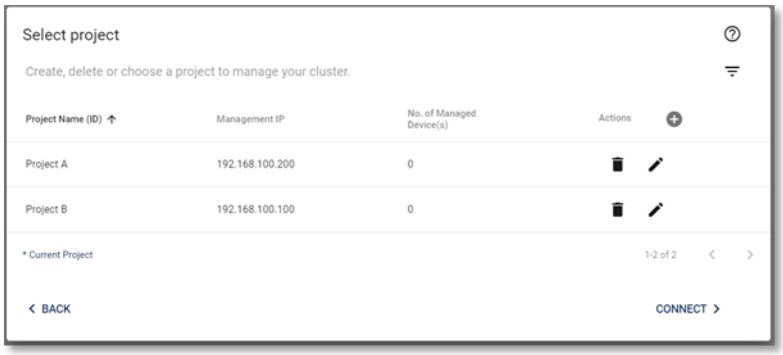


Figure 5.6.2F – Select project to edit

5) Edit the project information.

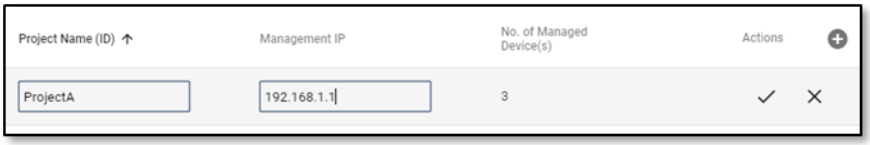


Figure 5.6.2G – Edit the project data

6) Click ✓ to confirm or click ✕ to cancel.

To remove a project

1) **Sign in to the A-NM (see page 25)**.
2) Click ***Project Management***.
3) Read the ***Guideline*** of the ***Project Management*** and click **NEXT** after that.

   Note: You can click **Do not show again** to hide the ***Guideline***.

4) Click the icon of the project.

   Note: You can click to reopen the ***Guideline***.

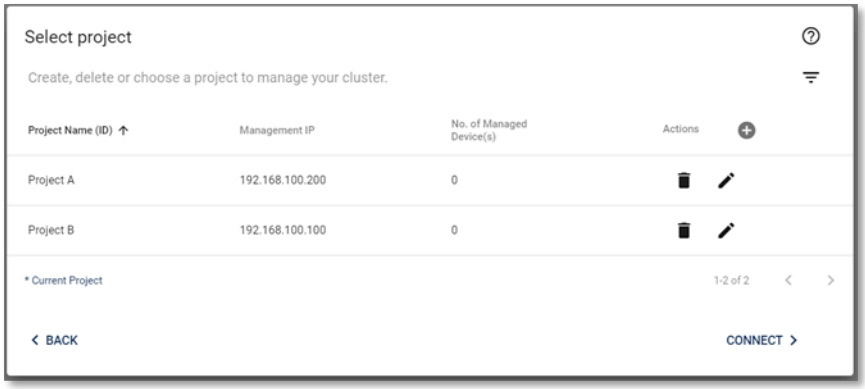


Figure 5.6.2H – Select project to remove

5) Click **OK** to confirm or click **CANCEL** to stop.

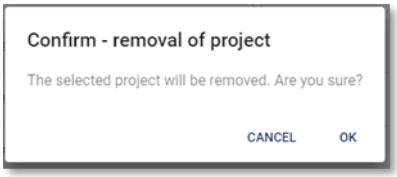


Figure 5.6.2I – Confirm to remove the project

To access a project

1) [Sign in to the A-NM (see page 25)](#).
2) Click ***Project Management***.
3) Read the ***Guideline*** of the ***Project Management*** and click **NEXT** after that.

   Note: You can click **Do not show again** to hide the ***Guideline***.
4) Double-click the project to connect or select the project and then click CONNECT ›.

   Note: You can click ⓘ to reopen the ***Guideline***.

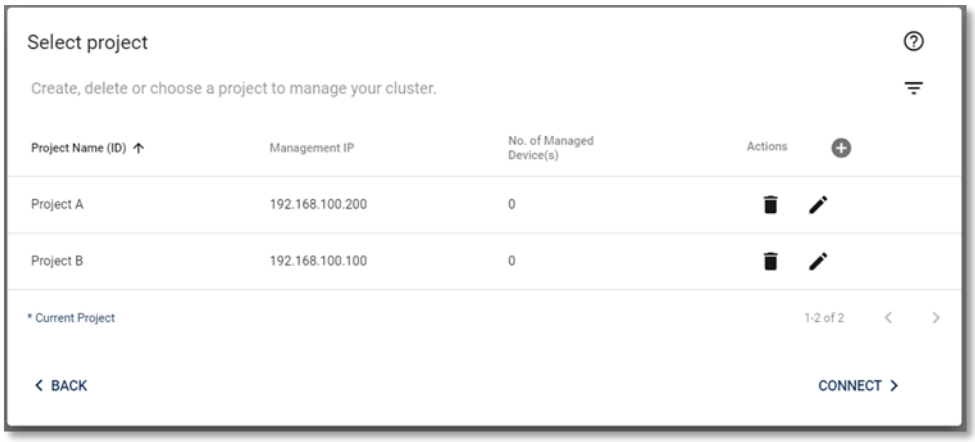


Figure 5.6.2J – Connect to the cluster through the project

5) Enter the **Management Secret** of the cluster.

   Note: You can check the **Remember** checkbox to save the password at the A-NM.

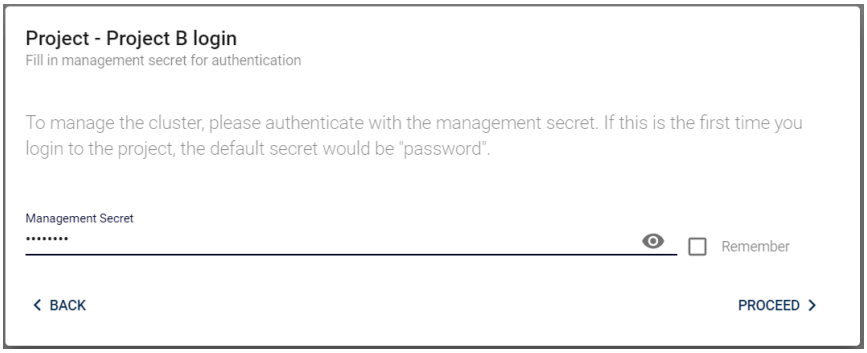


Figure 5.6.2K – Management Secret interface

5) A ***Guideline*** will be shown to briefly introduce the use of A-NM**.** Read the ***Guideline*** and click **COMPLETE** after that.

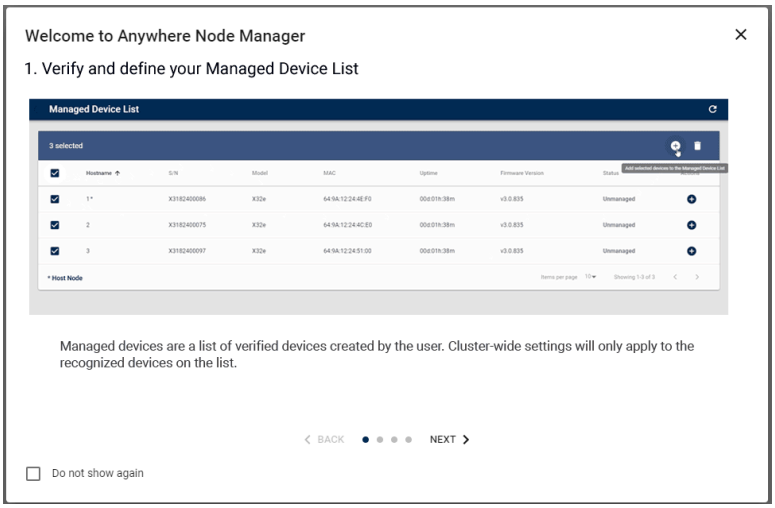


Figure 5.6.2L – Guideline of A-NM

6) You will be directed to the Cluster Topology page and the mesh network will be ready for configuration.

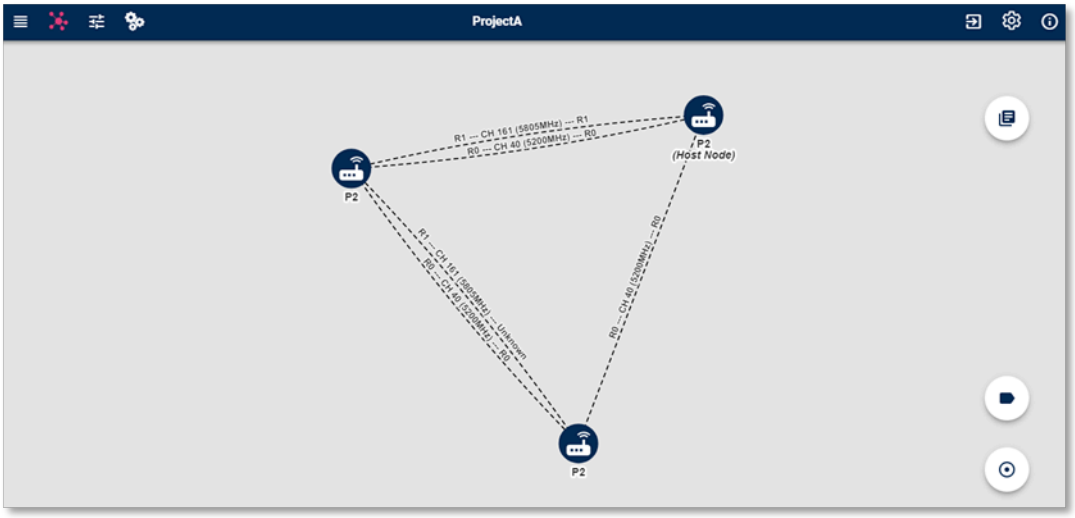


Figure 5.6.2M – The cluster topology of the project

5.7. Managed Device List

When the A-NM accesses a project for the first time, all the devices are unmanaged by default. A device list will pop up automatically to ask the user to define the managed devices in this project. Serial numbers and MAC addresses are listed for easy verification. This procedure is very important when all vanilla devices auto-connect and form a mesh network. The A-NM will only apply the cluster-wide configuration to managed devices. Node information and statistics of unmanaged devices are not accessible to the A-NM.

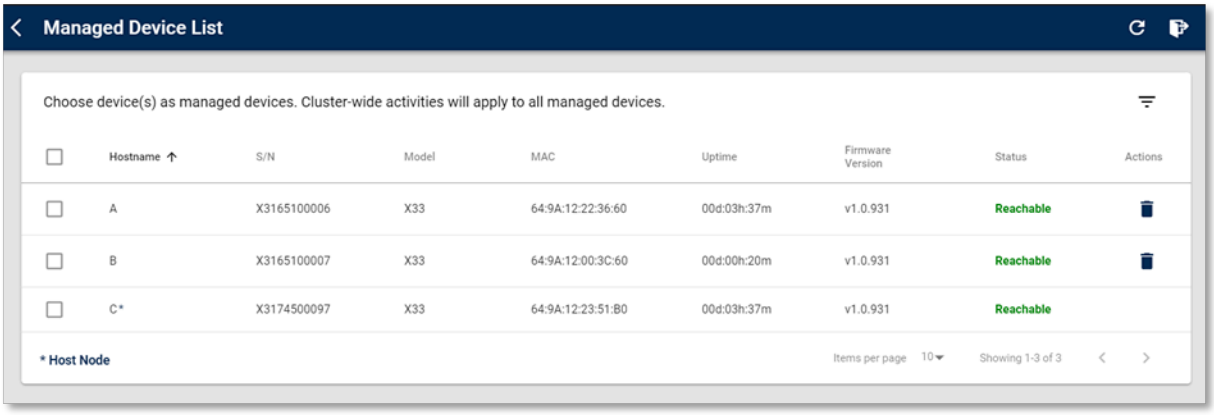


Figure 5.7A – ***Managed Device List*** user interface

The ***Managed Device List*** shows device information and status of the user-verified A-OS Devices:

Label/Icon	Description
Hostname	Displays the device hostname [* indicate the host node of the cluster]
S/N	Displays the serial number of the device
Model	Displays the model of the device
MAC	Displays the MAC address of the device
Uptime	Displays the device active uptime since last boot-up
Firmware Version	Displays the firmware version of the device
Status	Displays the status of node interfaces [Unmanaged/ Reachable/ Unreachable/ Secret Mismatch]
Action	Add device(s) to the list Remove device(s) from the list

Note: The ***Cluster Topology*** page and ***Managed Device List*** will not display unmanaged nodes with unreachable status.

The differences between managed and unmanaged devices:

	Managed	Unmanaged
Node Info	√	√
Link Info	√	√
Node Menu	√	X
Node Overview	√	X
Node Statistics	√	X
Node Configuration	√	X
Node Maintenance	√	X
Node Security	√	X
RSSI Viewer	√	X
Cluster Configuration	√	X
Cluster Maintenance	√	X

How to handle an unknown device?

If there is an unmanaged device with an un-recognized serial number or MAC address, it means that an unknown device is using the same cluster ID as your cluster, and thus forming links with the managed devices. It is recommended to change the cluster ID of your devices to avoid using the default value. For details of how to change the cluster ID, please refer to the section of ***Cluster Configuration***.

To use Managed Device List

1) Click  to go to the ***Managed Device List***. Or click **YES** when a message box with "Unmanaged device(s) found" is shown when you first access a project.

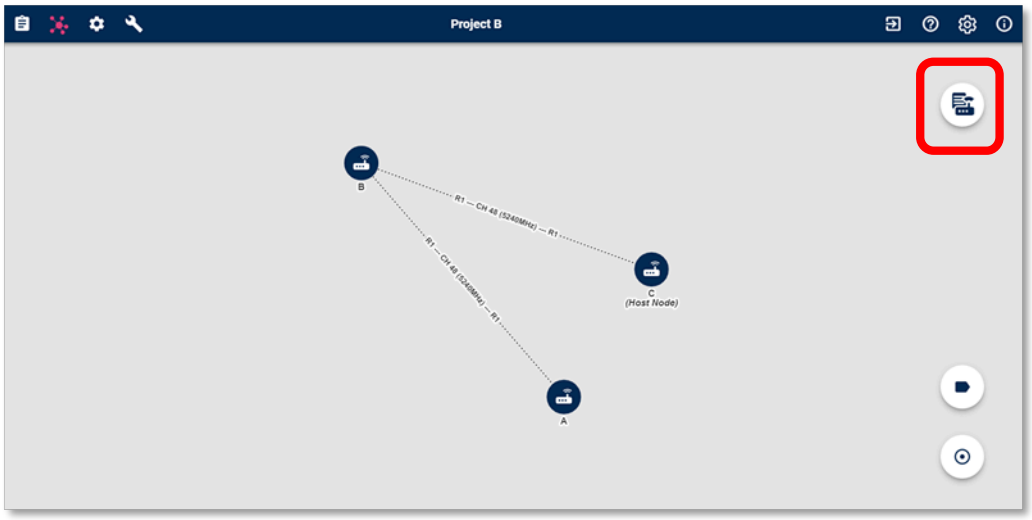


Figure 5.7B – Open ***Managed Device List***

2) Check the device info and status at the list to make sure that your devices are all reachable.

3) You can click to reload the device list as the list will not update automatically.

   Note: Click to open a search box to find the specific device. Click to logout the project.

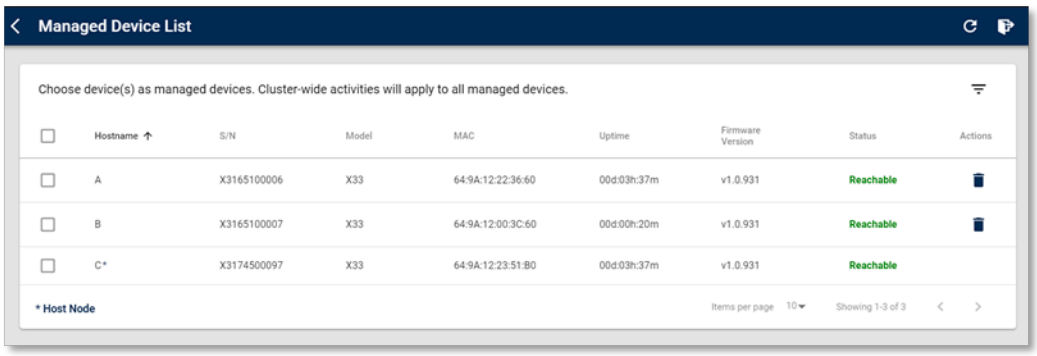


Figure 5.7C – Reload the device list

4) You can click to add a single device or select multiple devices with the checkbox and click to add multiple devices to the ***Managed Device List***. Also, by using the same practice, you can remove a single device or multiple devices from the list by clicking or .

   Note: Please make sure that the Host Node (indicated with * at the hostname field) has been added into Managed Device List, otherwise, you cannot further manage your project.

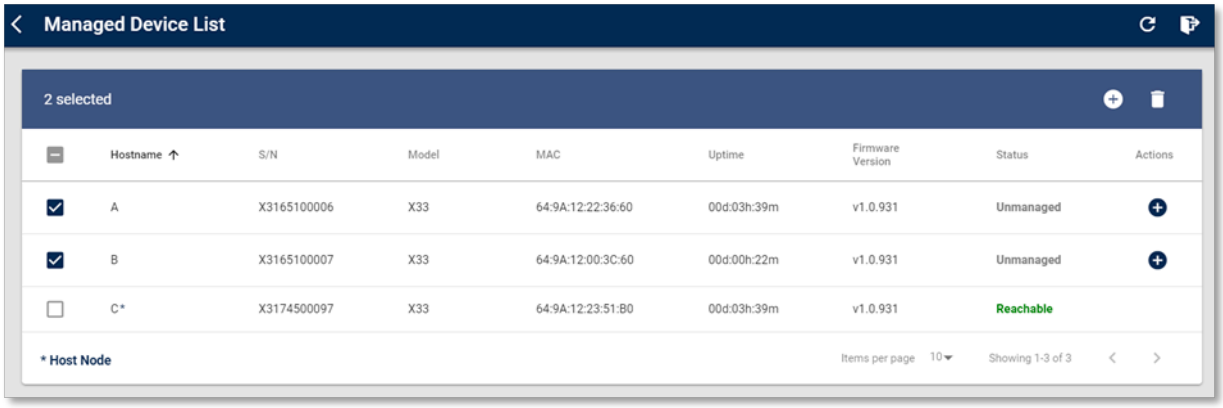


Figure 5.7D – Add device into ***Managed Device List***

5) Click to close the ***Managed Device List***.

5.7.1. Secret Mismatch

The A-NM will check if the ***Management Secret*** of all the managed nodes in the cluster are the same as the host node. A ***Secret Mismatch*** warning will be shown at the ***Managed Device List*** if the A-NM detects a different secret.

Note: You must synchronize the ***Management Secret*** of all the managed nodes in the cluster otherwise A-NM cannot retrieve any information of the secret mismatched node(s).

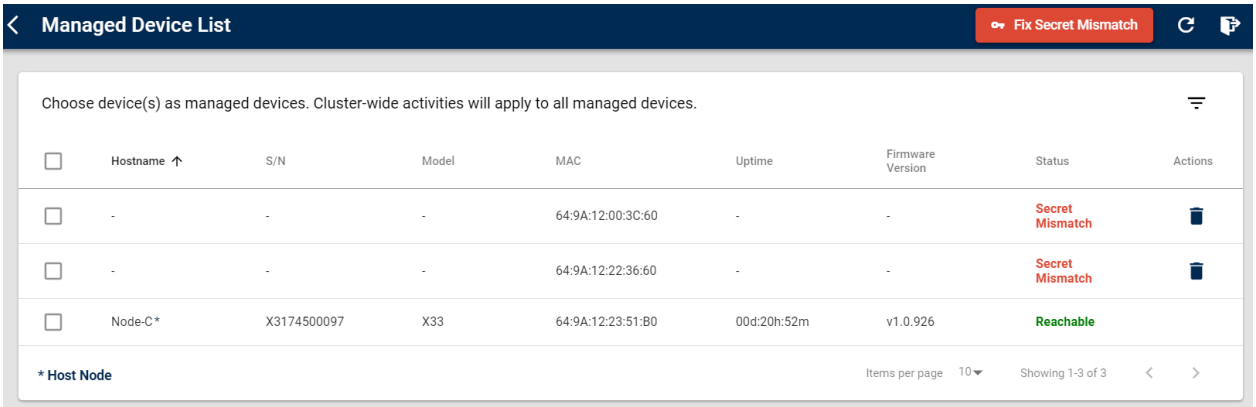


Figure 5.7.1A – Secret mismatch

To synchronize the mismatched secret

1) Click to go to the ***Managed Device List***.
2) Check the mismatched nodes.
3) Click **Fix Secret Mismatch**.

4) Enter the original **Management Secret** of the mismatched node.

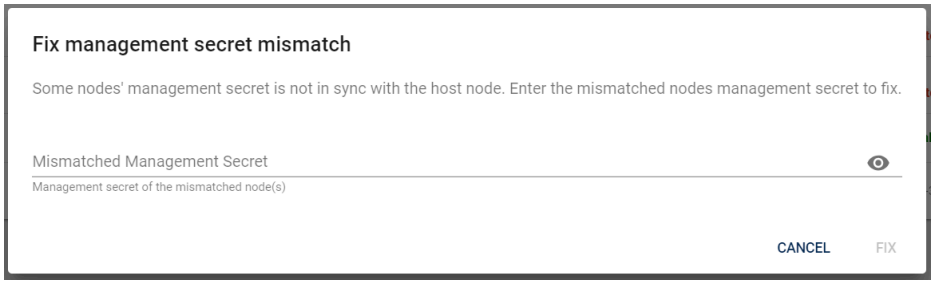


Figure 5.7.1B – Fix secret mismatch

5) Click **FIX**.

6) Click **CONTINUE** to return to the ***Managed Device List***.

Note: If there are many sets of mismatched management secret, please repeat **step 3 to 6**.

Figure 5.7.1C – Fix success

5.8. Main User Interface

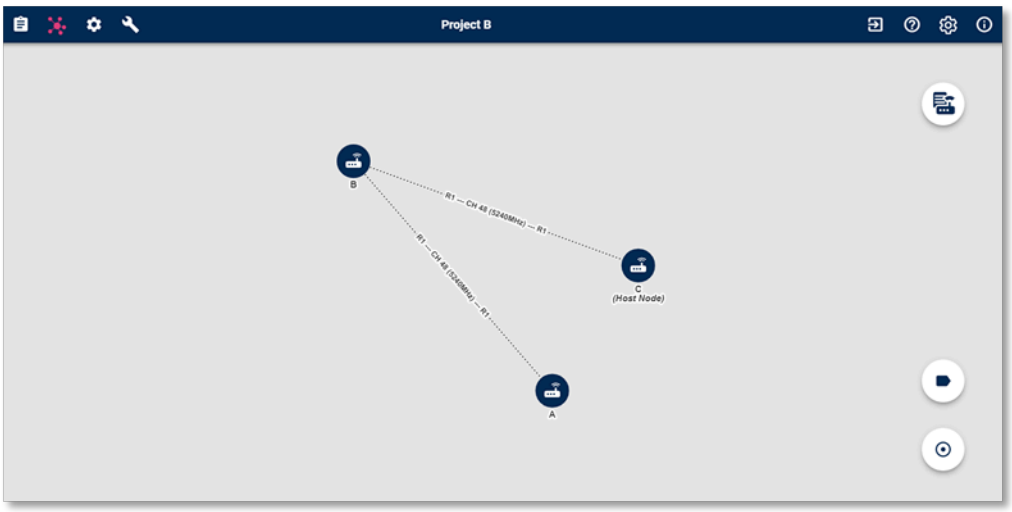


Figure 5.8A – Main User Interface

Button	Button Name	Description
	Project	Change Project (see page 43) Quick Staging (see page 27) Save Quick Stage Project As (see page 27) (Only available at Quick Staging)
	Cluster Topology	Go to Cluster Topology page (see page 46).
	Cluster Configuration	Go to Cluster Configuration page (see page 76).
	Cluster Maintenance	Go to Cluster Maintenance page (see page 83).
	Sign out	Sign out A-NM (see page 43)
	Help	Guideline of A-NM (see page 45)
	Settings	Settings of A-NM(see page 44)
	About	Show the A-NM version (see page 44)
	Managed Device List	Go to Managed Device List (see page 37)
	Show/Hide Link Label	Show/Hide link info at Cluster Topology (see page 45)
	Fit Canvas	Fit canvas at Cluster Topology (see page 46)

5.8.1. Change Project

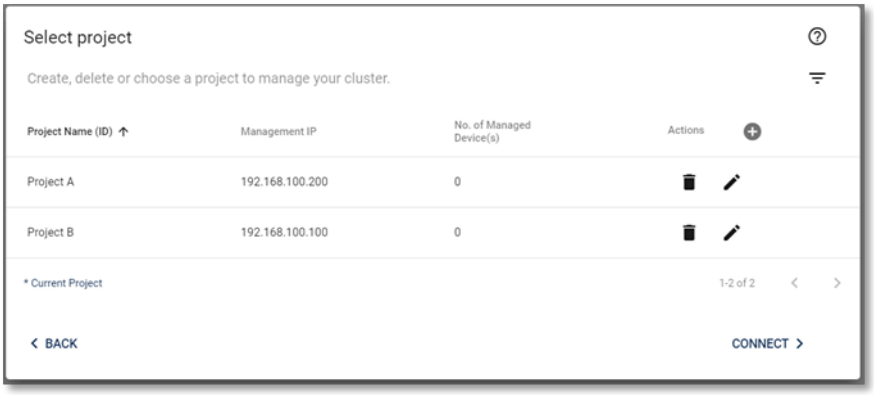


Figure 5.8.1A – Change project

To switch project at the A-NM without sign out

1) Click  at the top menu.
2) Click  at the sub menu.

3) Select your project at ***Project List***.
4) Double click the project to switch project.

5.8.2. Sign out

To sign out the A-NM

1) Click  at the top menu.
2) Click **YES** to sign out, click **CANCEL** to stop the sign out action.

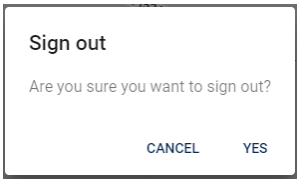


Figure 5.8.2A – Sign out the A-NM

5.8.3. Settings

To change A-NM Password

1) Click at the top menu.
2) Enter the **Current Password**, **New Password** and **Confirm New Password** to change the password.

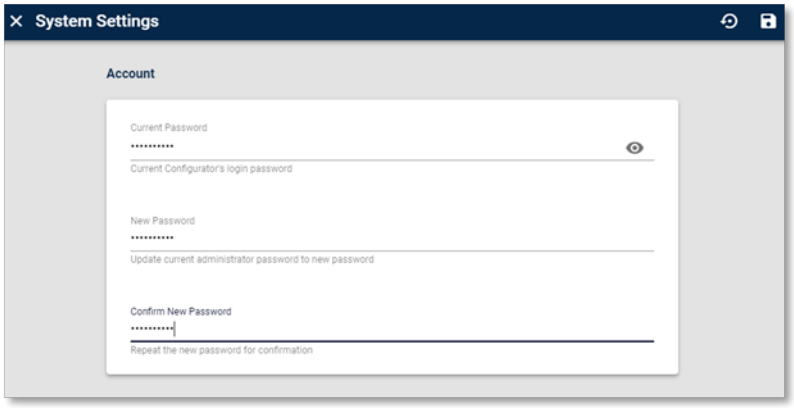


Figure 5.8.3A – Change the A-NM password

3) Click to save the changes or click to reset the changes.

   Note: This password should be between 8 to 32 alphanumeric characters.

Warning! If you forget the password, you must uninstall and install the A-NM again and all the saved information will be lost.

4) You will be redirect to the sign in page and you can sign in to the A-NM with the new password.

5.8.4. About

Click at the top menu.

Figure 5.8.4A – About the A-NM

5.8.5. Help

Click  at the top menu to show the ***Guideline***.

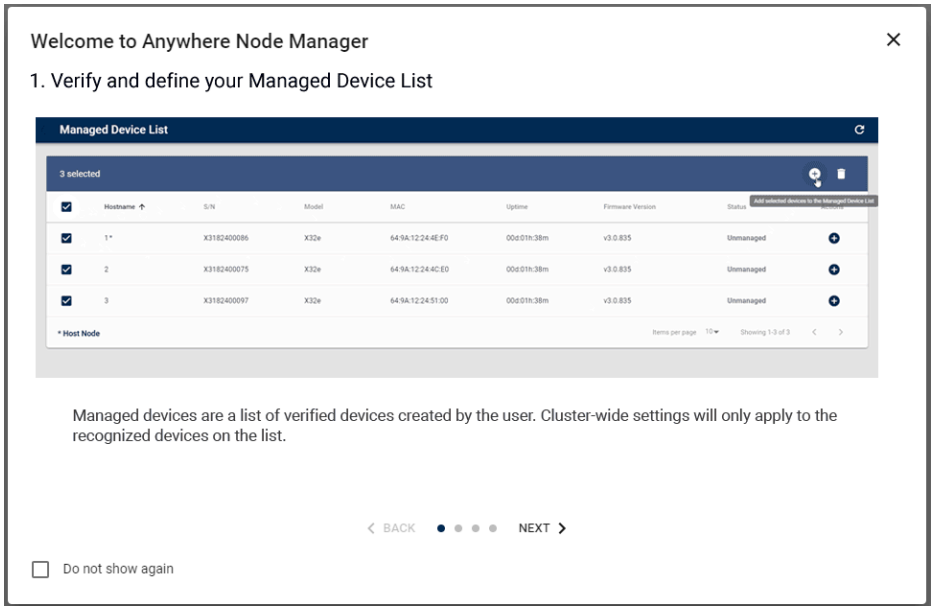


Figure 5.8.5A – ***Guideline*** of A-NM

5.8.6. Show/Hide Link Label

Click  to hide or show link label at Cluster Topology page.

Note: The link label includes the associated radio, channel and central frequency.

Note: The link label is shown by default.

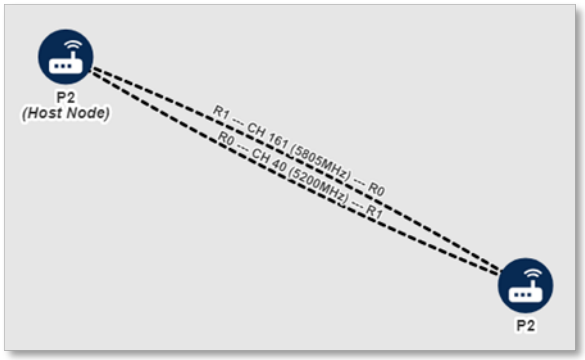


Figure 5.8.6A – Show Link Label

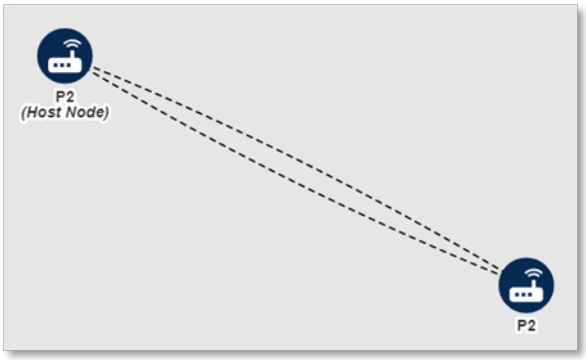


Figure 5.8.6B – Hide Link Label

5.8.7. Fit Canvas

Click  to center the network topology at the cluster topology page for a clearer view.

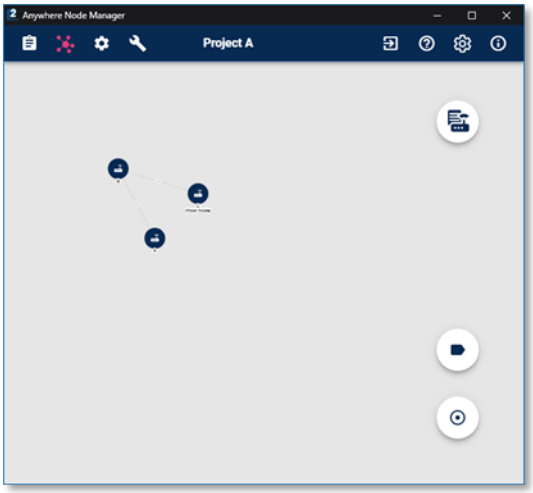


Figure 5.8.7A – Before fit canvas

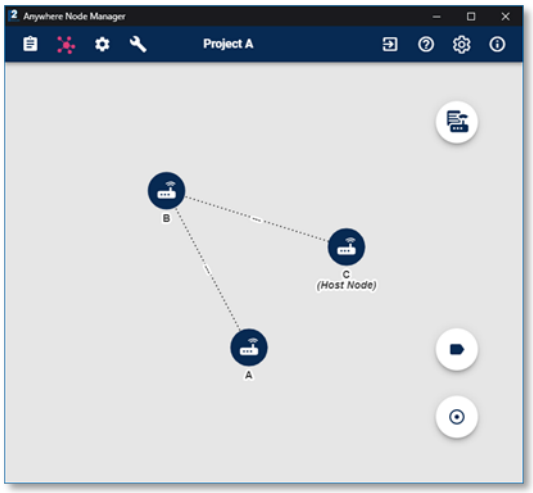


Figure 5.8.7B – After fit canvas

5.9. Cluster Topology

Cluster Topology provides a graphical view of the wireless mesh topology. Basic information is provided, including the hostname of each node, connection status, node info card and link info card.

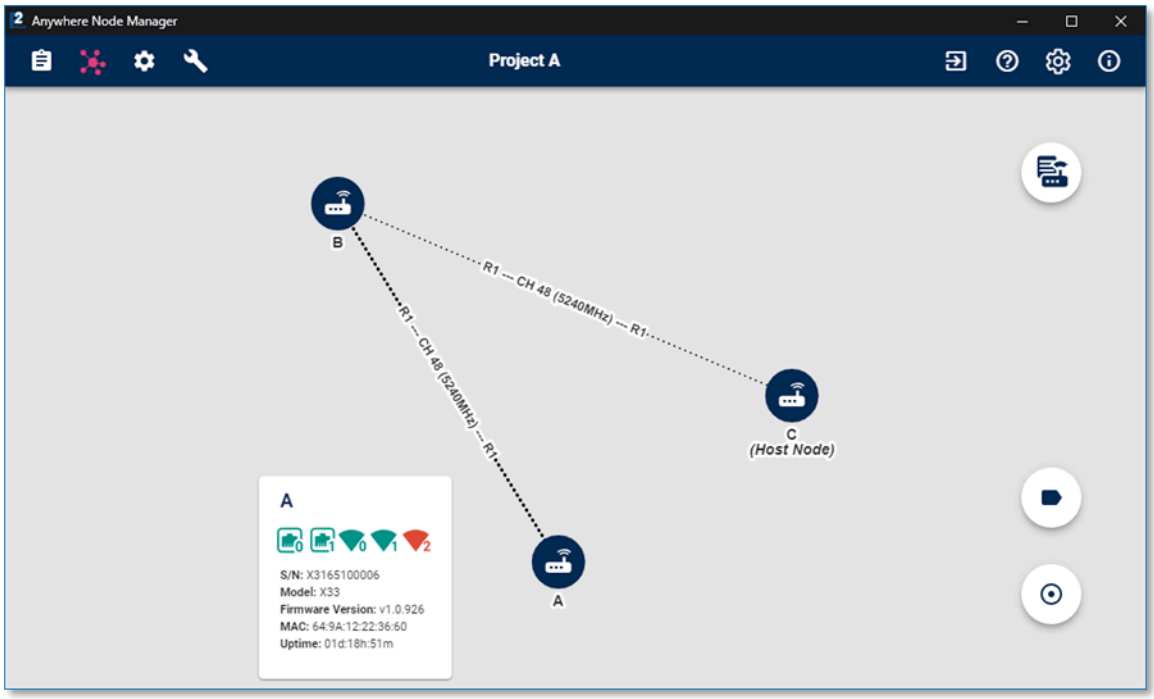


Figure 5.9A – ***Cluster Topology*** user interface

The labels provide the following information:

- Node Hostname
- Radio Interface
- Channel
- Central Frequency

Note: The host node of the cluster will be marked.

Note: Cluster Topology page will update every 10 seconds automatically.

The different colors of node icon represent different device statuses:

Icon	Status
	Unmanaged
	Reachable
	Unreachable
	Management Secret Mismatch

5.9.1. Node Info Card

You can place your mouse over the ***device icon*** to display the specific node info.

Figure 5.9.1A – Hover to display the ***Node Info Card***

Label/Icon	Description
 Figure 5.9.1B – ***Node Info Card*** interface	Displays the device hostname
	Displays the status of device interface Ethernet Icon: Enable Disable Radio Icon: Enable Disable
	Displays the serial number of device
	Displays the model of device
	Displays the firmware version of device
	Displays the MAC address of device
	Displays the device active uptime since last boot-up

5.9.2. Link Info Card

You can place your mouse over the ***link*** to view the specific link info.

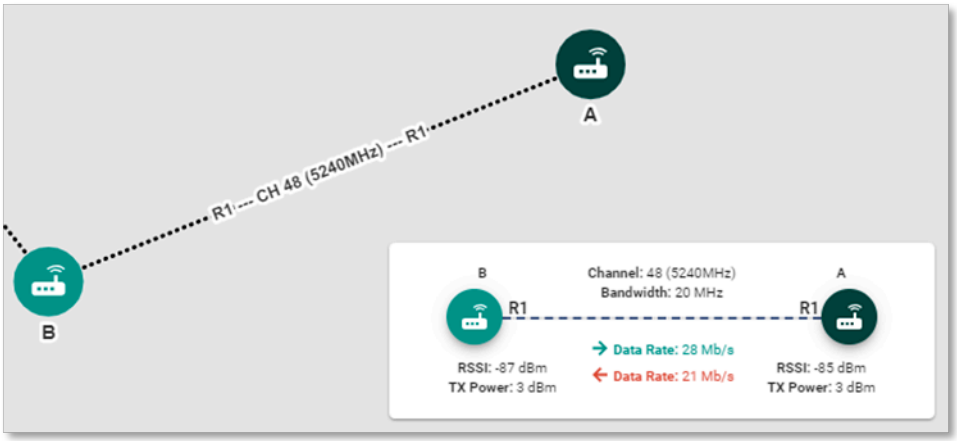
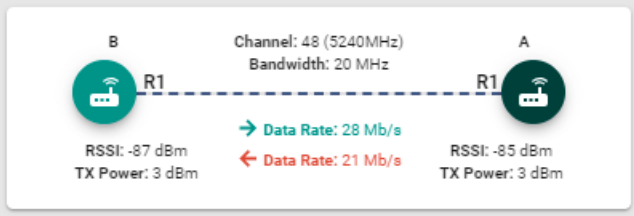


Figure 5.9.2A – Hover to display the ***Link Info Card***

Label/Icon	Description
 Figure 5.9.2B – ***Node Info Card*** user interface	Display the hostname of the two nodes
	Display the related radio of the link
	Displays the channel and central frequency of the link
	Displays the channel bandwidth of the link
	Displays the data rate of two directions
	Displays the RSSI of the related radio
	Displays the TX power of the related radio

5.9.3. Node Menu

You can right-click the ***device icon*** to display a floating menu of the specific node.

Figure 5.9.3A – Right-click to display the ***Node Menu***

Button	Description
	Overview (see page 51)
	Statistics (see page 52)
	Configuration (see page 55)
	Maintenance (see page 62)
	Security (see page 72)

	RSSI Viewer (BETA) (see page 75)

5.9.4. Node Dialog Box

By clicking the button at the node menu, a node dialog box for that node appears as a popup within the Cluster Topology page.

Each dialog box uses the device hostname as title and contains five sections, such as Overview, Statistics, Configuration, Maintenance and Security.

Note: You can open more than one node dialog box at the same time.

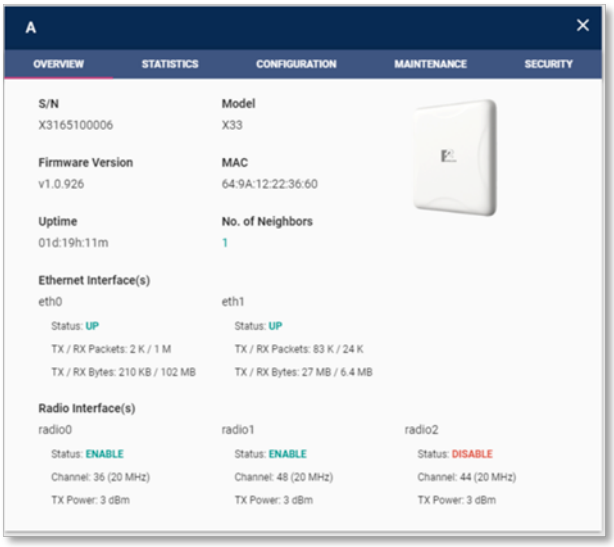
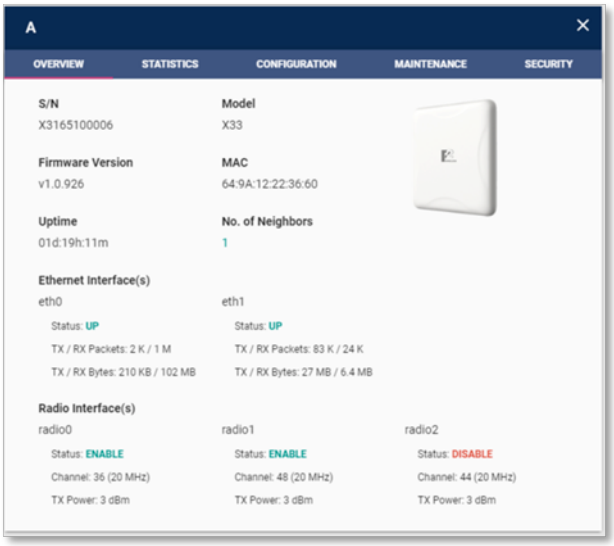


Figure 5.9.4A – ***Node Dialog Box***

5.10. Overview

The overview section displays the detailed information of the specific node.

Label/Icon	Description
 Figure 5.10A – Overview at ***Node Dialog Box***	Displays the serial number of the device
	Displays the model of device
	Displays the picture of device
	Displays the firmware version of device
	Displays the MAC address of device
	Displays the device active uptime since last boot-up
	Displays the number of connected neighbors which are • Online; and • on the same managed device list
	Displays the status of node interfaces • Ethernet Interface [**UP**/**DOWN**] • Radio Interface [**ENABLE**/**DISABLE**]
	Displays the TX/RX statistic of the ethernet interface
	Displays the channel and central frequency of the radio interface
	Displays the TX power of the radio interface

Note: The overview section will not update automatically, please reopen the dialog box to reload the information.

5.11. Statistics

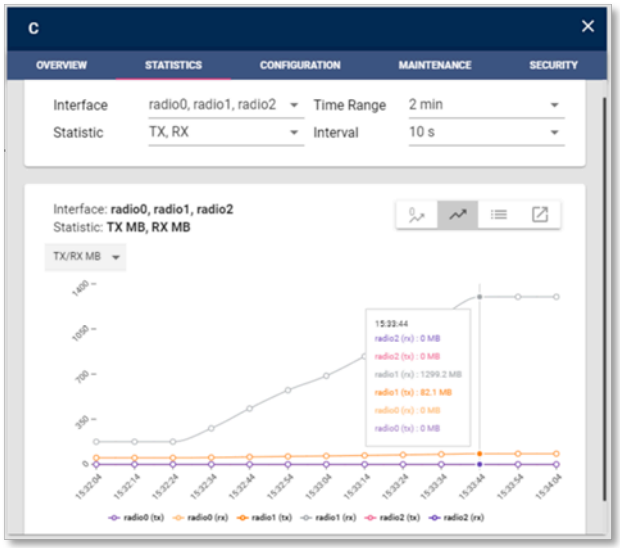


Figure 5.11A – Statistics at ***Node Dialog Box***

The *Node Statistics* section provides a visual representation of network traffic connected to the specific node. A visual graph (Graph View) represents the accumulated Tx/Rx usage versus time and you can mouse over at each data point to check the usage.

Note: The A-NM will start to capture statistic data when you move to the statistic section.

Note: The data of the graph will be reset if you close the node dialog box.

Item	Description
Display Interface	Define one/more interface to display on the graph. **Note**: The default interfaces are **eth0** and **eth1**.
Statistic Type	Define the type to display. • TX, RX • TX Packets, RX Packets **Note**: The default types are **TX** and **RX**.
Time Range	Define the x-axis of the graph, i.e. the selected time range for the data display. **Note**: The default value is **2 mins.**
Update Interval	Define the data update interval of the graph, i.e. the

	time difference between two data points. **Note**: The default value is **10 s.**

Besides that, you can view the node statistic using the table view and Overview view by clicking the following buttons.

Button	Description
	Normalize View (see page 53)
	Graph View
	Table View (see page 54)
	Detail View (see page 54)

5.11.1. Normalize View

The ***Normalize View*** displays a normalized statistic graph which makes the base starting from 0.

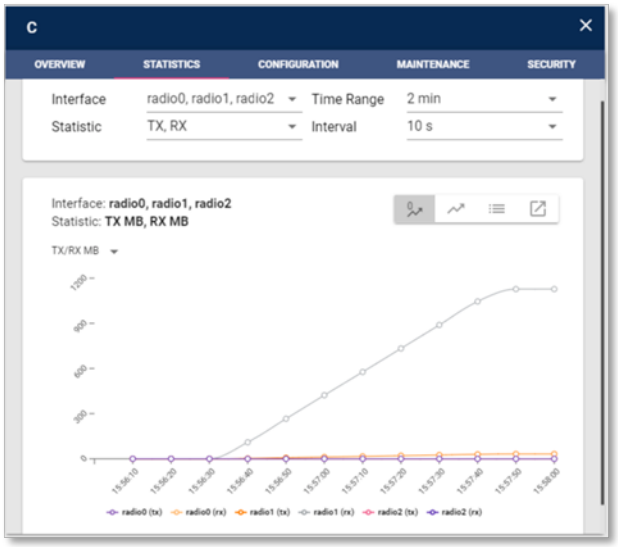


Figure 5.11.1A – Table view of statistics

5.11.2. Table View

The ***Table View*** displays a general list of network traffic with all node interfaces and statistic types.

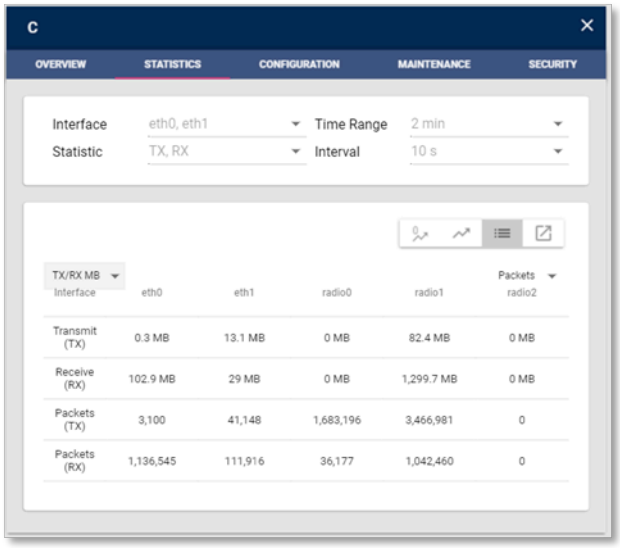


Figure 5.11.2A – Table view of statistics

5.11.3. Detail View

The ***Overview*** displays all the network traffic with separate statistics graph. It shares the same time range and update interval with the **Default View.** You can filter the display interface at the top right corner.

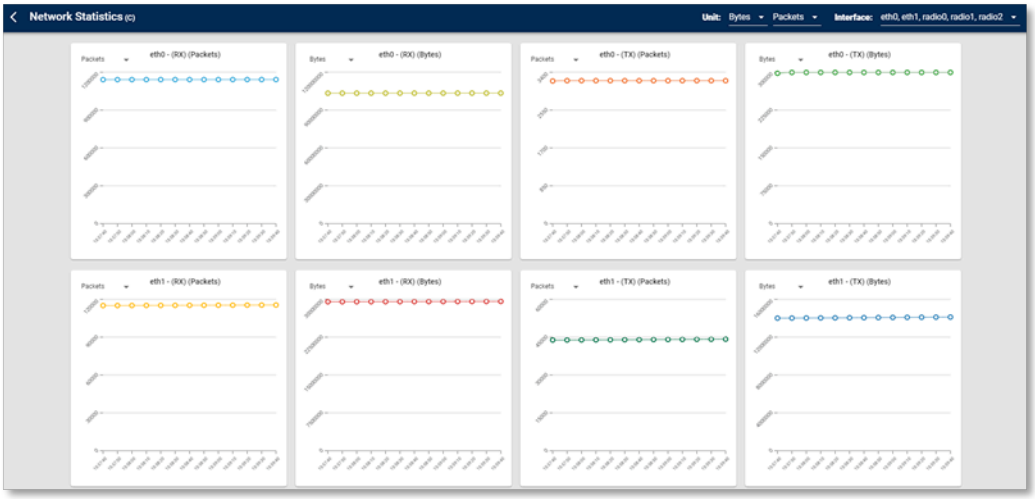


Figure 5.11.3A – Overview of statistics

5.12. Configuration

The ***Configuration*** section provides an interface to configure radio settings on a node by node basis. You can make changes to the following options:

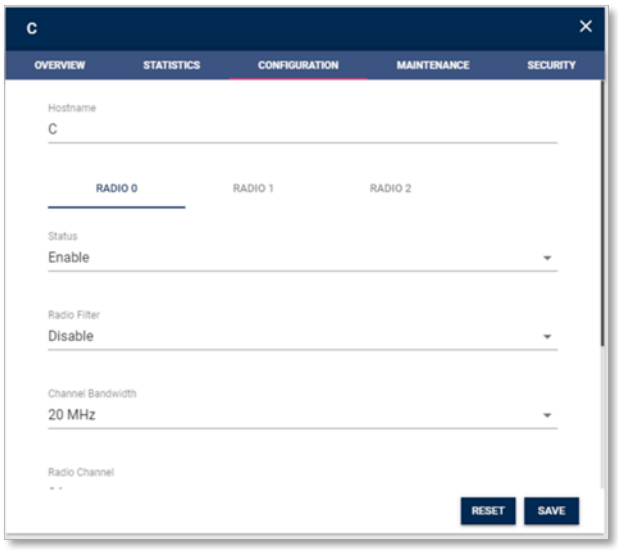


Figure 5.12A – Configuration at ***Node Dialog Box***

General Option	
Hostname	You can enter a unique, descriptive name for each node. The hostname will display at the Cluster Topology. **Note**: This name can be up to 32 characters long with hyphen and underscore.
Radio Status	Enable/Disable
Radio Channel	May vary on different countries and channel bandwidth
Channel Bandwidth	20MHz/40MHz/80MHz
Transmit Power	1 – 23 dBm (may vary on different models)

Advance Option (Optional)	
Radio Filter	Configurable bandpass filter that is used to attenuate the out of band signal. Options include: • Enable • Disable
Distance	Set the distance parameter between two devices. Options include: • Default (300m) • 300 – 24000 m **Note**: Please set the longest distance if the node is running at point to multiple point state.

Buttons	
RESET	Reset the unsaved changes.
SAVE	Save and apply the changes.

Note: If you want to connect two nodes with link, you must use the same channel and channel bandwidth.

Warning! All changes will be cleared if you close the dialog without save. A short disconnection time may be introduced after you apply the changes. Please wait until the reconnection of nodes.

Warning! As the ***Host Node*** is the only node that connected to the ***A-NM***, you must configure the ***Remote Nodes*** first (refer to the definition of node on page 7). Otherwise, the A-NM will lose the control of the Remote Nodes, resulting in an isolated network. Please refer to the following best practice for a step-by-step guide on how to make changes to a network without losing the connection to the A-NM.

To change channel of a daisy chain network

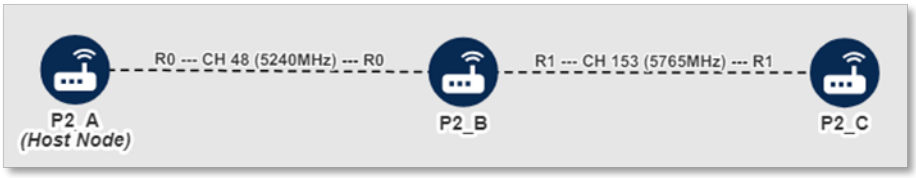


Figure 5.12B – Original Setting

Original Settings	
A-NN_A (Host Node)	• Radio0: Enable ○ Channel: 48 • Radio1: Disable

A-NN_B (Remote Node)	• Radio0: Enable
	  ○ Channel: 48
	• Radio1: Enable
	  ○ Channel: 153

A-NN_C (Remote Node)	• Radio0: Disable • Radio1: Enable ○ Channel: 153

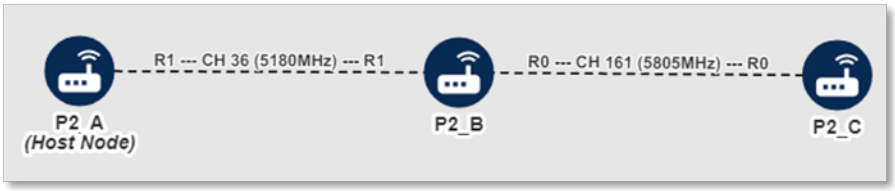


Figure 5.12C – New Setting

New Settings	
A-NN_A (Host Node)	• Radio0: Enable -> **Disable** • Radio1: Disable -> **Enable** ○ **Channel: 36**
A-NN_B (Remote Node)	• Radio0: Enable

	○ Channel: 48 -> **161** • Radio1: Enable ○ Channel: 153 -> **36**
A-NN_C (Remote Node)	• Radio0: Disable -> **Enable** ○ **Channel: 161** • Radio1: Enable -> **Disable**

Configure **A-NN_C** first as it is the furthest node from the host node:

1) Right-click 

to open the ***Node Menu***.

2) Click  to open the ***Node Dialog Box*** of ***Configuration***.

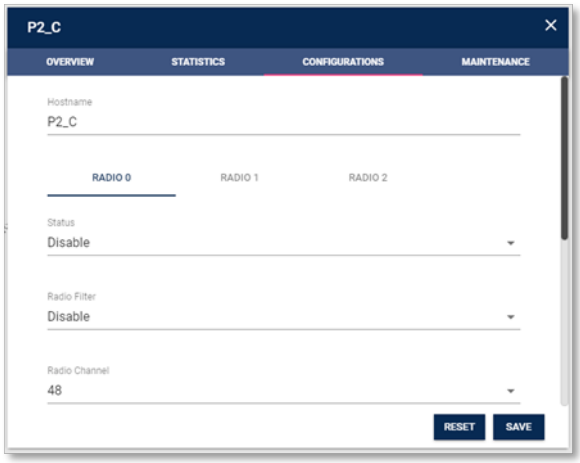


Figure 5.12D – ***Configuration*** of the node

3) Select **RADIO 0** tab.

4) Change the **Radio 0 status** and **channel** according to the New Setting table (see page **57**).

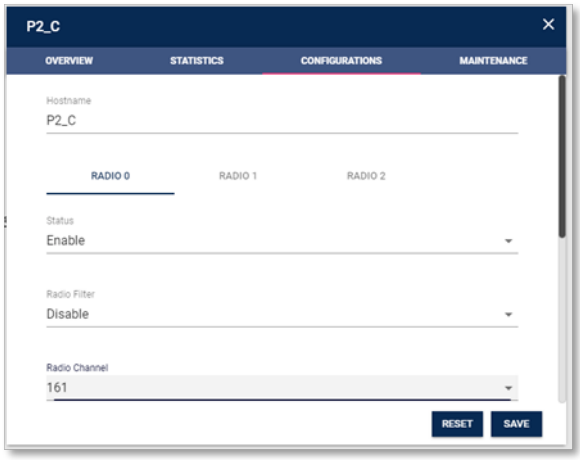


Figure 5.12E – Configure the channel of radio 0

5) Select **RADIO1** tab.

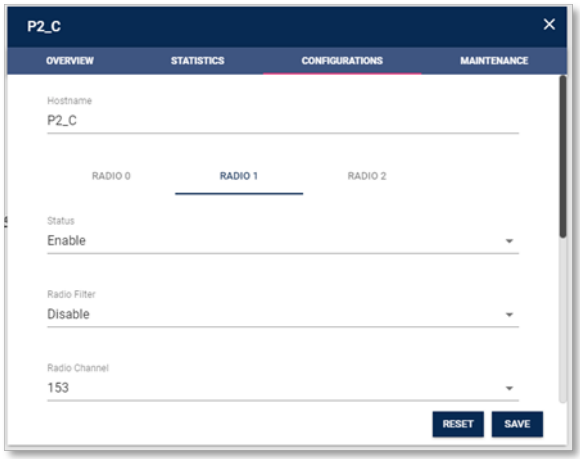


Figure 5.12F – Move to radio 1

6) Change the **Radio1 status** and **channel** according to the **New Setting table (see page 57)**

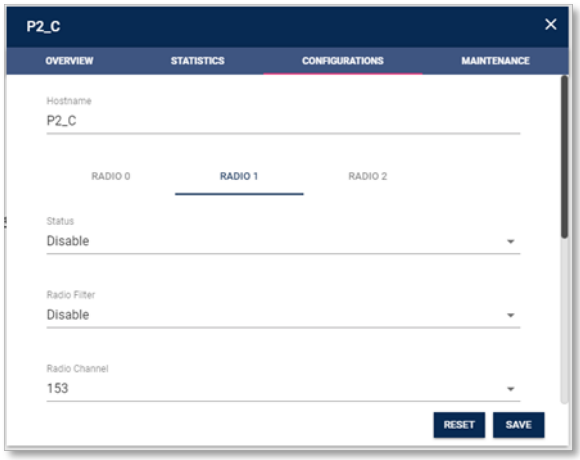


Figure 5.12G – Configure the channel of radio 1

7) Click OK to confirm the radio status changes.

Figure 5.12H – Warning for radio status changing

8) Click  to apply the changes.

9) Click **PROCEED**.

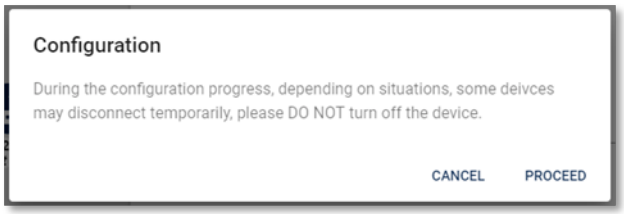


Figure 5.12I – Confirm to apply the changing

10) Wait for the process to be completed.

11) Click **OK**.

Figure 5.12J – Configuration completed

After we changed the channel of **A-NN_C**, the **A-NN_C** become unreachable (**Host Node** cannot reach **A-NN_C**) as the link between **A-NN_B** and **A-NN_C** cannot be formed.

Note: If you want to connect two nodes with link, you must use the same channel and channel bandwidth.

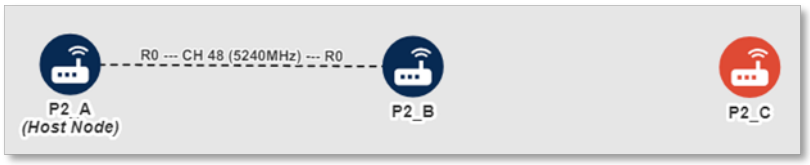


Figure 5.12K – Network topology after applied the configuration

Next, Configure **A-NN_B**:

12) Right-click  to open the ***Node Menu***.
13) Repeat Step 2 to Step 11 for **A-NN_B**. This will establish a link between **A-NN_B** and **A-NN_C**.

A-NN_B will become temporarily unreachable (**Host Node** cannot reach **A-NN_B**) as the link between **A-NN_A (Host Node)** and **A-NN_B** cannot be formed. Once the settings for **A-NN_A** are updated, status of both **A-NN_B** and **A-NN_C** will be visible in the A-NM.

Note: Remember to use the same channel and channel bandwidth to establish a link between two nodes.

Figure 5.12L – Network topology after applied the configuration

Last but not least, configure **A-NN_A** to complete the configurations update:

14) Right-click  to open the ***Node Menu***.

15) Repeat Step 2 to Step 11 at **A-NN_A** to establish a link between **A-NN_A** and **A-NN_B**.

After completing all the settings, all the nodes will be reachable again, with settings updated.

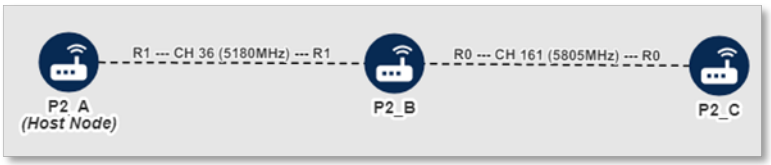


Figure 5.12M – Final network topology after configuration

5.13. Maintenance

The ***Maintenance*** section contains administrative options including ***Configuration Backup, Configuration Restore, Firmware Upgrade, Factory Reset***, and ***System Restart***.

5.13.1. Node Configuration Backup

The ***Configuration Backup*** feature helps you save a copy of the configuration file from one node (i.e. ***original node***) so that you can apply it to another node that has the same model and firmware version as the original node.

The backup file is encrypted. You cannot read or make changes to the file.

Note: The backup file does not contain any cluster-wide setting

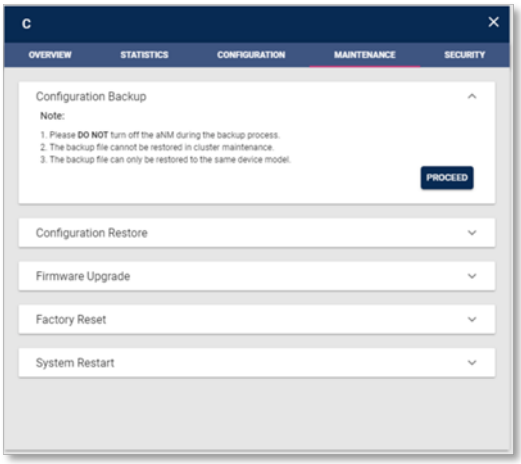


Figure 5.13.1A – ***Configuration Backup*** user interface

To backup a node

1) Right-click the ***device icon*** to open the ***Node Menu***.

2) Click  to open the ***Node Dialog Box*** of ***Maintenance***.

3) Click  to extend the **Configuration Restore** tab.

4) Click **PROCEED** to back up the configuration.

5) Check the backup file at Download or the selected location.

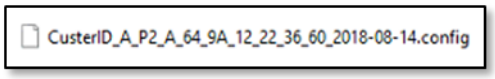


Figure 5.13.1B – The backup file

5.13.2. Node Configuration Restore

The ***Configuration Restore*** feature helps you to apply the backup file to the node that has the same model and firmware version as the original node.

Warning! As the ***Host Node*** is the only node that connected to the ***A-NM***, you must restore the ***Remote Nodes*** first (refer to the definition of node on page **7**). Otherwise, the A-NM will lose the control of the Remote Nodes, resulting in an isolated network. Please refer to the following best practice for a step-by-step guide on how to make changes to a network without losing the connection to the A-NM.

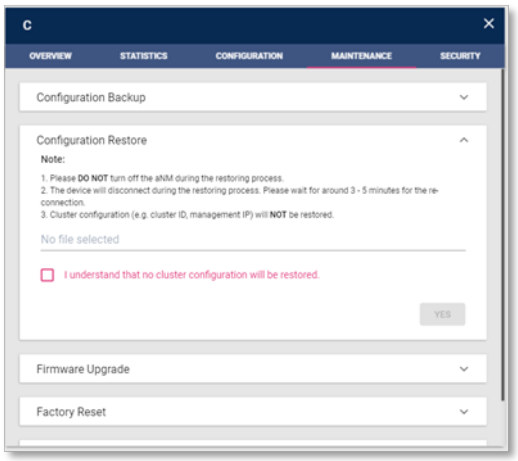


Figure 5.13.2A – ***Configuration Restore*** user interface

To restore nodes

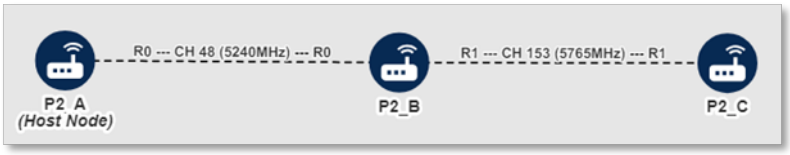


Figure 5.13.2B – Original topology

To restore configuration of the above daisy chain network, start with **A-NN_C**, then **A-NN_B**, and lastly with **A-NN_A**.

1) Prepare all the backup files of the nodes generated by ***Configuration Backup***.

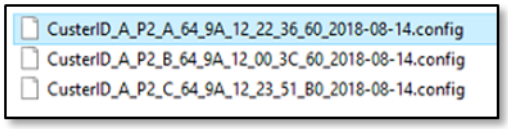


Figure 5.13.2C – The backup file of all nodes

Firstly, restore **A-NN_C** that is the furthest away from the host node:

2) Right-click 

to open the ***Node Menu***.

3) Click  to open the ***Node Dialog Box*** of ***Maintenance***.

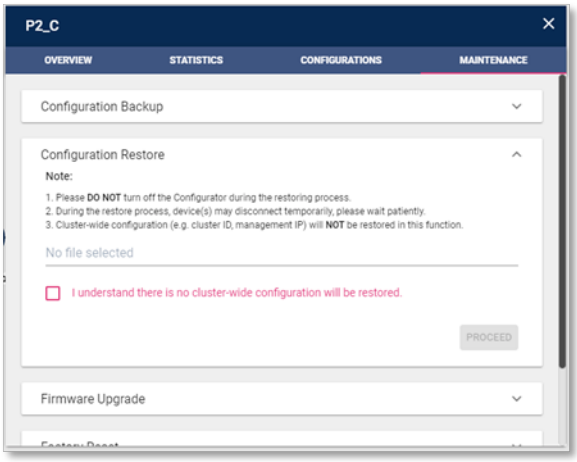


Figure 5.13.2D – Go to ***Configuration Restore***

4) Click 

to upload the backup file.

5) Select the appropriate backup file.

Figure 5.13.2E – Upload the backup file

6) Check the confirmation box to enable the button.

Figure 5.13.2F – Check the confirmation box

7) Click **PROCEED** at the ***Configuration Restore*** tab.
8) Click **PROCEED**.

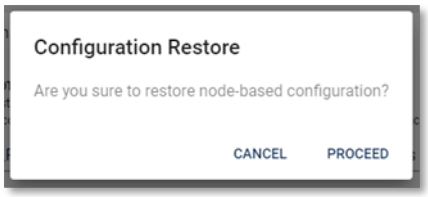


Figure 5.13.2G – Confirm the configuration restore process

9) Wait for the process to be completed.
10) Click **OK**.

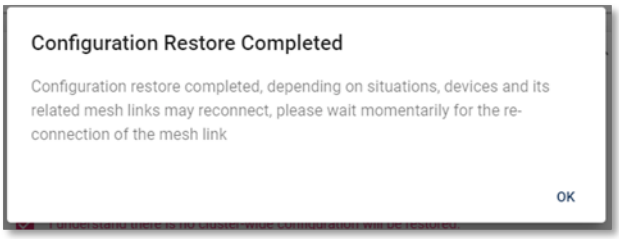


Figure 5.13.2H – Configuration restore completed

After we restored **A-NN_C**, the **A-NN_C** become unreachable (**Host Node** cannot reach **A-NN_C**) as the link between **A-NN_B** and **A-NN_C** is not yet formed.

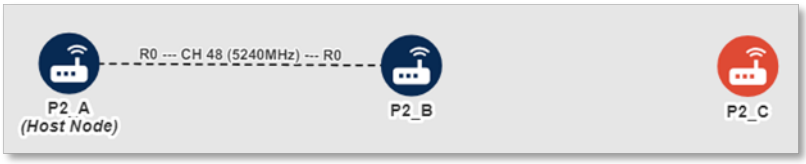


Figure 5.13.2I – Network topology after applied the configuration restore

Next, Restore **A-NN_B** to establish a link between **A-NN_B** and **A-NN_C.**:

11) Right-click 

to open the ***Node Menu***.

12) Repeat Step 3 to Step 10 for **A-NN_B**. This will establish a link between **A-NN_B** and **A-NN_C**.

A-NN_B will become temporarily unreachable (**Host Node** cannot reach **A-NN_B**) as the link between **A-NN_A (Host Node)** and **A-NN_B** cannot be formed. Once the settings for **A-NN_A** are updated, status of both **A-NN_B** and **A-NN_C** will be visible in the A-NM.

Figure 5.13.2J – Network topology after applied the configuration restore

Last but not least, restore **A-NN_A** to complete the update:

13) Right-click 

to open the ***Node Menu***.

14) Repeat Step 3 to Step 10 at **A-NN_A** to establish a link between **A-NN_A** and **A-NN_B**.

After completing all the settings, all the nodes will be reachable again, with settings updated.

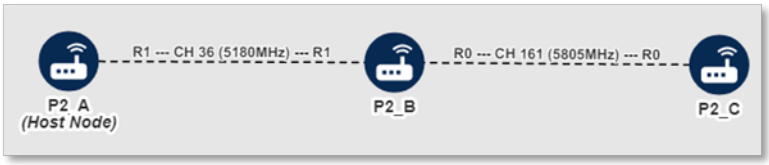


Figure 5.13.2K – Final network topology after configuration restore

5.13.3. Node Firmware Upgrade

The ***Firmware Upgrade*** feature helps you to upgrade your A-OS devices to the latest version.

Warning! Please make sure all the firmware version is the same at the same cluster

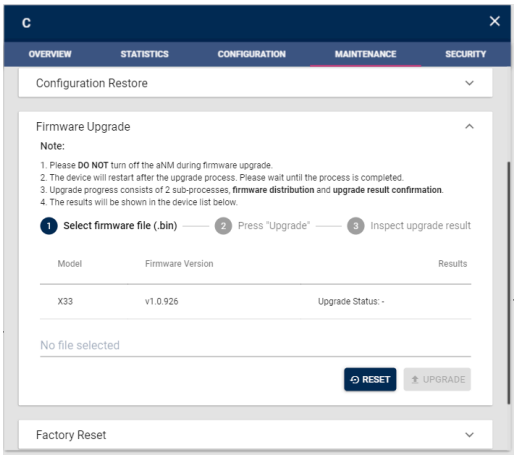


Figure 5.13.3A – ***Firmware Upgrade*** user interface

To upgrade a node

1) Download the latest firmware file from the partner portal.
2) Right-click the ***device icon*** to open the ***Node Menu***.
3) Click  to open the ***Node Dialog Box*** of ***Maintenance***.
4) Click to extend **Firmware Upgrade** tab.
5) Click  to upload the firmware file.
6) Select the appropriate firmware file.

   Note: You can click **Reset** to clear the selected firmware file

Figure 5.13.3B – Upload the firmware file

7) Click **UPGRADE**.
8) Click **Proceed** and wait for the checking progress.

   Note: The A-NM will verify the firmware file by checksum and the upgrade will not start with corrupt or invalid firmware file.

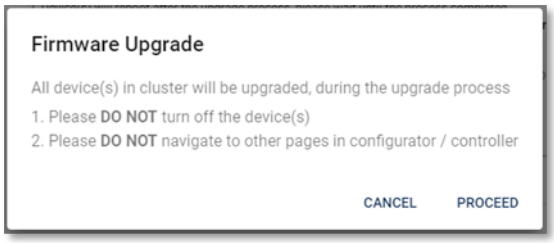


Figure 5.13.3C – Start the firmware upgrade process

9) Double confirm the firmware file and click **OK**.

   Note: Please wait for the upgrade process as it takes time to complete.

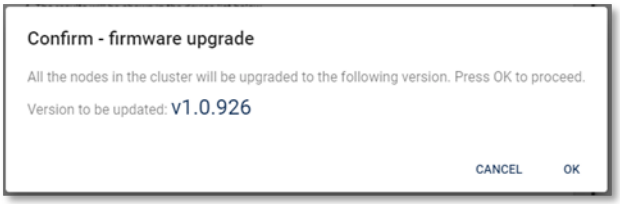


Figure 5.13.3D – Confirm to firmware upgrade process

10) Click **OK**.

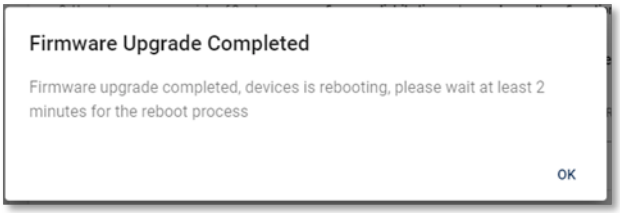


Figure 5.13.3E – Firmware upgrade completed

11) Check the upgrade status at the ***Node Dialog Box***.

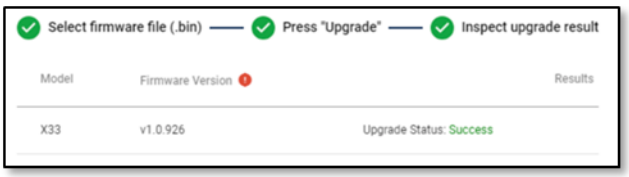


Figure 5.13.3F – Check the firmware upgrade result

12) Close the ***Node Dialog Box*** and check the firmware version via ***Node Info***.

    Note: Please wait for the reconnection as the device will reboot after upgrade.

Figure 5.13.3G – Check the new firmware version

5.13.4. Node Factory Reset

The Factory Reset feature helps you to reset the node to factory default setting.

Warning! Once a node is reset, it will no longer be reachable by the current project in the A-NM. To place the node under the management of a particular project, use the default management IP and management secret to access it and update its settings.

Note: It is recommended to perform configuration backup (refer to Configuration Backup on page 62) before the factory reset.

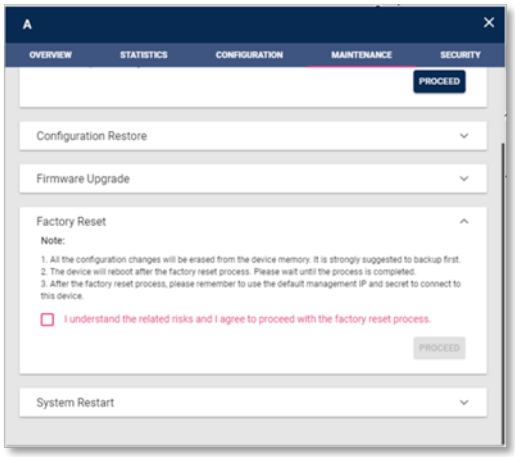


Figure 5.13.4A – ***Factory Reset*** user interface

To reset a node

1) Right-click the ***device icon*** to open the ***Node Menu***.
2) Click  to open the ***Node Dialog Box*** of ***Maintenance***.
3) Click to extend **Factory Reset** tab.
4) Check the confirmation box to enable the button.

Figure 5.13.4B – Check the confirmation box

5) Click **PROCEED**.
6) Click OK to continue.

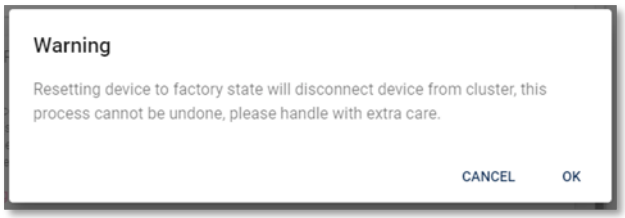


Figure 5.13.4C – Warning for the reset process

7) Click OK.

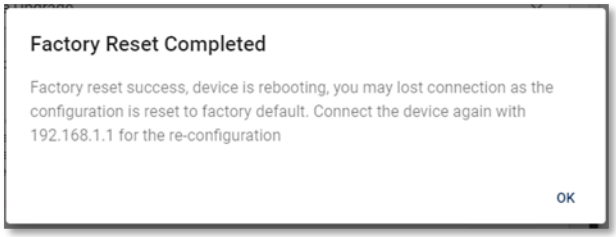


Figure 5.13.4D – Factory reset completed

After the factory reset process, all the settings of the node will be reset, and the node will become unreachable at the project in most of the cases. You can switch to the **Quick Staging (see page 27)** to further configure the node.

Note: Please make sure the A-NM is in the same subnet of the default Management IP (192.168.1.1) in order to reach the node.

5.13.5. Node System Restart

The ***System Restart*** feature helps you to reboot a node.

Note: Please wait around 3 - 5 minutes for the reconnection

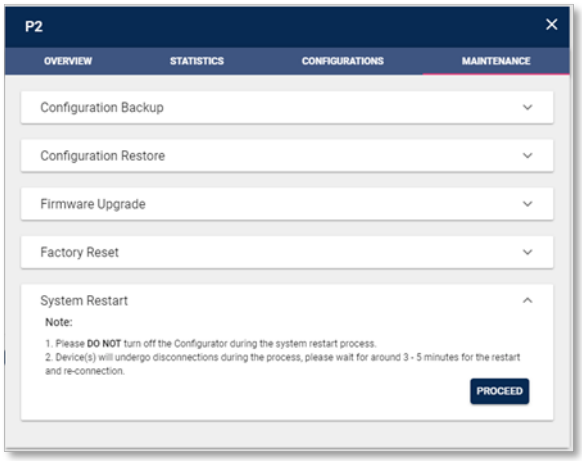


Figure 5.13.5A – ***System Restart*** user interface

To reboot a node

1) Right-click the ***device icon*** to open the ***Node Menu***.
2) Click  to open the ***Node Dialog Box*** of ***Maintenance***.
3) Click to extend **System Restart** tab.
4) Click **PROCEED**.
5) Click **OK** to continue.

   Note: You can click **CANCEL** to stop the process.

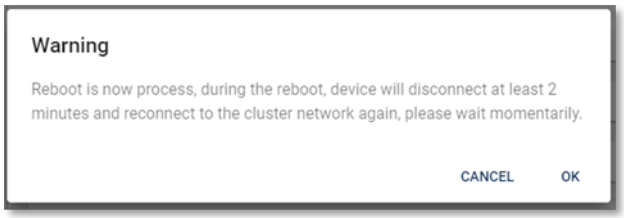


Figure 5.13.5B – Warning for the restart process

6) Wait for the process until the result box pops up and click **OK**.

   Note: Please wait for the reconnection of nodes.

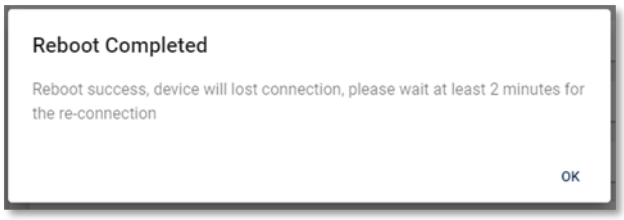


Figure 5.13.5C – Reboot completed

5.14. Security

5.14.1. Access Control List (BETA)

Access Control List (ACL) allows user to manage client device's access to the node and cluster.

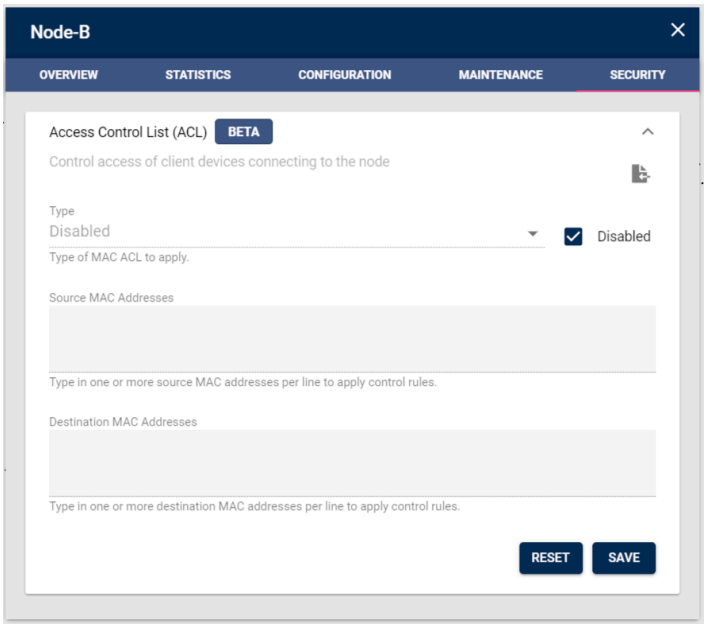


Figure 5.14.1A – ***ACL*** user interface

To set the ACL of a node

1) Right-click the ***device icon*** to open the ***Node Menu***.
2) Click  to open the ***Node Dialog Box*** of ***Security***.
3) Uncheck the checkbox of **Disabled**.
4) Enter the **MAC address(es)** at the appropriate field.
5) Click **SAVE**.

   Note: You can click **RESET** to clear the input.
6) Click **OK** on the confirmation box to continue.

   Note: You can click **CANCEL** to stop the process.

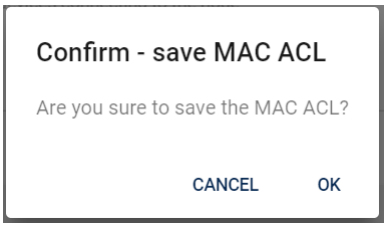


Figure 5.14.1B – Confirmation box of save process

7) Wait for the process until the result box pops up and click **OK**.

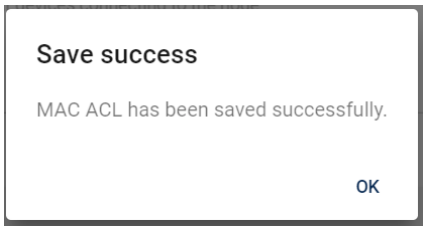


Figure 5.14.1C – Save ACL success

To export the ACL from a node

1) Right-click the device icon to open the Node Menu.
2) Click  to open the Node Dialog Box of Security.
3) Click  to export.

   Note: The button will be hidden if there is no MAC address at the list.
4) Check the ACL file at Download or the selected location.

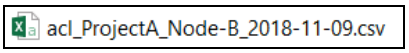


Figure 5.14.1D – The ACL file

To import ACL file to a node

1) Prepare an ACL file generated by export function of the ***Access Control List***.

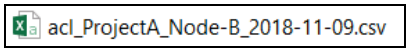


Figure 5.14.1E – The ACL file

2) Right-click the device icon to open the Node Menu.
3) Click  to open the Node Dialog Box of Security.
4) Click  to import ACL file.
5) Select the appropriate ACL file.
6) Check the MAC address(es) at the interface.
7) Click **SAVE**.

   Note: You can click **RESET** to clear the input.
8) Click **OK** on the confirmation box to continue.

   Note: You can click **CANCEL** to stop the process.

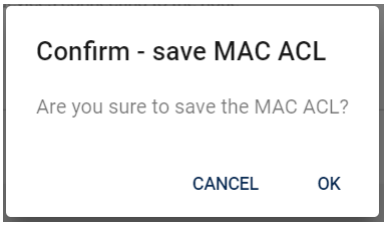


Figure 5.14.1F – Confirmation box of save process

9) Wait for the process until the result box pops up and click **OK**.

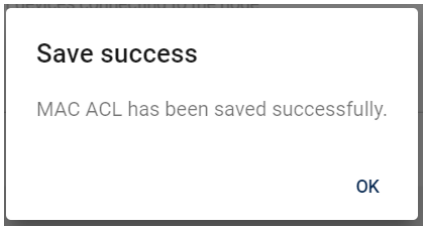


Figure 5.14.1G – Save ACL success

5.15. RSSI Viewer (BETA)

RSSI Viewer provides an interface to monitor the RSSI of a wireless link associated with the node.

Note: You can only open one RSSI Viewer window at the same time.

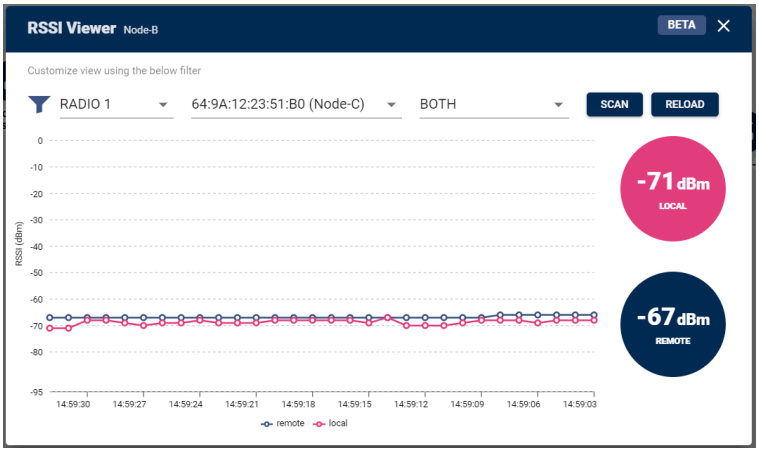


Figure 5.15A – RSSI Viewer user interface

The following parameters can be defined by the user:

Item	Description
Radio	Define the target radio for the monitoring.
Neighbors MAC	Define the target neighbor to display.
Show RSSI for	Choose which RSSI value to display. • LOCAL • REMOTE • BOTH

Buttons	
SCAN	Start the RSSI scanning.
STOP	Stop the RSSI scanning.
RELOAD	Reload the filter list.

5.16. Cluster Configuration

Cluster Configuration provides an interface to make changes to all managed nodes in the same cluster.

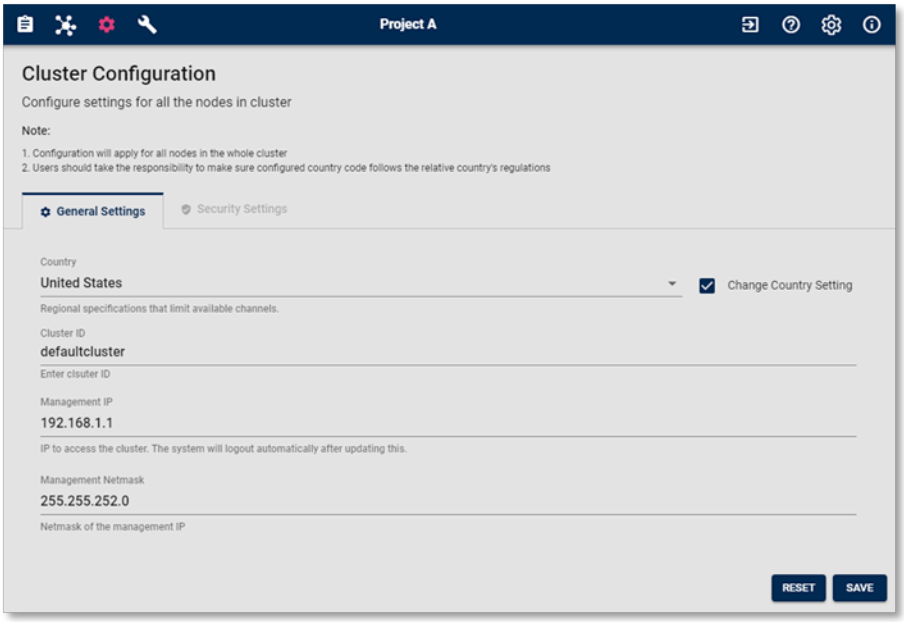


Figure 5.16A – ***Cluster Configuration*** user interface

General Option	
Country	• Select the appropriate country to ensure nodes operation adheres to regulatory. **Note:** The default Country is **United States**.
Cluster ID	• Enter a unique ID of the cluster. **Note:** This ID can be up to 16 characters long with hyphen and underscore. **Note:** The default Cluster ID is **defaultcluster**.
Management IP	• Set a valid IPv4 address at the same subnet. **Note:** The default Management IP is **192.168.1.1**. **Note**: The IP must not be in the same subnet with A-NM (192.168.99.X/24).
Management Netmask	• Set a valid IPv4 netmask at the same subnet. **Note:** The default Management netmask is **255.255.255.0**.

Security Option	
Wireless Encryption Key	• Define a unique security key for the wireless links. **Note:** The default Wireless Encryption Key is **defaultkey**.
Management Secret	• Define a unique secret for the communication between the A-NM and nodes. **Note:** The default Management Secret is **password**.

Warning! The ***Management IP*** must not be in the same subnet with the A-NM (192.168.99.X/24).

Warning! The A-NM will not apply the cluster-wide configuration changes to unmanaged devices. Please make sure that all the desired nodes are on the managed device list before proceeding with any changes. Otherwise, the A-NM will lose the control of the unmanaged devices, resulting in an isolated network.

To configure the cluster-wide setting

1) Click at the top menu to go to the ***Cluster Configuration*** page.
2) Make changes of the settings.

   Note: You can click **RESET** to clear the unsaved changes.
3) Click **SAVE** to apply the changes.
4) Click **PROCEED** to confirm the action.

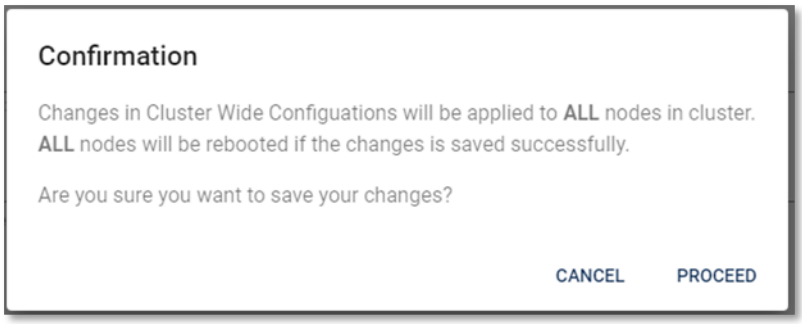


Figure 5.16B – Confirm the configuration process

5) A loading bar will appear at the top of the interface. A saving message will stay until the process completes and the result box pops up.

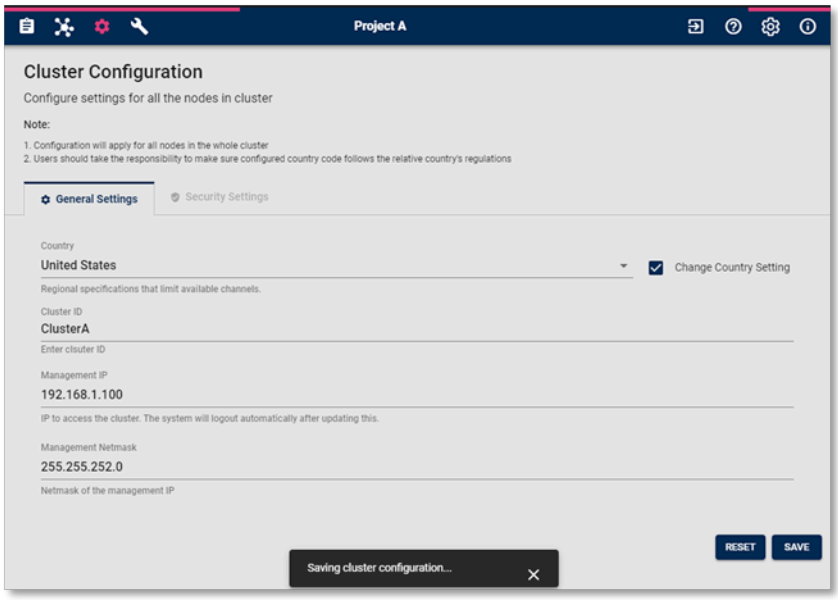


Figure 5.16C – Appling the configuration

6) Click **REDIRECT TO CLUSTER TOPOLOGY** in the pop-up box.

   Note: Device(s) will reboot after this process, please wait until the process is completed.

   Note: The Management IP of the project will be updated automatically.

Figure 5.16D – Save configuration successfully

To change the country of the cluster

1) Click  at the top menu to go to the ***Cluster Configuration*** page.
2) Check the **Change Country Setting** checkbox.
3) Read the **Disclaimer**.

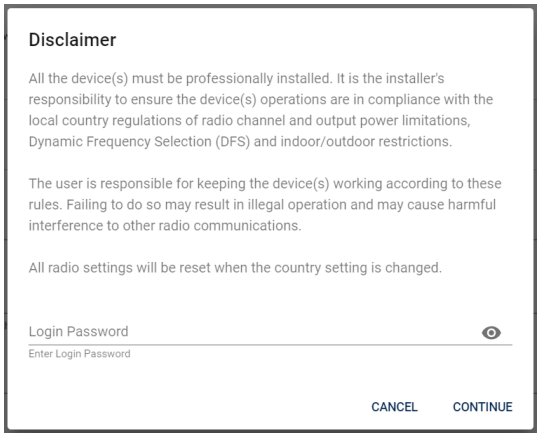


Figure 5.16E – Disclaimer

4) Enter the **sign in password** to enable the function.
5) Choose the appropriate country.

Warning! User is responsible to ensure the device(s) operations are in compliance with the local country regulations of radio channel and output power limitations, Dynamic Frequency Selection (DFS) and indoor/outdoor restrictions. Failing to do so may result in illegal operation and may cause harmful interference to other radio communications.

6) Click **SAVE** to apply the changes.

Note: You can click **RESET** to clear the unsaved changes.

Warning! All radio settings will be reset when the country setting is changed.

7) Click **PROCEED** to confirm the action.

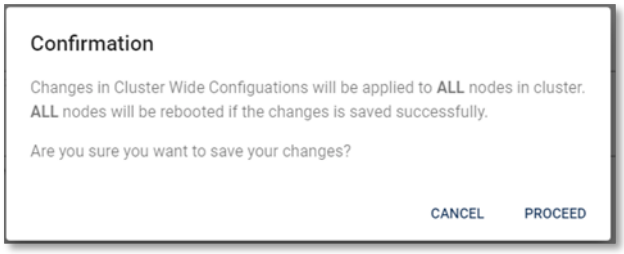


Figure 5.16E – Confirm the configuration process

8) A loading bar will appear at the top of the interface. A saving message will stay until the process completes and the result box pops up.

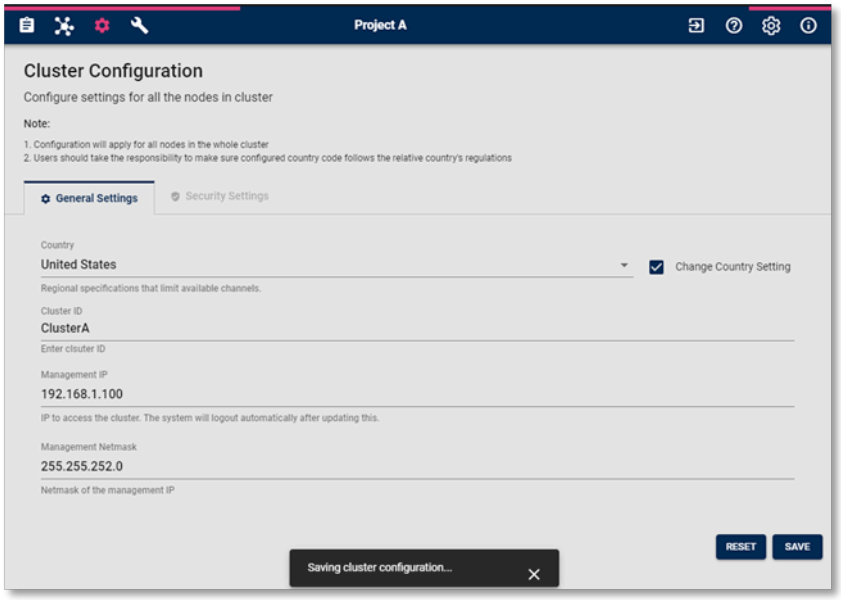


Figure 5.16F – Appling the configuration

9) Click **REDIRECT TO CLUSTER TOPOLOGY** in the pop-up box.

Note: Device(s) will reboot after this process. Please wait until the process is completed.

Note: The Management IP of the project will be updated automatically.

Figure 5.16G – Save configuration successfully

5.16.1. Cluster Configuration Mismatch

The A-NM will check the cluster settings consistency of all the managed nodes in the cluster. A ***Configuration Mismatch*** warning will be shown if the A-NM detects different settings with the host node (e.g. Country, Management IP and Management netmask).

Note: You should synchronize the cluster settings of all the managed nodes in the cluster to keep the consistency of the configuration.

Note: You can ignore the warning if you want to set new cluster settings. Simply make the changes and save it to overwrite the settings.

To synchronize the mismatched cluster configuration

1) Click  at the top menu to go to the ***Cluster Configuration*** page.
2) Check mismatched details at the **Configuration Mismatch** dialog box.

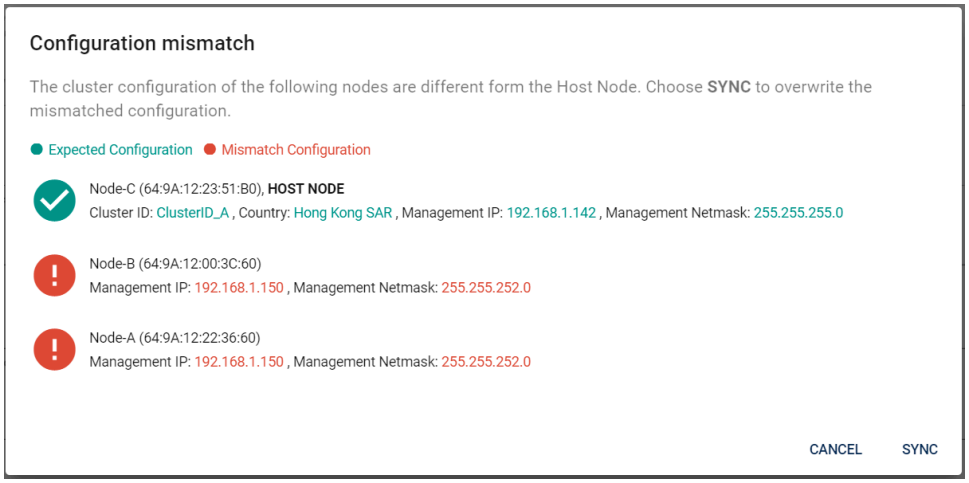


Figure 5.16H – Configuration Mismatch dialog box

3) Click **SYNC** to synchronize the cluster configuration to the managed nodes at the cluster.
4) A loading bar will appear at the top of the interface. A saving message will stay until the process completes and the result box pops up.

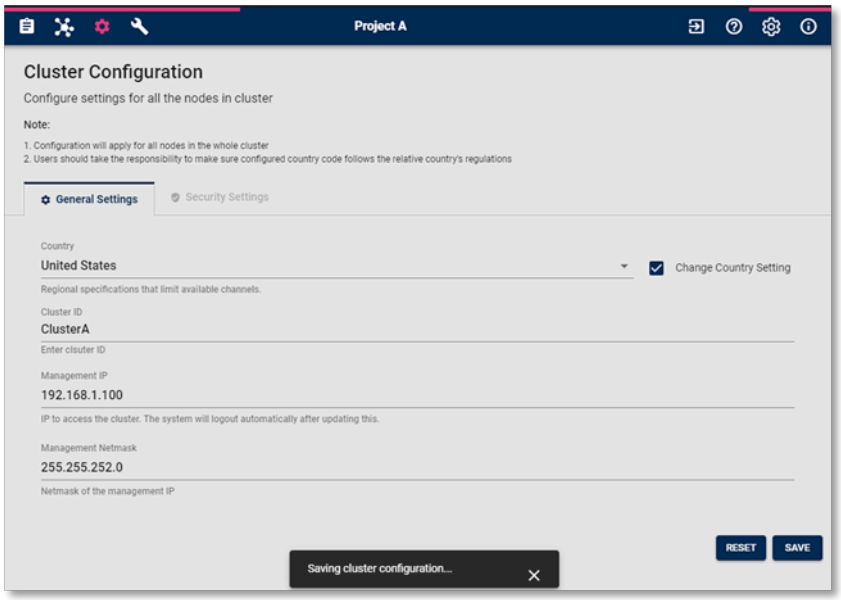


Figure 5.16I – Appling the configuration

5) Click **REDIRECT TO CLUSTER TOPOLOGY** in the pop-up box.

Note: Device(s) will reboot after this process, please wait until the process is completed.

Note: The Management IP of the project will be updated automatically.

Figure 5.16J – Save configuration successfully

5.17. Cluster Maintenance

The ***Cluster Maintenance*** section contains administrative options, including ***Firmware Upgrade***, ***System Restart***, ***Configuration Backup***, and ***Configuration Restore***.

5.17.1. Cluster Firmware Upgrade

The ***Cluster Firmware Upgrade*** helps you to upgrade all nodes on the managed device list.

When you upgrade the firmware for the mesh network, the A-NM will copy the new firmware file to all the managed nodes in the cluster.

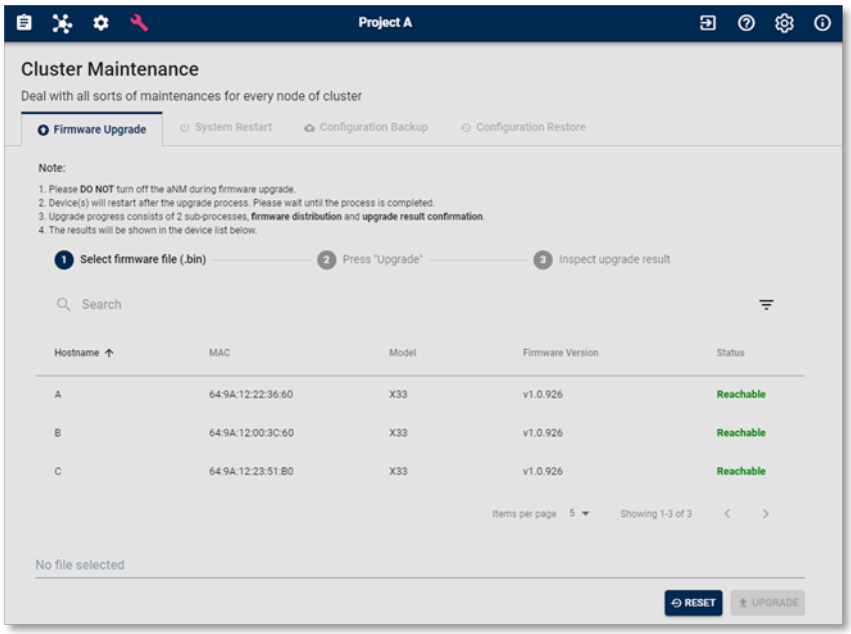


Figure 5.15.1A – ***Cluster Firmware Upgrade*** user interface

To upgrade a cluster

1) Download the latest firmware file from partner portal before launching the A-NM.
2) The status of all nodes on the managed device list will be shown in a table. Check if all nodes are reachable with hostname, model and version information shown properly. An empty entry denotes an unreachable node.

   Note: The upgrade will only proceed when all managed devices are reachable.
3) Click  to upload the firmware file.
4) Select the firmware file.

Note: You can click **Reset** to clear the selected firmware file

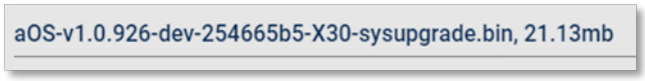


Figure 5.15.1B – Upload the firmware file

5) Click **UPGRADE**.
6) Click **Proceed** and wait for the checking progress.

   Note: The A-NM will verify the firmware file by checksum and the upgrade will not start with corrupt or invalid firmware file.

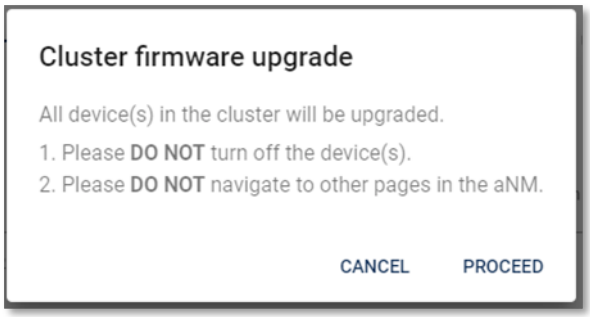


Figure 5.15.1C –Start the firmware upgrade process

Warning! Do not turn off any devices during the upgrade to avoid disruption.

7) Double confirm the firmware file and click **OK**.

   Note: Please wait for the upgrade process as it takes some time to complete.

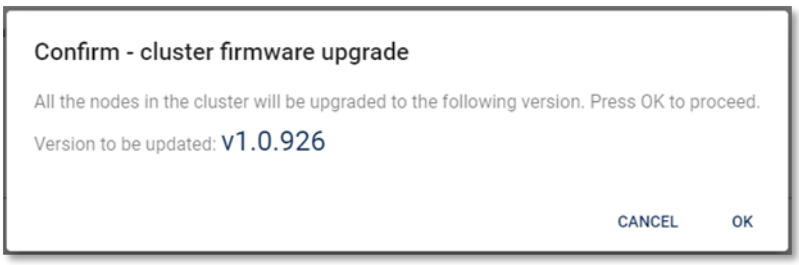


Figure 5.15.1D – Confirm to firmware upgrade process

8) A loading icon will appear until the process completes and the result box pops up.
9) Click **RETURN TO CLUSTER TOPOLOGY** and you will see the nodes and links when devices reboot is completed.

Note: Please wait for the reconnection of nodes as all the devices will reboot after the firmware upgrade.

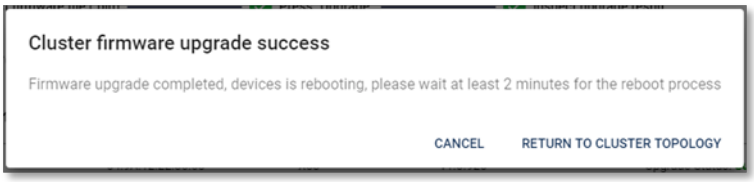


Figure 5.15.1F – Cluster firmware upgrade success

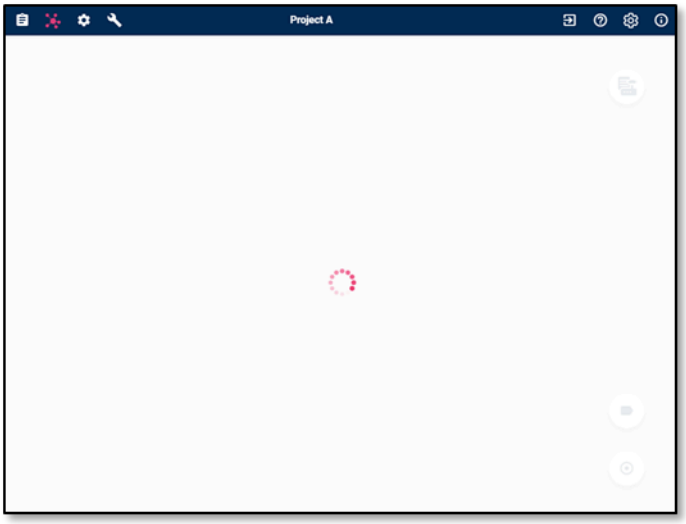


Figure 5.15.1G – Waiting for the reconnection of the nodes

5.17.2. Cluster System Restart

The ***Cluster System Restart*** feature can reboot all managed nodes in the cluster without changing any settings. This single action saves you the time of going to each node and rebooting them one by one.

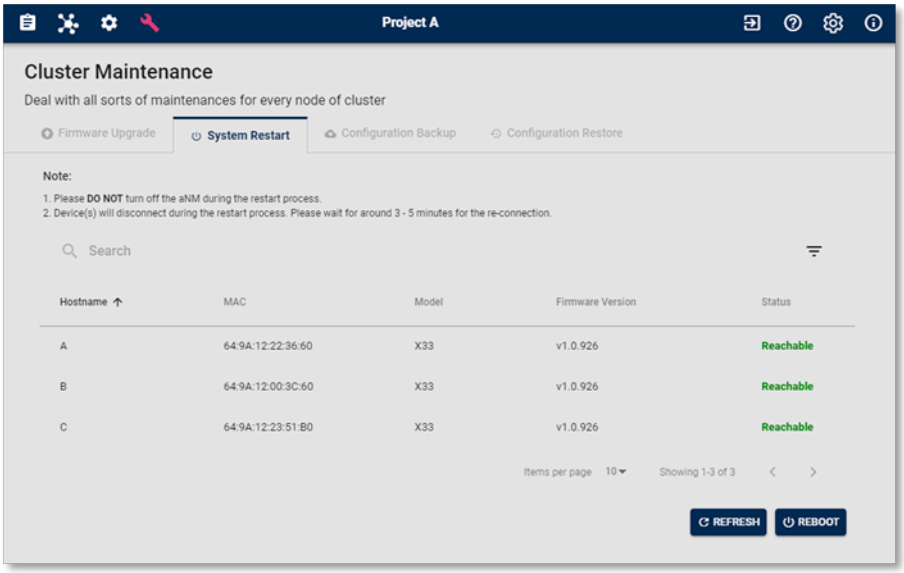


Figure 5.15.2A – ***Cluster System Restart*** user interface

To reboot a cluster

1) The status of all nodes on the managed device list will be shown in a table. Check if all nodes are reachable with hostname, model and version information shown properly. Resolve any unreachable nodes.

   Note: The reboot will only proceed when all managed devices are reachable.

2) Click **REBOOT** and wait for the reboot process to complete.
3) Go to **Cluster Topology** to review the connection status of the cluster.

5.17.3. Cluster Configuration Backup

The ***Cluster Configuration Backup*** feature helps to backup the configuration of all the managed nodes in the cluster using a single file. The backup file can be used to restore configuration using the ***Cluster Configuration Restore*** feature.

The backup file is encrypted. You cannot read or make changes to the file.

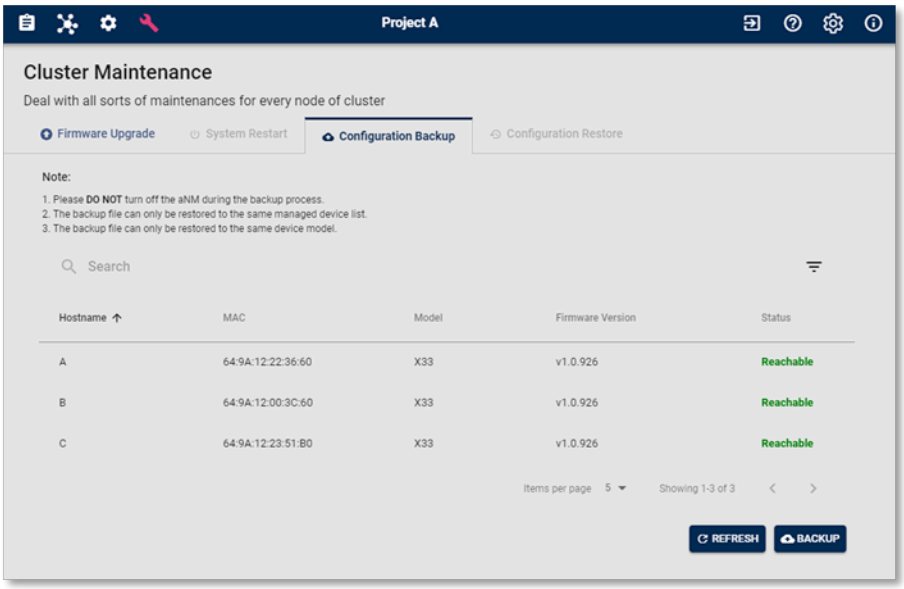


Figure 5.15.3A – ***Cluster Configuration Backup*** user interface

To backup a cluster

1) The status of all nodes on the managed device list will be shown in a table. Check if all nodes are reachable with hostname, model and version information shown properly. Resolve any unreachable nodes.
2) Click **BACKUP**.
3) You can find the backup file at Download or the selected location on your computer.

Figure 5.15.3B – The backup file

5.17.4. Cluster Configuration Restore

The ***Cluster Configuration Restore*** feature helps to apply the backup file to the cluster that has the same managed nodes with the same firmware version as the backup file.

As the file backup all the configuration of the whole cluster, you can choose to restore cluster-wide configuration only or restore all configuration, including node configuration.

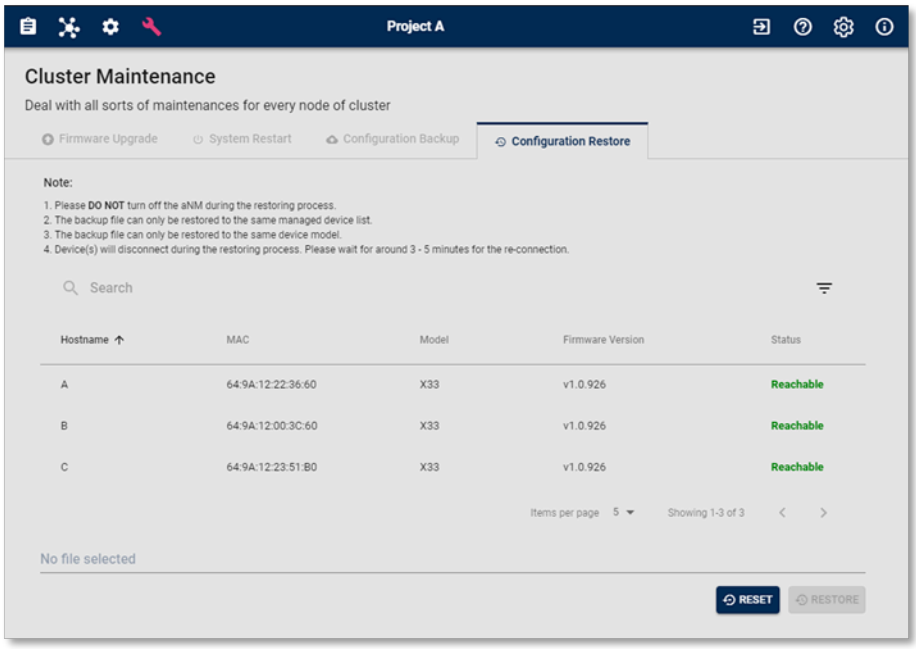


Figure 5.15.4A – ***Cluster Configuration Restore*** user interface

Warning! The backed-up configuration file can only be applied to the managed nodes from which they were copied, i.e. with the same MAC address.

To restore a cluster

1) Prepare a backup file of the cluster generated by ***Cluster Configuration Backup***.

Figure 5.15.4B – The backup file

2) Go to the A-NM. The status of all nodes on the managed device list will be shown in a table. Check if all nodes are reachable with hostname, model and version information shown properly. Resolve any unreachable nodes.

   Note: The restore will only proceed when all managed devices are reachable.

3) Click 

to upload the backup file.

4) Select the backup file.

Figure 5.15.4C – Upload the backup file

5) Click **RESTORE.**

   Note: Please make sure that all the managed nodes are reachable.

6) Select the appropriate option and click **PROCEED**.

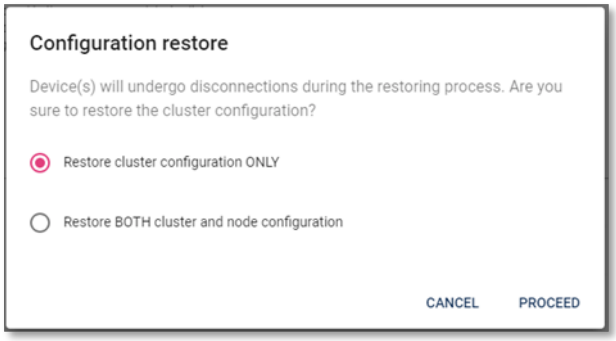


Figure 5.15.4D – Select the restore option

Warning! When the restore involves a country code change, all channel-related configurations will be lost. The user is required to read and acknowledge a disclaimer with the sign-in password to be able to proceed with the restore.

Warning! User is responsible to ensure the device(s) operations are in compliance with the local country regulations of radio channel and output power limitations, Dynamic Frequency Selection (DFS) and indoor/outdoor restrictions. Failing to do so may result in illegal operation and may cause harmful interference to other radio communications.

Note: You can click **CANCEL** if you do not want to change the country setting.

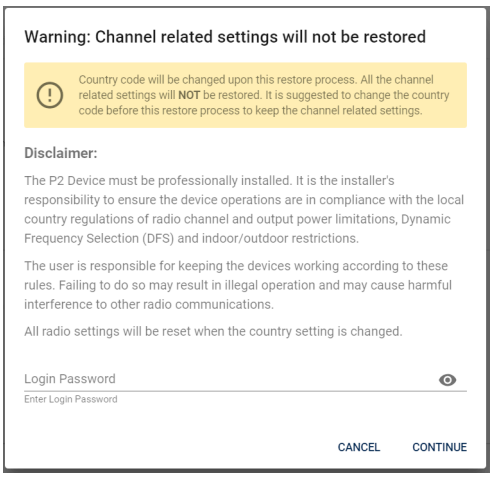


Figure 5.15.4E – Disclaimer for restore involves a country code change

7) Wait for the restore process to finish and click **RETURN TO CLUSTER TOPOLOGY.**

   Note: Device(s) will reboot after the process

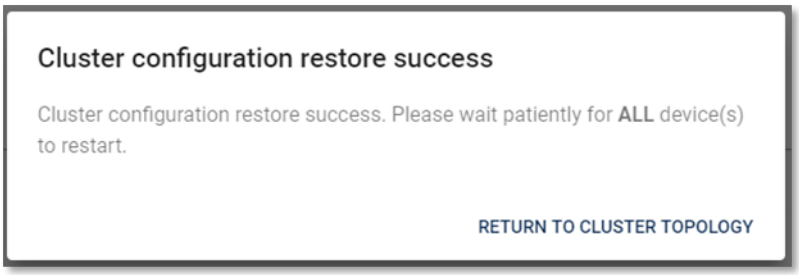


Figure 5.15.4F – Cluster configuration restore success

8) Move to ***Cluster Topology*** page and wait for the reconnection of nodes.

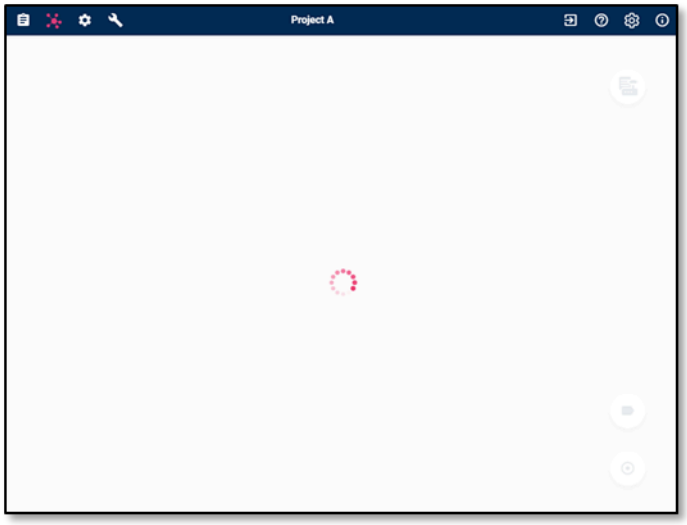


Figure 5.15.4G – Waiting for the reconnection of the nodes

6. Troubleshooting

6.1. A-NM Installation Issues

6.1.1. Computer already installed "Docker for Windows"

Make sure that you uninstall the "Docker for Windows" and disable the Hyper-V option if you have "Docker for Windows" installed on your computer.

1) Click the **Start** menu.
2) Enter **Control Panel** and select Control Panel from the results.

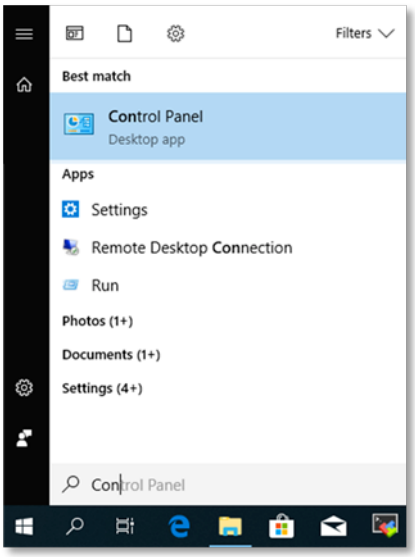


Figure 6.1.1A – Control Panel at Start Menu

3) Click **Programs**.

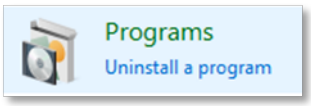


Figure 6.1.1B – Programs option at Control Panel

4) Click **Programs and Features**.

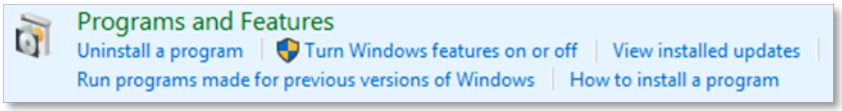


Figure 6.1.1C – Programs and Features at Programs option

5) Select **Docker for Windows** and click **Uninstall**.

6) Follow the instruction of the uninstall wizard.

7) Click the **Start** menu.

8) Enter **Control Panel** and select Control Panel from the results.

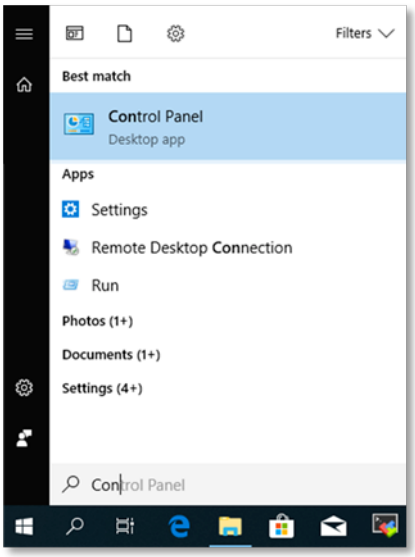


Figure 6.1.1D – Control Panel at Start Menu

9) Click **Programs**.

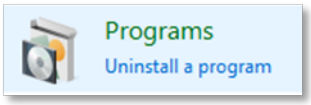


Figure 6.1.1E – Programs option at Control Panel

10) Click **Programs and Features**.

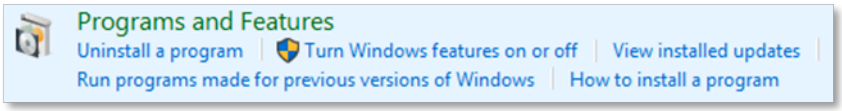


Figure 6.1.1F – Programs and Features at Programs option

11) Click **Turn Windows features on or off** at the left-hand menu.

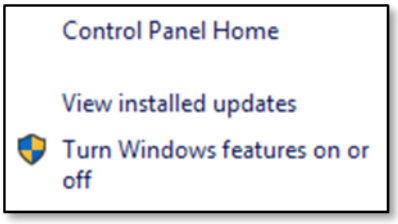


Figure 6.1.1G – Turn Windows features on or off

12) Uncheck **Hyper-V** and click **OK**.

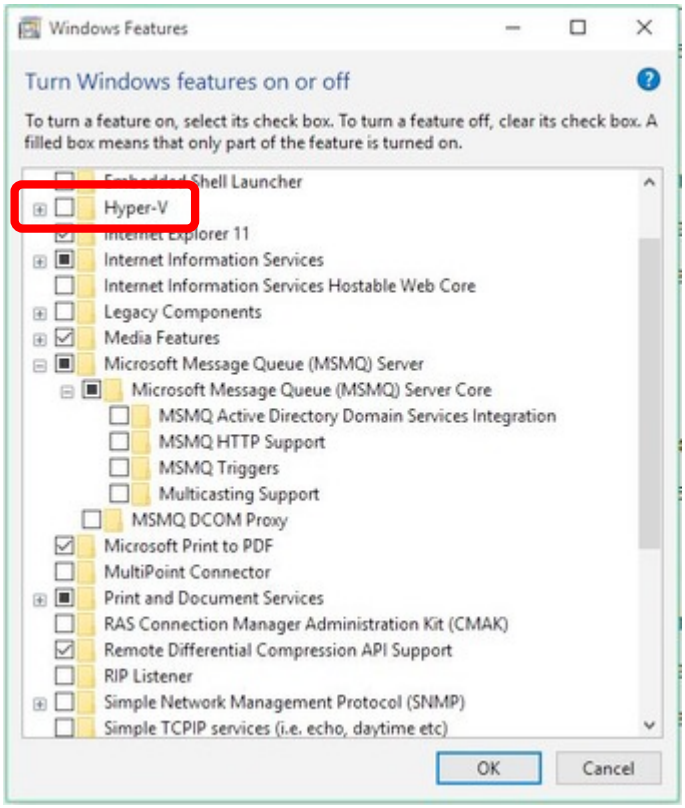


Figure 6.1.1H – Uncheck Hyper-V

13) Restart the computer.

14) Follow the instruction to **DockerToolBox (see page 12)** and **A-NM (see page 15)**.

6.2. System Issues

6.2.1. Forget the A-NM sign in password

You must uninstall the A-NM and install the Configuration again if you forget the sign in password.

1) **Uninstall the A-NM (see page 17)**
2) **Install the A-NM again (see page 15)**

6.2.2. Cannot access a project

- Please check the PWR, ETH0 and ETH1 LED of the host node are ON.
- Please make sure the port forwarding is enabled according to the **requirement (see page 11)**.
- Please make sure that the PC with the A-NM can access the IP address of Host Node through ping.
- If the PC cannot access the IP address of Host Node, please **check the PC and the nodes are at the same subnet (see page 19)**.

6.2.3. Configuration Restore failed

Cluster Configuration Restore

Configuration Restore fails when the system detects the mismatched managed device list at the project. Please make sure that the managed devices at the project are the same with the backup file as the A-NM will check the MAC address of all the managed device.

Node Configuration Restore

Configuration Restore fails when the system detects the mismatched model. Please check that the model and firmware version of the node must be the same with the backup file.

6.2.4. Recover an isolated network

An isolated network is where the remote nodes become unreachable. As in Figure 6.2.4B, A-NN-B and A-NN_C become isolated.

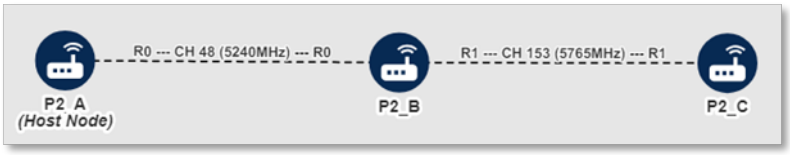


Figure 6.2.4A – Original Settings

Figure 6.2.4B – Isolated Network

Please refer to the following best practice for a step-by-step guide on how to recover an isolated network with the original network using the A-NM.

Please make sure that you have the network plan with all the setting of the nodes including Cluster ID, Management IP, Management Secret and the channels.

1) Use Ethernet Cable to directly connect the PC with A-NM to the isolated device (e.g. **A-NN_C**).

   Note: Make sure that the IP address of the **PC is in the same subnet with the connected device (see page 19)**.

2) Sign in the A-NM.
3) Click **Project Management (see page 31).**
4) Create a new project for that network.

   Note: Use the management IP of the isolated devices.

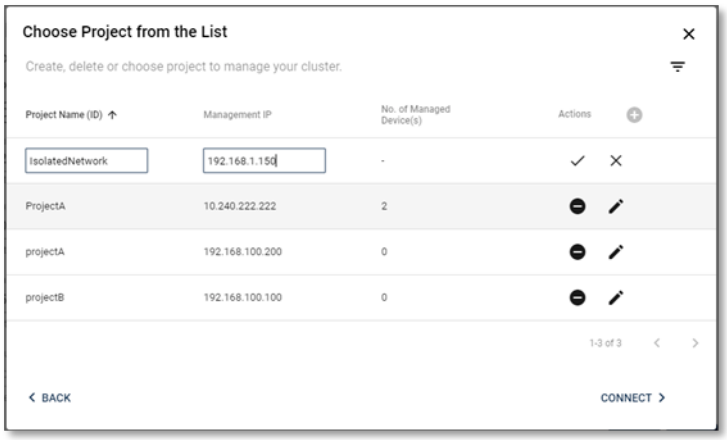


Figure 6.2.4D – Create project

5) Connect the project.
6) Add the node into **Managed Device List (see page 37)**.
7) Configure the **cluster-wide configuration (see page 76)** and **node configuration (see page 55)** of the nodes according to the network plan.
8) Wait for the reboot or reconnection of the nodes.
9) Switch the project to the original **project (see page 43)**.
10) Go to the Managed Device List and **add the new devices into the list (see page 37)**.
11) Repeat all the steps again if there are more than one isolated device.

6.2.5. Discover unknown devices at the project

If the A-NM discovers unknown devices and shows them at the Cluster Topology, you need to check if the devices are valid or not.

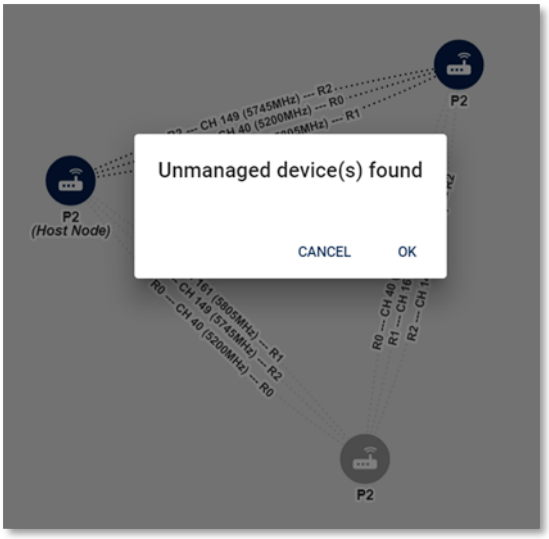


Figure 6.2.5A – Unknown unmanaged device found

1) Click **OK** to go to ***Managed Device List***.

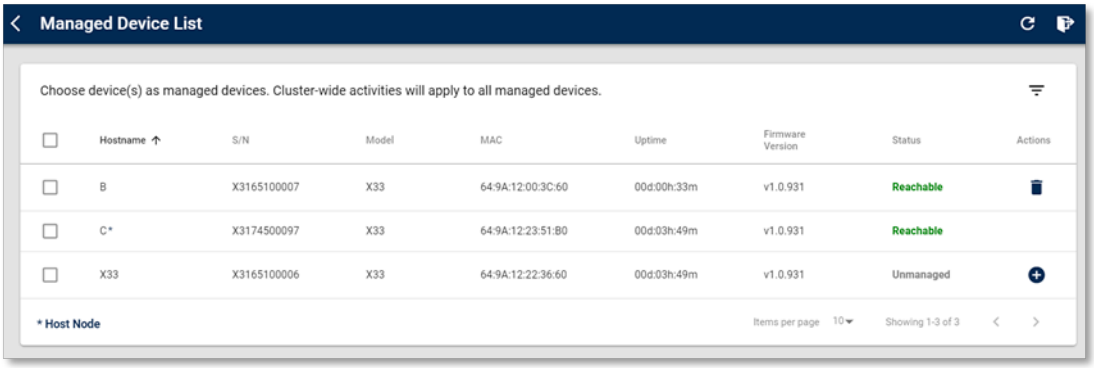


Figure 6.2.5B – Managed Device List

2) Verify the device list with the Serial Number / MAC.
   a. If it is your device, please add it into the managed device list.
   b. If it is not, please do not add it to the managed device list.

3) Click  to go the ***Cluster Configuration*** to check the settings of your cluster.

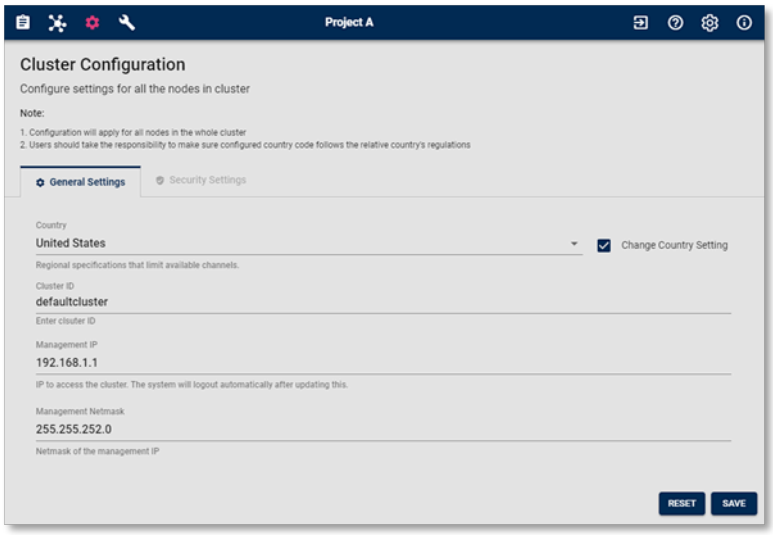


Figure 6.2.5C – Cluster Configuration

4) Change your own cluster-wide configuration to avoid using the default settings.
5) Click **SAVE** to apply the changes.

7. Appendix

7.1. Default Settings of A-OS Device

Cluster Configuration	
Country	United States
Cluster ID	defaultcluster
Management IP	192.168.1.1
Management Netmask	255.255.255.0
Wireless Encryption Key	defaultkey
Management Secret	password

Radios Configuration			
	Radio 0	**Radio 1**	**Radio 2**
Status	Enable	Enable	Disable
Radio Filter	Disable	Disable	Disable
Radio Channel	36	48	44
Channel Bandwidth	20MHz	20MHz	20MHz
Transmit Power	3	3	3
Distance	Auto	Auto	Auto

-End of User Guide-

Visit anywherenetworks.com to find out more about us.

Anywhere Networks