



Node Manager Guide

Contents

Contents	2
List of Tables	3
List of Figures	4
Preface	6
Document History	7
Definitions	8
1. Introduction	9
2. Versions	9
3. Opening Node Manager	10
4. Note: Restricted Backhaul Mode	12
5. Hub Configuration	13
6. Time Configuration.....	15
7. Beacon Configuration	15
8. Cellular.....	16
9. Wi-Fi Stats.....	17
10. Location	18
11. Power.....	18
12. Network Configuration.....	19
12.1. Network and Wireless LAN	19
12.2. IP Configuration.....	19
12.3. WLAN Configuration	20
12.4. Network Configuration – Scan (MEM Only).....	23
13. WAN Configuration	25
13.1. WAN Configuration Tab	25
13.2. WAN Interfaces Tab	26
13.3. WAN Static IP Tab	27
14. LAN Configuration	28
14.1. LAN Configuration	28
14.2. LAN DHCP Configuration	29
14.3. LAN Reserved IP.....	30
15. Wireless Access Point Configuration (2.4 GHz and 5 GHz)	31
15.1. Access Point Configuration (2.4 GHz and 5 GHz): Radio	31

15.2. Access Point Configuration (2.4 GHz and 5 GHz): Scan.....	34
15.3. Access Point Configuration (2.4 GHz and 5 GHz): SSIDs.....	35
15.4. Access Point Security Configuration (2.4GHz, and 5GHz)	37
16. Physical Port Configuration	41
17. Firewall Configuration	45
17.1. Adding an ACCEPT or DROP rule	45
17.2. Adding a FORWARD rule	46
18. LAN Configuration	48
18.1. Default Configuration	48
18.2. IP Conflict Resolution.....	49
18.3. DHCP Conflict	49
19. Troubleshooting	50
19.1. Configuration of VHE09 as MEN in Mixed 09/10 Configurations.....	50
20. Technical Support.....	52

List of Tables

Table 1: Hub Configuration.....	14
Table 2: Cellular Data	16
Table 3: Wi-Fi Stats Data	17
Table 4: Power Options.....	18
Table 5: Network Configuration First Tab	19
Table 6: IP Configuration.....	19
Table 7: Network Configuration – WLAN Tab	21
Table 8: Network Configuration: Scan Tab	23
Table 9: WAN Configuration	26
Table 10: WAN Interface Configuration.....	26
Table 11: WAN Static IP Configuration	27
Table 12: LAN Configuration	28
Table 13: DHCP Configuration.....	29
Table 14: Reserved IP Configuration.....	30
Table 15: AP Radio Configuration	32
Table 16: Access Points: Scan Tab.....	34
Table 17: AP SSIDs Configuration.....	35
Table 18: Security Configuration Description (2.4GHz, and 5GHz)	37
Table 19: PSK Security Configuration.....	38
Table 20: Enterprise Security Configuration	39
Table 21: RADIUS Configuration	40
Table 22: Physical Ports Configuration	43

Table 23: Firewall Rules Setup Options.....	46
---	----

List of Figures

Figure 1: Opening from Control Center	10
Figure 2: Opening from Enterprise Center.....	10
Figure 3: Node Manager Options (Hub).....	11
Figure 4: Node Manager Options (Network)	11
Figure 5: Restricted (Speedometer) badge	12
Figure 6: Hub Configuration Tab	13
Figure 7: Time Configuration Tab.....	15
Figure 8: Beacon Configuration Tab.....	15
Figure 9: Cellular Tab	16
Figure 10: Wi-Fi Stats Tab	17
Figure 11: Location Tab.....	18
Figure 12: Power Tab	18
Figure 13: Network Configuration Tab.....	19
Figure 14: IP Tab	19
Figure 15: WLAN Tab	21
Figure 16: Network Configuration: Scan Tab	23
Figure 17: WAN Configuration Tab	25
Figure 18: WAN Interfaces Tab	26
Figure 19: WAN Static IP Tab	27
Figure 20: LAN Configuration Tab	28
Figure 21: DHCP Configuration Tab.....	29
Figure 22: Reserved IP Configuration Tab.....	30
Figure 23: Access Points: Radio Configuration Tab.....	31
Figure 24: Access Points: Scan Tab	34
Figure 25: Access Points: SSIDs Configuration Tab	35
Figure 26: PSK Security Configuration.....	37
Figure 27: Enterprise Security Configuration	38
Figure 28: RADIUS Configuration	40
Figure 29: Physical Ports Configuration Tab	43
Figure 30: Input Firewall Rules Tab.....	45
Figure 31: Forward Firewall Rules Tab	46
Figure 32 – vMesh Screen (All Available Channels Whitelisted).....	51
Figure 33 – vMesh Screen (Channels 100 Plus Deselected from Whitelist).....	51
Figure 34 – vMesh Screen (Channels Below 100 Whitelisted).....	52

Preface

Information in this document is provided solely in connection with Veeva Inc. and its affiliates (collectively 'Veeva') products. Veeva reserves the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

Use of Veeva products and services is subject to the terms of use and/or separate agreements and warranties applicable to those products and services. Please [visit www.veea.com/legal](http://www.veea.com/legal) for these terms.

Evaluators (as defined in the Evaluation Agreement) are solely responsible for the choice, selection and use of the Veeva products and services described herein, and Veeva assumes no liability whatsoever relating to the choice, selection or use of the Veeva products and services described herein.

Trademark Credits

Veeva and all Veeva related trademarks are owned by Veeva Inc.

All other trademarks and tradenames are the property of their respective owners.

Copyright Information and Restrictions

Copyright © 2019-2021 Veeva Inc. All rights reserved.

Document Feedback

Veeva welcomes your suggestions for improving our documentation. If you have comments, send your feedback to: support@veeahub.com

Document History

Issue	Issue Date	Approved	Author	Description
1.0	2021-01-15		RB	First publication, taken from Enterprise Center Guide 1.5
1.1	2021-01-21		RB	Version 1.17.12: Multitenancy, Wi-Fi security
1.2	2021-03-10		RB	Version 1.18.9: Home, Settings, Port and SSID screens changed
1.3	2021-03-31		RB	Version 1.19.12: Client isolation, RADIUS, Port and SSID screens, WLAN changed
1.4	2021-04-26		RB	Version 1.20.4: IP Configuration moved into Network Configuration, Auto configuration for wired mesh
1.5	2021-05-28		RB	Version 1.21.14: 201.11r support, minor updates
1.6	2021-08-12		RJ	Version 1.23.1: Addition of wired mesh - wireless islands functionality and VHE09 (MEN) to VHE10 (MN) meshing channels configuration

Definitions

Term	Definition
AP (or WAP)	Wireless Access Point through which a wireless mobile device (such as a smartphone or tablet) connects to a Veeahub and to the wider network including the Internet.
Application	A program written for the Veeahub or a network of hubs.
Backhaul	The connection that a Veeahub network makes to the WAN or Internet Service Provider. Typically, an Ethernet connection, but could also be a wireless connection or a cellular connection to a mobile data provider. A different type of backhaul may be used as a backup in the case the main backhaul fails.
LAN	Local Area Network. The network on the local side of the router, including the Veeahub network. LAN can also refer to a subnet of the LAN that is configured to behave as if it is a separate LAN.
MEN	Mesh Edge Node, or gateway hub. A Veeahub that connects the Veeahub network to the WAN, and also has management functions in the network.
Mesh	A network of one or more Veeahubs, co-operating to host application services and provide additional functionality such as Wi-Fi internet access, cellular failback etc. 'Mesh' refers to the technology on which the network operates. Veeahub's proprietary mesh is called vMesh.
MN	Mesh Node, or network hub. A Veeahub in the mesh that does not have independent gateway connectivity but is capable of executing services deployed by the Enterprise Center and under control of the MEN.
Node	A Veeahub in a mesh, executing one or more services deployed by the Enterprise Center. A Mesh Edge Node (MEN) is the gateway hub that carries the backhaul and performs management functions in the mesh. The other hubs are Mesh Nodes (MN).
SSID	Wi-Fi Service Set Identifier. This is the identifier that is used to connect a wireless device to a Veeahub or network of Veeahubs. Typically, it is selected from the list of Available Networks on a mobile device.
Veeahub Cloud	The Veeahub Cloud is a collection of software and server functionality that is provided to enable deployment, authentication, and management of the vMesh and associated Veeahubs. Enterprise Center is the part of the cloud that gives users access to the management functions available to them.
WAN	Wide Area Network. The network on the far side of the router, which may be an enterprise network or an Internet Service Provider connecting to the Internet.

1. Introduction

This Guide is for users of Veeahub networks (meshes). It describes the use of Node Manager to manage and monitor Veeahub networks. It includes details of the screens and the controls on them.

Node Manager is a cloud-based management tool for managing Veeahub networks and individual Veeahubs. It is available through Control Center (for all users) and through Enterprise Center (for enterprise customers).

Node Manager (with some differences) provides most of the monitoring and configuration options in the Veeahub Manager app available on Apple and Android mobile devices.

Note: If you have services such as vTPN installed on your mesh, those may configure some of the options and they will not be configurable from Node Manager.

2. Versions

The Veeahub platform, including Node Manager, is undergoing continuous improvement, so version numbers and details may differ from those shown in this document. This document has been checked against the following versions:

MAS	2.16.0-2 Hotfix 21-July
Veeahub software	2.20.0
Node Manager	1.23.1

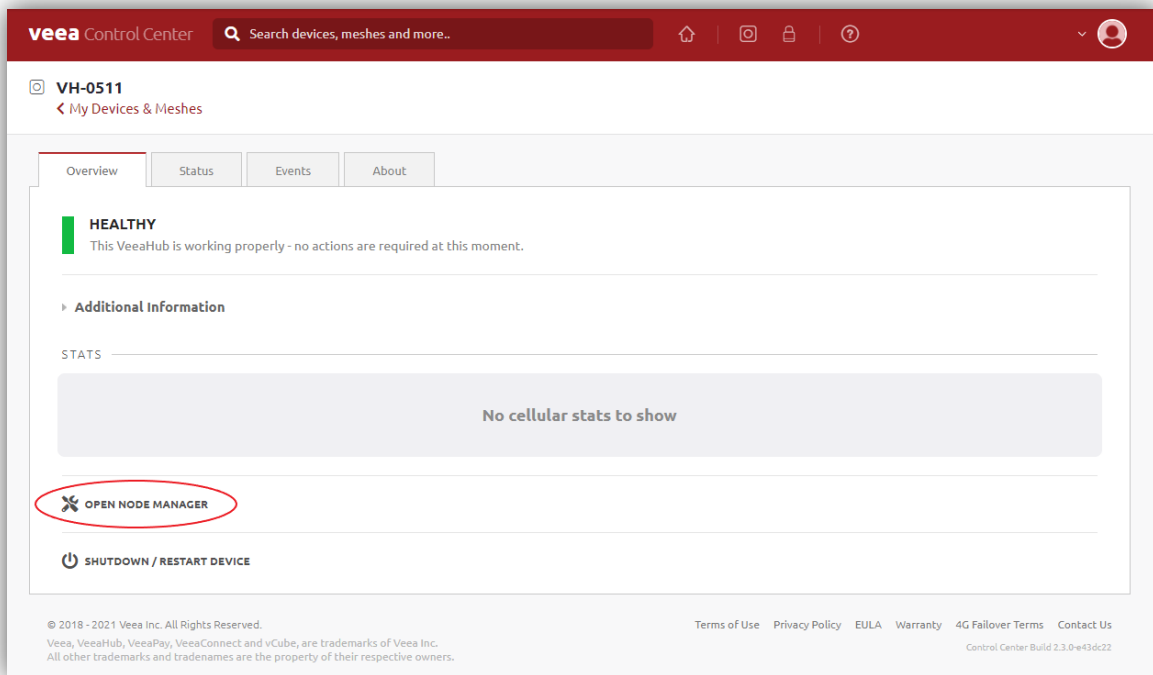
3. Opening Node Manager

Node Manager is a set of tabs for configuring a selected Veeahub. On the gateway hub (MEN), this can also be used to apply settings to the whole network.

Node Manager can be opened from either Control Center (Figure 1) or Enterprise Center (Figure 2).

In Control Center, go to the tab for the Veeahub you wish to configure, and click on **Open Node Manager**.

Figure 1: Opening from Control Center




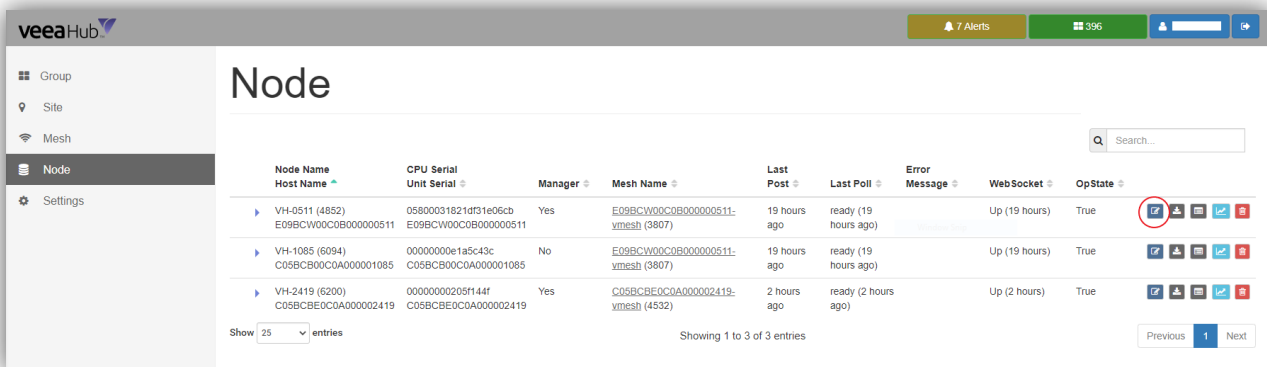
In Enterprise Center, on the Node page, on the line for the Veeahub you wish to configure, click the **Manage Node** icon .

Figure 2: Opening from Enterprise Center



By default, the Hub Configuration tab (section 4) is opened when Node Manager is opened. The tabs are grouped into two sets:

- **Hub:** Functions that apply only to individual Veeahubs
- **Network:** Functions that apply to a network of Veeahubs or can either apply network-wide, or to a single hub.

The available tabs and the controls on them vary, depending on which Veeahub model you are configuring and whether it is configured as the gateway hub or another hub in the network. The full set is shown in Figure 3 and Figure 4.

Figure 3: Node Manager Options (Hub)

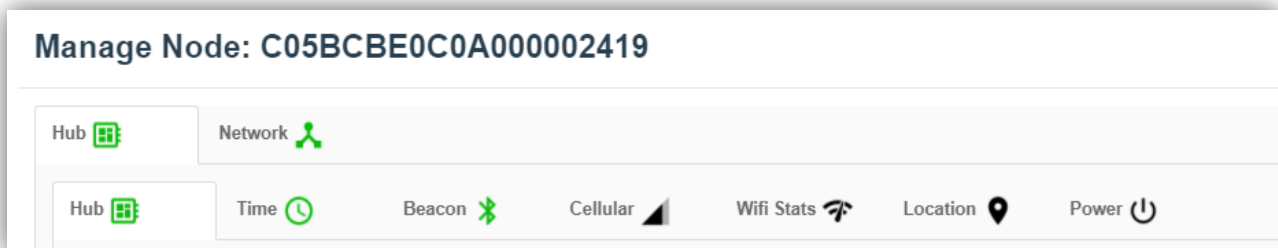
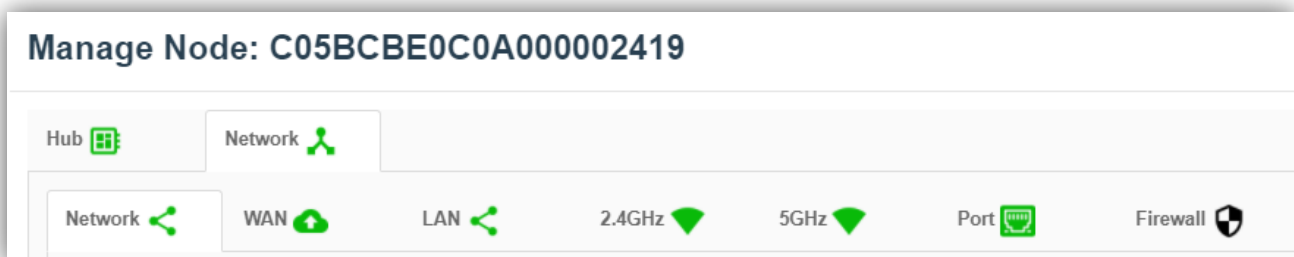


Figure 4: Node Manager Options (Network)



The colors of the icons on these tabs indicate the status of the function, **Green** for fully operational, **Amber** and **Red**. You can see the reason for the color by hovering the mouse pointer over the icon.

The color of the Hub or Network icon shows the 'worst' state of the icons on that tab.

On each tab, you can click **Apply** to make changes that you have entered in the Node Manager, or **Close** to close the tab without making any changes. These buttons close the Node Manager pop-up.

4. Note: Restricted Backhaul Mode

The user may apply a restricted data policy on the gateway node (MEN) to any or all supported backhaul interfaces (Ethernet, Wi-Fi or Cellular). When restricted backhaul is active, the MEN and Enterprise Center minimize the control data traffic on that interface. This is typically applied to a cellular backhaul to minimize the cellular data plan costs, but it may be applied to other backhaul types, for example, to the Ethernet backhaul if this traffic is subsequently routed through a cellular network.

A visual indication is given of restricted backhaul in the form of a 'speedometer' badge (Figure 5), against affected networks and their associated nodes. This is described in later sections where applicable.

Figure 5: Restricted (Speedometer) badge

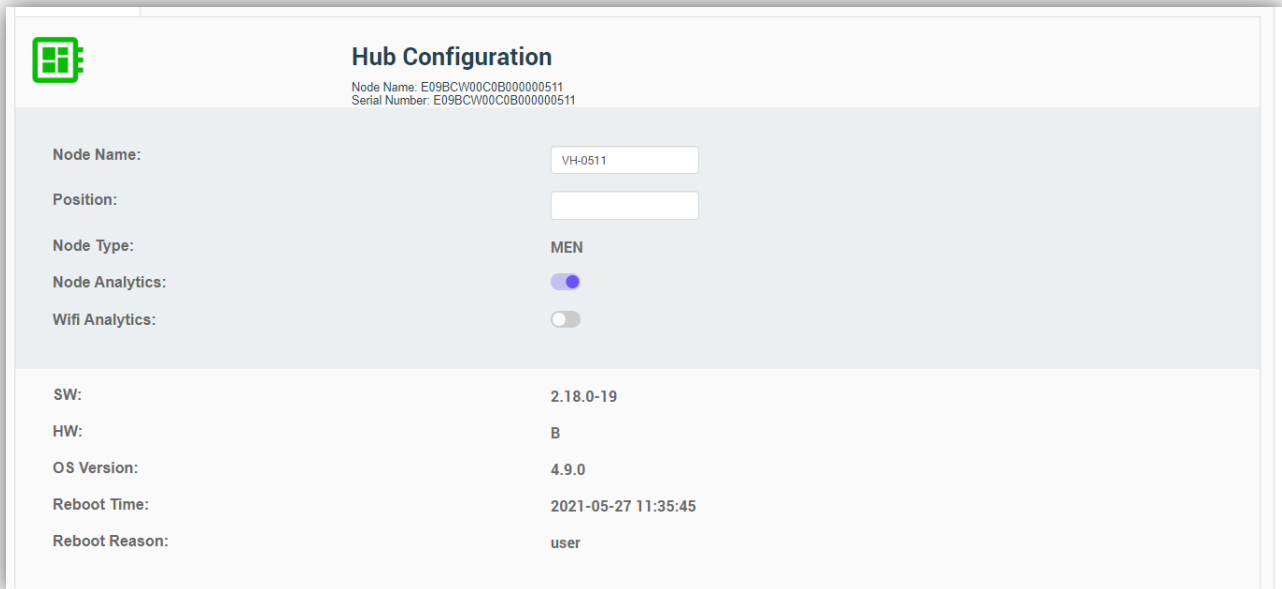


No logging files or analytics are sent from the gateway Veeahub (MEN) to Enterprise Center when the main backhaul is restricted, so available analytics is limited.

5. Hub Configuration

The information and configurations here apply only to the currently selected hub (Figure 6).

Figure 6: Hub Configuration Tab



Hub Configuration
Node Name: E09BCW00C0B000000511
Serial Number: E09BCW00C0B000000511

Node Name:	<input type="text" value="VH-0511"/>
Position:	<input type="text"/>
Node Type:	MEN
Node Analytics:	<input checked="" type="checkbox"/>
Wifi Analytics:	<input type="checkbox"/>
SW:	2.18.0-19
HW:	B
OS Version:	4.9.0
Reboot Time:	2021-05-27 11:35:45
Reboot Reason:	user

If the Hub icon is shown in red, the unit requires restarting (section 11).



The configurations here are shown in Table 1.

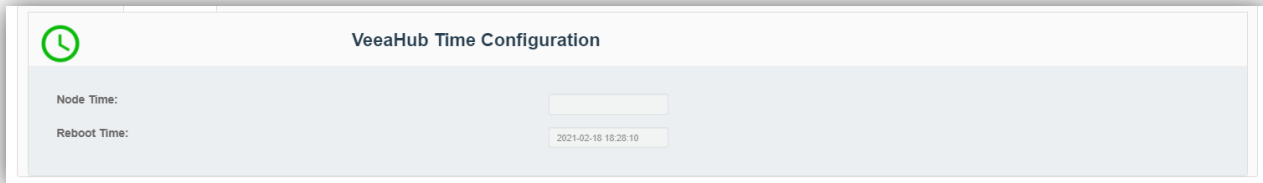
Table 1: Hub Configuration

Node Name	The Node Name is set when the Veeahub is added to your account. You can change it here.
Locale	Free text that can be used to give the location of the hub, for example, 'Back office' or 'Showroom'. It is not the country location (section 10).
Node Type	MEN or MN (for information only).
Node Analytics	Switch node analytics on and off for this node. See Enterprise Center Guide.
Wi-Fi Analytics	Switch Wi-Fi analytics on and off for this node. In particular, this enables Wi-Fi Access Point statistics per station, providing RSSI and connection time for every station (for example, smartphone) that is connected to a Veeahub Access Point. See Enterprise Center Guide.
SW	Software version (for information only).
HW	Hardware version (for information only).
OS Version	Operating system version (for information only).
Reboot time	Time unit was last rebooted (for information only).
Reboot reason	Cause of the reboot (for information only).

6. Time Configuration

This screen shows the time on the Veeahub and the last time it was rebooted (also shown on Node Configuration tab). This is for information only (Figure 7).

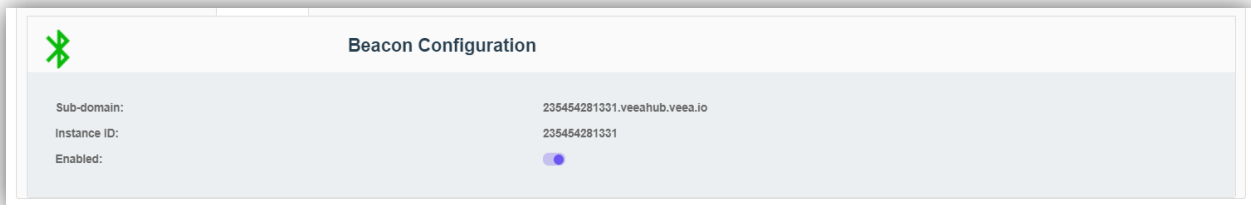
Figure 7: Time Configuration Tab



7. Beacon Configuration

A Veeahub advertises its presence through a Bluetooth beacon that broadcasts an advertisement consisting of a sub-domain and Instance ID. A client app uses the sub-domain and instance ID values. This is configured when you first add the hub to the Veeahub account, and is only for information here (Figure 8).

Figure 8: Beacon Configuration Tab



8. Cellular

The Cellular tab (Figure 9) is available only on a gateway Veeahub (MEN). It displays information about the current Cellular connection, where the 4G Failover package is installed. These fields are read-only.

The information shown is listed in Table 2.

Figure 9: Cellular Tab

Cellular	
PLMN:	23430
Cell ID:	4977152
Network Mode:	4G
IMEI:	866758045528060
IMSI:	206018818830815
Connect Time:	

Table 2: Cellular Data

PLMN	The Public Land Mobile Network identifier of the cellular operator.
Cell ID	ID of the cell served by the base station.
Network Mode	Cellular network mode, 3G or 4G.
IMEI	International Mobile Equipment Identity number.
IMSI	International Mobile Subscriber Identity.
Connect Time	The length of time this connection has been made.

9. Wi-Fi Stats

The Wi-Fi tab (Figure 10) is available only on a gateway Veeahub (MEN). It displays information about backhaul Wi-Fi quality (where installed) and mesh Wi-Fi quality. These fields (Table 3) are read-only.

Figure 10: Wi-Fi Stats Tab

The screenshot shows a web interface for 'WiFi Stats'. It features a Wi-Fi icon in the top left corner. Below the icon, there are four rows of data, each with a label and a corresponding input field:

- Backhaul Quality: [input field]
- Backhaul Signal: [input field]
- Vmesh Quality: [input field]
- Vmesh Signal: [input field]

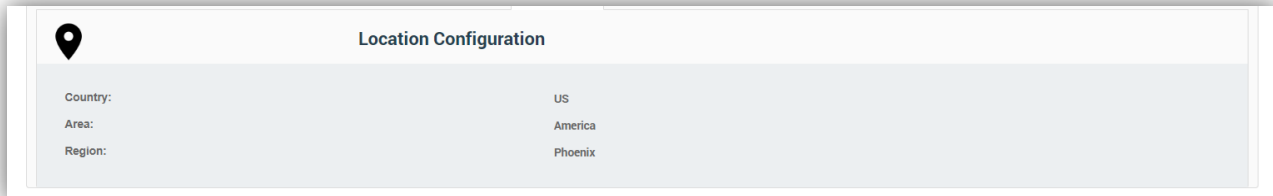
Table 3: Wi-Fi Stats Data

Backhaul Quality	Percentage based on the signal-to-noise ratio of the Wi-Fi interface used by the backhaul.
Backhaul Signal	Estimate of the signal level using the signal-to-noise ratio of the Wi-Fi interface used by the backhaul.
vMesh Quality	Percentage based on the signal-to-noise ratio of the Wi-Fi interface used by the mesh.
vMesh Signal	Estimate of the signal level using the signal-to-noise ratio of the Wi-Fi interface used by the backhaul.

10. Location

This tab displays the location information, which is set during when the hub is added to the Veea account and the software is installed. It cannot be changed. If you need to relocate the device to a different country, you must contact Veea Support to change it.

Figure 11: Location Tab



11. Power

This tab (Figure 12) offers controls for restarting, recovering, or powering off the node. The actions are listed in Table 4.

Figure 12: Power Tab

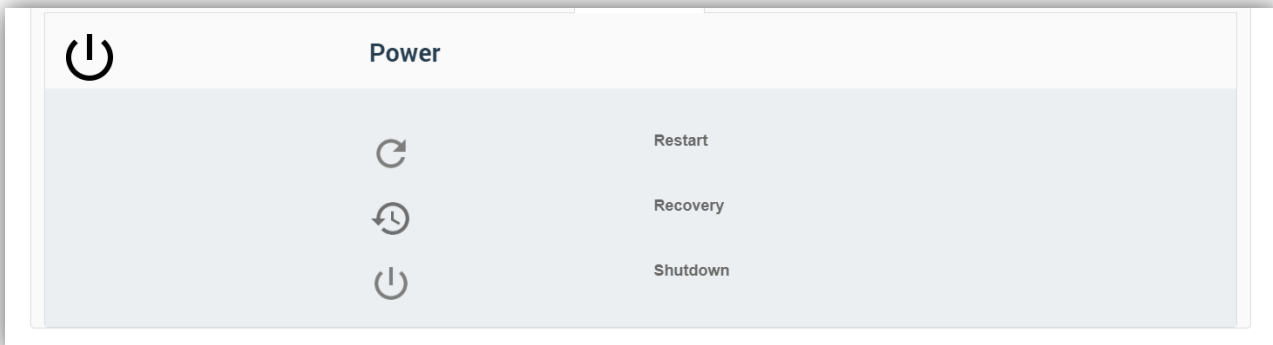


Table 4: Power Options

Restart	Restarts the Veeahub.
Recovery	<p>The Veeahub is restored by downloading software and configuration from the cloud.</p> <p>If a default backup (see Enterprise Center Guide) is configured, then the units are restored to match this configuration set. All units revert to the software versions and configuration settings at the time the backup was taken.</p> <p>If there is no default backup configured, all existing configuration information is wiped, and the Veeahub is restored to the current configuration held for this Veeahub on the Vee Cloud. Any local updates made since then are lost.</p>
Shutdown	Shuts down the Veeahub.

12. Network Configuration

12.1. Network and Wireless LAN

The information and configurations displayed in these tabs (Figure 13) apply to the network (mesh) to which the currently selected Veeahub belongs. The first tab is described in Table 5.

Figure 13: Network Configuration Tab

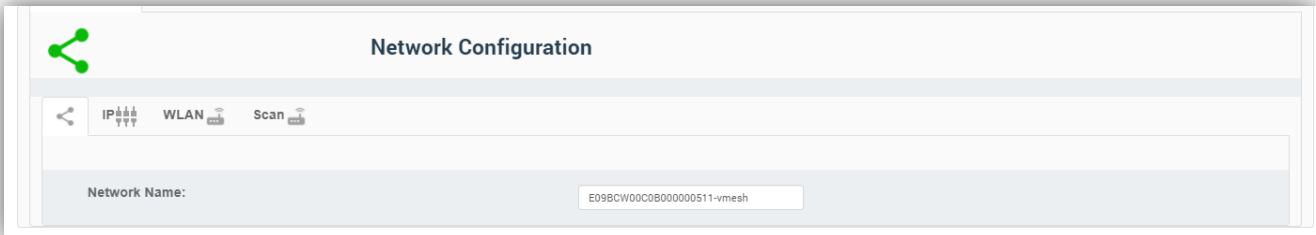


Table 5: Network Configuration First Tab

Network Name	The name of the network, usually assigned when the first Veeahub is added to the Veeah account and used to create the mesh. The name can be changed here.
---------------------	---

12.2. IP Configuration

The IP Configuration tab (Figure 14) is available only on a gateway Veeahub (MEN). The details are listed in Table 6.

Figure 14: IP Tab

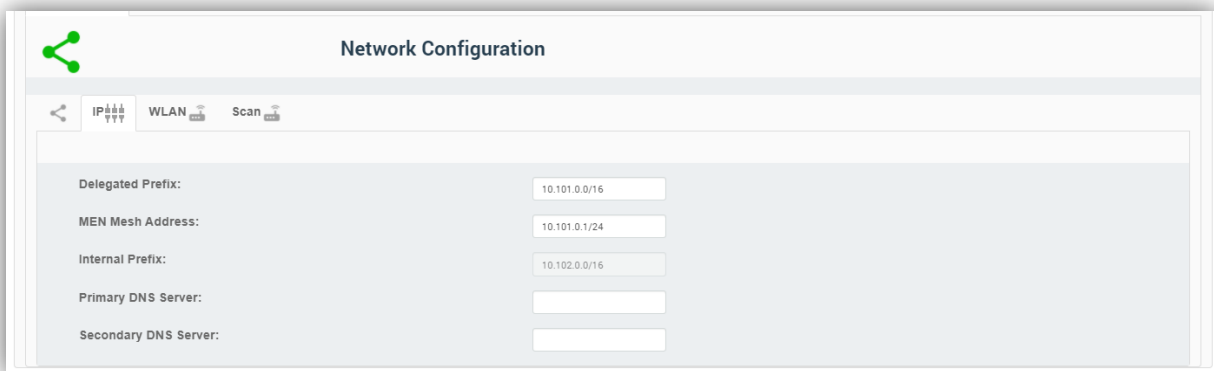


Table 6: IP Configuration

Delegated prefix	Used to assign IP addresses to Veeahub devices in the mesh. This is a private IP prefix space. You should not need to change this
-------------------------	---

	value, unless the backhaul interface also has the same prefix. Changing this field will cause the MEN to reboot.
MEN mesh address	Defines the IP address of the MEN on the mesh. This should be within the delegated prefix address range. Changing this field will cause the MEN to reboot.
Internal prefix	Used to assign IP addresses to stations connected to the Veeahub APs while the node is not connected to a mesh.
Primary DNS server	The backhaul network interface DNS will be propagated across the vMesh. If the backhaul network does not have DNS, this should be configured to point to an external DNS.
Secondary DNS server	The backhaul network interface DNS will be propagated across the vMesh. If the backhaul network does not have DNS, this should be configured to point to an external DNS.

12.3. WLAN Configuration

The configuration of the wireless LAN (mesh between Veeahubs) is covered here. The tab is shown in Figure 15 and the configuration options are listed in Table 7.

vMesh is Veeahub's proprietary technology that enables the Veeahubs in a network to work together. For further information, see the Veeahub Support Center.

By default, the mesh is established over 5GHz Wi-Fi. It is possible to reconfigure Veeahubs to connect over Ethernet by disabling the WLAN Mesh, and a Veeahub mesh can consist of wireless links, wired links or a mixture of the two.

The mesh name and default parameters are set up when the Veeahub is added to the account. You may wish to change the channel assignments and transmit power for improved operation in your particular circumstances (including location of units and usage of the mesh).

When Auto Selection is on, the Wi-Fi channel used for the mesh is automatically chosen for you, based on various measurements of the quality of the signal. These measurements can be seen on the **Scan** tab, which is only displayed when WLAN is enabled. You can override this selection by choosing a single channel from those available, and you can also restrict the selection of channels that Auto Select uses.

Auto Selection is currently available only on the VHE09 and VHE10 models.

Auto Select is not dynamic: once the channel has been selected, this applies until the Veeahub is restarted or a channel rescan is done.

Figure 15: WLAN Tab

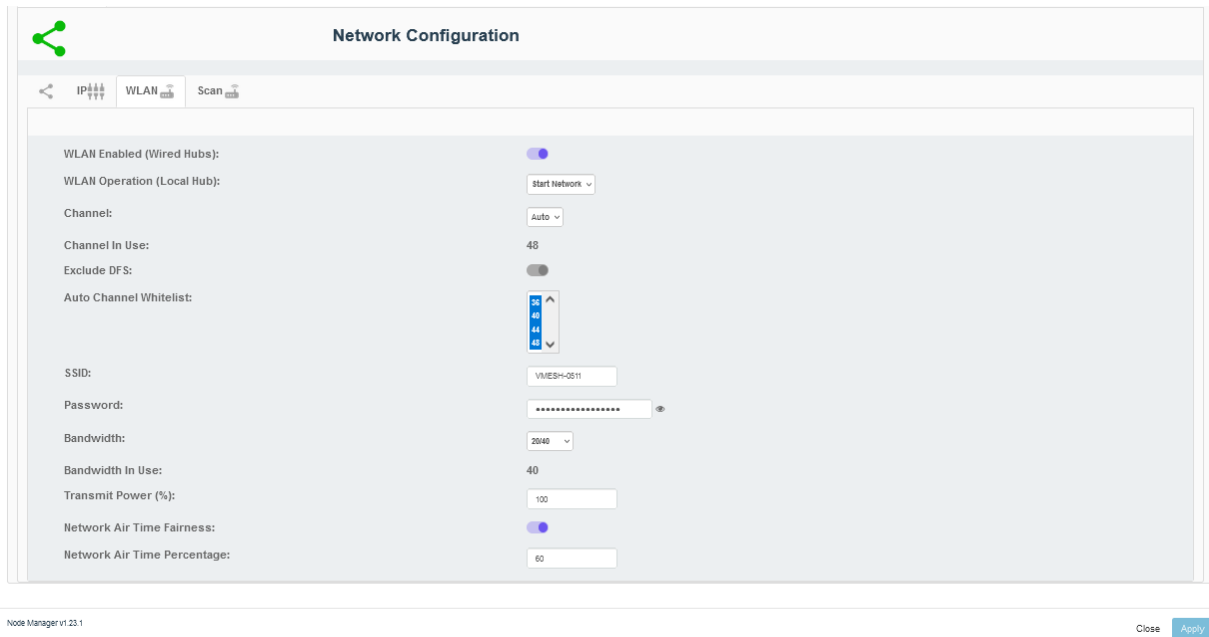
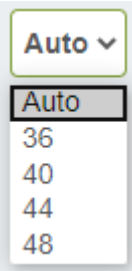
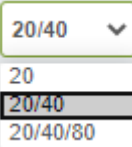


Table 7: Network Configuration – WLAN Tab

Name	Description
WLAN Enabled (Wired Hubs):⁽ⁱ⁾	<p>For a gateway Veeahub (MEN):</p> <p>In the on position, the wireless network operation is enabled for any connected wired hubs. This allows the network to extend wirelessly from these units.</p> <p>In the off position, the wireless networking is disabled on any directly wired, remote hubs that have WLAN Operation set to 'Automatic'. The network cannot be extended with wireless links from these units.</p> <p>For a non-gateway Veeahub (MN):</p> <p>This is a read-only setting that is configured at the gateway hub. In the on position, the wireless network operation is enabled according to the 'WLAN Operation (Local Hub)' setting. This allows the network to extend wirelessly from these units.</p> <p>In the off position, the wireless operation is disabled at this hub provided it has a direct wired link to the gateway hub and also that the 'WLAN Operation' setting is 'Automatic'. Otherwise, the normal 'WLAN Operation' setting behavior applies.</p>
WLAN Operation (Local Hub):⁽ⁱ⁾	<p>For a gateway Veeahub (MEN):</p> <ul style="list-style-type: none"> • With 'Start Network' selected, the hub supports wireless networking and will start a network identified by the SSID setting. Other hubs can connect to this unit wirelessly using the SSID and matching PSK. • With 'Disabled' selected, the wireless networking is disabled, and the network cannot be extended with wireless links from this hub. <p>For a non-gateway Veeahub (MN):</p> <ul style="list-style-type: none"> • With 'Disabled' selected, the wireless networking is disabled, and the network cannot be extended with wireless links from this hub. • With 'Automatic' selected, the behavior depends on whether this unit has a direct wired connection to the gateway hub, and the setting of

Name	Description
	<p>'WLAN Enabled (Wired Hubs)'. If there is no direct wired connection then this unit joins an existing wireless network, similar to the 'Join Network' setting. If there is a direct wired connection and 'WLAN Enabled (Wired Hubs)' is off, then wireless networking is disabled on this unit, similar to the 'Disabled' setting. If there is a direct wired connection and 'WLAN Enabled (Wired Hubs)' is on, then the unit first attempts to join an existing network and, if this is unsuccessful, it starts a new wireless network.</p> <ul style="list-style-type: none"> • With 'Join Network' selected, the hub will join an existing wireless network identified by the SSID and provided the PSK matches. The hub must be in range of the existing wireless network. • With 'Start Network' selected, the hub will start a wireless network using the SSID setting. Other wireless hubs can then connect to this. Note that if two hubs are in proximity and both start a network with the same SSID, then the networks are independent.
Channel:	<p>This dropdown enables selection of the Wi-Fi channel for the wireless mesh. The set of available channels is restricted, based on the configured Veeahub location.</p> <p>By default, Auto Selection is displayed. Several criteria are used to choose the best channel at the time the mesh starts up. If you prefer to override this and select one of the available channels, choose the channel number from the drop-down list.</p> 
Channel in Use:	The channel chosen by Auto Selection.
Exclude DFS:	This switch, when selected, prevents channels that are designated for Dynamic Frequency Selection being used for Auto Selection.
Auto Channel Whitelist:	This dropdown enables you to specify which channels Auto Select can use.
SSID:	The SSID used for the network WLAN. 1 to 32 characters.
Password:	<p>The password for the network WLAN. 8 to 63 characters (letters, digits or symbols).</p> <p>Tap the eye icon to reveal the password.</p>
Bandwidth:	<p>A dropdown to select the bandwidth for the network WLAN.</p> 
Bandwidth in Use:	This shows the currently selected bandwidth.
Enable Beacon:	Not available on a gateway Veeahub. This is used on a non-gateway node to create a new Wi-Fi mesh using the SSID above. In normal use this should be OFF at all nodes.

Name	Description
Transmit Power (%):	Enter the transmission power for the mesh Wi-Fi, as a percentage of full power.
Network Air Time Fairness:	This option is available only on the VHE09 Veeahub, where the mesh and the wireless access points share a single 5GHz radio. Use this switch to enable the 'Network Air Time' percentage option.
Network Air Time Percentage:	This option changes the proportion of the time on the 5GHz radio used by the mesh. In certain circumstances, increasing this proportion may improve performance of the mesh. The default is 60%.
<p>Note.</p> <p>⁽ⁱ⁾These settings support deployment of a mixed wireless and wired network, for example adding a wireless extension to a wired network. The default settings cover most configurations when first deploying a network, and once deployed, the default settings can be updated to match the network topology more precisely. For more information visit the Veeva Support site at: https://www.veea.com/support</p>	

12.4. Network Configuration – Scan (MEM Only)

This tab (Figure 16), when displayed, shows the measurements for each channel on which the Auto Channel selection is based. It also shows the date and time these measurements were made. An example result is shown here.

Figure 16: Network Configuration: Scan Tab

Channel	Number of BSS Detected	Minimum/Maximum RSSI for BSS	Noise Floor/dBm	Load	Rank
36	5	-80/-40	-110	5	2
44	1	-53/-53	-109	1	1
40	0	-95/-95	-110	1	3
48	0	-95/-95	-108	1	4

The measurements are listed in Table 8.

Table 8: Network Configuration: Scan Tab

Channel	The channel number.
#BSS	The number of basic service sets (BSS) detected on this channel.
Minimum/Maximum RSSI for BSS	The minimum and maximum Received Signal Strength Indicator for the BSSs on this channel.
Noise Floor / dBm	The noise floor on this channel.

Load	A measure of the time the channel is occupied.
Rank	A number calculated from the measurements. The highest-ranking channel is auto selected.

These measurements are combined to select a best channel for the Auto Channel selection. If a channel is ranked as 0, it is not considered suitable for auto selection. If all the channels show poor results, then moving the Veeahub to another position should be considered.

You can rescan the measurements by clicking **Rescan**. This may change the channel used.

13. WAN Configuration

The WAN tab is available only on a gateway Veeahub (MEN). There are three subsidiary tabs: WAN Configuration (section 13.1), WAN Interfaces (section 13.2) and WAN Static IP (section 13.3).

13.1. WAN Configuration Tab

This tab is shown in Figure 17. It is used for configuring the connections of the Veeahub network to the mesh.

Any or all of the backhaul types can be enabled or disabled, if installed on the network. On the WAN configuration screen, you can place the available connections in order, so that if one connection fails, the Veeahub will fail over to a different connection. The operational status of each backhaul type is shown.

The Backhaul icons can be dragged up and down to change the order of priority. The top icon represents the primary backhaul, and failover occurs to the next one. The configuration options here are listed in Table 9.

Figure 17: WAN Configuration Tab

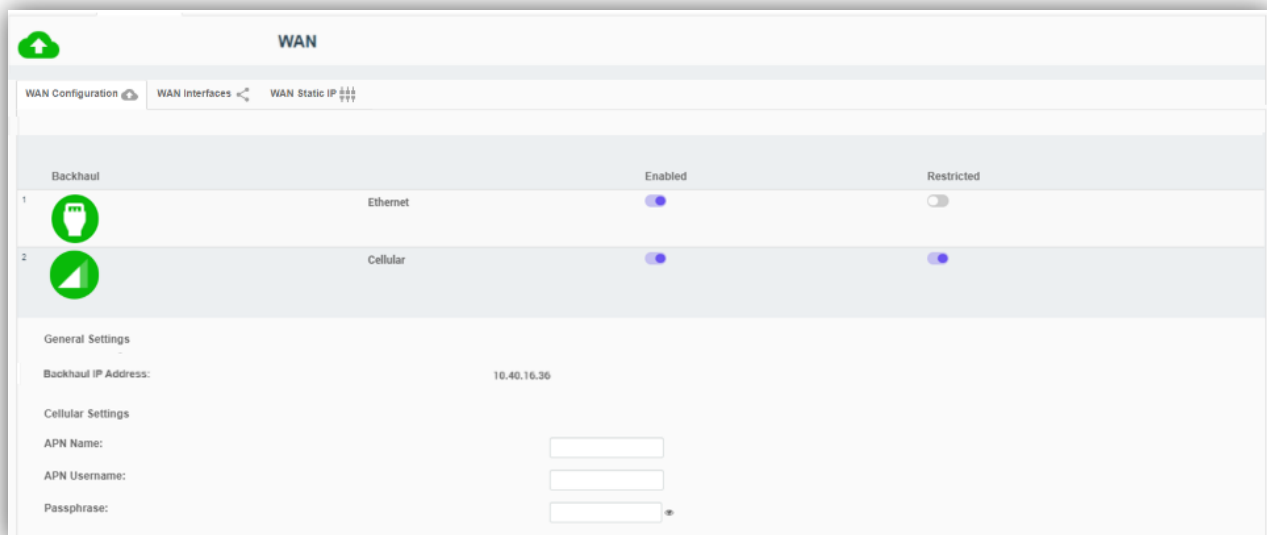


Table 9: WAN Configuration

Enabled	Enables the backhaul specified by the icon.
Restricted	Restricts data on this backhaul (see section 4).
General Settings	
Backhaul IP Address	The external IP address on the gateway hub.
Cellular Settings	
APN Name	Enter the Access Point Name (APN) for the cellular connection.
APN Username	Enter the Access Point username.
Passphrase	Enter the Access Point passphrase (use the eye icon to reveal it).

13.2. WAN Interfaces Tab

This tab (Figure 18) enables configuration of up to four WAN interfaces for up to four separate LANs configured on the LAN tab. The configuration options here are listed in Table 10.

You should configure this screen to match the LAN settings (section 14.1). If your Veeahub network is connected to an enterprise network, the necessary settings, including vLAN tags where relevant, should be obtained from your enterprise WAN administrator.

Figure 18: WAN Interfaces Tab

WAN Id	Use	Name	Port	VLAN Tag
1	<input checked="" type="checkbox"/>	default	Port 2	0
2	<input type="checkbox"/>			0
3	<input type="checkbox"/>			0
4	<input type="checkbox"/>			0

Table 10: WAN Interface Configuration

WAN ID	Number of the WAN to be configured
Use	Use this WAN interface on the network.
Name	Text to identify this WAN interface.
Port	Select the port on the gateway Veeahub (MEN) used for this WAN interface.

VLAN Tag	Specifies a VLAN tag to associate with this WAN interface, in connection with a VLAN on the WAN. A tag of 0 (zero) means no VLAN tag. Consult the administrator of your enterprise WAN if necessary.
-----------------	--

13.3. WAN Static IP Tab

This tab (Figure 19) is used to configure a static IP address for the gateway Veeahub (MEN) on the WAN. This is usually necessary only when the WAN does not have a DHCP server.

The configuration options are listed in Table 11.

Figure 19: WAN Static IP Tab

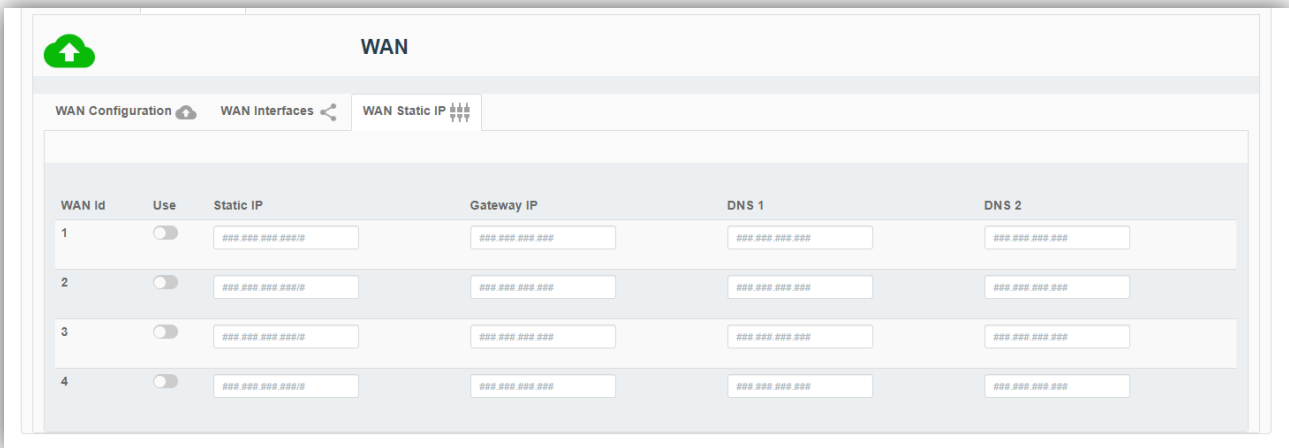


Table 11: WAN Static IP Configuration

WAN ID	You can set static IP addresses for any of the WAN interfaces you have defined.
Use	Set this gateway Veeahub (MEN) as a static IP on the WAN.
Static IP	Set the static address and subnet mask in CIDR format (###.###.###.##/#)
Gateway	Set the Gateway IP address.
DNS 1, DNS 2	Assign DNS nameservers.

14. LAN Configuration

This tab, with three sub-tabs, is available only on the gateway Veeahub (MEN).

14.1. LAN Configuration

These settings are used to configure up to four LANs on the Veeahub mesh (Figure 20). You must associate these subnets with the WAN interfaces (section 13.2), the APs configured in section 15 and the Ethernet ports (section 16). You should ensure that for each active AP (1-4) on the AP configuration tabs there is a corresponding check mark for that 2.4GHz or 5GHz AP on this tab.

The configuration options here are listed in Table 12.

Figure 20: LAN Configuration Tab

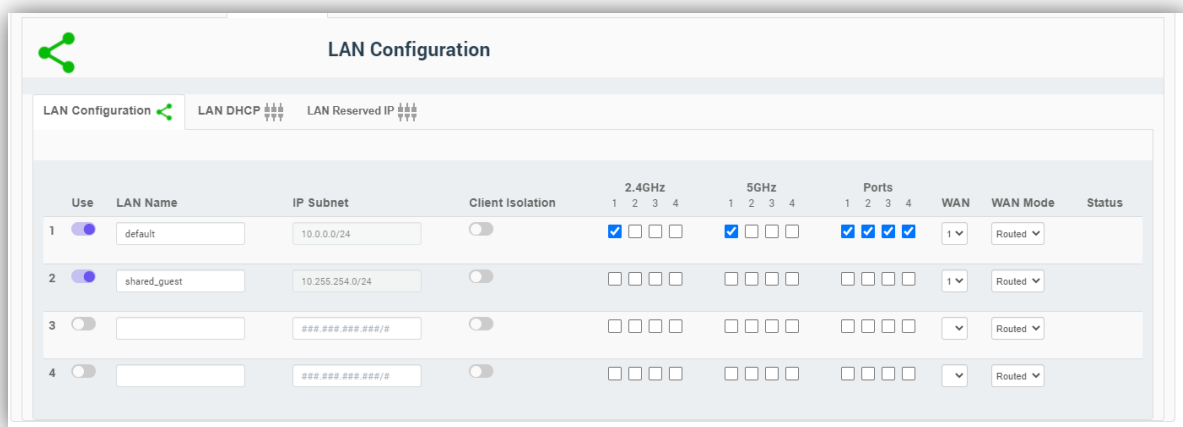


Table 12: LAN Configuration

1, 2, 3...	Number of the LAN to be configured
Use	Select this to use the LAN interface in this configuration
LAN Name	Text to identify the LAN.
IP Subnet	Specify the allowable IP addresses for this subnet, using CIDR notation. For example, 192.168.100.0/24
Client Isolation	If this switch is set to ON, devices on this LAN cannot see each other.
Status	Status message.
2.4GHz APs 1-4	Connect the LAN to a 2.4 GHz virtual AP.
5GHz APs 1-4	Connect the LAN to a 5GHz virtual AP.
Ports	Connect the LAN to one or more physical port.
WAN #	Connect the LAN to a WAN interface. More than one LAN can be connected to a WAN.
WAN Mode	Specify whether this subnet is routed or bridged to the LAN.
Status	Status message

On the VHC05, the 5GHz column will appear only if the wireless mesh is turned off and the 5GHz radio is available for access point use.

14.2. LAN DHCP Configuration

This tab (Figure 21) enables you to configure a DHCP server for each LAN (section 14.1) and also DNS servers. The configuration options are listed in Table 13.

Figure 21: DHCP Configuration Tab

Lease Time (mins)	DNS 1	DNS 2	Start IP	End IP	#IPs/#IPs in subnet	Subnet
1 60	8.8.8.8	8.8.8.8	10.100.1.0	10.100.1.254	-/254	10.100.1.0/24
2 0	8.8.8.8	8.8.8.8			-/-	
3 0	8.8.8.8	8.8.8.8			-/-	
4 0	8.8.8.8	8.8.8.8			-/-	

Table 13: DHCP Configuration

LAN #	The number of the LAN for which the DHCP is being configured.
Lease Time	The Lease Time: in the range 60 to 260000 or empty.
DNS 1	The primary nameserver, for example, 8.8.8.8 for Google.
DNS 2	The secondary nameserver, for example, 8.8.4.4 for Google.
Start IP	The start IP of the range for this LAN. This is automatically set as the first available IP address in the subnet, but can be changed. Its value must be in the subnet and before or the same as the End IP. The first and last IP address in the subnet are not available because they are used as the network prefix and broadcast addresses respectively.
End IP	The end IP of the range for this LAN. This is automatically set as the last available IP address in the subnet, but can be changed. Its value must be in the subnet and after or the same as the Start IP. The first and last IP address in the subnet are not available because they are used as the network prefix and broadcast addresses respectively.
#IPs/#IPs in subnet	This calculates automatically the number of IP addresses in the start/end IP range compared with all available ones in the subnet.
Subnet Mask	Automatically populated using the subnet defined in section 14.1.

14.3. LAN Reserved IP

Individual devices on wireless APs or LAN ports can be assigned Reserved IP addresses using the options here (Figure 22 and Table 14).

There is one tab for each of the LANs. By scrolling down, you can add up to 10 Reserved IP addresses on each LAN.

This option is available only on the gateway Veeahub (MEN). The setting is disabled if it is managed on the WAN, for example, if the LAN is bridged to the WAN, or if it is managed by an installed service such as vTPN.

To add an IP definition, click **Add Reserved IP** on the relevant LAN tab. To remove an IP that has been configured, click **Remove** against it. You can reserve the IP address for the device using either the device name (if known) or the MAC address. You can also enter a free text comment for information.

When you make changes here, you need to restart the hub for the changes to take effect.

Figure 22: Reserved IP Configuration Tab

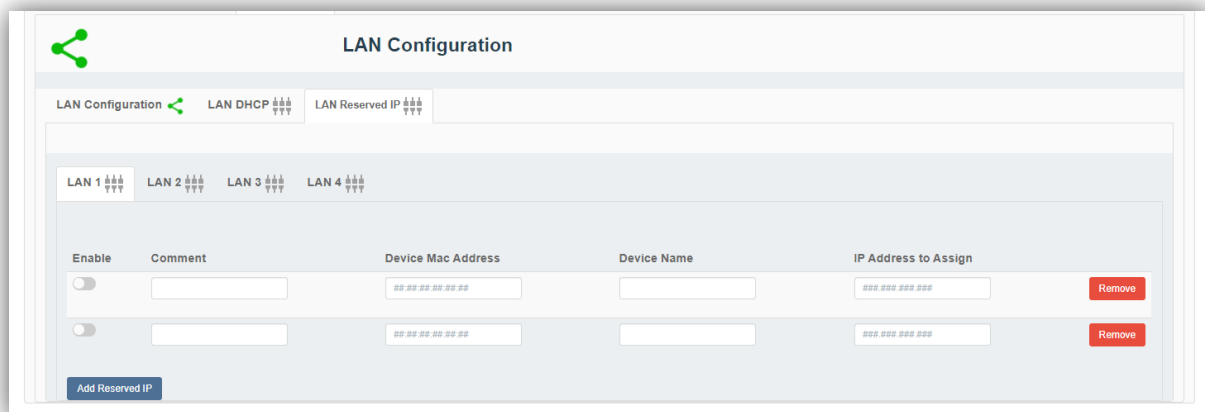


Table 14: Reserved IP Configuration

Enable	The reserved IP can be enabled or disabled on the selected LAN.
Comment	A text field to record information about this reserved IP.
Host MAC address	Specify the MAC address of the device you wish to assign the IP to. This is an alternative to specifying the Device Name.
Device Name	Specify the name of the device you wish to assign the IP address to. This is an alternative to specifying the MAC address. How to find the device name depends on the type of the device.
IP Address to Assign	Enter the IP address to assign to this device on this LAN.

15. Wireless Access Point Configuration (2.4 GHz and 5 GHz)

15.1. Access Point Configuration (2.4 GHz and 5 GHz): Radio

There are corresponding tabs for the 2.4 GHz and 5 GHz bands (Figure 23). The controls are similar on the two tabs. The VHC05 model does not have the 5 GHz tab unless the wireless mesh WLAN has been disabled (section 12). The configuration options on these tabs are listed in Table 15.

Use this tab to set radio configuration options for the APs.

The available channels depend on the country where the Veeahub has been registered, because local regulations vary.

When Auto Selection is on, the AP channel is automatically chosen for you, based on various measurements of the quality of the signal. These measurements can be seen using the **Wi-Fi Network Scan** option. You can override this selection by choosing a single channel from those available, and you can also restrict the selection of channels that Auto Select uses.

Auto Select is not dynamic: once the channel has been selected, this applies until the Veeahub is restarted or until you choose a different channel.

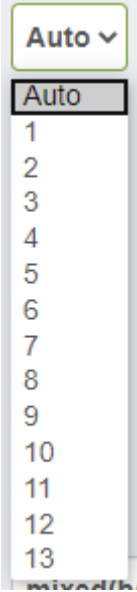
Auto Select is not available in certain circumstances, for example, on the VHC09 the 5 GHz radio is shared by the APs and the wireless mesh, and the frequency channel is selected by the option on the Network tab (section 12).

Figure 23: Access Points: Radio Configuration Tab

The screenshot displays the '2.4GHz Configuration' interface. At the top, there is a green Wi-Fi icon and the title '2.4GHz Configuration'. Below the title, there are fields for 'Node Name:' and 'Locale:'. The main configuration area is divided into three tabs: 'Radio' (selected), 'Scan', and 'SSIDs'. The 'Radio' tab contains the following settings:

- Channel:** Auto (dropdown menu)
- Channel In Use:** 11
- Auto Channel Whitelist:** 1-11 (range selector)
- Bandwidth:** 20 (dropdown menu)
- Bandwidth In Use:** 20
- Mode:** mixed(big/niac) (dropdown menu)
- Max Stations:** 128 (text input)
- Max Inactivity (in seconds):** 300 (text input)
- Transmit Power:** 100 (text input)

Table 15: AP Radio Configuration

Channel	<p>This is used by all four APs. By default, Auto Selection is displayed. Wi-Fi uses several criteria to choose the best channel at the time the APs start up. If you prefer to override this and select one of the available channels, choose the channel number from the drop-down list.</p> 
Channel in Use	Displays the actual channel in use, whether auto selected or selected manually.
Auto Channel Whitelist	This enables you to select the channels from which the auto selection occurs. Hold down the Ctrl key and select the channels you want Auto Channel Select from. Or hold down the shift key and select a range of channels from the list.
Bandwidth	<p>This sets the channel selection spread. Dropdown menu options include:</p> <ul style="list-style-type: none"> • 20MHz • 20MHz/40MHz • 20MHz/40MHz/80MHz. <p>If you are selecting this when ACS is active, ensure that the bonded channels are included in the Auto Channel Whitelist.</p>
Bandwidth in Use	This displays the channel bandwidth currently in effect.
Mode	Specify the 802.11 standards allowed for mobile devices to connect.
Max Stations	The maximum number of stations (such as mobile devices) that can connect to the AP (up to 225).
Max Inactivity (in seconds)	The time out before a station is disconnected for inactivity (30 to 600).
Transmit Power	Set the transmission power on the APs (0 to 100).

Certain options are not shown if the APs and the mesh share the same radio, as is the case for the 5GHz band on VHE09. These are:

Channel

Channel in Use

Auto Channel Whitelist

Bandwidth

Bandwidth in Use

Transmit Power

An on/off slider control **Access Band Lower** is shown for the VHE10 only. This sets the AP channel to be in the lower range of the 5GHz band.

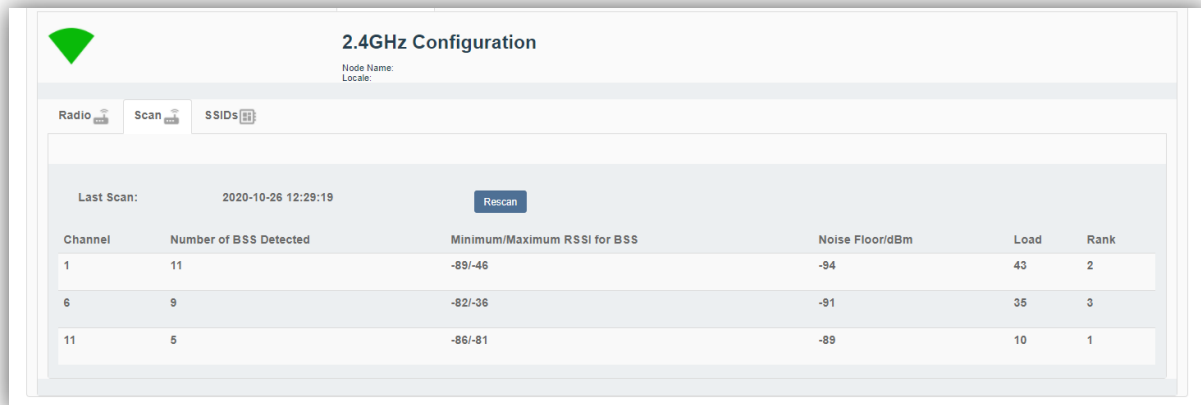
For Veeahubs registered in the UK: UK regulations were changed in August 2017 to allow Wi-Fi usage on channels 144, 149, 153, 157, 161 and 165. Older mobile devices supplied in the UK may not be able to connect to those channels. If there are problems connecting to the Veeahub network on the 5GHz band, we recommend excluding those channels from the Auto Channel Whitelist.

15.2. Access Point Configuration (2.4 GHz and 5 GHz): Scan

This tab (Figure 24), when it appears, shows the measurements for each channel on which the Auto Channel selection is based. It also shows the date and time these measurements were made. A typical result is shown here.

Auto Channel Scan is available on the VHC05, but these metrics are not displayed.

Figure 24: Access Points: Scan Tab



The measurements are listed in Table 16

Table 16: Access Points: Scan Tab

Channel	The channel number.
#BSS	The number of basic service sets (BSS) detected on this channel.
Minimum/Maximum RSSI for BSS	The minimum and maximum Received Signal Strength Indicator for the BSSs on this channel
Noise Floor / dBm	The noise floor on this channel
Load	A measure of the time the channel is occupied
Rank	A number calculated from the measurements. The highest ranking channel is auto selected.

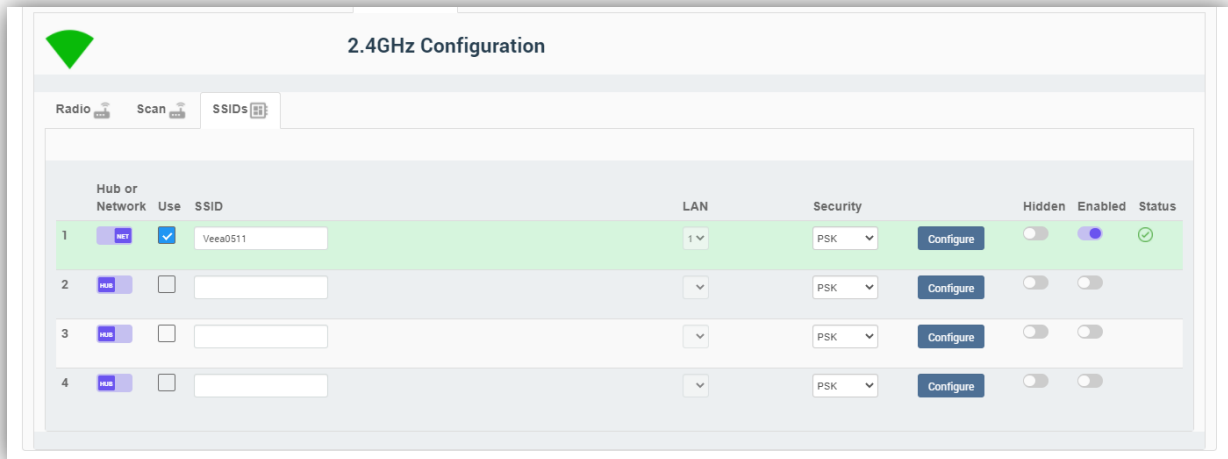
These measurements are combined to select a best channel for the Auto Channel selection. If a channel is ranked as 0, it is not considered suitable for auto selection. If all the channels show poor results, then moving the VeevaHub to another position should be considered.

You can rescan the measurements by clicking **RESCAN**. This may change the channel used.

15.3. Access Point Configuration (2.4 GHz and 5 GHz): SSIDs

This tab (Figure 25) is used to configure the SSIDs for the virtual APs in the 2.4GHz or 5 GHz band. The options are described in Table 17.

Figure 25: Access Points: SSIDs Configuration Tab









In order to use one of the APs, select Use and enter the chosen SSID. Also enter the password that the user must have in order to connect to this AP. If the SSID is marked as Hidden, the user will also need to know the SSID in order to connect the mobile device to it.

Table 17: AP SSIDs Configuration

AP number	The number of the AP being configured.
Hub or Network	On the gateway Veeahub (MEN), set this to Network to apply the settings to this AP number on all nodes across the Veeahub network. On any Veeahub, set this to Hub to apply the settings to the AP on this node alone. This overrides any mesh-wide settings on this AP.
Use	Select the Use control to use this AP on this hub. If the Enabled switch is on, the AP has the settings that are configured here. If the Enabled switch is off, the AP is disabled on this Veeahub, even if it is configured for the whole network (see Hub or Network, above).
SSID	The broadcast name of the AP.
Security	This drop-down, with the Configure button, is used to set security options on the wireless AP. See section 15.4. Note: This option is not available on the VHC05.
Configure	See Security, above. Not available on the VHC05.
Hidden	Set whether the AP SSID is broadcast to nearby mobile devices.
Enabled	See Use above.
Status	Displays the current status of the AP.

Icons and Colors

The icon and background color of an SSID entry give information about the state of the AP. For further details, see the Status message displayed.

	Green	The AP is active and properly configured for this setting
	Blue	The AP is configured for the network (if Hub is selected) or configured for this Veeahub (if Network is selected)
	Orange	The AP is disabled
	Red	The AP is non-operational
	Yellow	The configuration of this AP is incomplete
	No color	The AP is waiting for you to Apply a change in configuration

15.4. Access Point Security Configuration (2.4GHz, and 5GHz)

The **Security** option is used to change the security settings on an AP. When a Veeahub is first added to a Veea account, one AP is initially created with PSK security by default and with the password assigned by the user.

These options are not available on the VHC05.

The options from the drop-down are shown in Table 18.

Table 18: Security Configuration Description (2.4GHz, and 5GHz)

Open	No password is required for anyone to connect to this AP. There are no further options.
PSK	A password must be set up on the Veeahub. This password must be known by a user in order to connect their mobile device to this AP. The options are shown in Figure 26 and described in Table 19.
Enterprise	This option is for Veeahubs in enterprise networks. Your administrator will provide necessary information for this option. See Figure 27 and Table 20. Authentication is performed by contacting a specialized server, called a RADIUS Authentication server. RADIUS may also be used to collect data on usage for billing purposes (Accounting server). RADIUS servers must be set up on the gateway Veeahub (MEN) before a selection can be made on other nodes in the mesh.

Figure 26: PSK Security Configuration

The screenshot shows a configuration window titled "PSK Security Configuration". It contains the following fields and controls:

- SSID:** A text input field containing "Veeah0511".
- Password:** A password input field with masked characters (dots) and a visibility toggle icon.
- WPA Mode:** A dropdown menu currently set to "WPA2 Only".
- 802.11r:** A toggle switch that is currently turned on (blue).
- 802.11w:** A dropdown menu currently set to "Enabled".

At the bottom right of the form, there are two buttons: "Cancel" and "Done".

Table 19: PSK Security Configuration

SSID	Not editable here, see section 15.3.
Password	Enter the password here, 8-63 characters. Click on the eye icon to view.
WPA Mode	WPA2 Only, WPA3 Only or WPA2 and WPA3.
802.11r	When set, this enables client devices to fast transition between network APs that are configured with the same SSID. This is currently available only on the 09/10 models. Enabling 802.11r may mean that some older devices cannot connect to this SSID.
802.11w	This option is available only when WPA2 Only is selected. The values are Enabled, Disabled or Required . This enhancement to security is set to Enabled by default: devices with or without 802.11w can connect. If set to Required, only devices that support 802.11w will be able to connect.

Figure 27: Enterprise Security Configuration

The screenshot displays the 'Enterprise Security Configuration' dialog box. It features a share icon in the top left corner. The configuration options are as follows:

- SSID:** Veea0511
- WPA Mode:** WPA2 Only (dropdown menu)
- 802.11r:** Enabled (toggle switch)
- 802.11w:** Enabled (dropdown menu)
- RADIUS Authentication Primary:** None (dropdown menu)
- RADIUS Authentication Secondary:** None (dropdown menu)
- RADIUS Accounting:** Disabled (toggle switch)

There is a 'Configure Servers' button below the RADIUS Authentication settings. At the bottom right, there are 'Cancel' and 'Done' buttons.

Table 20: Enterprise Security Configuration

SSID	Not editable here, see section 15.3.
WPA Mode	WPA2 Only, WPA3 Only or WPA2 and WPA3.
802.11r	When set, this enables client devices to fast transition between network APs that are configured with the same SSID. This is currently available only on the 09/10 models. Enabling 80.11r may mean that some older devices cannot connect to this SSID.
802.11w	This option is available only when WPA2 Only is selected. The values are Enabled, Disabled or Required . This enhancement to security is set to Enabled by default: devices with or without 802.11w can connect. If set to Required, only devices that support 802.11w will be able to connect.
RADIUS Authentication Primary	Select the primary RADIUS Authentication server from the drop-down. If no servers have already been set up, click on the Configure Servers button (Figure 27 and Table 20).
RADIUS Authentication Secondary	Optional. Select from the drop-down if required. The secondary servers is optional and acts as a backup if the primary server is unavailable.
Configure Servers	Used to set up the servers from which you can select the primary and secondary servers.
RADIUS Accounting:	If required, enable this using the switch. A form for specifying the Accounting servers then appears. You can configure primary and (optional) secondary Accounting servers in the same way as the Authentication servers (Figure 27 and Table 20).

After clicking the **Configure Servers** button, you can define up to four RADIUS servers. This must be done on the gateway Veeahub (MEN). See Figure 28 and Table 21.

After the server details have been entered, one can be selected as the primary server and one as the secondary from the drop-down list (Figure 27).

Once configured on the gateway server, the RADIUS servers can also be selected for SSIDs on the other nodes on the mesh.

Figure 28: RADIUS Configuration

	IP Address	Port	Secret	
1	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>	
2	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>	
3	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>	
4	<input type="text"/>	<input type="text" value="1812"/>	<input type="text"/>	

Table 21: RADIUS Configuration

IP Address	Enter the IP address of the RADIUS server (Authentication or Accounting).
Port	Enter the Port number for the RADIUS service. By default, this is 1812 for the Authentication server and 1813 for the Accounting server.
Secret	Enter the secret (passphrase) for the server. Click on the eye icon to make the secret visible. The passphrase must be known by a user in order to connect their mobile device to this AP.
	Click to delete the entry.

16. Physical Port Configuration

Configurations of Ethernet ports (LAN ports) are made on this tab, shown in Figure 29. The configuration options are listed in Table 22.

Port configuration

A port can be configured as a WAN or LAN port:

- **WAN:** this port is used as the wired connection (backhaul) to the Internet. This is available on the gateway Veeahub (MEN) only. The WAN settings are described in section 13.2.
- **LAN:** this port is in use to connect a device to the Veeahub network with an Ethernet cable. Several devices can be connected to this port if you use a switch. The LAN settings are described in section 14.1.

Mesh ports

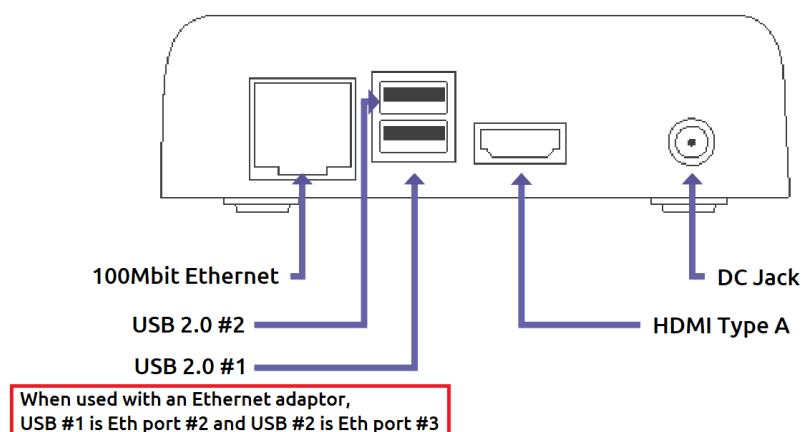
A port can also be used to create a wired connection to another Veeahub and thus to the mesh network. This might be used, for example, to bridge the gap with a cable between two nodes where the distance is too great for effective Wi-Fi communication. A Veeahub mesh can consist of any mixture of wired and wireless links. The mesh configures itself to provide full connectivity and redundancy. When a port is in use as a mesh port, this is displayed by the Mesh switch on this tab against that port.

if all the Veeahubs in the network are wired, the wireless mesh can be switched off (section 12.1), although that is not necessary.

There are certain cases where some manual configuration may be needed. For more information about automatic configuration for wired mesh, please see veea.com/support

VHC05 ports

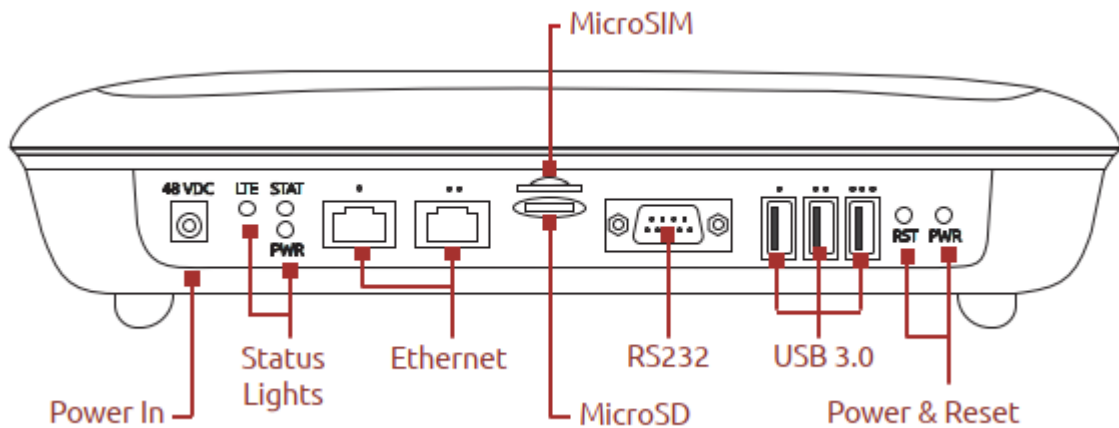
On the VHC05, there is only one Ethernet port. In the typical case of Ethernet backhaul, the Ethernet port on the MEN is already dedicated to the WAN. You can use the USB ports as Ethernet ports with suitable adaptors. In these cases, Port 2 is the lower USB socket, and Port 3 is the upper USB socket.



VHE09/VHE10 ports

On the VHE09/10, there are two Ethernet ports. They are marked on the casing with one dot for Port 1 and two dots for Port 2. Either port can be used as the WAN port, and the other can be configured as LAN. By default, Port 2 on the gateway Veeahub (MEN) is configured for WAN. If you change the cable to the other port, you must restart the Veeahub. Port 1 can be used for Power over Ethernet, as an alternative to the regular power supply. Note that on the gateway Veeahub (MEN) it is not possible to configure both Ethernet ports as LAN ports.

There are also two USB ports that can be used as Ethernet ports with adaptors. They are Port 3 (one dot) and Port 4 (two dots). The USB port with three dots cannot be used as a LAN port.



Example uses of Physical Ports configuration

An example of the use of the Port number and Enabled/Disabled controls is:

- On the gateway Veeahub (MEN), select a Port number, select **NETWORK**, then select **Enabled**. The configuration of that port (WAN, LAN or Mesh) is then copied to all the nodes in the mesh.
- On another node, select the same Port Number and then set to **Disabled**. This turns off the function on that port on that Veeahub. This might be used, for example, where you wish to disable the LAN port on a node in a public area so that it is not possible to plug in an unauthorized device.
- Alternatively, on the other node, you can select **HUB**, then configure the port for a specific use on that Veeahub alone.

Figure 29: Physical Ports Configuration Tab

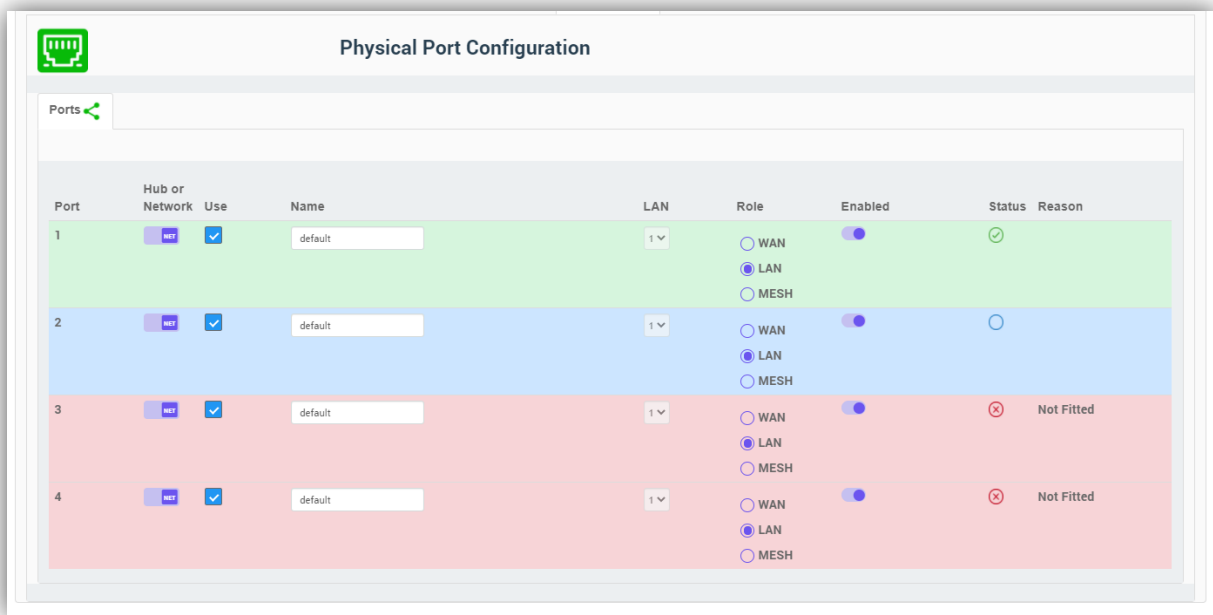
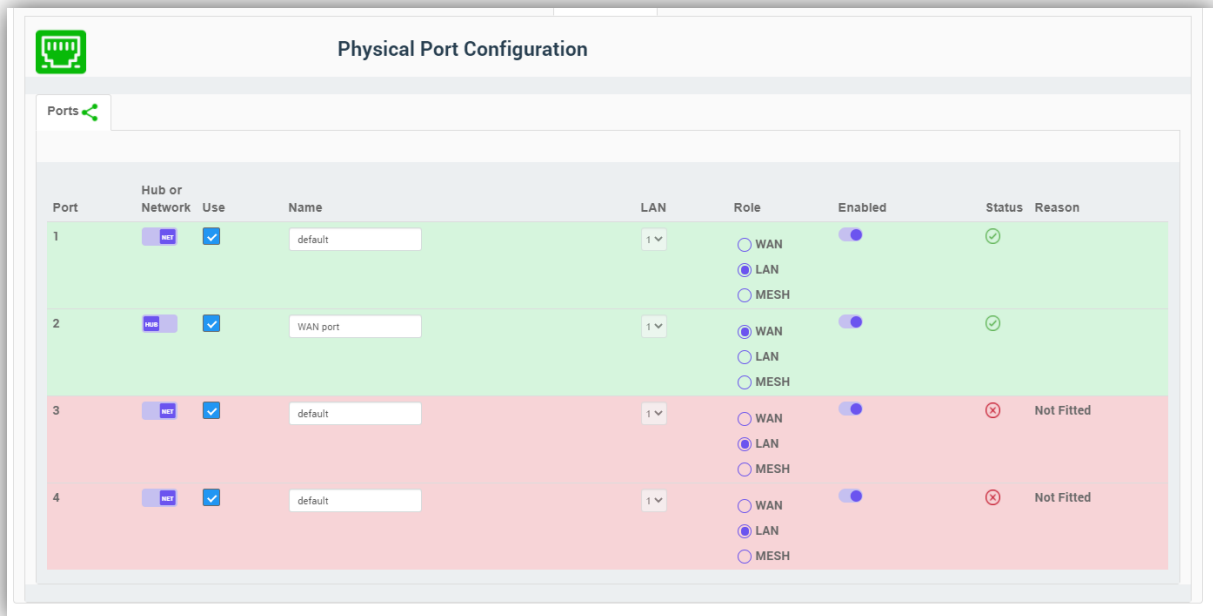


Table 22: Physical Ports Configuration

Port number	The number of the port being configured.
Hub or Network	<p>On the gateway Veeahub (MEN), set this to Network to apply the settings to this port number across the Veeahub network.</p> <p>On any Veeahub, set this to Hub to apply the settings to the port on this node alone. This overrides any mesh-wide settings on this port.</p> <p>Settings that are in use and correctly set are highlighted in green. If the hub setting is in conflict with the network setting, it is highlighted in red.</p>

Port 1 Use	Select the Use control to use this node on this hub. If the Enabled switch is set on, the port has the settings that are configured here. If the Enabled switch is off, the port is disabled on this Veeahub, even if it is configured for the whole network (see Hub or Network, below).
Name	Give a name to this port for reference only.
Role	Select the usage of this physical port: WAN, LAN or Mesh (see above for more information).
Enabled	Set this in conjunction with the Use check box: see above.
Status Information	The status of the active port configuration is reported here.

Icons and Colors

The icon and background color of an SSID entry give information about the state of the AP. For further details, see the Status message displayed.



Green

The AP is active and properly configured for this setting



Blue

The AP is configured for the network (if Hub is selected) or configured for this Veeahub (if Network is selected)



Orange

The AP is disabled



Red

The AP is non-operational



Yellow

The configuration of this AP is incomplete



No color

The AP is waiting for you to **Apply** a change in configuration

If the message 'DHCP conflict' is displayed on the Physical Ports configuration screen against an Ethernet port configured as LAN, this means that another DHCP server has been detected on the LAN. This is an error situation. You must resolve the error by removing the DHCP server. This may require intervention by the network administration. Or if the cable has been connected incorrectly, reconnect it in correct configuration. To subsequently clear the error status, disable and re-enable the port, or remove the cable from the port and reconnect it.

When an Ethernet port is In Use and Enabled but has no connected device, the message 'Port Down' is displayed.

If a USB port has been configured as a LAN port but no Ethernet adaptor is present, the message 'Not Fitted' is displayed.

17. Firewall Configuration

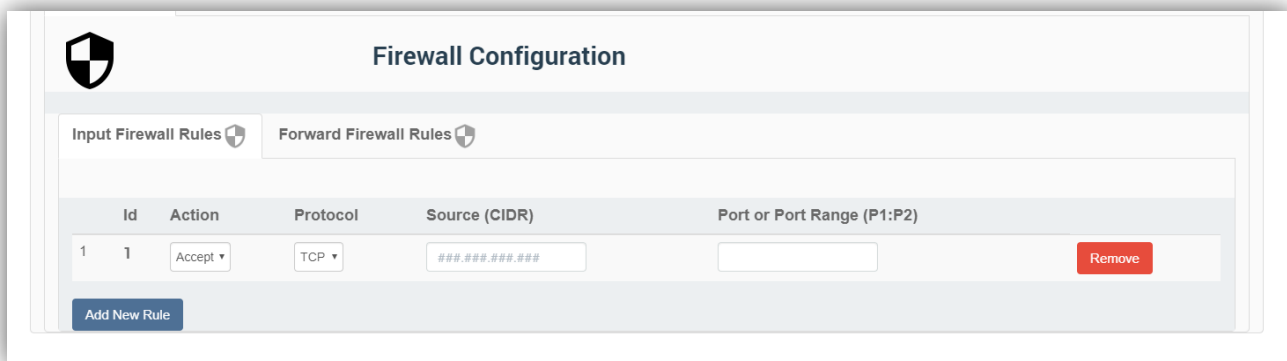
This tab enables you to configure firewall rules on a Veeahub. The Input Firewall Rules tab enables you to configure ACCEPT and DROP rules. For FORWARD rules, use the Forward Firewall Rules tab.

You do not need to configure these settings if your system is protected by a firewall between the mesh and the Internet. You may, however, need to make changes for specific applications.

The Forward Firewall Rules subsidiary tab is available only on a gateway Veeahub (MEN).

17.1. Adding an ACCEPT or DROP rule

Figure 30: Input Firewall Rules Tab



1. On the Input Firewall Rules tab (Figure 30), click **Add New Rule**.
2. From the Action drop-down menu, select **Accept** or **Drop**, as required.
3. From the Protocol drop-down menu, select the packets you wish to filter: Transmission Control Protocol (**TCP**) or User Datagram Protocol (**UDP**).
4. Enter the Source IP address you wish to accept or drop packets from. This can be either a single dotted IP address or a subnet address specified in CIDR notation, for example, 192.168.1.0/16. This field must be present.
5. Enter the port or range of TCP/UDP ports you wish to accept or drop packets from. The lower and upper range values are separated by a colon (:) character. This field is required if the selected protocol requires a port to be defined.
6. Click **Apply** to complete the setup process and save the new rule.

To modify a rule, change the data as necessary and click **Apply**.

To delete a rule already entered, click **Remove** against the rule.

To change the order in which the rules are applied, click and drag a line up or down. The rules are applied in ascending order.

17.2. Adding a FORWARD rule

Figure 31: Forward Firewall Rules Tab

The screenshot shows the 'Firewall Configuration' window with the 'Forward Firewall Rules' tab selected. Below the tab are two buttons: 'Input Firewall Rules' and 'Forward Firewall Rules'. A table displays the current rules:

Id	Protocol	Port or Port Range (P1:P2)	Local IP	Local Port	
1	TCP		#####		Remove

An 'Add New Rule' button is located at the bottom left of the table area.

1. On the Forward Firewall Rules tab (Figure 31), click **Add New Rule**.
2. From the Protocol drop-down menu, select the packets you wish to forward: Transmission Control Protocol (**TCP**), or User Datagram Protocol (**UDP**).
3. Enter a single TCP/UDP port number or a range of port numbers where the lower and upper range values are separated by a colon (:) character. This field is required if the selected protocol requires a port to be defined.
4. Enter the Local IP address to forward traffic to, in single dotted IP address notation.
5. Enter the Local Port number to which traffic is forwarded. This must be given unless the Port or Port Range specifies a range of TCP/UDP ports, in which case the port range will also be applied for the local ports to which traffic is forwarded.
6. Click **Apply** to complete the setup process and save the new rule.

To modify a rule, change the data as necessary and click **Apply**.

To delete a rule already entered, click **Remove** against the rule.

To change the order in which the rules are applied, click and drag a line up or down. The rules are applied in ascending order.

Table 23: Firewall Rules Setup Options

Action	Protocol	Source IP	Port or Range	Local IP	Local Port
Accept	TCP	Enter source IP address to ACCEPT.	Enter port or port range to ACCEPT.	Not used.	Not used.
	UDP	Enter source IP address to ACCEPT.	Enter port or port range to ACCEPT.	Not used.	Not used.
Drop	TCP	Enter source IP address to DROP.	Enter port or port range to DROP.	Not used.	Not used.
	UDP	Enter source IP address to DROP.	Enter port or port range to DROP.	Not used.	Not used.
Forward	TCP	Not used.	Enter port or port range to FORWARD.	Enter IP address to Forward to.	Enter port to Forward to.
	UDP	Not used.	Enter port or port range to FORWARD.	Enter IP address to Forward to.	Enter port to Forward to.

18. LAN Configuration

18.1. Default Configuration

When a Veeahub is enrolled as the first unit in the network, it automatically becomes the gateway Veeahub (MEN), which also has management functions on the network. The LAN is established with the defaults in the table below, using the gateway option above. These settings can be changed using the relevant screens in Veeahub Manager or Enterprise Center.

LAN Attribute	Notes
WAN Interface	The WAN interface used for the LAN is the interface that is connected to the Internet when the Veeahub is enrolled.
Mode	Routed (NAT)
Internal DHCP	Enabled
Wi-Fi Access Points	First Wi-Fi entry for 2.4GHz and 5GHz. See below.
Ethernet Ports	All ports (other than the Gateway WAN interface) are configured as LAN by default, on the single subnet.
DNS Lease Time (minutes)	60
Default LAN	10.100.1.0/24
Guest Wi-Fi	10.100.2.0/24
Public Wi-Fi	10.100.5.0/24
LAN 3	10.100.3.0/24 - optional reserved
LAN 4	10.100.4.0/24 - optional reserved
Layer 3 Mesh (internal use)	10.101.0.0/16
Layer 3 Local (internal use)	10.102.0.0/16 (mesh internal prefix)
Docker	172.17.0.0/24
	172.18.0.0/24
LoRaWAN	169.254.0.0/16
Privafy	
<future>	

The port used for WAN connection is configured on power up. The physical connection can be changed, then the hub can be restarted.

The default for the first Wi-Fi entry is an SSID that matches the mesh name chosen when the first Veeahub on the network is enrolled. For example, if the mesh name given during enrollment is 'MyNetwork', the first user SSID is also 'MyNetwork'. The mesh name can be changed in the vMesh Configuration screen of Veeahub Manager, or the network name in the Network Configuration tab of Enterprise Center.

This SSID is configured across the Veeahub network, so any other Veeahubs in the same network also have a Wi-Fi access point with a 'MyNetwork' SSID, for both the 2.4GHz radio and 5GHz radio.

Note: On a VHE09/10, the 5GHz AP is enabled by default. On a VHC05, the 5GHz AP can only be enabled if the wireless mesh used to connect peer Veeahubs is first disabled.

Note: Failover is available only on a LAN configured as Routed (the default). Failover is not supported in Bridged mode.

18.2. IP Conflict Resolution

The Veeahub platform uses specific IP ranges for internal purposes. These default LAN and guest and public Wi-Fi ranges can be manually configured, if required for specific purposes.

In the event that the gateway hub detects a conflict with the IP addresses on the WAN it can switch automatically to the alternate IP ranges listed below.

Subnet	Alias	Principal	Alternate
Default LAN	shared:trusted	10.100.1.0/24	172.20.1.0/24
Guest Wi-Fi	shared:guest	10.100.2.0/24	172.20.2.0/24
Public Wi-Fi	Shared:public	10.100.5.0/24	172.20.5.0/24
L3 standard		10.101.0.0/16	172.21.0.0/16
L3 alternate		10.102.0.0/16	172.22.0.0/16

A LAN is switched to its alternate subnet if a WAN interface for the LAN is in conflict, and the subnet has been automatically assigned.

If the subnet has been manually assigned, and a WAN interface is in conflict, the LAN is marked as non-operational. If a LAN is non-operational, this is reported in Node Manager and in Veeahub Manager.

18.3. DHCP Conflict

If the message 'DHCP conflict' is displayed on the Physical Ports configuration screen against an Ethernet port configured as LAN, this means that another DHCP server has been detected on the LAN. This is an error situation.

First, you must resolve the error by removing the DHCP server. This may require intervention by the network administration. Or if the cable has been connected incorrectly, reconnect it in correct configuration.

To subsequently clear the error status, disable and re-enable the port, or remove the cable from the port and reconnect it.

19. Troubleshooting

19.1. Configuration of VHE09 as MEN in Mixed 09/10 Configurations

When a VHE09 gateway Veeahub (MEN) is wirelessly meshed with a VHE10 non-gateway Veeahub (MN), this can impact the VHE10 (MN) ability to connect wirelessly to the VHE09 (MEN).

This happens when the VHE09 (MEN) 5GHz channel selection is set to automatic. In this case, the 5GHz channel is determined automatically by the Veeahub software. Regulated 5GHz channel allocations vary from country to country. Some configurations of VHE09 units, for example, the US, have an extended channel capability with both low and high band channels available, whereas the VHE10 units, default to low band channels for wireless meshing. If the automatic channel selection on the VHE09 (MEN) selects a channel above 100, the VHE10 (MN) unit will not see the channel when it scans and cannot connect.

Solution:

Restrict the VHE09 (MEN) high band channels available for use by the automatic channel selection. This is implemented by use of the 'Auto Channel Whitelist' control as follows:

1. Login to the Control Center account and go to the Node Manager (NM) for the VHE09 (MEN) unit in focus.
2. In the NM select tabs **Network > Network > WLAN** to access the network Configuration WLAN screen (Figure 32):
 - Locate the 'Auto Channel Whitelist' and on each channel 100 and above, select '**Ctrl**' + '**Left Click**' to deselect it (Figure 33). This function toggles the selection and deselection of a channel. Deselected channels have a white background and selected channels have a blue background color (Figure 34).
 - Select **Apply** to save the setting
 - Confirm the configuration change has resolved the connection issue
 - Procedure completed.

Note. The configuration changes described above can also be implemented from the Veeahub Manager (VHM). Refer to the VHM Guide which describes the alternative procedure.

Figure 32 – vMesh Screen (All Available Channels Whitelisted)

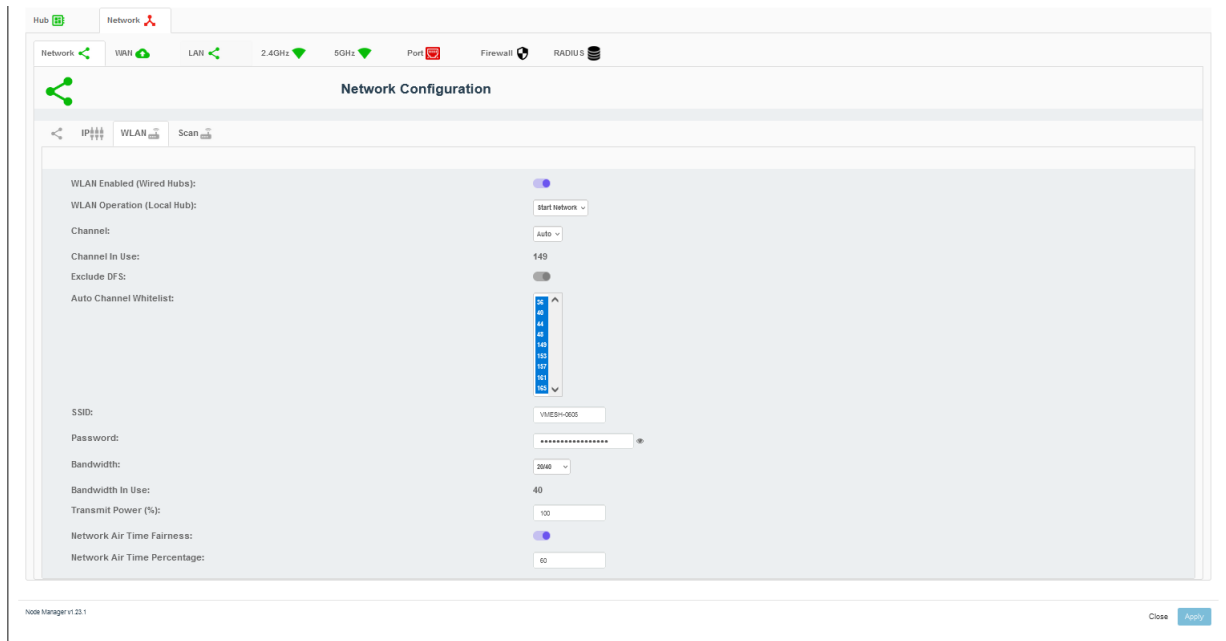


Figure 33 – vMesh Screen (Channels 100 Plus Deselected from Whitelist)

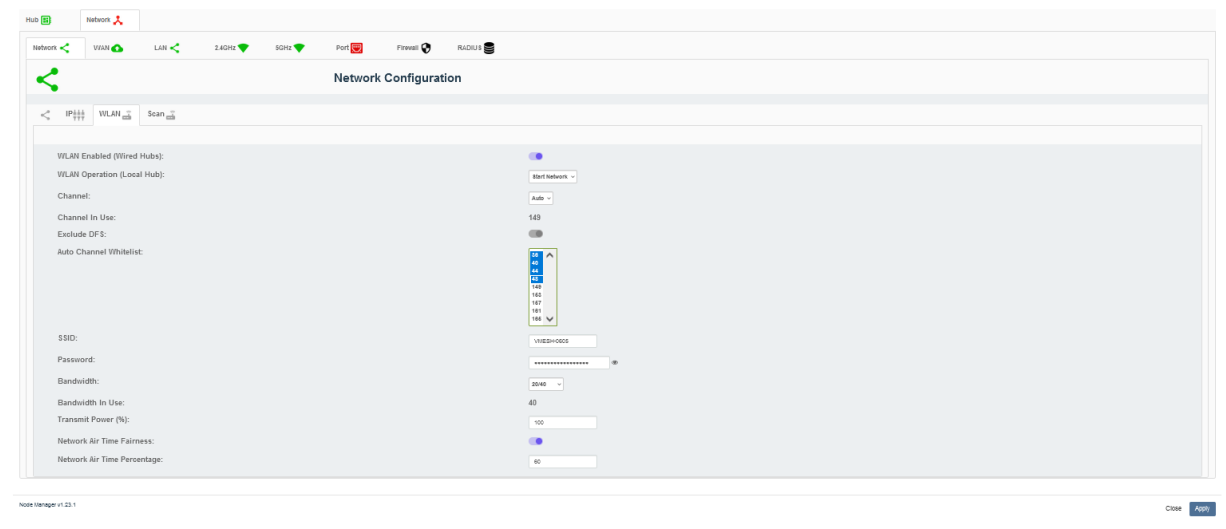


Figure 34 – vMesh Screen (Channels Below 100 Whitelisted)

The screenshot displays the 'Network Configuration' interface for vMesh. The 'WLAN' tab is selected, showing the following settings:

- WLAN Enabled (Wired Hubs):
- WLAN Operation (Local Hub): Start Network
- Channel: Auto
- Channel In Use: 48
- Exclude DFS:
- Auto Channel Whitelist: 36, 48, 44, 45
- SSID: VMESH-0511
- Password: [Redacted]
- Bandwidth: 2040
- Bandwidth In Use: 40
- Transmit Power (%): 100
- Network Air Time Fairness:
- Network Air Time Percentage: 60

At the bottom left, it says 'Veeva Manager v1.23.1' and at the bottom right, there are 'Close' and 'Apply' buttons.

20. Technical Support

Before contacting Technical Support, please consult the documentation, tutorials, and community topics available on the support web site www.veea.com/support/. Please sign up, if you don't already have an account, and sign in.

For unresolved queries, click on the Submit a request link.

Please complete the form with an appropriate subject, and as much detail as possible in the description field. Please include any relevant information such as Veea hardware serial numbers, logs, screenshots, etc.

An email will automatically be sent to your email address to confirm the request has been received.