



QUANTUM[®]
ACCESS UNLIMITED

QUANTUM COLLAB

COLLAB Configuration Guide (Access Point in Gateway Mode)



Copyright Information

Copyright & trademark specifications are subject to change without prior notice. Copyright © 2018 Quantum Networks (SG) Pte. Ltd. All Rights Reserved. Quantum Networks® & the logo are trademarks of Quantum Networks (SG) Pte. Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners. Mentioned contents of this document can't be used, translated or transmitted in any form or by any means without taking prior written permission from Quantum Networks (SG) Pte. Ltd.



Contents

Prerequisites	4
Configuration Steps	4
Create a Gateway Profile	5
Create MAC Whitelist Profile	6
Create Authentication Profile	7
Create Hotspot Profile	8
Create Hotspot SSID	9



Prerequisites

- Existing network gateway IP, Subnet Mask and VLAN.
- Need to bypass RADIUS IP, authentication and accounting port (UDP 1812, 1813 and TCP 80, 443 in case of QN COLLAB) from firewall policy.

Configuration Steps

- Go to particular site.
- Create a Gateway Profile.
- Create Authentication Profile.
- Create MAC Whitelist Profile.
- Create Hotspot Profile.
- Create Hotspot SSID.



Create a Gateway Profile

Select the site:

- Go to **Configuration > Network > Router**, click “**Add NAT Profile**”. Below screen appears.

Sites / Configuration / Network / Gateway

NAT CONFIGURATION

Name: CHLS

IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0 (/24)

DNS1: 8.8.8.8

DNS2: 4.2.2.2

MTU Size: 1500

DHCP Server:

DHCP Range Start: 10.10.10.2

DHCP Lease Count: 250

Lease Time: 12 Hrs

Enable DHCP Reservation:

Vlan Id: 22

Network Type: LAN

Submit Back

Configuration Parameter:

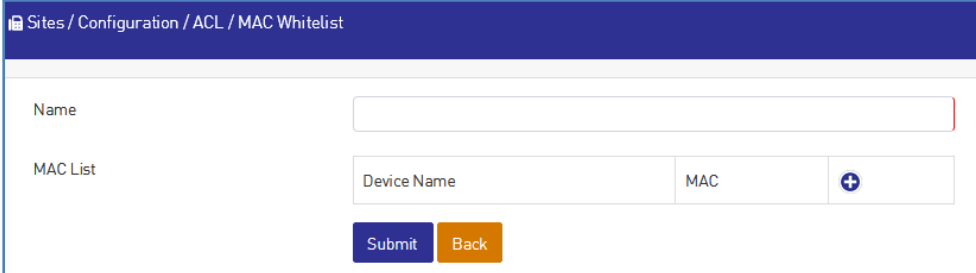
Parameter	Description
Name	Type a name for the NAT Profile.
IP Address	Assign NAT Profile IP address.
Subnet Mask	Assign Subnet Mask address.
DNS1	Assign DNS1.
DNS2	Assign DNS2.
MTU Size	MTU is the size of the largest protocol data unit that can be passed in single network layer transmission.
DHCP Server	Enable DHCP server if required and assign the IP pool range and lease count.
DHCP Range Start	Assign IP pool range.
DHCP Lease Count	Assign DHCP lease count.
Lease Time	Assign lease time.
Enable DHCP Reservation	Enabled feature will provide option to pre-set IP address to a specific client based on its physical MAC address.
Vlan Id	Assign the respective VLAN ID.
Network Type	Select network type – LAN / Guest.



Create MAC Whitelist Profile

With whitelisting- Devices get access without authentication. To create a profile,

- Go to **Configuration > ACL > MAC Whitelist**, click “**Add**”. Below screen appears.



Sites / Configuration / ACL / MAC Whitelist

Name

MAC List

Device Name	MAC

Configuration Parameter:

Parameter	Description
Name	Profile name.
MAC List	Add MAC Addresses to be Whitelisted.

Note: Create this profile if needed.



Create Authentication Profile

- Go to **Configuration > Authentication > click "Add"**. Below screen appears.

Sites / Configuration / Authentication

Name: COLLABAUTH

Description:

Authentication Method: AAA

AUTHENTICATION SERVER

Server IP Address: 36.255.3.166

Secondary Server IP Address:

Authentication Port: 1812

Shared Secret:

Confirm Shared Secret:

ACCOUNTING SERVER

Server IP Address: 36.255.3.166

Secondary Server IP Address:

Accounting Port: 1813

Shared Secret:

Confirm Shared Secret:

Submit Back

Configuration Parameter:

Parameter	Description
Name	Name of Authentication Profile.
Description	Detail for reference.
AUTHENTICATION SERVER	
Server IP Address	Authentication server primary IP address.
Secondary Server IP Address	Authentication server secondary IP address.
Authentication Port	Authentication port provided by Hotspot service provider.
Shared Secret	Shared Secret provided by Hotspot service provider.
Confirm Shared Secret	Confirm shared Secret provided by Hotspot service provider.
ACCOUNTING SERVER	
Server IP Address	Accounting server primary IP address.
Secondary Server IP Address	Accounting server secondary IP address.
Authentication Port	Accounting port provided by Hotspot service provider.
Shared Secret	Shared Secret provided by Hotspot service provider.
Confirm Shared Secret	Confirm secret provided by Hotspot service provider.



Create Hotspot Profile

- Go to **Configuration > Hotspot** > click **“Add”**. Below screen appears.

The screenshot shows a web configuration page for creating a Hotspot Profile. The page is organized into several sections:

- HOTSPOT PROFILE:** Includes fields for Name (COLLABHotspot) and Description.
- CAPTIVE PORTAL:** Includes fields for Portal URL (https://wsmp.qntmnet.com/subscriber/index), Portal Secret, and Confirm Portal Secret.
- USER SESSION:** Includes fields for Session Timeout (1800 second) and Ideal Timeout (3600 second).
- NETWORK SETTINGS:** Includes a field for DNS Domain (mydomain.com).
- WALLED GARDEN:** Includes a field for Exception URL with a list of domains (cc.qntmnet.com, wsmp.qntmnet.com) and a MAC Whitelist toggle.

At the bottom, there are 'Submit' and 'Back' buttons.

Configuration Parameter:

Parameter	Description
Name	Name of Hotspot profile.
Description	Detail for reference.
CAPTIVE PORTAL	
Portal URL	Captive portal (splash page) redirection URL.
Portal Secret	User define field- same as configured in COLLAB.
Confirm Portal Secret	User define field- same as configured in COLLAB.
USER SESSION	
Session Timeout (second)	Assign time limit after which user will get disconnects and required to login again.
Ideal Timeout (second)	It's a period of inactivity from user. When there is no traffic from the user, once the timeout is reached, user will be disconnected from the Hotspot.
NETWORK SETTINGS	
DNS Domain	Use this option to Domain Name for the Hotspot.
NAS ID	Enter the Network Access Server identifier of this device. The NAS-ID parameter is sent in RADIUS access and accounting request messages.
WALLED GARDEN	
Auth Exception	Use this option to allow domains which can be accessed by users without Authentication. Clients accessing these domains will not be redirected to the splash page.
Enable MAC Whitelist	Selected list devices will be Whitelisted and allow getting access without authentication.



Create Hotspot SSID

- Go to **Configuration > Wireless** > click **"Add"**. Below screen appears.

The screenshot shows the Rudder configuration interface for creating a Hotspot SSID. The interface is divided into several sections:

- GENERAL SETTING**:
 - WLAN Name: HotspotSSID
 - SSID: HotspotSSID
 - SSID Description: (empty)
 - Enable SSID:
 - Broadcast SSID:
 - Client Isolation:
 - Radio: 2.4 GHz 5 GHz
- METHOD**:
 - Access Type: Hotspot (WSPri)
 - Authentication Method: Open
 - Authentication Profile: COLLABAUTH
 - Hotspot Profile: COLLABHotspot
- SECURITY SETTINGS**:
 - Encryption Method: None
- NETWORK SETTINGS**:
 - Routing Option: NAT to WAN
 - NAT Profile: CHLS
 - VLAN: 22
- ADVANCED SETTINGS**:
 - NAS ID: (empty)
 - NAS ID Delimiter: Colon
 - NAS Request Timeout: 10 Seconds
 - NAS Max Number of Retries: 4 Times
 - Called Station ID: WLAN BSSID AP MAC

At the bottom, there are expandable sections for **ADVANCE WIRELESS SETTINGS**, **DHCP SETTINGS**, and **ACL / SECURITY SETTINGS**, each with a plus sign. At the very bottom, there are **Submit** and **Back** buttons.



Configuration Parameter:

Parameter	Description
GENERAL SETTING	
WLAN Name	This Wireless LAN name is a unique name for management purposes only and is not visible to wireless clients.
SSID	The SSID name that is visible by the wireless clients (Network). SSID can contain up to 32 alphanumeric characters and are case-sensitive.
SSID Description	Detail for reference.
Enable SSID	To enable a Broadcasting SSID. Choose Yes/No checkbox to enable/disable the SSID.
Broadcast SSID	Choose Yes/No checkbox to enable/disable the Broadcasting SSID. By selecting Yes the SSID name is visible to the wireless Clients and will be able to connect to the SSID. By selecting No the SSID name is not visible to the wireless Clients and is in Hidden mode and can add connect to the correct SSID required by the user.
Client Isolation	Choose Yes/No checkbox to prevent wireless clients from communicating to each other. Wireless client isolation enables subnet restrictions for connected clients. Click Enable if you want to prevent wireless clients associated with the same AP from communicating with each other locally.
Radio	Enable required Radio channels.
METHOD	
Access Type	Select Hotspot (WISPr)(Before configuring Access Type as Hotspot (WISPr), create Authentication Profile and Hotspot Profile).
Authentication Method	Open (Any encryption method can be used. It allows you to configure a WPA2 or WPA-Mixed or "none" based encryption. By Choosing a WPA or WPA-Mixed, you can then enter a passphrase or key text of our choice).
SECURITY SETTING	
Encryption Method	Choose encryption method WPA2, None or WPA-Mixed.
Algorithm	Select AES – in case of Encryption Method is selected to WPA2.
Key	Set PW in case of WPA2.
Other options	Will remain as default- inactive.
NETWORK SETTING	
Routing Option	Use this option to select routing option as "Bridge To WAN" or "NAT To WAN". Select as "NAT To WAN".
NAT Profile	Select predefined NAT Profile.
VLAN	Select predefined Bridge Profile.
ADVANCE RADIUS SETTING	
NAS ID	Select AP_MAC.
NAS ID Delimeter	Select MAC format supported by Hotspot service provider.
NAS Request Timeout	Will remain as default.
NAS Max Number of Retries	Will remain as default.
Called Station ID	Select AP MAC.

