



CONFIGURATION GUIDE

MPSK Network Configuration Guide

Personal Area Network (PAN) Setup in
Shasta Cloud

DOCUMENT TYPE

Network Configuration Guide

PLATFORM

Shasta Cloud v4.1

LAST UPDATED

April 21, 2026

VERSION

1.0

Contents

Table of Contents

- Overview
- 1 Navigate to Networks
- 2 General Tab – Network Identity & VLAN Configuration
- 3 Wireless Tab – SSID & Radio Configuration
- 4 Wired Tab – Wired Authentication
- 5 Association Tab – Assign to Venues / APs
- 6 Create the Network
- 7 PAN Tab – Managing Individual MPSK Units
- Summary of Key Configuration Values

Overview

An MPSK (Multi-Pre-Shared Key) network in Shasta Cloud is configured as a **Personal Area Network (PAN)** type. This network type allows each unit or tenant to have its own unique Wi-Fi passphrase and dedicated VLAN, creating isolated personal Wi-Fi spaces within a shared infrastructure. This is ideal for MDU (Multi-Dwelling Unit), hospitality, and enterprise deployments where per-user or per-unit network isolation is required.

This guide covers the full setup process from network creation through individual PAN unit management, including VLAN assignment, wireless settings, and passphrase management.

Network Type: PAN

Auth: MPSK Service

Use Case: MDU / Multi-Tenant

Shasta Cloud Platform

Step 1 — Navigate to Networks

From the left navigation panel, click **Networks**. The Networks page displays all existing networks with their type, authentication method, organization, and associated venues. Click the **Add** button in the top-right corner to begin creating a new network.

The screenshot shows the 'Networks' page in the Rohde Corp interface. The left sidebar contains navigation links: Dashboard, Venues, Clients, Networks (highlighted), Infrastructure, Organizations, Support, Marketplace, Admin, and P-Admin. The main content area features a search bar and filters for 'All (4)', 'Wireless (4)', and 'Wired (0)'. Below this is a table of existing networks:

NAME ↑	NETWORK TYPE	APPLIED TO	WIRELESS AUTH	ORGANIZATION	VENUES	
EVOLVE	Wireless only (Legacy)		Passphrase	Rohde MDU		
ShastaAdmin	Wireless only (Legacy)		Passphrase	Rohde MDU		
ShastaResident	Personal Area Network (PAN)		MPSK Service	Rohde MDU	Shasta MDU	
ShastaVisitor	Wireless only (Legacy)		Passphrase	Rohde MDU		

An 'Add' button is located in the top right corner of the table area. The Shasta Cloud logo is visible in the bottom left corner of the sidebar.

Figure 1 — The Networks page showing existing networks. Click Add to create a new network.

Step 2 — General Tab – Network Identity & VLAN Configuration

The first configuration tab is **General**, at the path Networks / New Network / General. This tab defines the core identity of the network and its VLAN structure.

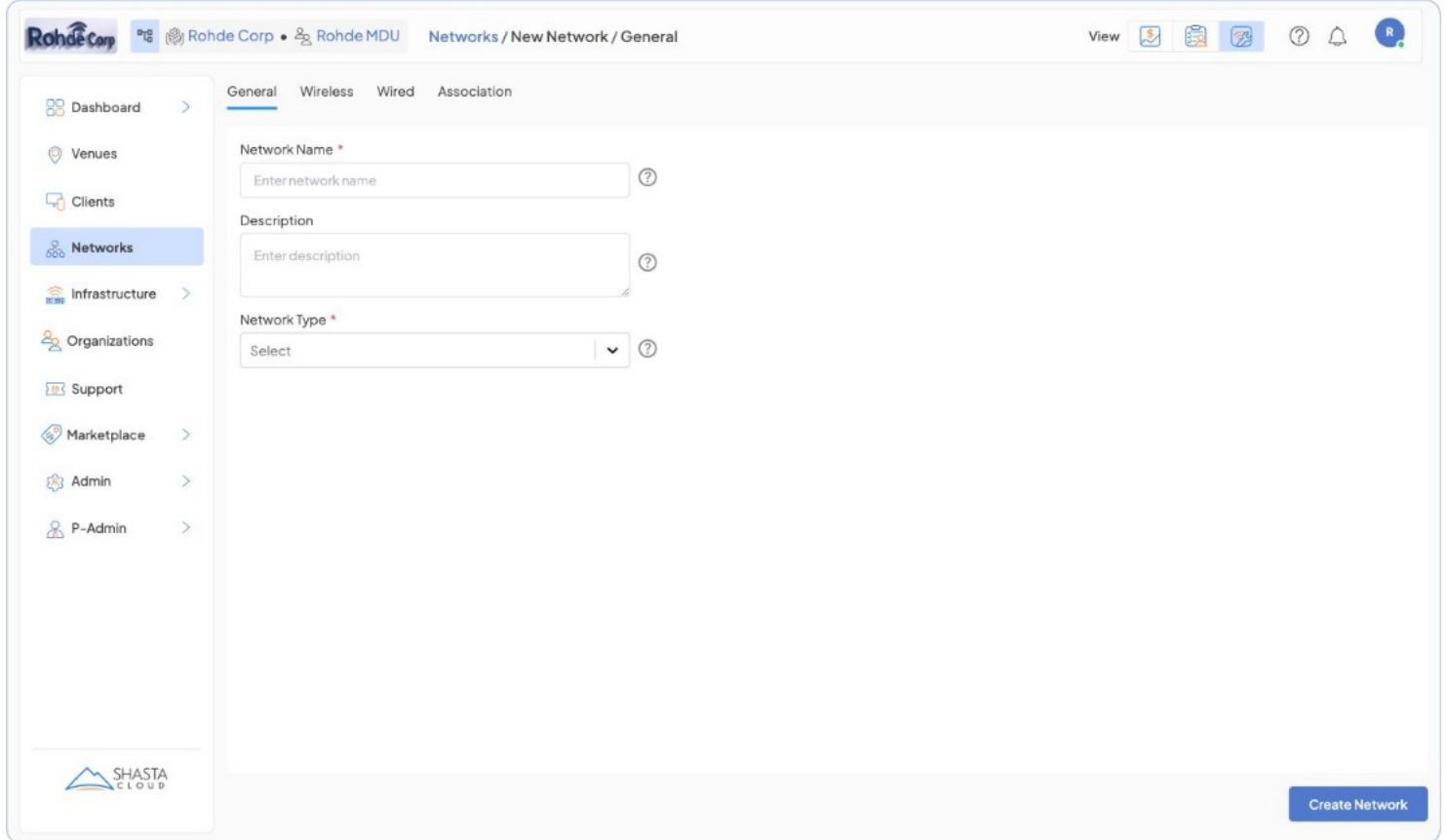


Figure 2 — The New Network General tab with Network Name, Description, and Network Type fields.

Field	Required	Description	Default
Network Name	Required	A unique, descriptive name for the network (e.g., <i>ResidentWiFi</i>).	—
Description	Optional	A free-text description to help identify the purpose of the network.	—
Network Type	Required	Select Personal Area Network (PAN) from the dropdown. This is found under the "Access" category and enables MPSK functionality.	—

After selecting **Personal Area Network (PAN)** as the Network Type, three additional fields appear for VLAN configuration:

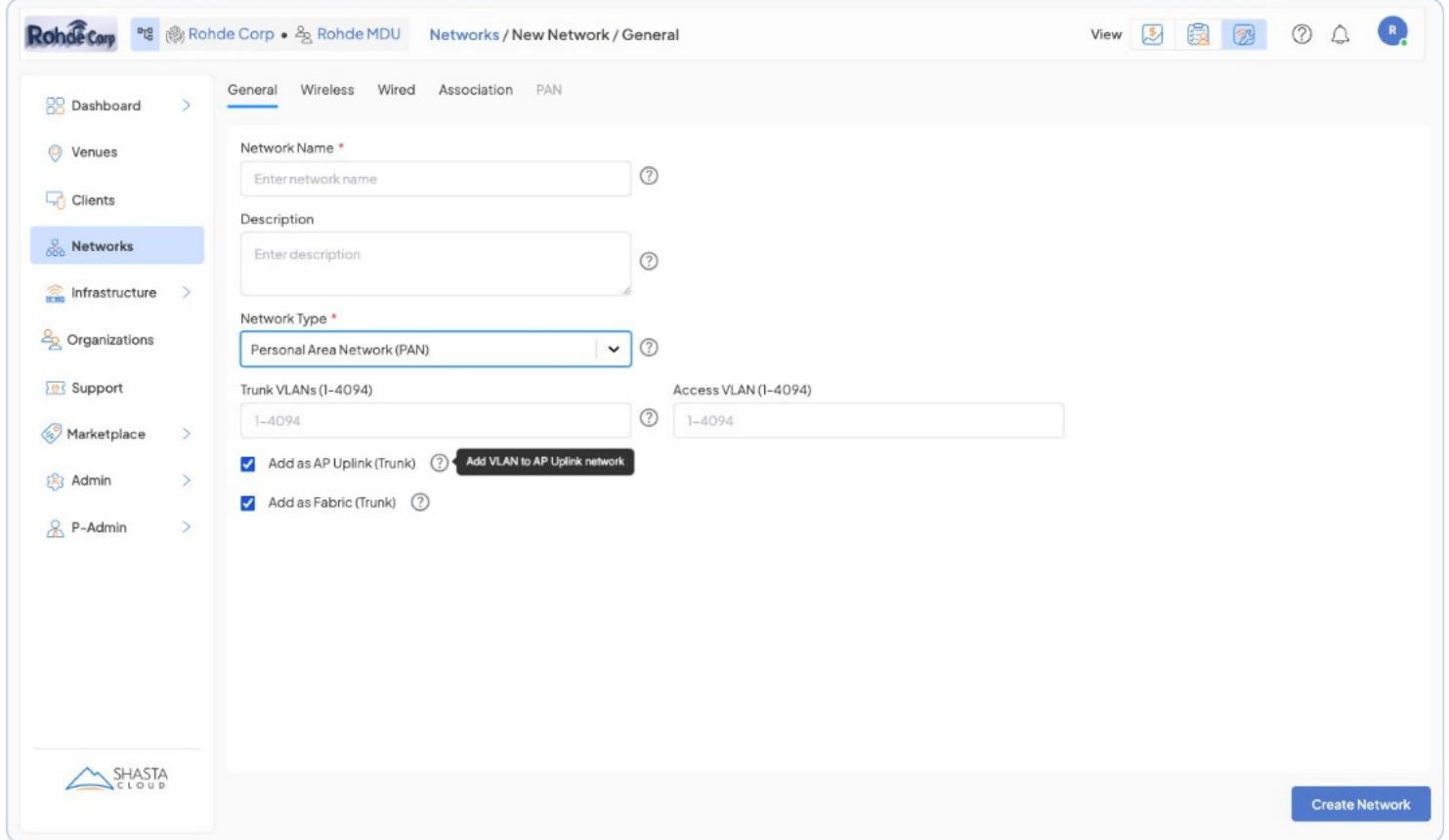


Figure 3 — After selecting PAN, the VLAN fields and a new PAN tab appear in the navigation.

Field	Required	Description	Example
Trunk VLANs (1–4094)	Optional	The range of VLANs available for individual PAN units. Each unit will be assigned one VLAN from this pool. Use a range notation (e.g., 1001-1199).	1001-1199
Access VLAN (1–4094)	Optional	The default/management access VLAN for the network. Used when a client is not matched to a specific PAN VLAN.	2000
Add as AP Uplink (Trunk)	Optional	When enabled, the defined VLANs are added to the AP uplink network as trunk VLANs, allowing APs to carry multiple VLAN-tagged streams.	Enabled
Add as Fabric (Trunk)	Optional	When enabled, the VLANs are also added to the fabric/switching infrastructure as trunk VLANs.	Enabled

Tip: Plan your VLAN range carefully before creating the network. The Trunk VLAN range should be large enough to accommodate all anticipated tenant units. For a 199-unit MDU, a range of 1001–1199 provides one VLAN per unit.

Step 3 — Wireless Tab – SSID & Radio Configuration

Click the **Wireless** tab at Networks / New Network / Wireless to configure over-the-air settings for the network.

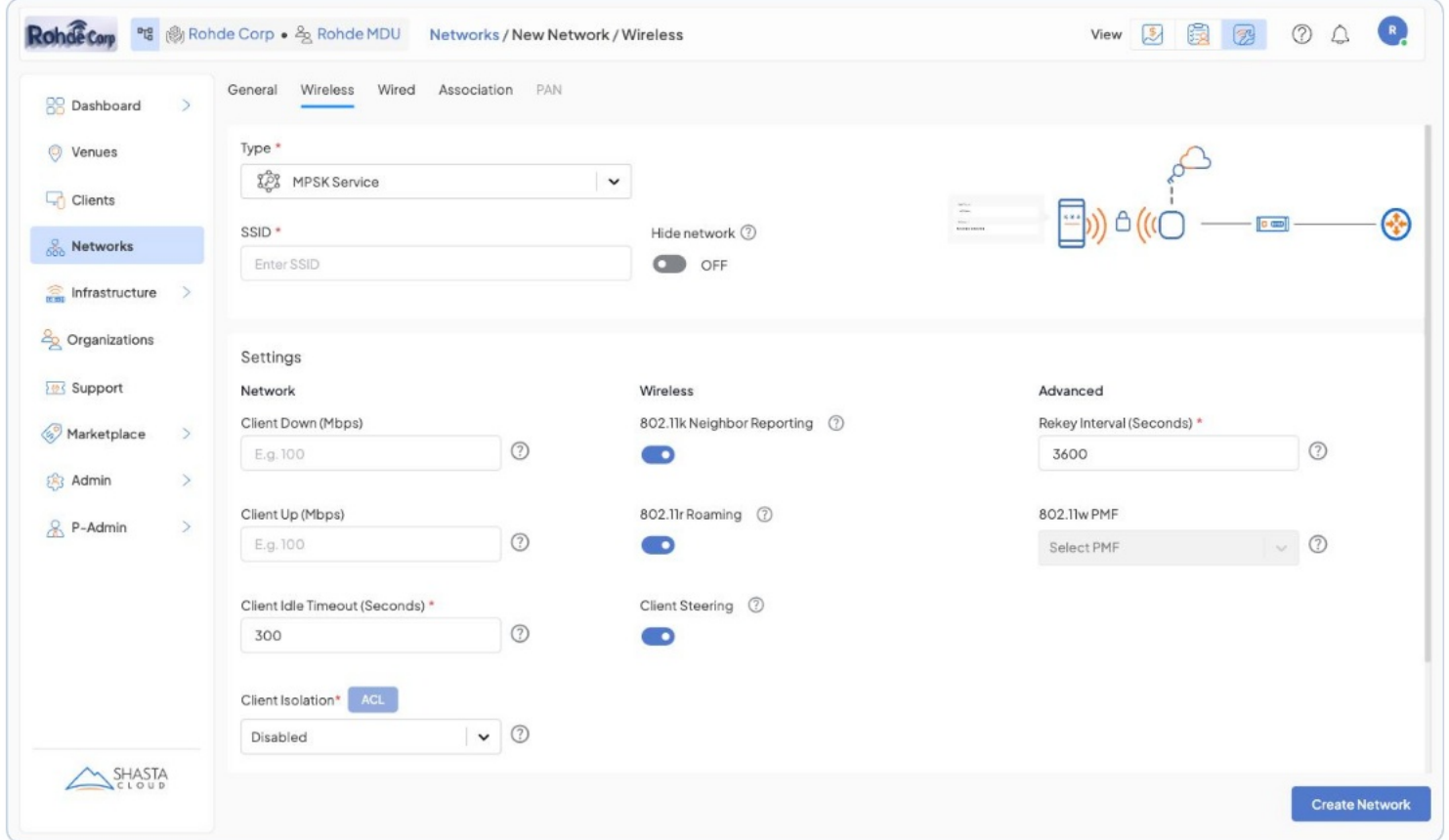


Figure 4 — The Wireless tab showing the MPSK authentication type, SSID, and all wireless settings.

Authentication Type

Option	Description
MPSK Service Recommended	Integrated MPSK authentication engine built into Shasta Cloud. Passphrases are created and managed directly within the platform's PAN tab. No external RADIUS server required.
MPSK AAA	Uses an external AAA (RADIUS) server for Multi-PSK authentication. Choose this option if your organization manages MPSK credentials through an existing external RADIUS infrastructure.

SSID Settings

Field	Required	Description	Default
SSID	Required	The Wi-Fi network name visible to end-user devices (e.g., <i>ResidentWiFi</i>).	—
Hide Network	Optional	When enabled, the SSID is not broadcast and devices must manually enter the network name to connect.	<i>OFF</i>

Network Settings

Field	Required	Description	Default
Client Down (Mbps)	Optional	Per-client download speed limit. Leave blank for no limit.	<i>Unlimited</i>

Client Up (Mbps)	Optional	Per-client upload speed limit. Leave blank for no limit.	<i>Unlimited</i>
Client Idle Timeout (Seconds)	Required	Number of seconds of inactivity before a client is disconnected from the network.	<i>300</i>
Client Isolation	Required	Controls whether wireless clients on the same SSID can communicate with each other. Options: Disabled, ACL-based modes.	<i>Disabled</i>

Wireless Settings

Field	Description	Default
802.11k Neighbor Reporting	Enables clients to receive neighboring AP information for improved roaming decisions.	<i>ON</i>
802.11r Roaming	Enables fast BSS transition (fast roaming) for seamless handoffs between access points.	<i>ON</i>
Client Steering	Allows the network to intelligently steer clients to the optimal AP or frequency band.	<i>ON</i>

Advanced Settings

Field	Required	Description	Default
Rekey Interval (Seconds)	Required	How frequently the encryption keys are automatically rotated. Lower values improve security but may cause brief interruptions.	<i>3600</i>
802.11w PMF	Optional	Protected Management Frames. Options: Select PMF, Optional, Required. Improves resistance to management frame attacks.	<i>—</i>

Scheduling

The **Scheduling** toggle (default: OFF) allows the network to be active only during defined time windows. Enable this if the network should only operate during certain hours (e.g., business hours only).

Step 4 — Wired Tab – Wired Authentication

Click the **Wired** tab to configure authentication for any wired switch ports associated with this network.

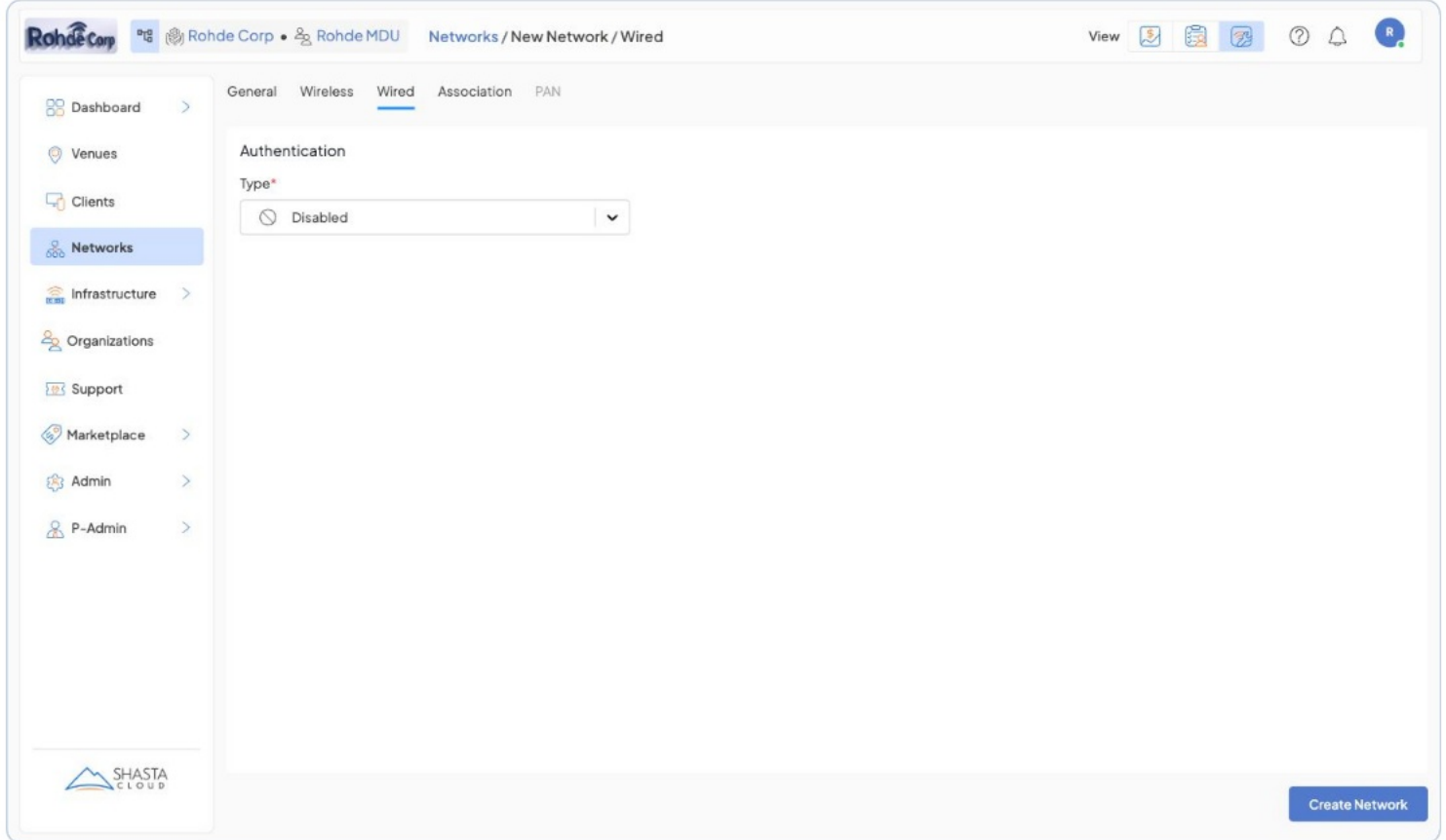


Figure 5 — The Wired tab with Authentication Type options.

Option	Description
Disabled Default	No wired ports are associated with this network. Wired authentication is completely off. Use this for wireless-only MPSK deployments.
None	Wired ports are added to the network without 802.1x authentication. All connected wired devices will have access without credentials.
802.1x	Enables port-based network access control (NAC) for wired clients. Requires a RADIUS server configuration.

Note: For a standard MPSK wireless network (PAN), the Wired tab can be left as **Disabled** unless wired switch ports also need to be associated with the same VLAN structure.

Step 5 — Association Tab – Assign to Venues / APs

Click the **Association** tab to assign the network to one or more venues and their access points.

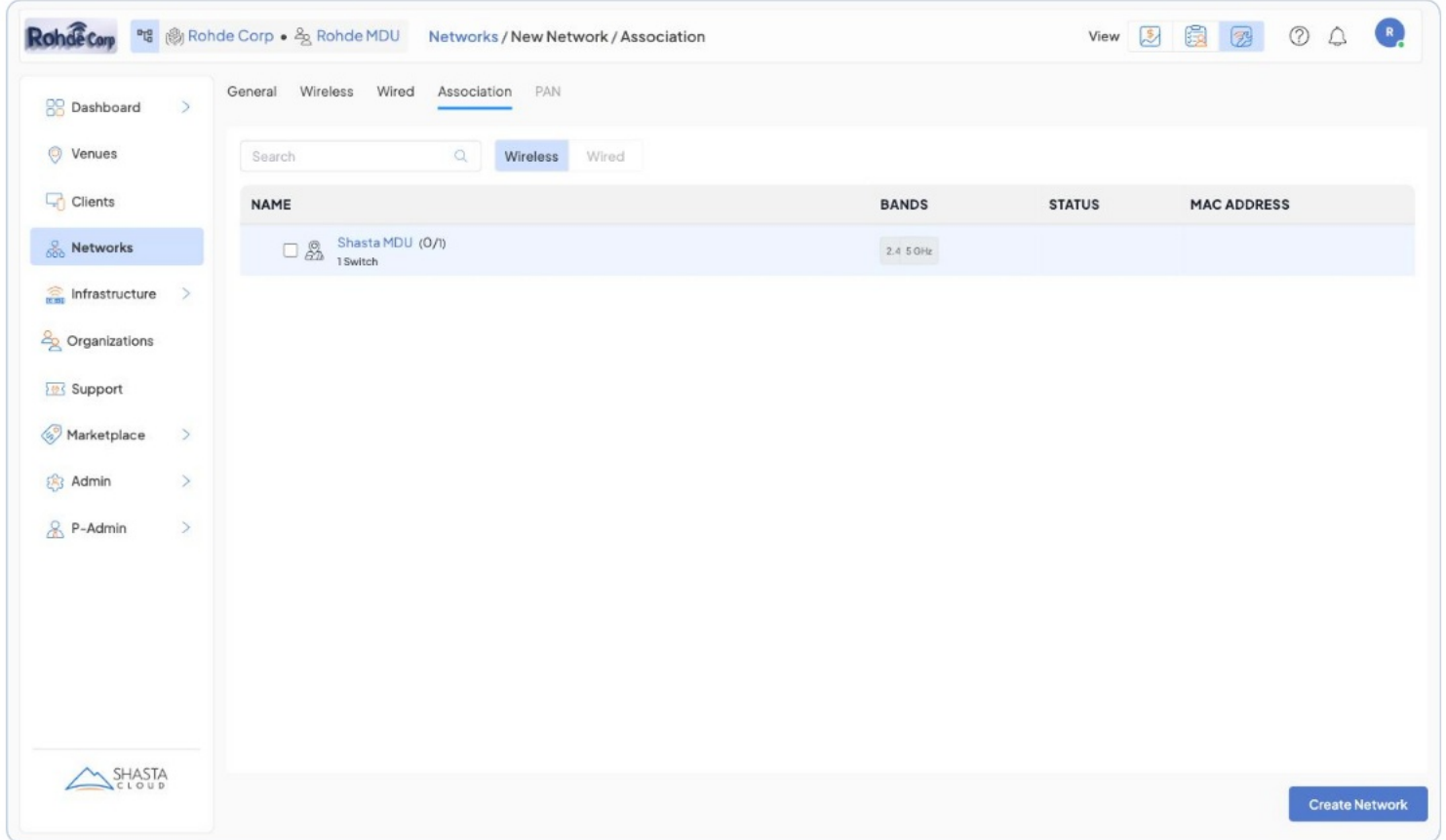


Figure 6 — The Association tab showing available venues with band support information.

The tab presents a list of available venues showing venue name, supported wireless bands (2.4 GHz / 5 GHz), status, and MAC address. Use the **Wireless** or **Wired** sub-tabs to assign to wireless APs or wired switch ports respectively. Check the checkbox next to each venue to assign the network to it. The counter next to the venue name (e.g., 0/1) shows how many APs in that venue have the network applied versus the total.

Tip: You can assign the network to venues before or after creating it. The network can also be re-associated to additional venues at any time from this tab.

Step 6 — Create the Network

Once all tabs are configured, click the **Create Network** button in the bottom-right corner of any tab. The network will be provisioned and you will be redirected to the network's detail view.

Important: The **PAN** tab is not accessible during initial network creation — it becomes available only after the network has been saved. A tooltip will confirm this: *"PAN management will be available after network is created."*

After creation, the network detail view includes additional tabs: **PAN**, **Banned Wireless Clients**, and **P Admin**. The General tab will also display a summary panel showing Wireless Auth, Wired Auth, Ports, and Venues count.

The screenshot displays the Rohde Corp network management interface. The top navigation bar includes the Rohde Corp logo, user information (Rohde Corp, Rohde MDU), and the current page title (Networks / ShastaResident / General). On the right, there are utility icons for View, currency, calendar, help, and notifications, along with a user profile icon.

The left sidebar contains a navigation menu with the following items: Dashboard, Venues, Clients, Networks (highlighted), Infrastructure, Organizations, Support, Marketplace, Admin, and P-Admin.

The main content area is titled "General" and features several tabs: General, Wireless, Wired, Association, PAN, Banned Wireless Clients, and P Admin. A "Last 7 Days" filter and an "Update" button are located in the top right of the main area.

The "Network Details" section on the left shows the following configuration:

- Wireless Auth: MPSK Service
- Wired Auth: Disabled
- Ports: 0
- Venues: 1

To the right of the details is a "Wireless Throughput" chart showing data for the period from April 14 to April 20. The chart displays three metrics: Up Max (orange), Up Avg (yellow), and Up Min (red). The current value is 1.

The main configuration form includes the following fields and options:

- Network Name ***: ShastaResident
- Description**: Enter description
- Network Type ***: Personal Area Network (PAN)
- Trunk VLANs (1-4094)**: 1001-1199
- Access VLAN (1-4094)**: 2000
- Add as AP Uplink (Trunk)
- Add as Fabric (Trunk)

The Shasta Cloud logo is visible in the bottom left corner of the interface.

Figure 7 — A fully created PAN network showing the Network Details summary and all management tabs.

Step 7 — PAN Tab – Managing Individual MPSK Units

After the network is created, navigate to the **PAN** tab to manage individual tenant/unit passphrases. PAN changes are applied automatically and do not require clicking "Update".

PAN ↑	VLAN	EXPIRES ON	STATUS	CONTACT	PHONE NO.	FRIENDLY NAME
Unit-1001	1001	-	Active	Bulbasaur ✉ bulbasaur@shasta.com	-	Bulbasaur
Unit-1002	1002	-	Active	Ivysaur ✉ ivysaur@shasta.com	-	Ivysaur
Unit-1003	1003	-	Active	Venusaur ✉ venusaur@shasta.com	-	Venusaur
Unit-1004	1004	-	Active	Charmander ✉ charmander@shasta.com	-	Charmander
Unit-1005	1005	-	Active	Charmeleon ✉ charmeleon@shasta.com	-	Charmeleon
Unit-1006	1006	-	Active	Charizard ✉ charizard@shasta.com	-	Charizard
Unit-1007	1007	-	Active	Squirtle ✉ squirtle@shasta.com	-	Squirtle
Unit-1008	1008	-	Active	Wartortle ✉ wartortle@shasta.com	-	Wartortle
Unit-1009	1009	-	Active	Blastoise ✉ blastoise@shasta.com	-	Blastoise
Unit-1010	1010	-	Active	Caterpie ✉ caterpie@shasta.com	-	Caterpie
Unit-1011	1011	-	Active	Metapod ✉ metapod@shasta.com	-	Metapod

Figure 8 — The PAN tab showing the list of all active MPSK units with their VLAN assignments, status, and contact details.

The PAN list displays all units with the following columns:

Column	Description
PAN	The unique identifier/name for the unit (e.g., Unit-1001).
VLAN	The specific VLAN assigned to this unit from the trunk VLAN range.
Expires On	Optional expiration date. Displays "-" when no expiration is set.
Status	Current state: Active, Expired, or Disabled. Filter buttons at the top allow filtering by status.
Contact	The unit owner's name and email address.
Phone No.	Contact phone number (optional).
Friendly Name	A display-friendly label for the unit (e.g., resident name).

Adding a PAN Entry (Individual)

Click the **Add** button to open the PAN creation modal.

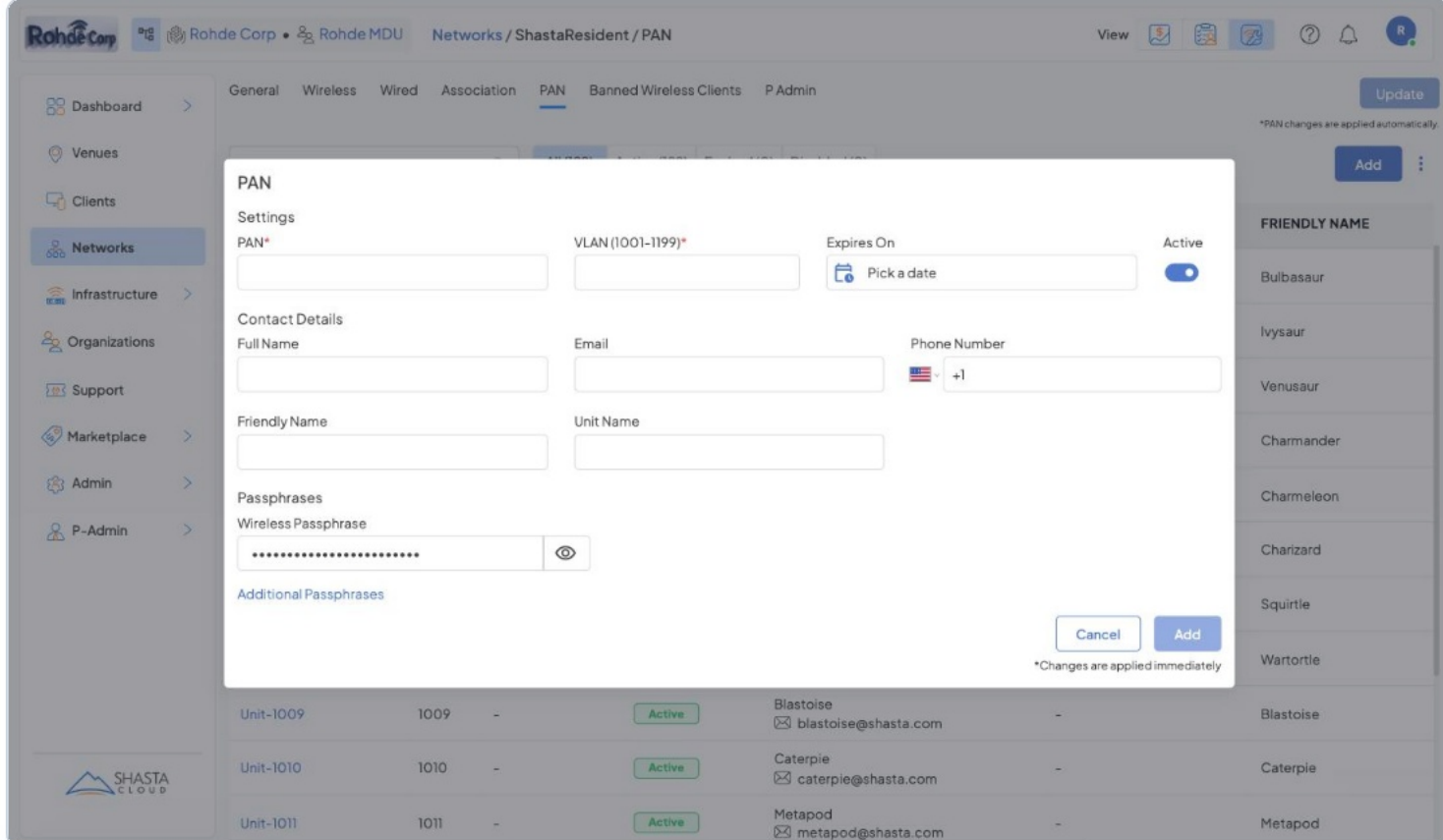


Figure 9 — The Add PAN modal with all configuration fields and an auto-generated wireless passphrase.

Settings

- PAN *Required** — Unique identifier for this unit (e.g., Unit-1001).
- VLAN *Required** — Specific VLAN from the trunk range (e.g., 1001).
- Expires On** — Optional expiration date for this PAN entry.
- Active Toggle** — Enable or disable this unit immediately.

Contact Details

- Full Name** — Resident or unit owner's full name.
- Email** — Contact email address.
- Phone Number** — Contact phone with country code.
- Friendly Name** — Display-friendly label.
- Unit Name** — Physical unit identifier (e.g., Unit 1).

Managing Passphrases

Each PAN unit has a primary **Wireless Passphrase** that is auto-generated when the entry is created. Click the eye icon to reveal the passphrase.

PAN

Settings

PAN* VLAN (1001-1199)* Expires On Active

Contact Details

Full Name Email Phone Number

Friendly Name Unit Name

Passphrases

Wireless Passphrase

Connected Clients: 0

[Additional Passphrases](#)

*Changes are applied immediately

Unit-1009	1009	-	<input checked="" type="checkbox"/> Active	Blastoise ✉ blastoise@shasta.com	-	Blastoise
Unit-1010	1010	-	<input checked="" type="checkbox"/> Active	Caterpie ✉ caterpie@shasta.com	-	Caterpie
Unit-1011	1011	-	<input checked="" type="checkbox"/> Active	Metapod ✉ metapod@shasta.com	-	Metapod

Figure 10 — PAN unit detail showing the auto-generated wireless passphrase, connected clients count, and access to additional passphrases.

Click **Additional Passphrases** to expand the full passphrase management table, which supports multiple passphrases per unit:

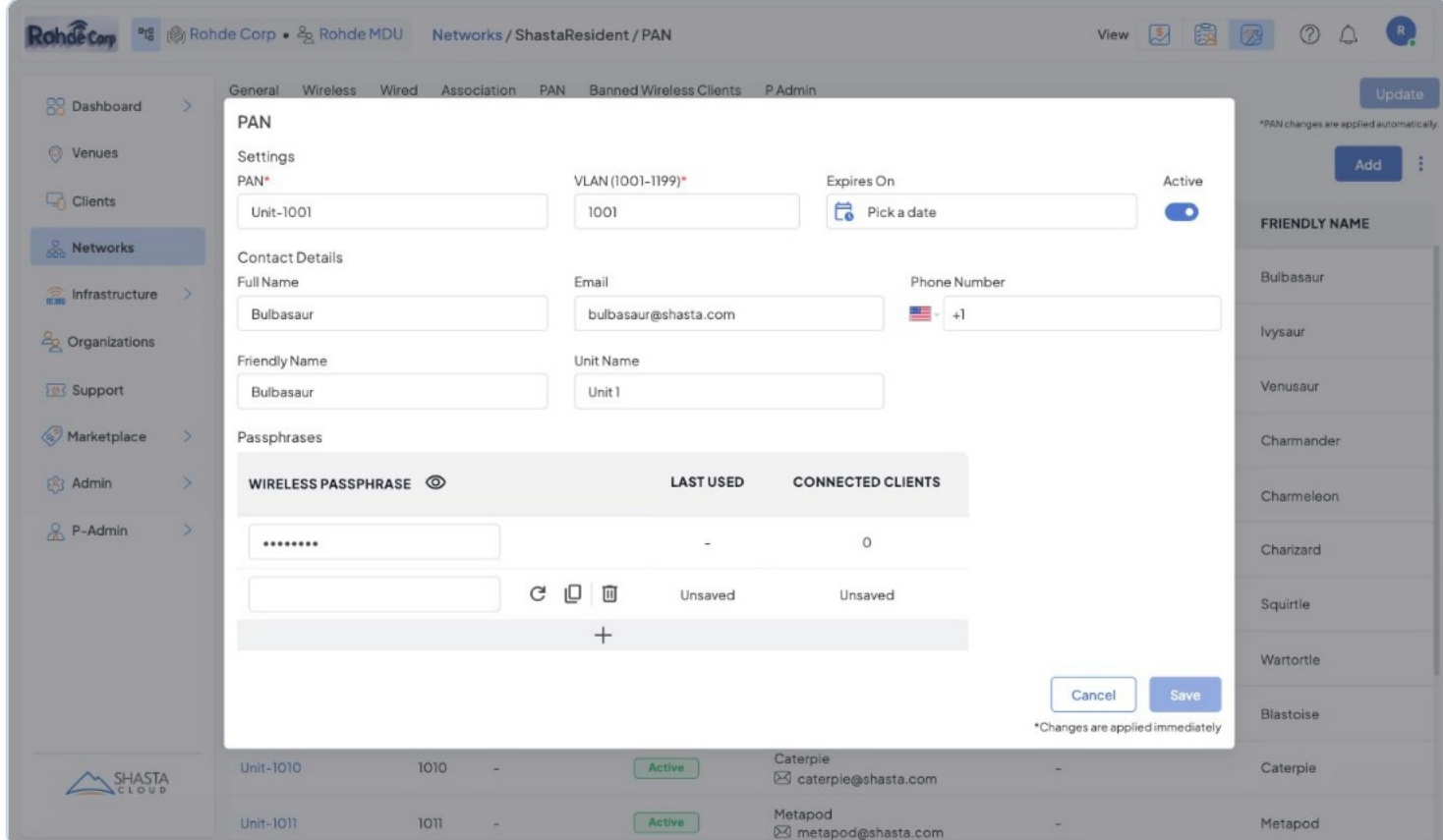


Figure 11 — The expanded passphrase table showing the primary passphrase plus an additional passphrase entry with Last Used and Connected Clients tracking.

Column / Action	Description
Wireless Passphrase	The passphrase string (shown masked). Use the eye icon to reveal.
Last Used	Timestamp of the most recent connection using this passphrase.
Connected Clients	Number of devices currently connected using this passphrase.
Regenerate (↻)	Generate a new random passphrase for this slot.
Copy (📄)	Copy the passphrase to clipboard.
Delete (🗑️)	Remove this additional passphrase entry.
+ Button	Add another passphrase slot. Allows multiple passphrases per unit (e.g., for IoT devices vs. resident devices).

Note: All PAN changes (adding, editing, or deleting entries) are applied immediately. A note at the bottom of each modal confirms: "Changes are applied immediately."

Bulk PAN Management (Import / Export)

Click the three-dot menu (⋮) next to the Add button to access bulk operations:

Figure 12 — The three-dot menu revealing Import and Export options for bulk PAN management.

Import

Bulk-import PAN entries from a file. Ideal for large deployments where many units need to be provisioned simultaneously. Refer to the Shasta Cloud import template for the required file format.

Export

Export the full PAN list to a file for record-keeping, auditing, or migrating unit data to another network or system.

Summary of Key Configuration Values

Setting	Tab	Recommended Value
Network Type	General	Personal Area Network (PAN)
Trunk VLANs	General	e.g., 1001–1199
Access VLAN	General	e.g., 2000
Add as AP Uplink (Trunk)	General	Enabled ✓
Add as Fabric (Trunk)	General	Enabled ✓
Wireless Auth Type	Wireless	MPSK Service
SSID	Wireless	Your chosen network name

802.11k Neighbor Reporting	Wireless	ON
802.11r Roaming	Wireless	ON
Client Steering	Wireless	ON
Client Idle Timeout	Wireless	300 seconds
Rekey Interval	Wireless > Advanced	3600 seconds
Wired Auth Type	Wired	Disabled (wireless-only)
Per-Unit VLAN	PAN Entry	One from the trunk range