MACHFU

Simplifying IoT from edge to enterprise

MACH-3

Installation and Configuration Manual

September 9, 2019

Revision 6.0

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Table of Contents

Revision History

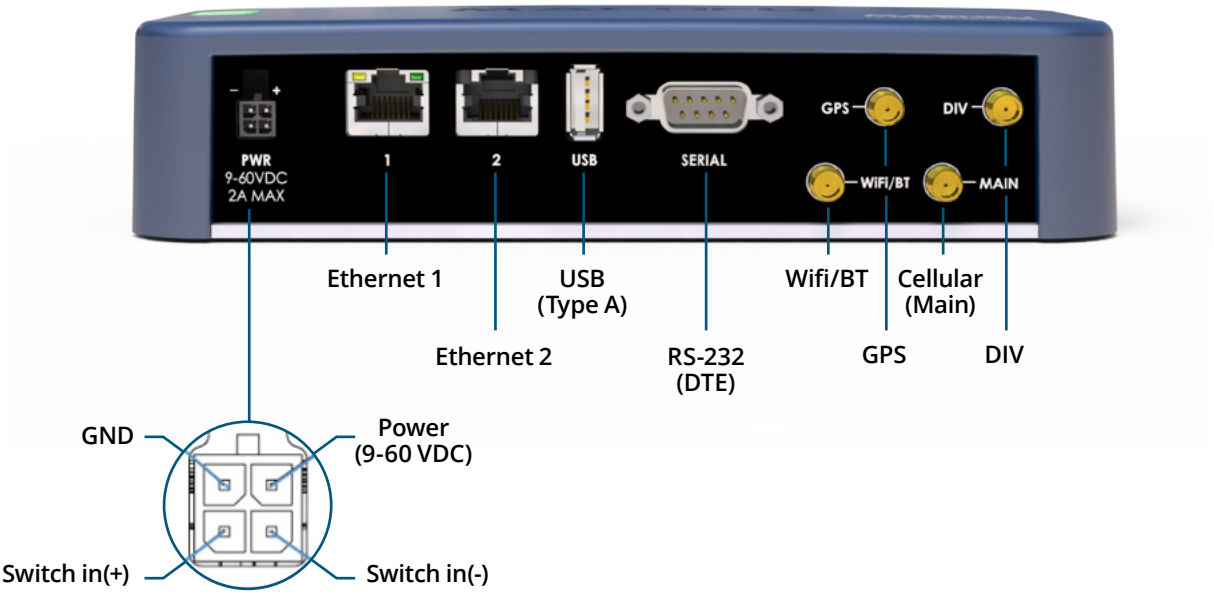
Revision	Description	Date
1.0	**Initial release**	**1/4/2017**
2.0	**Revision**	**1/5/2018**
3.0	**Revision**	**8/1/2018**
4.0	**Revision**	**10/3/2018**
5.0	**Revision**	**1/31/2019**
6.0	**Revision**	**9/9/2019**

1. Overview

The MACH-3 Gateway is an Industrial Internet-of-Things (IIoT) device. It is deployed on the MACH-3 Edge network, enabling you to securely collect, analyze, and act on data from multiple devices and sensors. It enables you to connect with industrial devices used in the electric grid, oil & gas, manufacturing, and other applications. The MACH-3 Gateway has a low-power architecture, which is capable of supporting industrial automation workloads while remaining fan-less for environmental and reliability requirements.

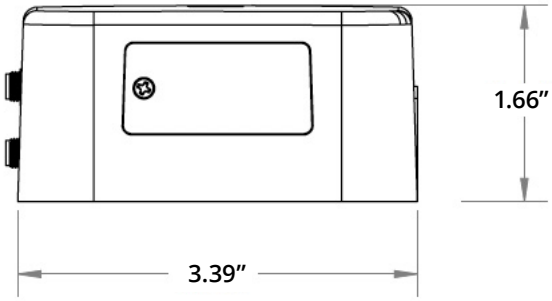
1.1 System Views

1.1.1 Front Panel View

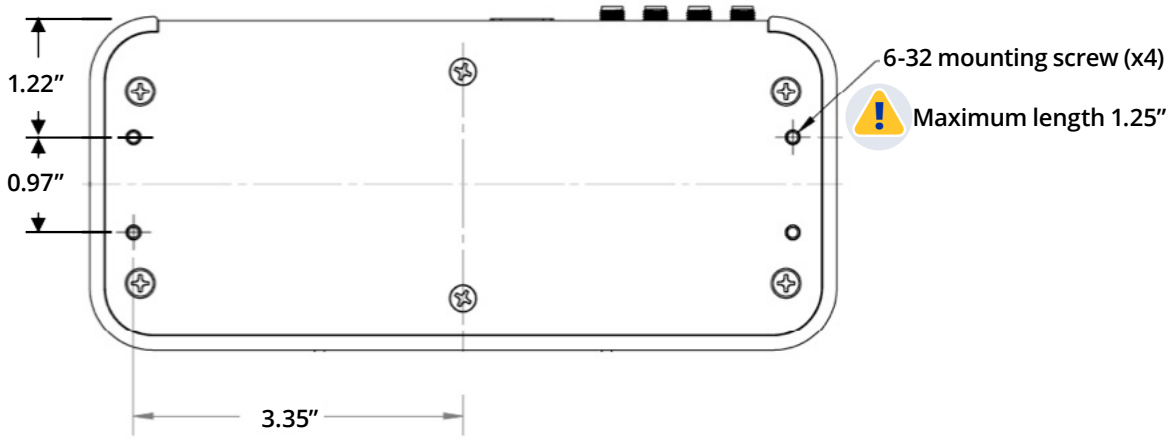


Features			
1	Power Connector	6	Wi-Fi / BT
2	Ethernet 1	7	GPS
3	Ethernet 2	8	Cellular (Main)
4	USB	9	Cellular (Diversity)
5	RS-232		

1.1.2 Right Side SIM Door View



1.1.3 Bottom View



2. Installing your MACH-3 Gateway

WARNING: Before you begin any of the procedures in this section, read the **safety and regulatory information** that is shipped with your system. For additional best practices information, go to **www.machfu.com/regulatory_compliance**.

WARNING: The MACH-3 Gateway must be installed by knowledgeable and skilled personnel familiar with local and/or international electrical statutes and regulations.

WARNING: The MACH-3 Gateway is not designed for use in wet environments. If the MACH-3 Gateway is to be installed in a wet environment, depending on the location and environment, it must be installed in a panel box or enclosure with an Ingress Protection (IP) rating of IP54, IP65, or higher.

WARNING: To reduce the risk of electric shock, power to the DC+ and DC- terminals must be provided by a power supply or transformer/rectifier circuit that is designed with double-insulation. The power supply or power circuit source must comply with local codes and regulations; for example, in the USA, NEC Class 2 (SELV/limited energy circuit, or LPS circuitry). If powered by a battery, double-insulation is not required.

WARNING: Ensure that the power source providing power to the MACH-3 Gateway is reliably grounded and filtered such that the peak-to-peak ripple component is less than 10 percent of the input DC voltage.

WARNING: When installing the MACH-3 Gateway, use a cable appropriate for the load currents: 3-core cable rated 5 A at 90°C (194°F) minimum, which conform to either IEC 60227 or IEC 60245. The system accepts cables from 0.8 mm to 2 mm. The maximum operating temperature of the MACH-3 Gateway is 80°C (176 °F). Do not exceed this maximum temperature while operating the MACH-3 Gateway inside an enclosure. Internal heating of the MACH-3 Gateway electronics, other electronics, and the lack of ventilation inside an enclosure can cause the operating temperature of the MACH-3 Gateway to be greater than the outside ambient temperature. Continuous operation of the MACH-3 Gateway at temperatures greater than 80°C(176°F) may result in an increased failure rate and a reduction of the product life. Ensure that the maximum operating temperature of the MACH-3 Gateway when placed inside an enclosure is 80°C (176 °F) or less.

WARNING: The ⚠ symbol indicates hot surface or adjacent hot surface that can cause a burn. Allow equipment to cool or use protective gloves when handling to reduce risk of a burn.

WARNING: Always ensure that the available power source matches the required input power of the MACH-3 Gateway. Check the input power markings next to power connector(s) before making connections. The 9-60 VDC power source must be compliant with local Electrical Codes and Regulations.

WARNING: To ensure the protection provided by the MACH-3 Gateway is not impaired, do not use or install the system in any manner other than what is specified in this manual.

WARNING: If a battery is included as part of the system or network, the battery must be installed within an appropriate enclosure in accordance with local fire and electrical codes and laws.

WARNING: The system is for installation in a suitable industrial enclosure with tool-removable cover or door only.

WARNING: The system is for installation in Class I, Division 2, Groups A, B, C, D hazardous locations or non-hazardous locations only.

WARNING: EXPLOSION HAZARD: DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN ENERGIZED. Perform connections or disconnections to equipment only when not energized or the area is known to be non-hazardous.

2.1 Professional Installation Instructions

2.1.1 Installation Personnel

This product is designed for specific applications and needs to be installed by qualified personnel with RF and regulatory-related knowledge. The general user shall not attempt to install or change the settings.

2.1.2 Installation Location

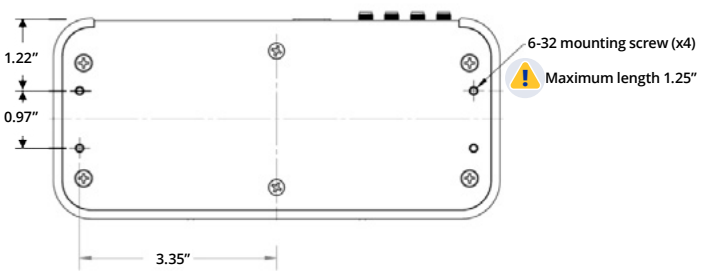
The product shall be installed at a location where the radiating antenna is kept 20 cm from nearby people in its normal operation condition in order to meet regulatory RF exposure requirements.

2.1.3 External Antenna

Use only approved antennae. Non-approved antennae may produce spurious or excessive RF transmitting power which may lead to a violation of FCC/IC limits.

2.2 Gateway Mounting Options

2.2.1 Bottom Mount



2.2.2 Din-Rail Mount

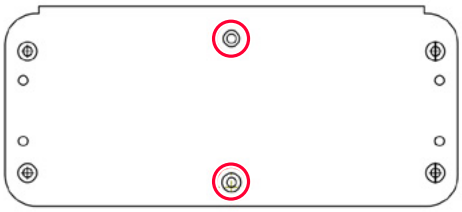
Note: MACH-3 Din-Rail mounting option sold separately

2.2.3 Mounting Plate

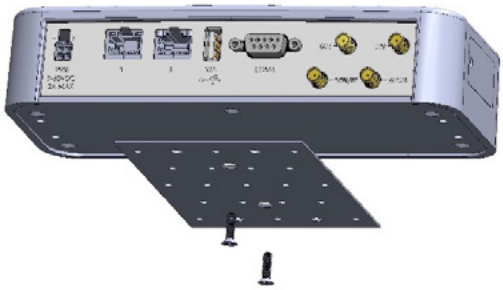
Note: MACH-3 Mounting Plate option sold separately

2.2.3.1 Mounting Instructions

1. Remove the two center screws from the base plate of the Machfu gateway. (marked with a red circle in the picture below.)



2. Align the mounting plate's counter screw holes with the center screw holes on the base plate of the gateway and screw them together as indicated in the picture below.



3. Mount the gateway into your unit using the exposed screw holes available on the mounting plate.

2.3 Setting up MACH-3 Gateway

1. Connect an Ethernet RJ45 cable to Ethernet 1 as shown in Figure 1: Front Panel View.
2. Connect antennae as shown in Figure 1: Front Panel View using antennae that meet the minimum configuration specified in the Appendix on page 44.
3. Open the micro-SIM/micro-SD card access door and insert the micro-SIM card in the SIM-Card slot as shown in Figure 2: SIM Card Installation before turning on the MACH-3 gateway.
4. The gateway power connector is a Molex Microfit 3.0 four pin connector wired as shown in Figure 3. The four pin connector accepts a 9 - 60 VDC power supply input and a contact closure input.

   Pin 1: Contact Input common
   Pin: 2 Contact Input
   Pin: 3 Power (9- 60 VDC)
   Pin: 4 Ground

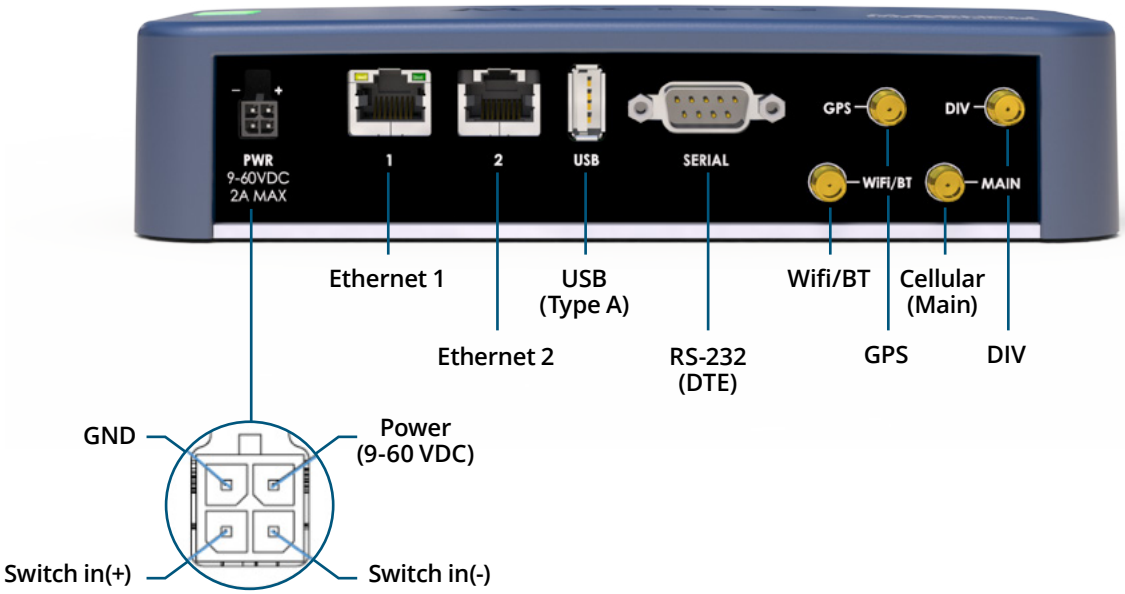
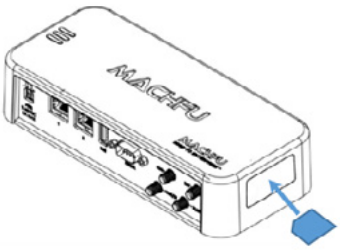
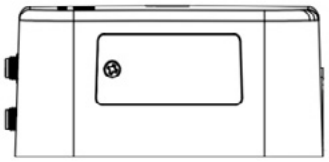


Figure 1: Front Panel View

Unscrew and remove the SIM door.



Slide SIM card into holder through opening and push until latch clicks. To remove push again until latch disengages, and slide SIM card out.



Replace and screw in the SIM door.

Figure 2: SIM Card Installation

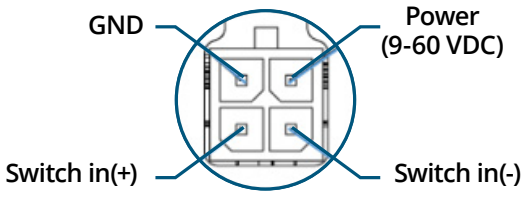


Figure 3: Power connector pinout

3. Gateway Configuration

3.1 Overview

The MACH Gateway Configuration Tool is used to configure MACH-3 Gateway products. This User Guide describes how the tool can be used to configure and set various parameters in the gateway for optimizing your Industrial Internet-of-Things Network and Application.

3.1.1 System Requirements

- Microsoft Windows 7, Windows 8;
- Linux; or
- Mac OS X
- Web Browser:
  - Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 11 (or above)

3.1.2 Log in

To access the MACH Gateway Configuration Interface, perform the following steps:

1. Launch your web browser.
2. Enter https://192.168.1.1:8443 in the address field.
3. Press Enter (PC) or Return (Mac).

The Login screen appears as below.

Enter the Username and Password fields and click the 'Login' button.

3.1.3 Navigation

The Mach Gateway Configuration Interface contains six main tabs, seen in the navigation bar on the left side of the interface. Each tab may contain multiple sections and each web-based management page is used to configure a specific aspect of the Gateway.

DASHBOARD is a synopsis of all the network configuration, and state elements of the Gateway. It displays device information such as name and serial number, and the current state of physical and virtual network interfaces. In addition, it displays the GPS information of the device. Page 9 provides details on the DASHBOARD configuration page.

WIRELESS configures operating mode of the cellular and the two Wi-Fi interfaces. Page 14 provides details on the WIRELESS configuration pages.

WIRED configures the operating mode of the two Ethernet interfaces; and the Serial Terminal settings. Page 19 provides details on the WIRED configuration pages.

NETWORK configures system management services: Bridge, VPN, Port Forwarding, SNAT, Routing, Diagnostics. Page 23 provides details on the NETWORK configuration pages.

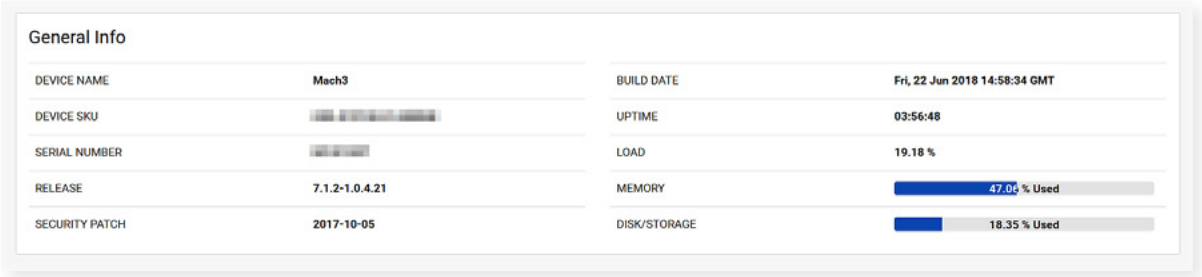
SETTINGS handles the user and password management of the MACH Gateway. Page 31 provides details on the SETTINGS configuration pages.

SYSTEM handles system upgrade, device reboot, remote support setting and applications management. Page 24 provides details on the SYSTEM configuration pages.

3.2 Dashboard

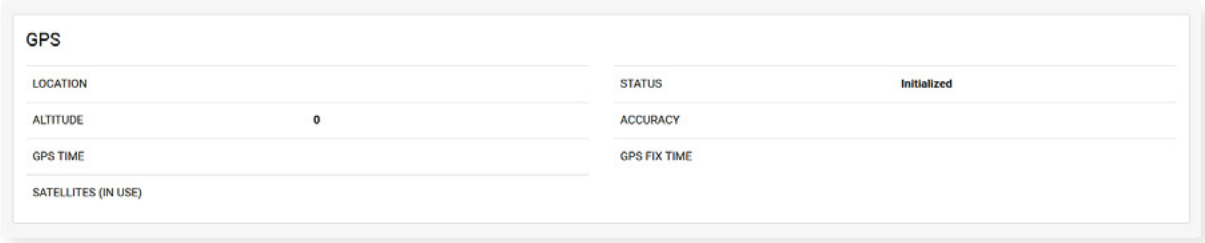
DASHBOARD is a synopsis of all the network configuration, and state elements of the Gateway. It provides a high-level view of the device and network interfaces as well as the GPS information.

3.2.1 General Information



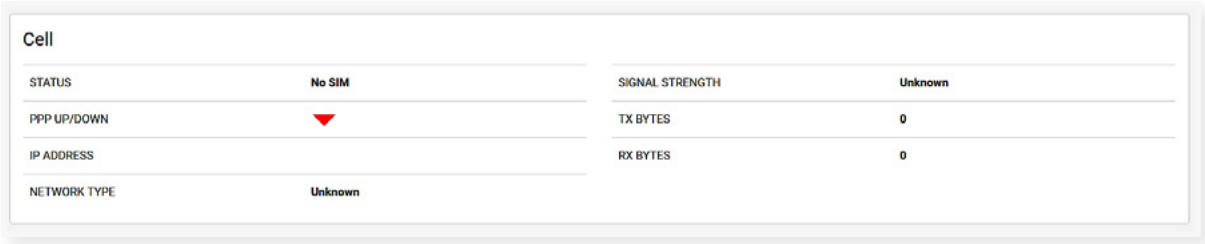
- **Device name** – Classification of the MACH Gateway.
- **Device SKU** – Stock Keeping unit of the Gateway.
- **Serial number** – Unique serial number of the Gateway. Filled by the Gateway.
- **Release** – Current version number of system image.
- **Security Patch** – Date of the last security patch update.
- **Build Date** – Date of the last system build.
- **Uptime** – Time elapsed since the last boot-up. It is shown in days, hours, minutes and seconds.
- **Load** – CPU usage of the Gateway.
- **Memory** – Memory currently used in the Gateway.
- **Disk/Storage** – Storage available for Applications in the Gateway.

3.2.2 GPS



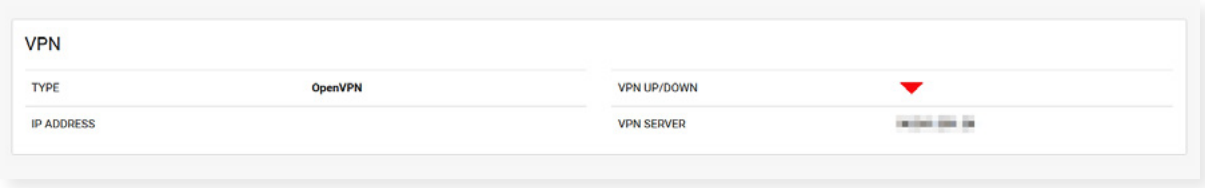
- **Location** – Latitude/Longitude of the Gateway.
- **Altitude** – Altitude of the Gateway.
- **GPS Time** – UTC time as received by GPS.
- **Satellites (In Use)** – Number of GPS satellites in use by the Gateway.
- **Accuracy** – GPS readings accuracy.
- **GPS Fix Time** – Last fix from the GPS satellites.

3.2.3 Cellular Information



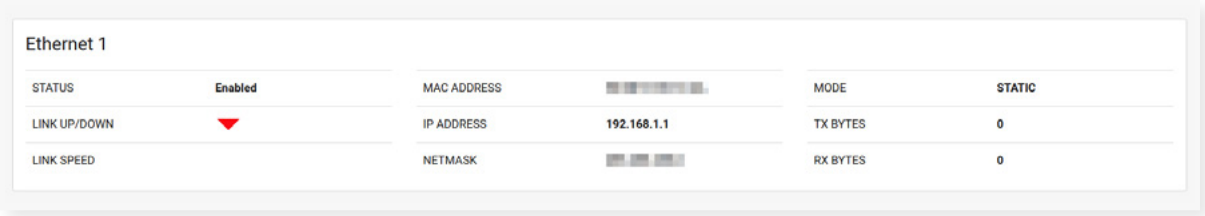
- **Status** – Indicates if the Cellular link is Enabled or Disabled.
- **PPP UP/DOWN** – Indicates if the Cellular link is UP or DOWN.
- **IP Address** – IP address of the PPP link.
- **Network Type** – Type of Cellular network.
- **Signal Strength** – Signal strength of the cellular link in dBm.
- **Tx Bytes** – Number of bytes transmitted since boot-up.
- **Rx Bytes** – Number of bytes received since boot-up.

3.2.4 VPN



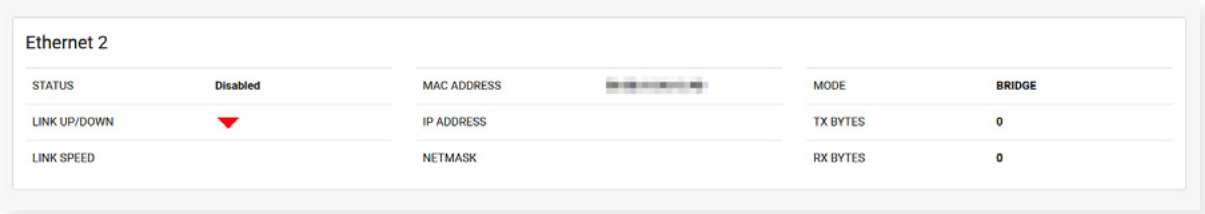
- **Type** – Type of VPN connection.
- **IP Address** – IP address of VPN connection.
- **VPN UP/DOWN** – Indicates if VPN connection is UP or DOWN.
- **VPN Server** – IP address of VPN server.

3.2.5 Ethernet 1



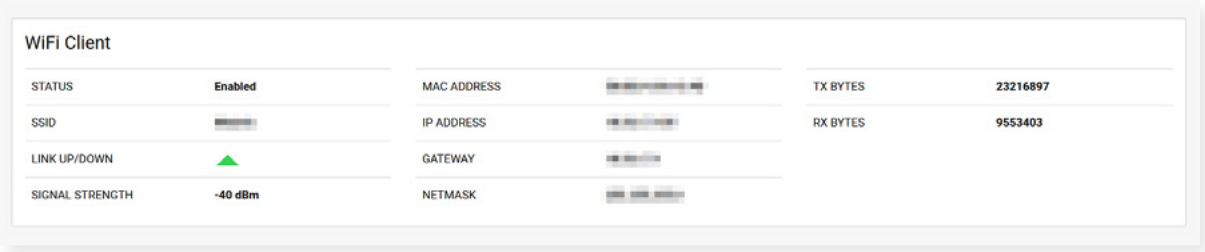
- **Status** – Indicates if the Ethernet connection is Enabled or Disabled.
- **Link UP/DOWN** – Indicates if the Ethernet link is UP or DOWN.
- **Link Speed** – Data rate on the Ethernet 1 (eth0) Interface.
- **MAC Address** – MAC address of the Ethernet link.
- **IP Address** – IP address of the Ethernet link.
- **Netmask** – Subnet definition.
- **Mode** – Indicates if the connection mode is STATIC, DHCP Client or Bridge.
- **Tx Bytes** – Number of bytes transmitted since boot-up.
- **Rx Bytes** – Number of bytes received since boot-up.

3.2.6 Ethernet 2



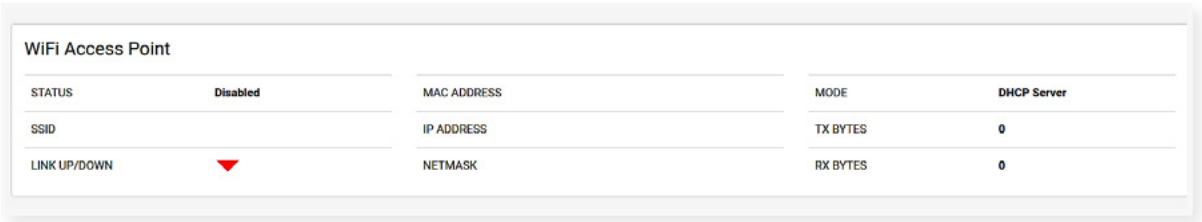
- **Status** – Indicates if the Ethernet connection is Enabled or Disabled.
- **Link UP/DOWN** – Indicates if the Ethernet link is UP or DOWN.
- **Link Speed** – Data rate on the Ethernet 2 (eth1) Interface.
- **MAC Address** – MAC address of the Ethernet link.
- **IP Address** – IP address of the Ethernet link.
- **Netmask** – Subnet definition.
- **Mode** – Indicates if the Ethernet is acting as STATIC IP, DHCP Server or Bridge.
- **Tx Bytes** – Number of bytes transmitted since boot-up.
- **Rx Bytes** – Number of bytes received since boot-up.

3.2.7 Wi-Fi Client



- **Status** – Indicates if the Wi-Fi client or station is Enabled or Disabled.
- **SSID** – Specifies the wireless network name or SSID (Service Set Identifier) used to identify the WLAN.
- **Link UP/DOWN** – Indicates if the Wi-Fi link is UP or DOWN.
- **MAC Address** – MAC address of the Wi-Fi link.
- **IP Address** – The IP address of the Wi-Fi link.
- **Gateway** – IP Address of the Gateway.
- **Netmask** – Subnet definition.
- **Tx Bytes** – Number of bytes transmitted since boot-up.
- **Rx Bytes** – Number of bytes received since boot-up.

3.2.8 Wi-Fi Access Point

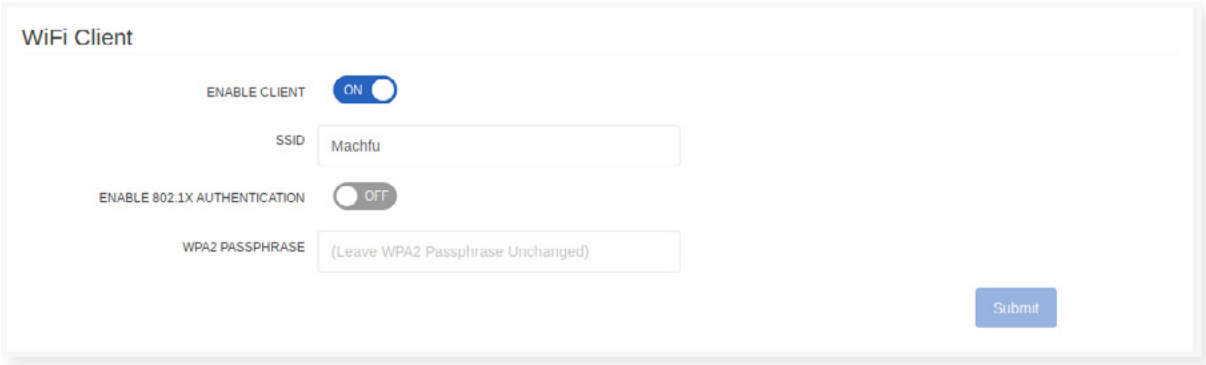


- **Status** – Indicates if the Wi-Fi Access Point is Enabled or Disabled.
- **SSID** – Specifies the wireless network name or SSID (Service Set Identifier) used to identify the WLAN.
- **Link UP/DOWN** – Indicates if the Wi-Fi link is UP or DOWN.
- **MAC Address** – MAC Address of the Wi-Fi Access Point.
- **IP Address** – IP Address of the Wi-Fi Access Point.
- **Netmask** – Subnet definition.
- **Mode** – Indicates if the AP is acting as DHCP Server or Bridge.
- **Tx Bytes** – Number of bytes transmitted since boot-up.
- **Rx Bytes** – Number of bytes received since boot-up.

3.3 Wireless Interfaces

The wireless interface configurations are used to configure the Wi-Fi and Cellular radios on the MACH Gateway.

3.3.1 Wi-Fi Client



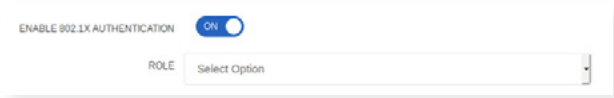
In the Client mode, the following configurations are seen

- Set the 'Enable' button to use the Wi-Fi in the Client mode.
- SSID – Specify the wireless network name or SSID (Service Set Identifier) used to identify the WLAN.
- Enter the WPA2 Passphrase.

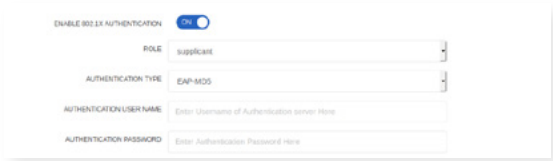
3.3.1.1 Enterprise Network Authentication

802.1X Authentication: Set the web toggle switch for 802.1X Authentication to 'ON' to enable enterprise network authentication between the Supplicant and the Authenticator depending on the Role selected. When this authentication is enabled, two new sub fields appear in this page as shown in the Figure below.

Role: For 'Wifi Client' ONLY Supplicant role is applicable.

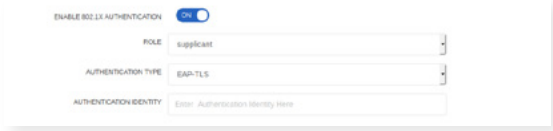


- Select the appropriate Authentication Type from the Authentication Type drop down menu.
- If you choose MDS as the Authentication Type:
- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.



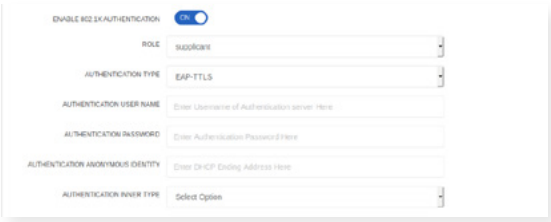
If you choose TLS as the Authentication Type:

- Enter the Authentication Identity in the Authentication Identity dialog box.



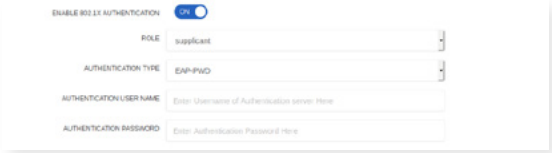
If you choose TTLS as the Authentication Type:

- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.
- Enter the Authentication Identity in the Authentication Anonymous Identity dialog box.
- Select the required Authentication Inner Type from the Authentication Inner Type drop down menu.



If you choose PWD as the Authentication Type:

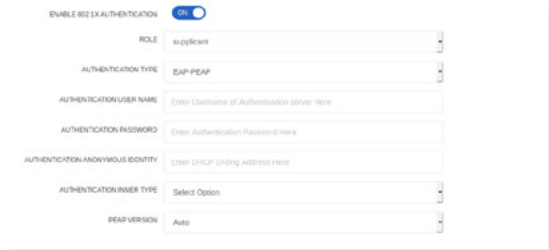
- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.



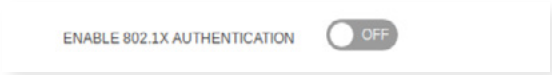
If you choose PEAP as the Authentication Type:

- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.

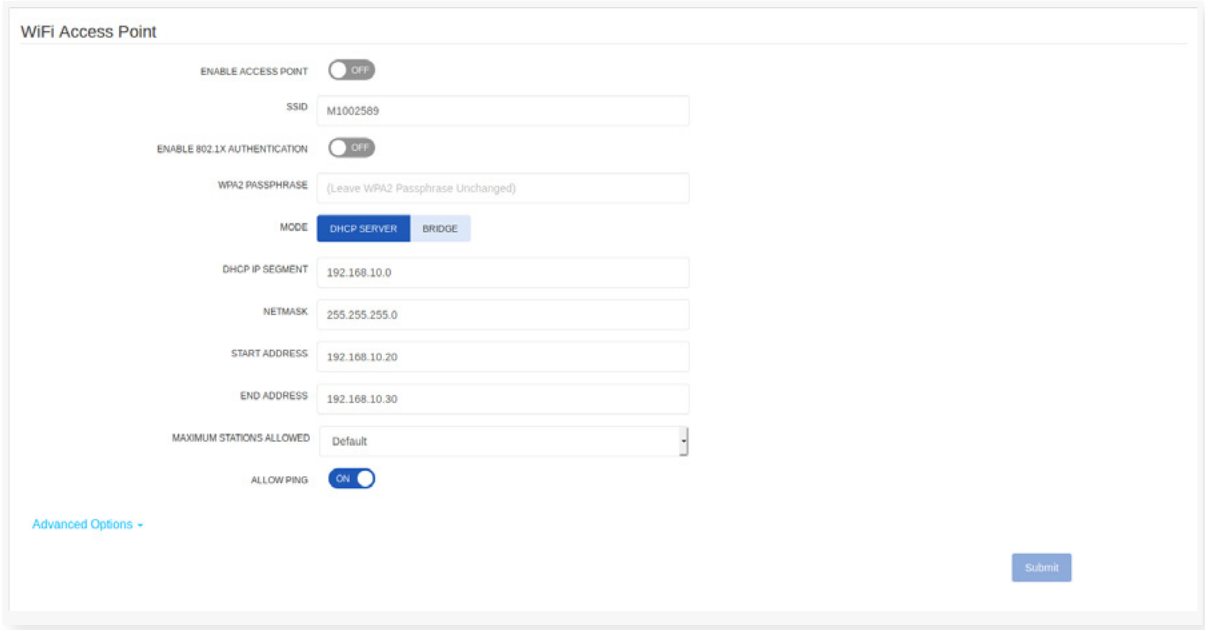
- Enter the Authentication Identity in the Authentication Anonymous Identity dialog box.
- Select the required Authentication Inner Type from the Authentication Inner Type drop down menu.
- Select the appropriate PEAP version from the PEAP version drop down menu.



802.1X Authentication: Set the web toggle switch for 802.1X Authentication to OFF to disable enterprise network authentication between the Supplicant and the Authenticator depending on the Role selected.



3.3.2 Wi-Fi Access Point



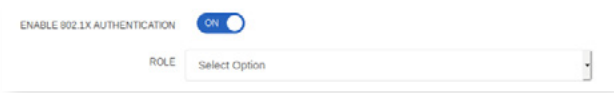
In the Access Point mode, the following configuration panel is seen.

- Set the 'Enable' button to use the Wi-Fi in the access point mode
- SSID – Specify the wireless network name or SSID (Service Set Identifier) used to identify the WLAN
- Set the 'Broadcast SSID' button if you want the SSID to be visible
- Enter the WPA2 passphrase
- Set the 'Mode' to DHCP SERVER or BRIDGE
- Enter IP address
- Enter Netmask value
- Enter the DHCP range of values
- Set 'Allow Ping' if you want the AP to be ping-enabled

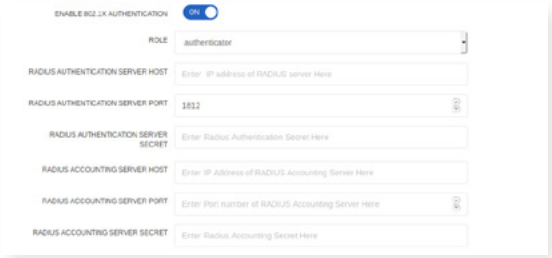
3.3.2.1 Enterprise Network Authentication

802.1X Authentication: Set the web toggle switch for 802.1X Authentication to 'ON' to enable enterprise network authentication between the Supplicant and the Authenticator depending on the Role selected. When this authentication is enabled, two new sub fields appear in this page as shown in the Figure below.

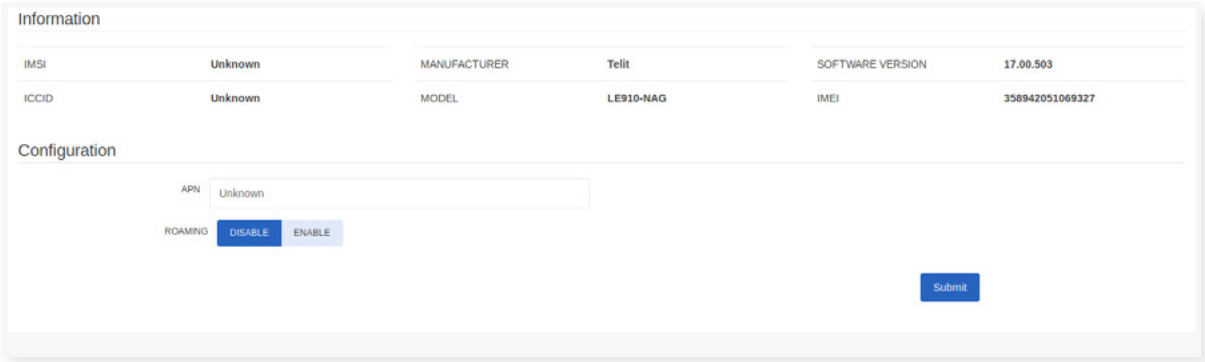
Role: For 'Wifi Access point' ONLY Authenticator role is applicable.



- Enter the IP address of the Radius Server in the Radius Authentication Server Host IP dialog box.
- Enter the port number in the Radius Authentication Server Port dialog box.
- Enter the Authentication Secret in the Radius Authentication Server Secret dialog box.
- Enter the IP Address of the Accounting server in the Radius Accounting Server Host dialog box.
- Enter the Port Number of the Radius Accounting Server Port dialog box.
- Enter the Radius Accounting Secret in the Radius Accounting Server Secret dialog box.



3.3.3 Cellular



In the Cellular section, the following information is seen.

- **IMSI** – The International Mobile Subscriber Identity (IMSI) identifies the user of the cellular network.
- **ICCID** – The Integrated Circuit Card Identifier (ICCID) is a 19-digit identification number for SIM.
- **Manufacturer** – The manufacturer of cellular modem in the MACH Gateway.
- **Model** – The model of cellular modem in the MACH Gateway.
- **Software Version** – The version number of the cellular modem software.
- **IMEI** – The International Mobile Equipment Identity (IMEI).

The following configuration can be seen

- Set the 'APN' of the cellular SIM.
- Set cellular 'Operator' (for select models).

In most Geographical locations within the United States AT&T and Verizon will have primary coverage, hence Machfu Gateway when provisioned with a SIM card from either network carriers will NOT be subject to Roaming conditions. When SIM cards from other carriers, say T-Mobile are used it is generally a good idea to enable Roaming while configuring the Machfu Gateway.

NOTE: The data connectivity under roaming conditions is subject to the policy of the primary carrier in that region and for certain locations may not always be reliable.

- Set Roaming to 'ON' to enable cellular Data Roaming on the Cellular page.
- Set Roaming to 'OFF' to disable Cellular Data Roaming on the Cellular page. By default, it is disabled.
- Click the submit button when you're done configuring on this page.

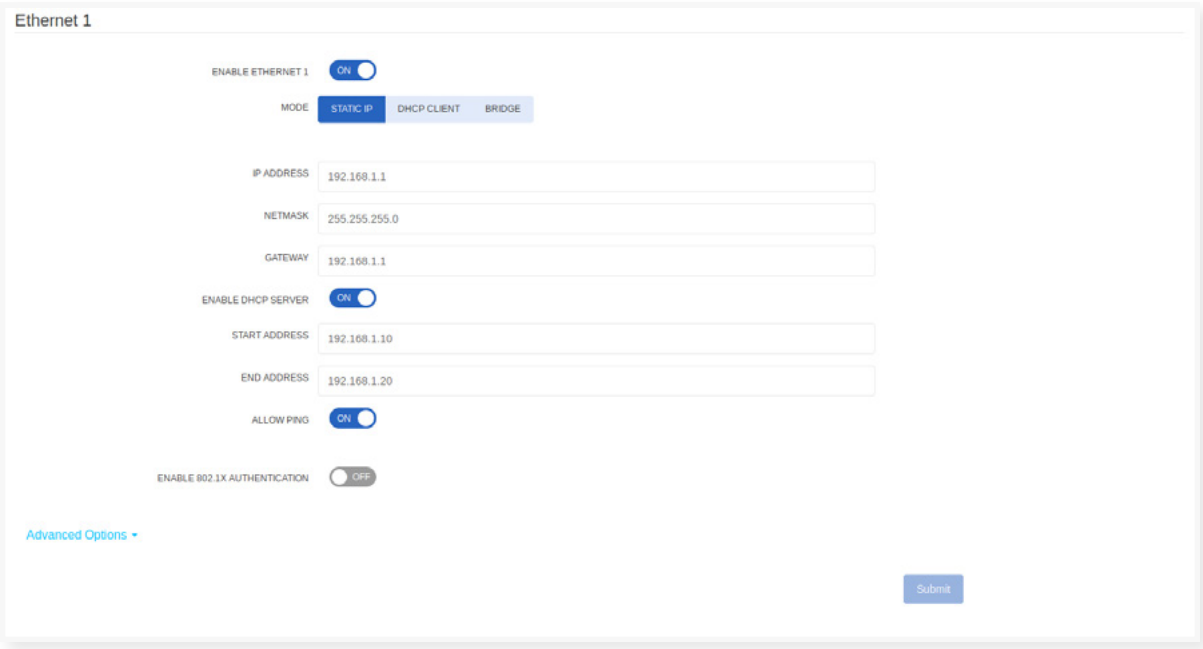
3.4 Wired Interfaces

The MACH Gateway has two wired interfaces: Ethernet and Serial. However, the Ethernet has two ports: Ethernet 1 (eth0) and Ethernet 2 (eth1). To configure Ethernet or Serial interface, click the WIRED Tab on the left panel.

3.4.1 Ethernet

The two Ethernet ports have identical configuration elements. The help guide applies to both ports.

You have the option of enabling or disabling an Ethernet interface even if the interface is physically connected. To Enable, set Enable Ethernet switch to 'ON' and to disable, set it to 'OFF'.



3.4.1.1 IP Addressing

If the Gateway has a static IP address, select 'STATIC IP' and enter the address in the IP address dialog box. If the Gateway is assigned dynamic addresses, then select 'DHCP Client' and the Gateway address dialog box will be automatically filled.

3.4.1.2 NETMASK Address

Fill in the NETMASK address in the NETMASK address dialog box. If the Gateway is assigned dynamic addresses, then the NETMASK address dialog box will be automatically filled.

3.4.1.3 DHCP Server

The DHCP server can be enabled or disabled. Set the web toggle switch for 'Enable DHCP Server' to 'ON' to enable DHCP server and set it to 'OFF' to disable the server. If the server is enabled, you may fill in the start address and the end address of the DHCP server.

3.4.1.4 PING

Set the web toggle switch for 'Allow Ping' to 'ON' to allow ping and set it to 'OFF' to disallow ping.

3.4.1.5 Enterprise Network Authentication

802.1X Authentication: Set the web toggle switch for 802.1X Authentication to 'ON' to enable enterprise network authentication between the Supplicant and the Authenticator depending on the Role selected. When this authentication is enabled, two new sub fields appear in this page as shown in the Figure below.

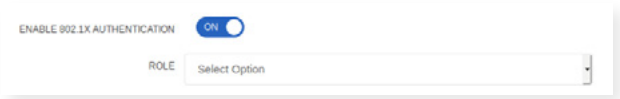
Role: Select the appropriate Role between Supplicant and Authenticator from the Role drop down menu.

For 'Ethernet 1' or 'Ethernet 2' both supplicant and authenticator roles are applicable.

HINT: For WAN ethernet, most probably the role is to be a Supplicant.

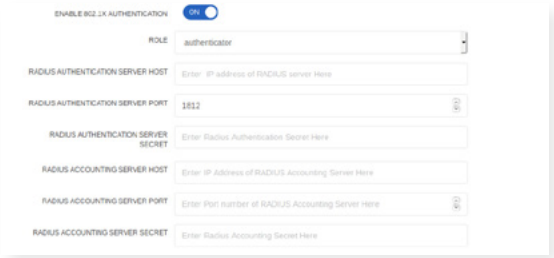
HINT: For LAN ethernet, most probably the role is to be an Authenticator.

Authentication Type: Select the appropriate Authentication Type from the Authentication Type drop down menu.



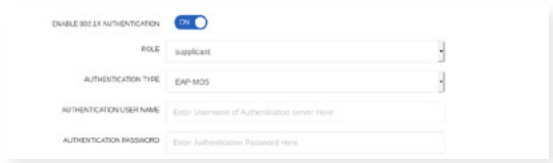
If you choose the Authenticator Role:

- Enter the IP address of the Radius Server in the Radius Authentication Server Host IP dialog box.
- Enter the port number in the Radius Authentication Server Port dialog box.
- Enter the Authentication Secret in the Radius Authentication Server Secret dialog box.
- Enter the IP Address of the Accounting server in the Radius Accounting Server Host dialog box.
- Enter the Port Number of the Radius Accounting Server Port dialog box.
- Enter the Radius Accounting Secret in the Radius Accounting Server Secret dialog box.



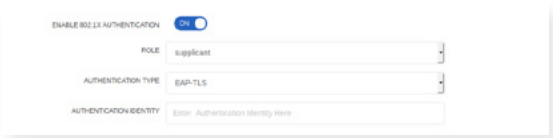
If you choose the Supplicant Role:

- Select the appropriate Authentication Type from the Authentication Type drop down menu. If you choose MDS as the Authentication Type:
- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.



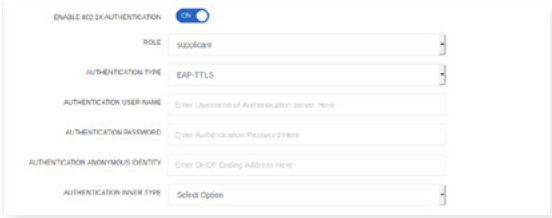
If you choose TLS as the Authentication Type:

- Enter the Authentication Identity in the Authentication Identity dialog box.



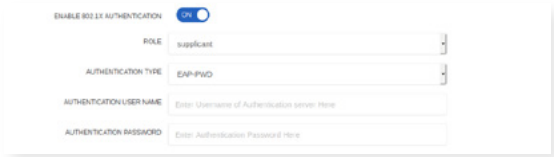
If you choose TTLS as the Authentication Type:

- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.
- Enter the Authentication Identity in the Authentication Anonymous Identity dialog box.
- Select the required Authentication Inner Type from the Authentication Inner Type drop down menu.



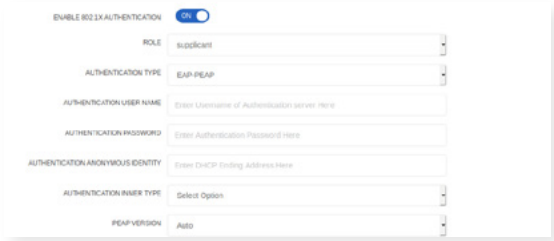
If you choose PWD as the Authentication Type:

- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.

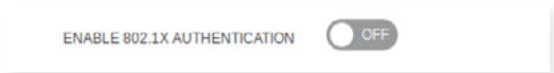


If you choose PEAP as the Authentication Type:

- Enter the Username of the Authentication server in the Authentication User Name dialog box.
- Enter the Password in the Authentication Password dialog box.
- Enter the Authentication Identity in the Authentication Anonymous Identity dialog box.
- Select the required Authentication Inner Type from the Authentication Inner Type drop down menu.
- Select the appropriate PEAP version from the PEAP version drop down menu.



802.1X Authentication: Set the web toggle switch for 802.1X Authentication to 'OFF' to disable enterprise network authentication between the Supplicant and the Authenticator depending on the Role selected.



3.4.1.6 BRIDGE

Bridge is a logical device used to connect different physical or virtual network interfaces (bridge ports). If the Ethernet interface is used to bridge data coming over the interface to other communication means such as Wi-Fi etc., select the 'BRIDGE' in the MODE dialog box. There is no IP address associated in this mode of operation.

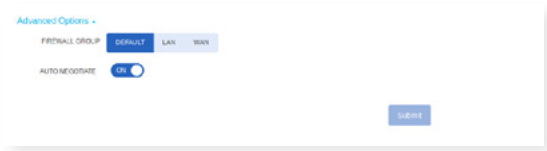
3.4.1.7 Firewall Group

Under 'Advanced Options', select any of the three options given for 'Firewall Group'

3.4.1.8 Auto Negotiate

A procedure used by Ethernet in which two connected networking devices determine common data transmission parameters such as speed, duplex mode and flow control. Initially, both the connected devices share their transmission capabilities and then choose the highest performance transmission mode they both support.

Under Advanced Options, "The Auto Negotiate" feature can be enabled or disabled. Set the web toggle switch for 'Auto Negotiate' to 'ON' to enable Auto Negotiate and set it to 'OFF' to disable the option. Typically one should keep the Auto Negotiate 'ON'.



If the Auto Negotiate web toggle switch is off, the user is allowed to manually configure the transmission parameters(Full Duplex and Speed)based on the capabilities of the equipment, as shown below:

3.4.2 Serial

The serial terminal server can be enabled or disabled. Set the ENABLE TERMINAL SERVER switch to 'ON' to enable the terminal server and set it to 'OFF' to disable it. The other configuration parameters include protocol, server port, baud rate, data frame size, parity, stop frame size and flow control.

3.4.2.1 Protocol

The protocol selected for the serial connection can be TCP/UDP. Set the PROTOCOL switch to 'TCP' to select the TCP protocol or set it to 'UDP' to select the UDP protocol.

3.4.2.2 Server Port

Fill in the port number of the terminal server in the SERVER PORT dialog box.

3.4.2.3 Baud Rate

Fill in the preferred rate of data transfer for the serial connection in the BAUDRATE dialog box.

3.4.2.4 Data Bits

The data size of a character can be 7 or 8 bits. Set the DATA BITS switch to '7' to select 7 bits as the size of each character or set it to '8' to select 8 bits as the size of each character.

3.4.2.5 Parity

Parity is used for error detection in data transfer and a parity bit is added to each character to achieve this. This bit can be None, Odd or Even. Set the PARITY switch to 'NONE' for no parity or set it to 'ODD' to send an odd parity bit or set it to 'EVEN' to send an even parity bit.

3.4.2.6 Stop Bits

The stop bits are used to signify the end of data character and can be one bit or two bits. Set the STOP BITS switch to '1' to send one stop bit or set it to '2' to send two stop bits.

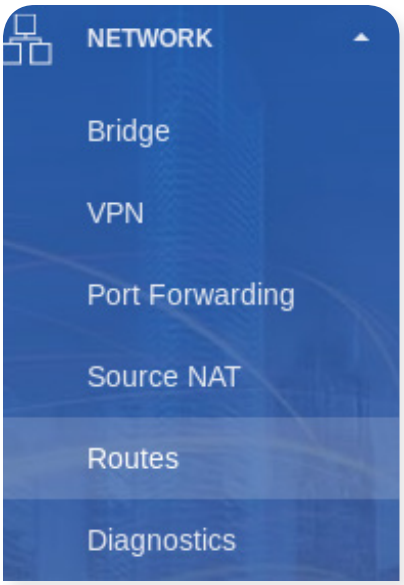
3.4.2.7 Flow Control

This setting informs the data receiver on how to process the data transfer, specifically with a method known as 'handshaking' which can be enabled or disabled. Handshaking helps to ensure that all the sent data are processed by the receiver. Set the FLOW CONTROL switch to 'NONE' to disable the handshaking method or set it to 'RTS/CTS' to enable hardware handshaking for the connection.

3.5 NETWORK

The MACH Gateway has multiple network interfaces and a number of different ways of configuring these interfaces. The configurations include upstream WAN side as well as the downstream LAN side. They include advanced functionalities such as VPN, Firewalls, provisioning IP addresses etc.

When you click on the NETWORK Tab on the left nav panel, the following user interface shows up:



Click on the item you wish to configure.

CAUTION: When setting IP Address for various interfaces (Ethernet, Wi-Fi, Bridge etc.), make sure they are all not set to the same address. For example if one interface is set to 192.168.1.1, then the IP address to other interfaces should be set to something different, for example, 192.168.21.1

3.5.1 Bridge

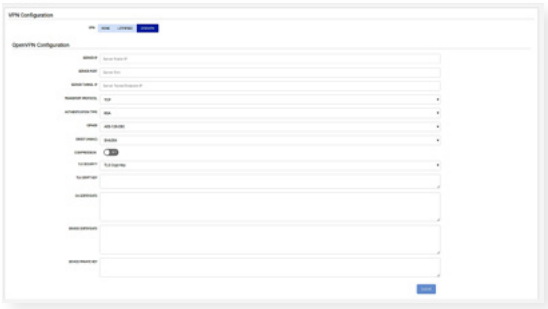
In the bridge mode, any broadcast that comes on the Wi-Fi, Ethernet 1 (eth0) or Ethernet 2 (eth1) ports are automatically sent over through the other 2 ports. Unicast messages for the MACH Gateway are sent only to the MACH unit.

- Wi-Fi Access Point
- Ethernet 1 (eth0)
- Ethernet 2 (eth1)

IP Address (Optional) - Enter the IP address of the bridge

3.5.2 VPN

VPN can be configured to three options: None, L2TPISEC or OPENVPN.

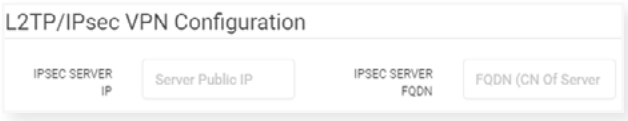


3.5.2.1 L2TP/IPSEC

Configure the Layer 2 Tunneling Protocol(L2TP) or Internet Protocol Security(IPSEC) by setting the VPN switch to 'L2TPIPSEC'.

The L2TP protocol implemented is L2TPv3 in unmanaged mode, configured to transport 'Ethernet Pseudowire'. IETF RFC 3931 defines L2TPv3.

VPN can be configured through Ethernet or Cellular.



3.5.2.1.1 L2TP Ethernet

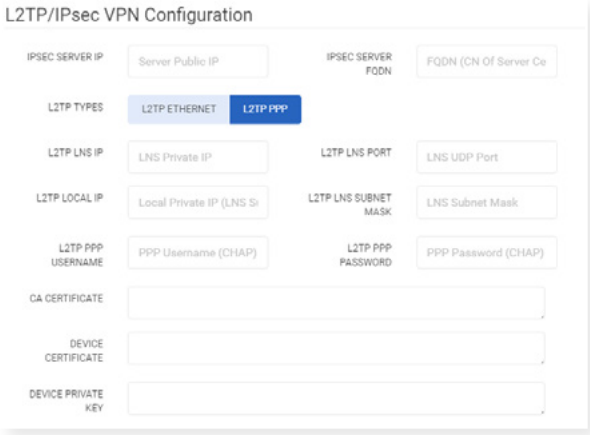
To configure the VPN through Ethernet:

- Set the L2TP TYPE switch to 'L2TP ETHERNET'
- Enter the public IP address of the IPSEC server in the IPSEC SERVER IP dialog box.
- Enter the Domain name (FQDN) of the IPSEC server in the IPSEC SERVER FQDN dialog box.
- Enter the private IP address for the MACH Gateway in the L2TP LOCAL IP dialog box.
- Type the port number of the local port (MACH) in the L2TP LOCAL PORT dialog box. The number can also be incremented and decremented by 1.
- Type the local tunnel ID (MACH) in the L2TP LOCAL TUNNEL ID dialog box. The number can also be incremented and decremented by 1.
- Type the local session ID (MACH) in the L2TP LOCAL SESSION ID dialog box. The number can also be incremented and decremented by 1.
- Enter the private IP address of the IPSEC server (PEER) in the L2TP PEER IP dialog box.
- Type the port number of the peer port in the L2TP PEER PORT dialog box. The number can also be incremented and decremented by 1.
- Type the peer tunnel ID in the L2TP PEER TUNNEL ID dialog box. The number can also be incremented and decremented by 1.
- Type the peer session ID in the L2TP PEER SESSION ID dialog box. The number can also be incremented and decremented by 1.
- Paste the CA certificate in PEM format in the CA CERTIFICATE dialog box.
- Paste the DEV certificate in PEM format in the DEVICE CERTIFICATE dialog box.
- Paste the DEV private key in PEM format in the DEVICE PRIVATE KEY dialog box.

3.5.2.1.2 L2TP Cellular

To configure the VPN through Cellular:

- Set the L2TP TYPES switch to 'L2TP PPP'.
- Enter the public IP address of the L2TP Network Server in the L2TP LNS IP dialog box.

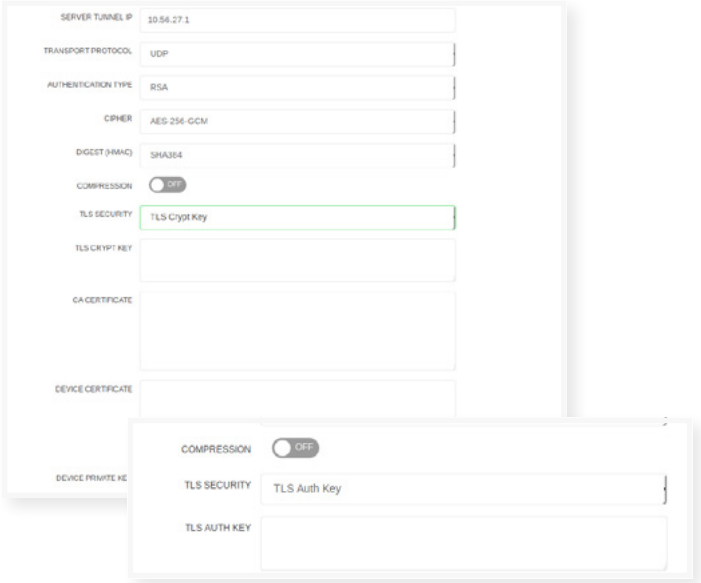


- Enter the private IP address for the MACH Gateway in the L2TP LOCAL IP dialog box.
- Enter the port number of the L2TP Network Server in the L2TP LNS PORT dialog box. The number can also be incremented and decremented by 1.
- Enter the Subnet mask number of the L2TP Network Server in the L2TP LNS SUBNET MASK dialog box. The number can also be incremented and decremented by 1.
- Enter the username for the Cellular VPN connection in the L2TP PPP USERNAME dialog box.
- Enter the password for the Cellular VPN connection in the L2TP PPP PASSWORD dialog box.
- Paste the CA certificate in PEM format in the CA CERTIFICATE dialog box.
- Paste the DEV certificate in PEM format in the DEVICE CERTIFICATE dialog box.
- Paste the DEV private key in PEM format in the DEVICE PRIVATE KEY dialog box.

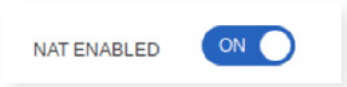
3.5.3 Open VPN

Configure Open VPN on the MACH Gateway by setting the VPN switch to 'OPENVPN'. The OpenVPN configuration panel is displayed:

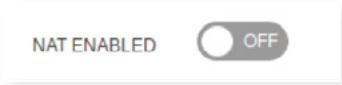
- Enter the IP address of the Remote server in the SERVER IP dialog box.



- Enter the Port of the Remote server in the SERVER PORT dialog box.
- Enter the TunneL IP address of the Remote server in the SERVER TUNNEL IP dialog box.
- Select transport protocol as ‘UDP’ or ‘TCP’ in the TRANSPORT PROTOCOL dropdown list.
- NAT Enabled web toggle switch allows you to configure how Network Address Translation (NAT) should work with VPN through the UI.



NAT Enabled: Set the web toggle switch for NAT enabled to 'ON' so that any LAN traffic routed through the VPN tunnel will be NAT'd to the VPN tunnel IP address.



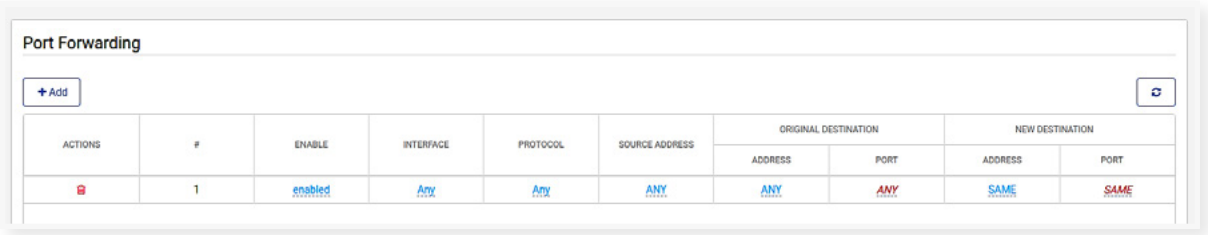
NAT Disabled: Set the web toggle switch for NAT enabled to 'OFF' so that any LAN traffic routed through the VPN tunnel won’t be NAT’d to the VPN tunnel IP address and will still have the LAN IP address. In other words, LAN IP address will be visible on the VPN server.

- Select authentication type as ‘RSA’ in the AUTHENTICATION TYPE dropdown list.
- Select ‘AES-128-CBC’ for 128-bit AES encryption or ‘AES-256-CBC’ for 256-bit AES encryption in the CIPHER dropdown list.
- Select ‘SHA384’ for DIGEST(HMAC) from the dropdown list.
- Set the COMPRESSION switch to ‘ON’ to enable compression or set it to ‘OFF’ to disable it.
- Select TLS Security Type from the dropdown list and paste the TLS authentication or crypt key in PEM format in the TLS AUTH or CRYPT KEY dialog box.
- Paste the CA certificate in PEM format in the CA CERTIFICATE dialog box.
- Paste Device certificate in PEM format in the DEVICE CERTIFICATE dialog box.
- Paste the Device private key in PEM format in the DEVICE PRIVATE KEY dialog box.

3.5.4 Port Forwarding

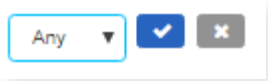
The Port forwarding rules are displayed in a tabular format.

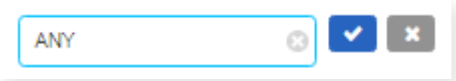
Editable cells can exist in a display mode where it only shows the value of the cell or in an edit mode, where the value of the cell can be changed. Cells in the editable mode may contain a dropdown list of pre-existing values or a dialog box with a gray round button for clearing the box, along with a colored check button to save the change and a gray button to cancel the change.



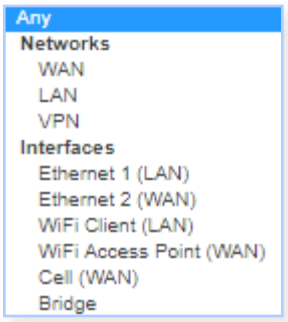
3.5.4.1 Table Columns/Fields

- **ACTIONS** – It contains icons for deleting a rule/row or moving it upward or downward in the table.





- **#** – It shows the ordering of the rows.
- **ENABLE** – In display mode, it shows if the particular rule/row is 'enabled' or 'disabled'. In edit mode, it shows a dropdown list with values: 'enabled' or 'disabled'.
- **INTERFACE** – In display mode, it shows the chosen interface for a rule/row. In edit mode, it shows a dropdown list with the values below. The default value is 'Any'.
- **PROTOCOL** – In display mode, it shows the chosen protocol for a rule/row. In edit mode, it shows a dropdown list with values: 'Any', 'TCP' or 'UDP'. The default value is 'Any'.
- **SOURCE ADDRESS** – In display mode, it shows the IP address of the source. In edit mode, a dialog box is shown with the existing value of the source IP address. The default value is 'ANY'.



- **ORIGINAL ADDRESS**
  - **ADDRESS** – In display mode, it shows the IP address of the original destination. In edit mode, a dialog box is shown with the existing value of the original destination address. The default value is 'ANY'.
  - **PORT** – In display mode, it shows the port number of the original destination. In edit mode, a dialog box is shown with the existing value of the original destination port number. The default value is 'ANY'.
- **NEW DESTINATION**
  - **ADDRESS** – In display mode, it shows the IP address of the new destination. In edit mode, a dialog box is shown with the existing value of the new destination address. The default value is 'SAME'.
  - **PORT** – In display mode, it shows the port number of the new destination. In edit mode, a dialog box is shown with the existing value of the new destination port number. The default value is 'SAME'.

3.5.4.2 Add New Rule

To add a new rule, click the 'ADD' button and a new row is added in the table with default values. After changing the values, click the 'SUBMIT' button to save the new rule in the MACH Gateway.

3.5.4.3 Change Existing Rule

An existing rule (as a table row) can be edited by changing the individual cells, then click the 'SUBMIT' button to save the updated rule in the MACH Gateway.

3.5.4.4 Delete Existing Rule

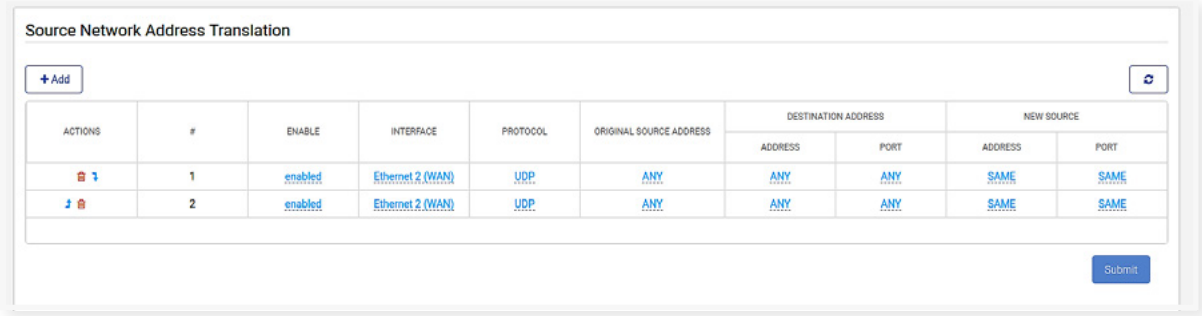
An existing rule can be deleted by clicking the trash icon in the 'ACTIONS' column. However, the 'SUBMIT' button must be clicked to remove the deleted rule in the Port forwarding configuration file on the MACH Gateway.

3.5.4.5 Update Rules/Table

The table is updated or refreshed whenever a change in the table is committed to the configuration file using the 'SUBMIT' button. However, the table can be refreshed manually using the refresh button located on the right side of the 'Add' button.

3.5.5 Source Network Address Translation

The Source Network Address Translation (NAT) rules are represented in a tabular format similar to Port forwarding. The principle of adding, changing, deleting rules and refresh tables are the same as Port forwarding.



3.5.5.1 Table Columns/Fields

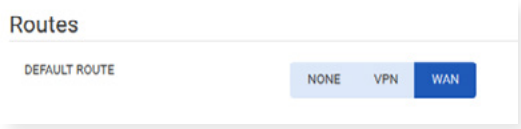
The columns are:

- **ACTIONS** – It contains icons for deleting a rule/row or moving it upward or downward in the table.
- **#** – It shows the ordering of the rows.
- **ENABLE** – In display mode, it shows if the particular rule/row is 'enabled' or 'disabled'. In edit mode, it shows a dropdown list with values: 'enabled' or 'disabled'. The default value is 'enabled'.
- **INTERFACE** – In display mode, it shows the chosen interface for a rule/row. In edit mode, it shows a dropdown list with the values below. The default value is 'Ethernet 2 (WAN)'.

- **PROTOCOL** – In display mode, it shows the chosen protocol for a rule/row. In edit mode, it shows a dropdown list with values: 'TCP' or 'UDP'. The default value is 'UDP'.
- **ORIGINAL SOURCE ADDRESS** – In display mode, it shows the IP address of the original source. In edit mode, a dialog box is shown with the existing value of the original source address. The default value is 'ANY'.
- **DESTINATION ADDRESS**
  - **ADDRESS** – In display mode, it shows the IP address of the destination. In edit mode, a dialog box is shown with the existing value of the destination address. The default value is 'ANY'.
  - **PORT** – In display mode, it shows the port number of the destination. In edit mode, a dialog box is shown with the existing value of the destination port number. The default value is 'ANY'.
- **NEW SOURCE**
  - **ADDRESS** – In display mode, it shows the IP address of the new source. In edit mode, a dialog box is shown with the existing value of the new source address. The default value is 'SAME'.
  - **PORT** – In display mode, it shows the port number of the new source. In edit mode, a dialog box is shown with the existing value of the new source port number. The default value is 'SAME.

3.5.6 Routes

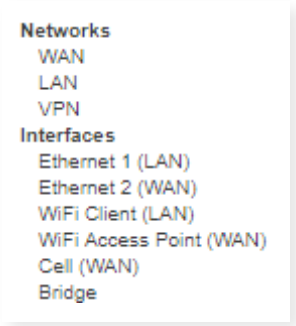
The default route can be 'None', 'VPN', or 'WAN'. The routing rules are represented in a tabular format. The principle of adding, changing, deleting rules and refresh tables are the same as Port forwarding.



3.5.6.1 Table Columns/Fields

- **ACTIONS** – It contains icons for deleting a rule/row or moving it upward or downward in the table.
- **#** – It shows the ordering of the rows.
- **ENABLE** – In display mode, it shows if the particular rule/row is 'enabled' or 'disabled'. In edit mode, it shows a dropdown list with values: 'enabled' or 'disabled'.

- **DESTINATION** – In display mode, it shows the destination address. In the edit mode, a dialog box is shown with the existing value of the destination address.
- **NETMASK** – In display mode, it shows the size of the subnet prefix. In edit mode, a dialog box is show with the existing value of the subnet prefix size. The default value is '/8'.
- **INTERFACE** – In display mode, it shows the chosen interface for a rule/row. In edit mode, it shows a dropdown list with the values below. The default value is 'WAN.

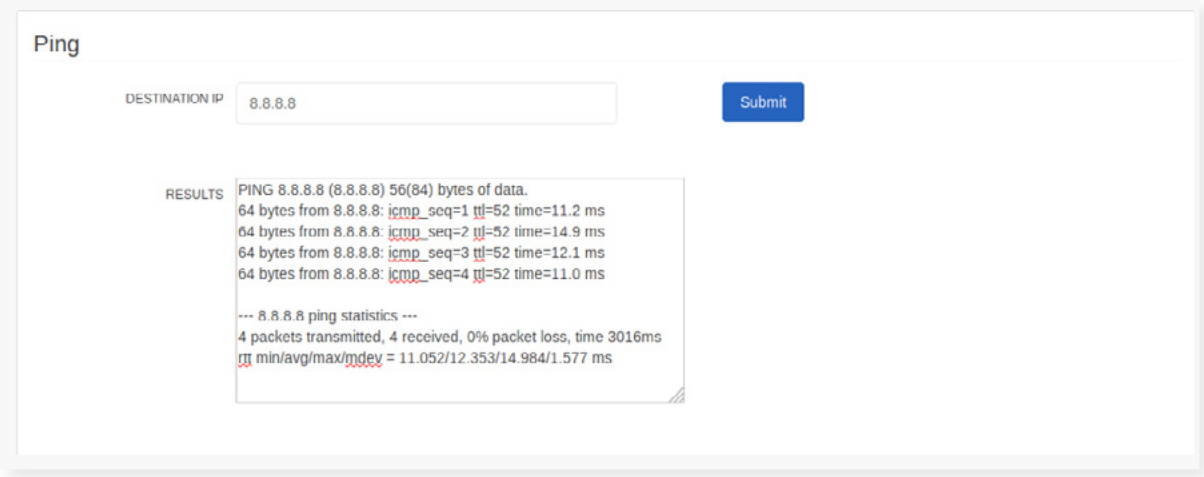


- **GATEWAY** – In display mode, it shows the gateway address. In edit mode, it shows the existing value of the gateway address.

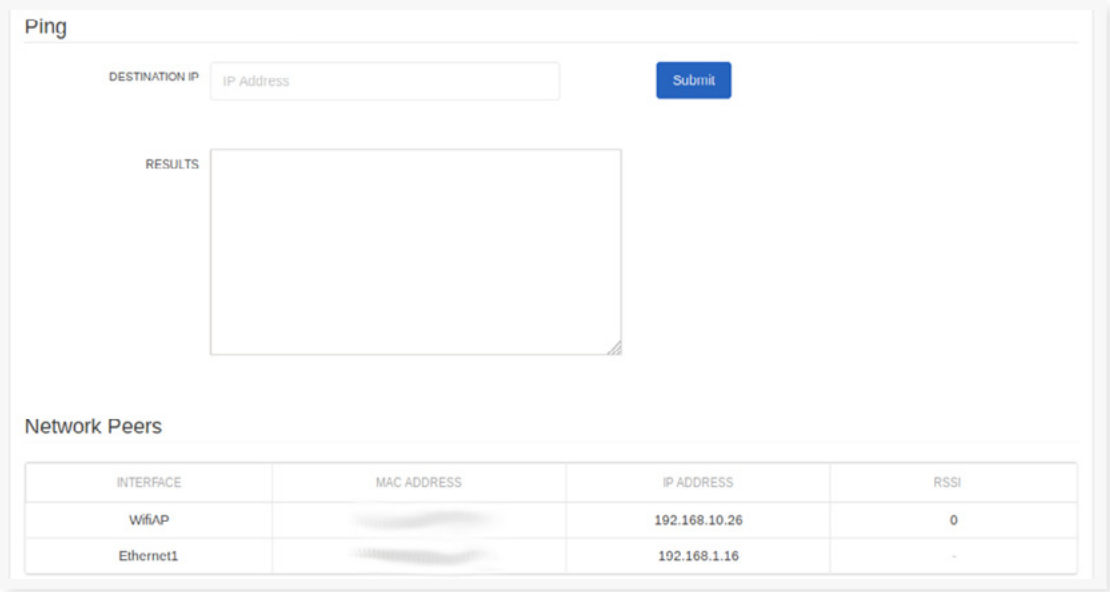
3.5.7 Diagnostics

This page enables you to ping test a destination IP and check if the network interfaces in the Gateway are properly configured and are up.

- Enter the appropriate destination IP.
- Click the 'Submit' button.
- The results for the ping test show up right away after hitting Submit in the Results dialog box.

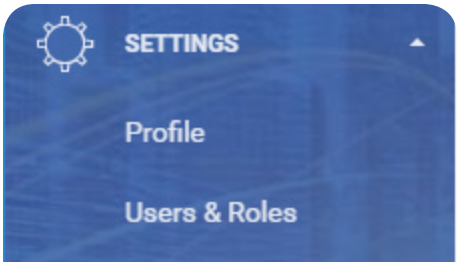


- The ‘Network Peers’ table displays the Interface, IP, MAC addresses and RSSI values of all the devices connected to the Gateway.

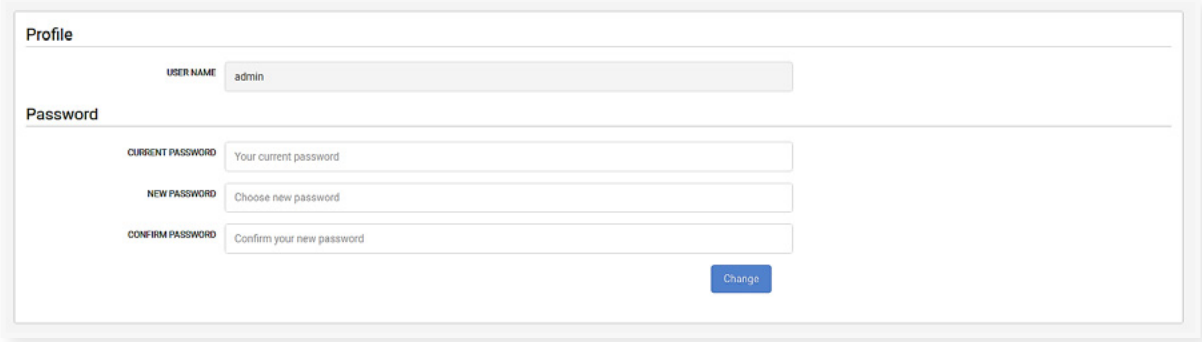


3.6 SETTINGS

The Settings tab has two sections on the left panel: ‘Profile’ and ‘Users & Roles’.



3.6.1 Profile



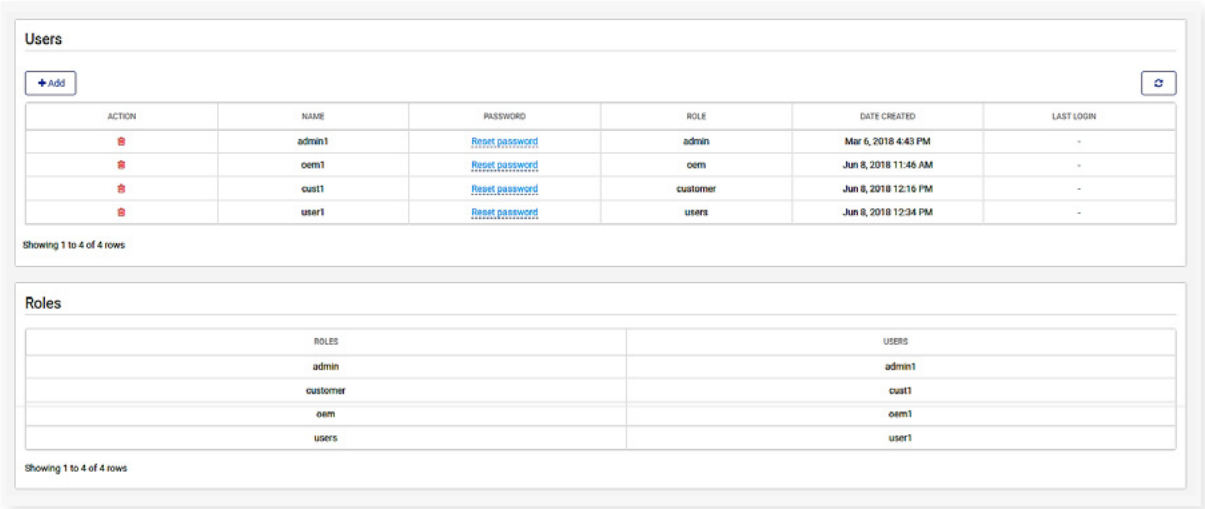
3.6.2 Users & Roles

This section is only visible for users with administrative (admin) role. It allows the admin user to view all other users of the MACH Gateway, add new users, delete existing users and reset users' password.

3.6.2.1 Show All Users

The users table displays all the other users of the MACH Gateway. The table columns/fields include:

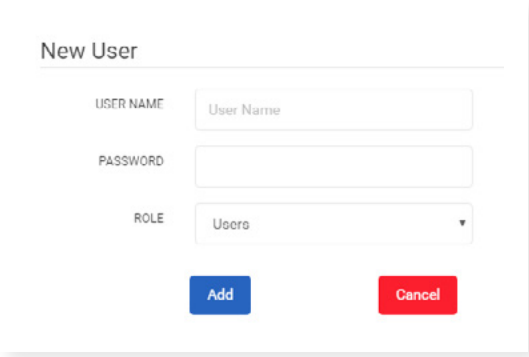
- **ACTION** – It contains a clickable icon for deleting an existing user.
- **NAME** – It displays the identity of the user.
- **PASSWORD** – The 'Reset Password' link is used to reset the user's password.
- **ROLE** – It displays the assigned role of the user.
- **DATE CREATED** – It displays the date the user was created.
- **LAST LOGIN** – It displays the last date/time the user logged in.



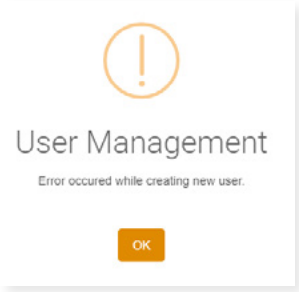
3.6.2.2 Add/Register New User

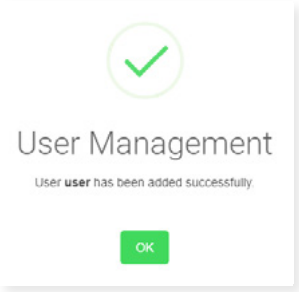
To register/add a new user to the Gateway, follow the steps below.

- Click the 'Add' button above the users table. A form section titled 'New User' appears.
- Type the name of the user.
- Type the password of the user. The password must be six characters or more.
- Select the preferred role for the user. The selections are: 'Admin', 'OEM', 'Users' and 'Customer'.



- Click the 'Add' button to register the new user or click the 'Cancel' button to cancel the registration.
- A dialog box appears and it indicates if the registration was successful or not.



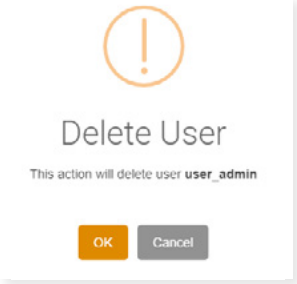


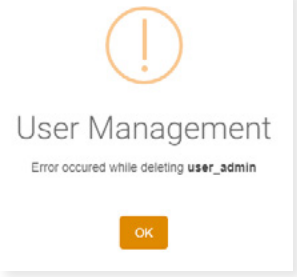
- If the registration was successful, the new user should appear in the users table and the roles table.

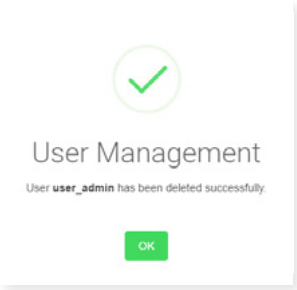
3.6.2.3 Delete User

To delete an existing user, follow the steps below.

- Click on the trash icon in the 'ACTION' column.
- A dialog appears to warn the user about the action.
- Click the 'OK' button to confirm the delete action or click the 'Cancel' button to cancel the action.
- A dialog box appears and it indicates if the deletion was successful or not.
- If the action was successful, the user's row is removed from the table.



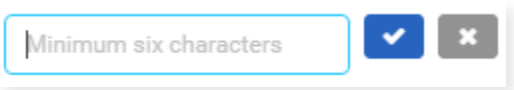




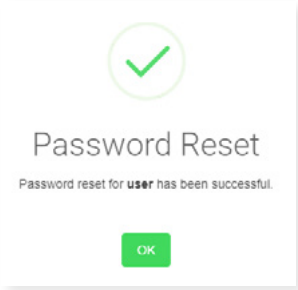
3.6.3 Reset User's Password

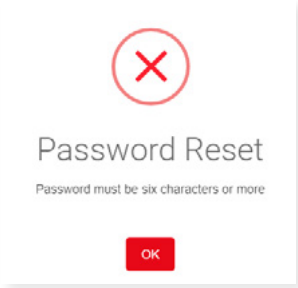
To reset the password of a user, follow the steps below.

- Click the 'Reset Password' link in the 'PASSWORD' field/column of the user.
- An inline dialog box appears with the hint 'Minimum six characters' to signify the password requirement.



- Type the new password for the user.
- Click the check button to set the new password or the grey button to cancel the reset action.
- A dialog box appears and it indicates if the password reset was successful or not.

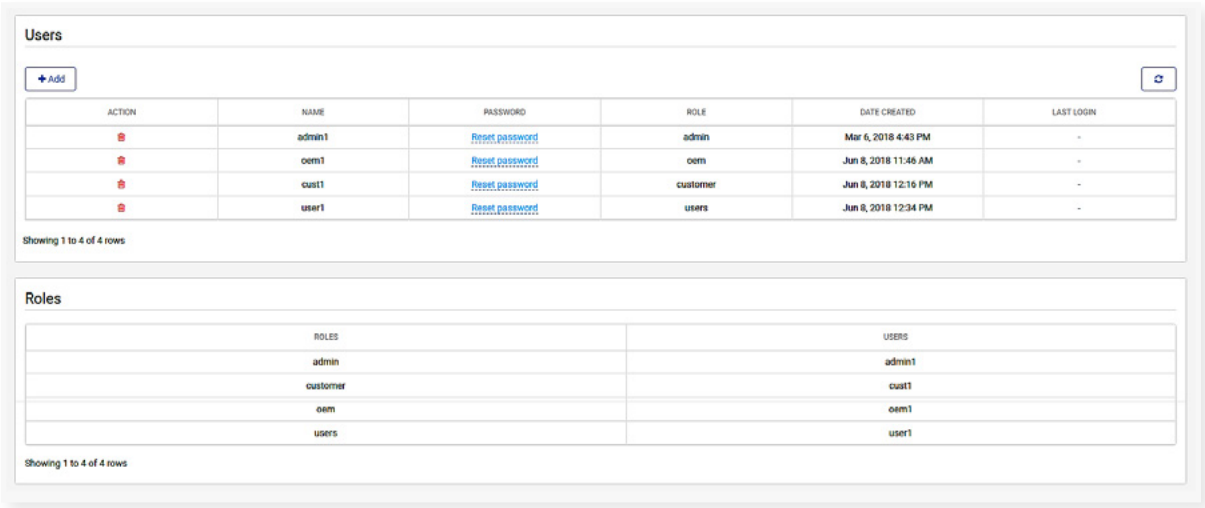




3.6.3.1 Show All Roles

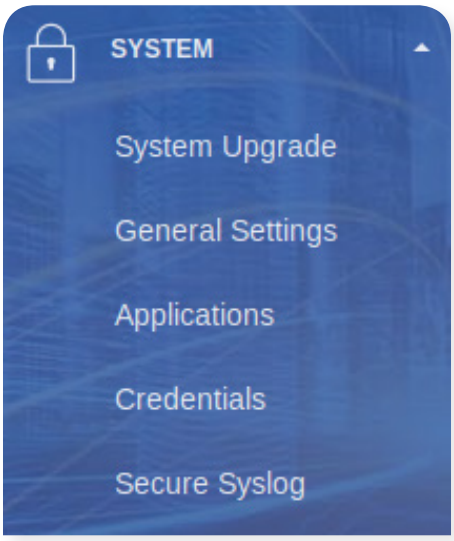
The 'Roles' table has two columns/fields:

- **ROLES** – It displays the acceptable roles for the MACH Gateway.
- **USERS** – It displays users of the MACH Gateway based on their assigned role.



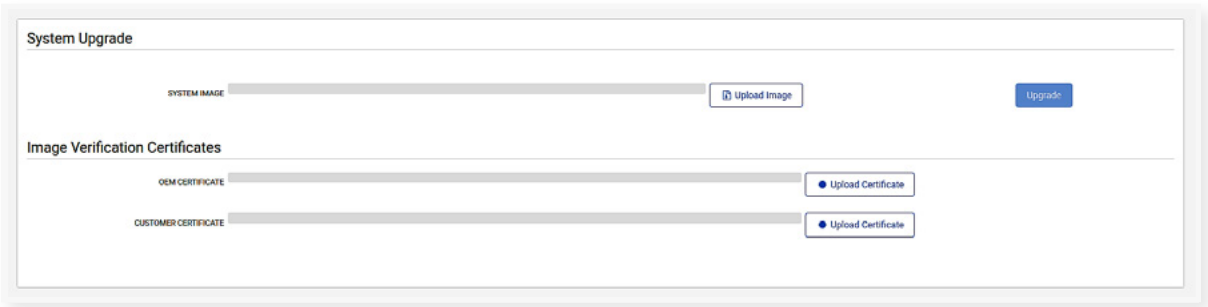
3.7 SYSTEM

The SYSTEM tab has five sections on the left panel: 'System Upgrade', 'General Settings', 'Applications', 'Credentials' and 'Secure Syslog'.



3.7.1 System Upgrade

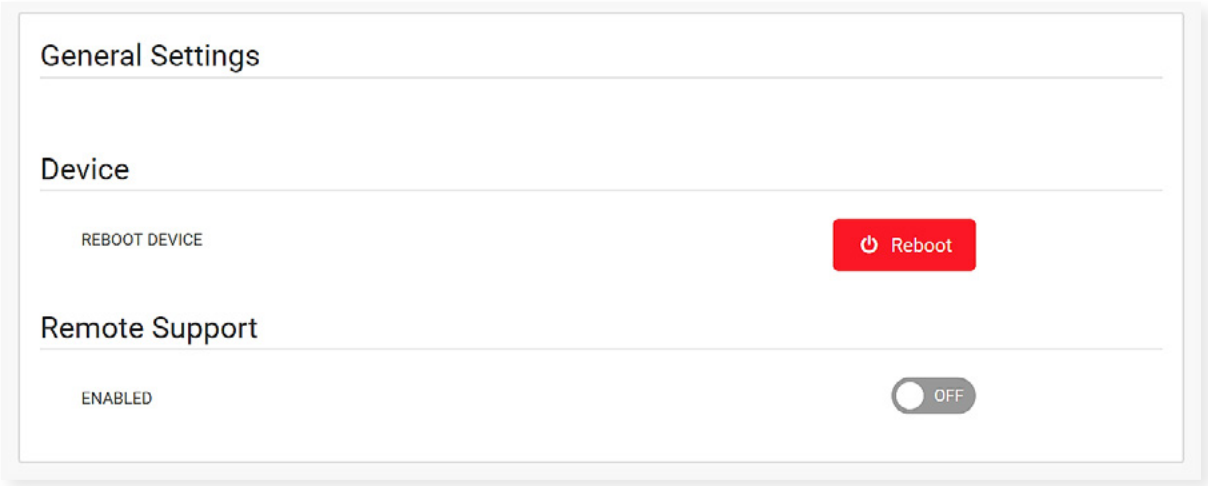
This page allows the user with the roles ‘admin’, ‘oem’ or ‘customer’ to perform the system image update. The following steps show how to update the system image of a MACH Gateway.



- Click the ‘Upload Certificate’ button to select the Image verification certificate. The ‘oem’ user should upload an OEM certificate while the ‘customer’ user should upload a Customer certificate. The ‘admin’ user can upload either an OEM certificate or a Customer certificate.

3.7.2 General Settings

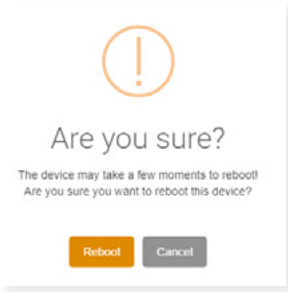
This page allows any user to reboot the MACH Gateway and set remote support option.



3.7.2.1 Reboot Device

To reboot the MACH Gateway, follow the steps below.

- Click the ‘REBOOT’ button.
- A dialog appears and it warns the user about the action to be performed.

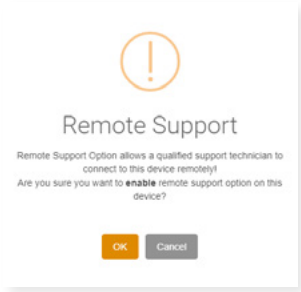


- Click the 'Reboot' button to confirm the action or click the 'Cancel' button to cancel the reboot action.

3.7.2.2 Remote Support

To set the Remote Support option, follow the steps below:

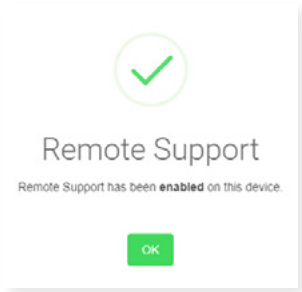
- Set the 'ENABLED' button to 'ON' to enable remote support or set it to 'OFF' to disable it.

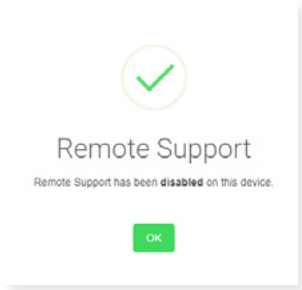


- A pop-up dialog appears and it warns the user about the intended action.

- Click the 'OK' button to confirm the action or click the 'Cancel' button to cancel the action.

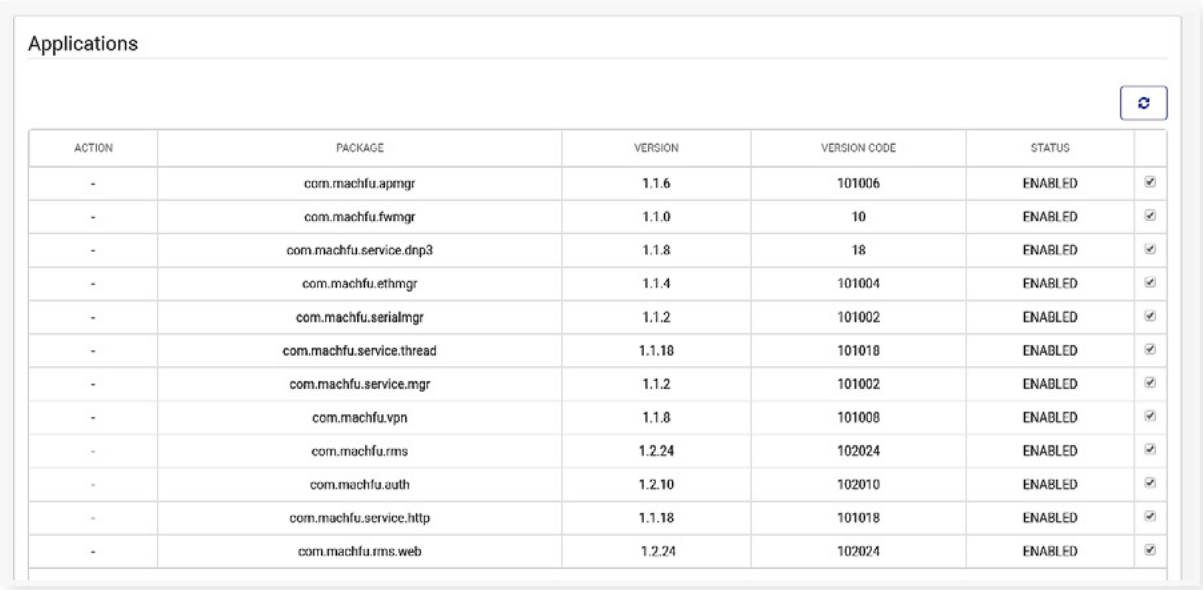
- A pop-up dialog appears and it informs the user if the chosen action is successful or not.





3.7.3 Applications

The applications table shows some applications/services running on the MACH Gateway. There are two pre-defined categories of applications/services: System Apps and Machfu Apps.



3.7.3.1 Categories

- **System Apps** – These apps/services are always running and are essential to the overall operation of the MACH Gateway. The user cannot uninstall or close them from the applications table.
- **Machfu Apps** – These apps/services can be uninstalled or closed from the table.

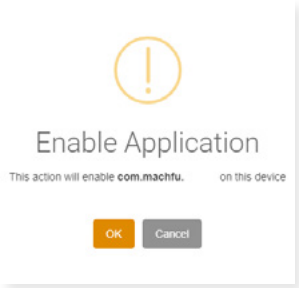
3.7.3.2 Table Columns/Fields

- **ACTION** – This contains the delete icon for 'Machfu Apps'. This column appears only for users with 'admin' role.
- **PACKAGE** – This shows the package name of the application/service.
- **VERSION** – This shows the version name of the application/service.
- **VERSION CODE** – This shows the version code of the application/service.
- **STATUS** – This indicates if the application/service is running (ENABLED) or not (DISABLED).
- **ENABLE** – This contains a checkbox that allows the user to start or stop 'Machfu Apps'. The checkbox is disabled for 'System Apps'. This column appears only for users with 'admin' role.

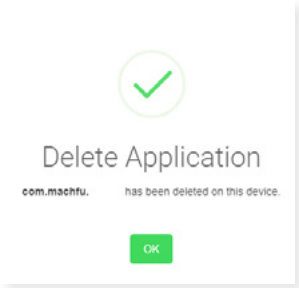
3.7.3.3 Delete/Uninstall App

To delete a 'Machfu app', follow the instructions below:

- Click the icon in the 'ACTION' field.
- A pop-up dialog appears and it warns the user that the selected app/service would be uninstalled.



- Click the 'OK' button to confirm deleting/ uninstalling the app or click the 'Cancel' button to cancel the action.
- A pop-up dialog appears and it informs the user if the app has been uninstalled successfully or not.

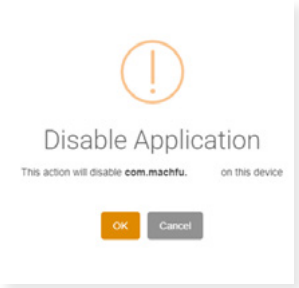


- The table refreshes automatically to show that the app has been removed/ uninstalled.

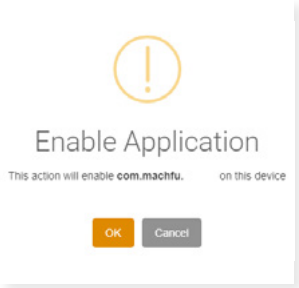
3.7.4 Start/Stop App

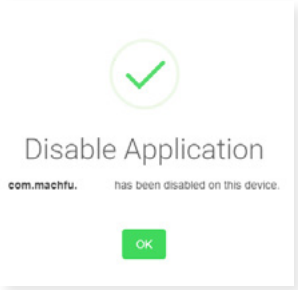
To start(enable) or stop(disable) an app, follow the steps below:

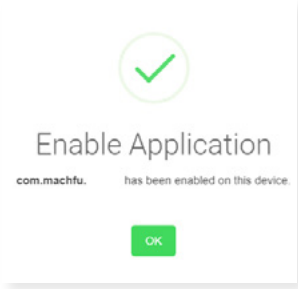
- Click the checkbox in the 'ENABLE' field to change the running state of the app.
- A pop-up dialog appears and it warns the user about changing the state of the app.



- Click the 'OK' button to confirm the action or click the 'Cancel' button to cancel the action.
- A pop-up dialog appears and it informs the user if the action is successful or not.







- The table refreshes automatically to show that the updated status of app.

3.7.5 Credentials

To use SSL/TLS connections to publish data to a MQTT broker, an appropriate credential set has to be uploaded and configured on the Machfu Gateway.

Machfu Gateway only supports enrolling the public, private key in PKCS12 format. If your key pair is in some other format, you may use 'OpenSSL' to convert it into PKCS12 format.

A PKCS12 file can contain a private key, a certificate chain, and CA certificates. In addition to that, there may be multiple private keys and certificate chains. In practice we mostly see a single key, but

one could generate PKCS12 with multiple keys. The private key and certificate chain are referred by a friendly name that we call 'Alias.'

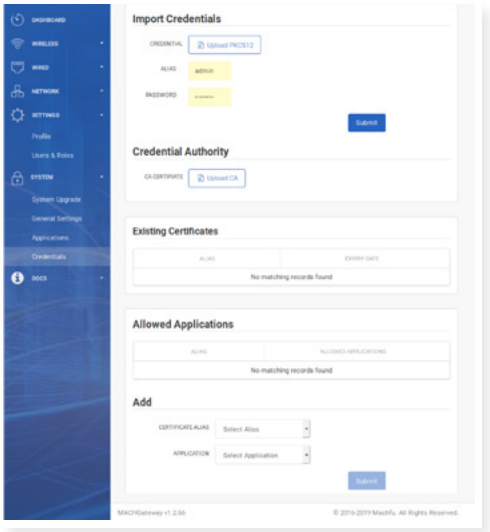
Example: In case the keys are in PEM format, *openssl pkcs12 -export -out <PKCS12 File Name>.pfx -inkey <Private Key File Name> -in <Public Key File Name> -name <Alias>*

The newly created <PKCS12 File Name>.pfx is in PKCS12 format and contains the key pair.

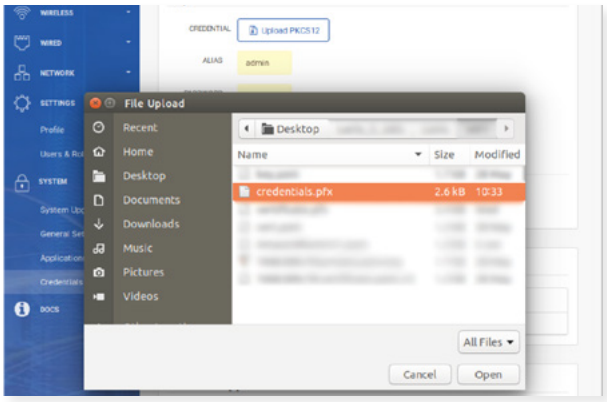
3.7.5.1 Uploading Credentials

Please follow the steps below to upload a credential set:

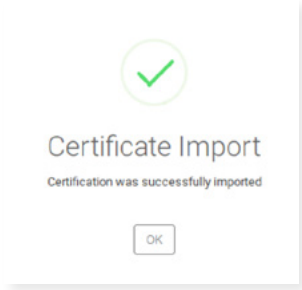
- Go to the Machfu Gateway web UI.
- Using the navigation menu on the left panel, select 'Credentials' under 'System tab'.



- The Credentials page will appear on your browser.
- In the 'Import Credentials' section, click the Upload PKCS12 button and select the PKCS12 file containing the public and private key you would like to use for the connection.
- Enter the 'Alias' that was used while creating the 'PKCS12 file'.
- Enter the 'Password' that was used while creating the 'PKCS12 file'.



- Click the 'Submit' button.
- If successfully installed, a confirmation message will pop up.

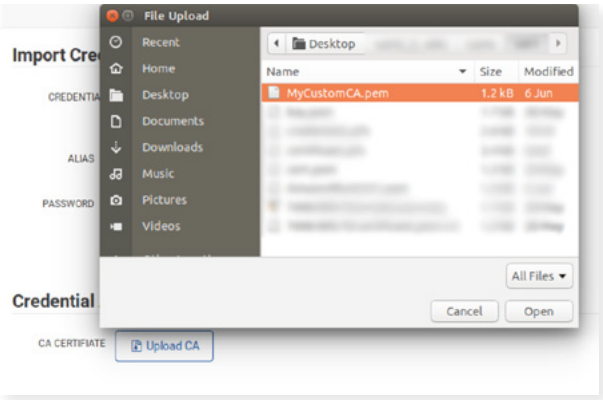


- The installed credentials are now displayed in the 'Existing Certificates' section.

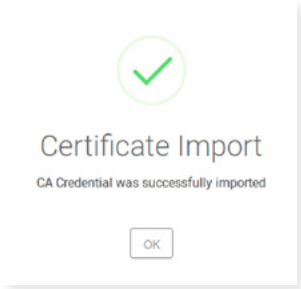
3.7.5.2 Upload CA

The Machfu Gateway already comes installed with well known CAs. In case you are using a self signed key pair you may need to install the CA. This can be done using the following steps:

- Click the 'Upload CA' button in the 'Credential Authority' section and choose the CA certificate file in PEM format.



- If successfully installed, a confirmation message will pop up.

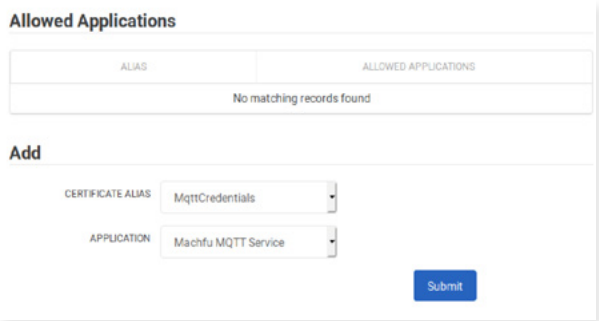


3.7.5.2 Allowing MQTT Service Access to Credentials.

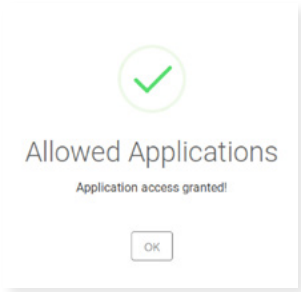
Now that you have installed the credentials, the Machfu MQTT Service must be allowed to access them.

This can be done, by following the steps below.

- In the 'Allowed Applications/Add' section, Select the 'Alias' installed in the previous section.
- In the 'Application' field select 'Machfu MQTT Service'.



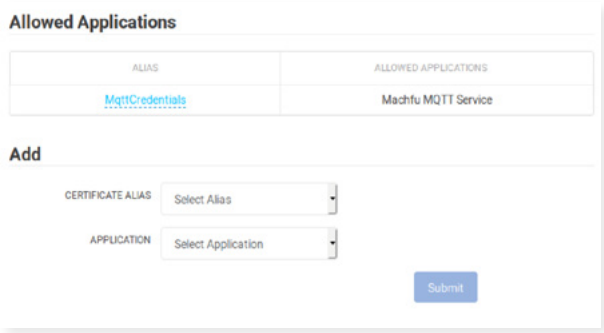
- Click the 'Submit' button.
- If successfully installed, a confirmation message will pop up.



- Once completed, the alias and application name shall appear in the Allowed Applications table.

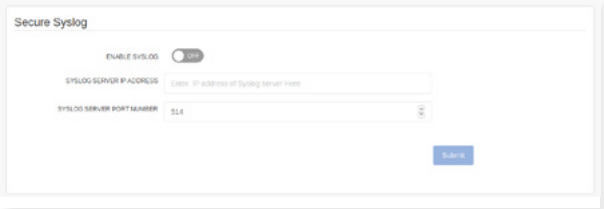
3.7.6 Secure Syslog

To use SSL/TLS connections to publish data to a MQTT broker, an appropriate credential

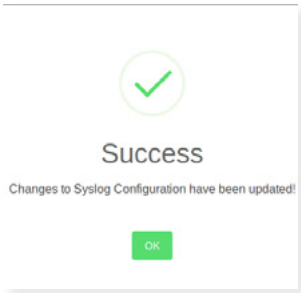


set has to be

- Set the 'Enable Syslog' web toggle switch on to enable Syslog feature.
- Enter the appropriate 'Syslog Server IP Address' in the adjacent dialog box.
- Enter the Port Number in the 'Syslog Server Port Number' dialog box.
- Click the 'Submit' button.



- A dialog box appears, and it indicates if the Syslog Configuration was successful or not.



4. Regulatory Notices

FCC Statement

This equipment has been tested and found to comply with the limits of a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antennae used for this transmitter must be installed to provide a separation distance of at least 20 cm from all people and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Industry Canada Statement

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage;

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Cet émetteur ne doit pas être Co-placé ou ne fonctionnant en même temps qu'aucune autre antenne ou émetteur.

Cet équipement devrait être installé et actionné avec une distance minimum de 20 centimètres entre le radiateur et votre corps.

Industry Canada Radiation Exposure Statement

This radio transmitter with model: Mach3 Gateway has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio with model: Mach3 Gateway a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

No.	Brand	Model name	Antenna type	Connector	Gain (dBi)
1	Taoglas	GW.05	Monopole	Standard RP-SMA (M)	1.25

5. Appendix

5.1 Cellular Bands

The supported bands are 2, 4, 5, 6 and 13.

5.2 Antenna Specification

The Mach-3 Gateway is a professionally-installed equipment. The Radio Frequency (RF) output power does not exceed the maximum limit allowed in the country of operation.

CAUTION: Unauthorized antennae, modifications, or attachments may damage the device and potentially violate regulations.

NOTE: Use only the supplied or an equivalent replacement antenna.

NOTE: Modifications to the device or use of unauthorized antennae as not expressly approved by Machfu is the sole responsibility of the user, configurator or operator, who must reassess the equipment in accordance to all applicable international Safety, EMC, and RF standards.

The Machfu-authorized antenna specifications are as follows:

- Mobile Broadband (SMA male)
  - Main: Dipole
  - LTE Auxiliary: Dipole

Frequency	Typ. Avg Gain (dBi)	Peak Gain (dBi)
698-806	-3	3
824-894	-2	3
880-960	-2	3
1710-1880	-1	4.5
1850-1990	-1	4.5
1920-2170	-1	4.5

- Mobile Broadband (SMA male)

Frequency	Typ. Avg Gain (dBi)	Peak Gain (dBi)
2200-2483	1.5	4

- GPS: Monopole (SMA male)

Frequency	Typ. Avg Gain (dBi)	Peak Gain (dBi)
1571 - 1578	28	-
1601-1603	28	-

5.3 Contacting Machfu

For technical assistance or customer service issues please contact support@machfu.com.