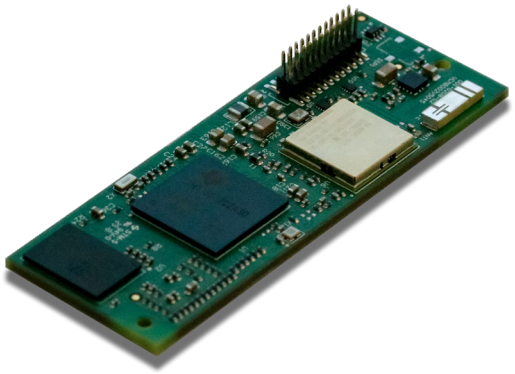
VT8000 Room Controllers

Wi-Fi Module
Installation & Quick Start Guide

VCM8002V5031 firmware version 1.4



VICONICS
Beyond Comfort

Version 7

CONTENTS

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with ISED Canada's license-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.

In order to comply with FCC/ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

CAUTION
FCC and ISED RF Radiation Exposure Statement:
This equipment complies with FCC and ISED RF radiation exposure limits set forth for an uncontrolled environment. End-users must follow the specific operating instructions for satisfying RF exposure limits. This transmitter and its antenna must not be collocated or operating with any other antenna or transmitter.

NOTICE

LOSS OF CONNECTIVITY

Wireless networks (including Wi-Fi) are inherently less stable than wired networks. When designing your Building Management System (BMS) system, consider if it must have access to devices at all times. If so, wired connectivity may be more suitable.

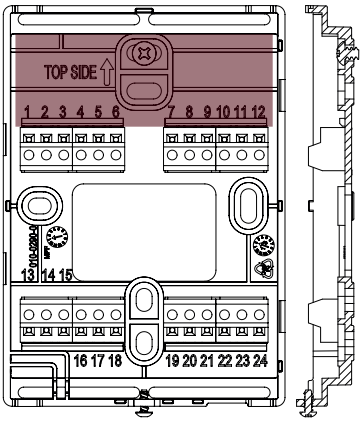
Failure to follow these instructions can result in a loss of connection or data.

SYSTEM REQUIREMENTS

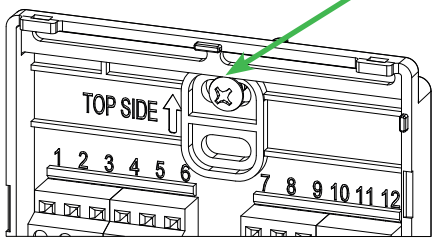
The Wi-Fi Module requires firmware 2.5.1 or later on a VT8000 Room Controller (RC).

SAFETY INSTRUCTIONS

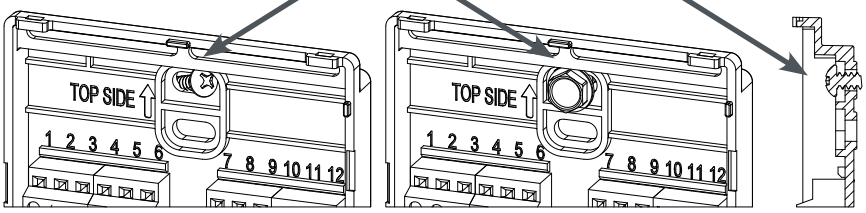
- Electronic controls are static sensitive devices. Discharge yourself correctly before manipulating Room Controllers.
- The Wi-Fi Module is Electro-Static Discharge (ESD) sensitive material and must be handled with caution. ESD can permanently damage electronics.
- Tampering with the devices or unintended application of the devices will result in a void warranty.
- Before installation, make sure the Room Controller surface is clean and free of dust or debris.
- Ensure that the darkened area (in the image below) of the backplate, where the Wi-Fi Module will be located, is free of mechanical interferences (i.e. screw heads, wiring, etc.).



Good installation:
Screw in and fully tighten to backplate.



Bad installations:
Skewed screw, wrong screw type, screw not fully tightened to backplate.



INSTALLATION

To install the Wi-Fi Module on a VT8000 Room Controller (RC):

1. Remove security screw from the bottom of the Room Controller cover (if present).
2. Open unit by pulling on the bottom of the Room Controller (Figure 1).

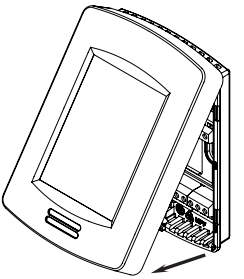


Figure 1

NOTE: Visually inspect the Wi-Fi Module for bent contact pins.

3. Below the gap in the upper-right corner of the Room Controller's motherboard, locate holes to insert the Wi-Fi Module.
4. Align the connector pins on the Wi-Fi Module with the holes on the motherboard (Figure 2).

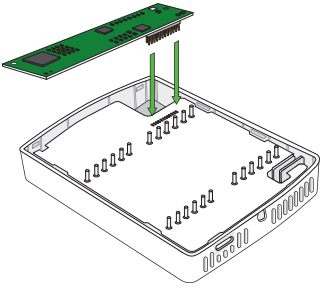


Figure 2

NOTE: Ensure alignment of pins is correct to avoid damaging the Wi-Fi Module.

5. Gently press the Wi-Fi Module into the Room Controller's motherboard until it fits snugly in place (Figure 3).

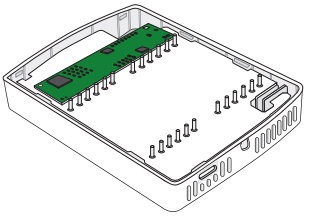


Figure 3

NOTE: Do not press too hard to avoid damaging the Wi-Fi Module.

6. Gently align the cover with the top of the base and snap in place from the bottom (Figure 4).
7. Install the security screw.

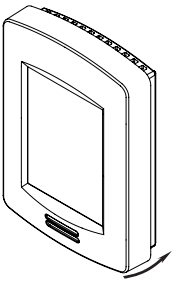


Figure 4

COMMISSIONING VIA WI-FI

Once installed, follow the steps below to commission the Wi-Fi Module.

NOTE: If you intend to connect the module to a hidden Wi-Fi Network (SSID Broadcast is disabled), it must be done before making the connection. Once the module is connected, the network configuration must not be changed, or the module may lose connection or fail to reconnect after power is cycled to the device or router. If you do change the network configuration, the module should be disconnected from the network and reconnected again.

Connect To The Wi-Fi Module

1. Touch and hold this point for 3 seconds to enter set-up mode.

   NOTE: If a configuration/installer password is activated to prevent unauthorized access to configuration menu parameters, a password entry prompt is displayed.

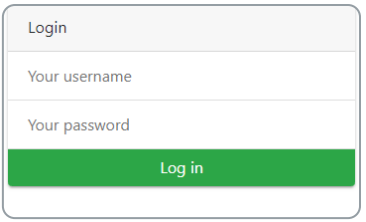
2. Navigate to the Network menu.
3. Using the left and right arrows navigate to the Wi-Fi configuration screens.
4. Enable the Wi-Fi Access Point.
5. The SSID, Password, and IP address fields will be populated.
6. Connect your PC or smartphone to the Access Point using the SSID and Password shown on the RC's screen.
7. Open your Internet browser and connect to the IP address 192.168.71.1

NOTE: When connecting to the Configuration Web Page, the web browser will present a warning due to the use of a self-signed certificate. Although strong security is in use, this warning appears as the web browser is not able to authenticate the website with an online certificate authority. The warning must be accepted to proceed to the Configuration Web Page.

8. Enter the default credentials:

   username: admin
   password: admin8000

   NOTE: Upon the first log-in a password change is required.



   Passwords must have at least 8 characters, one uppercase character, one lowercase character, and one number or symbol.

   Each user should have a strong and unique password. Do not re-use passwords for multiple users.

9. Enter a new password and click Submit.

You are now ready to manage your RC via the Configuration Web Page.

Connect To The Building Wi-Fi Network

1. Navigate to the Network tab in the web browser and connect to your desired Wi-Fi network.
2. Once connected, on your RC Wi-Fi network screen 3/5, the status will be displayed as Ready. The SSID and IP address to access the RC via the browser are displayed.
3. You can continue configuring your RC using the Access Point or via the building Wi-Fi network.

   NOTE: The Access Point will be disabled after the timeout period.

4. On the Admin tab, enable and configure Ping Remote Machine to ensure that the end-to-end connectivity of the device is monitored and fixed if the connection is lost (refer to “Device Monitoring” on page 12).

COMMISSIONING VIA USB

For sites where multiple RCs need to be commissioned, a sub-set of commissioning is supported from the VT8000 Uploader Tool via the USB port on the Room Controller. This provides a simple, fast, repeatable method to connect the Wi-Fi Module to the building's Wi-Fi network and enable the most common features. Advanced features can then be commissioned via the Configuration Web Pages across the building Wi-Fi network, saving commissioning time as it is not necessary to connect to the Access Point of each Wi-Fi Module. For more information refer to the Uploader Tool Installation Guide.

Commissioning from the Uploader Tool supports:

- User authentication and first admin password change
- Wi-Fi network connection (SSID)
- IP Configuration (DHCP or Static)
- Enable and configure BACnet/IP
- Enable NTP time source

Minimum system requirements:

- VT8000: 2.5.1
- VCM8002: 1.4
- Uploader tool: 3.3

To enable/disable Commissioning via USB, go to the Admin tab (refer to "Configuration" on page 11), or go to USB access on the RC Configuration screen.

NOTICE

INFORMATION DISCLOSURE/UNAUTHORIZED ACCESS

When the Wi-Fi Module is commissioned from the Uploader Tool, user and network password hashes are sent from the Uploader Tool, via USB and the Room Controller to the Module. If intercepted by a USB Eavesdropping Attack, these hashes may be used to access the Module and Wi-Fi network. Care should be taken to help ensure communications are not eavesdropped on.

Failure to follow these instructions may lead to unauthorized users accessing the Wi-Fi Module or the Wi-Fi network.

NOTICE

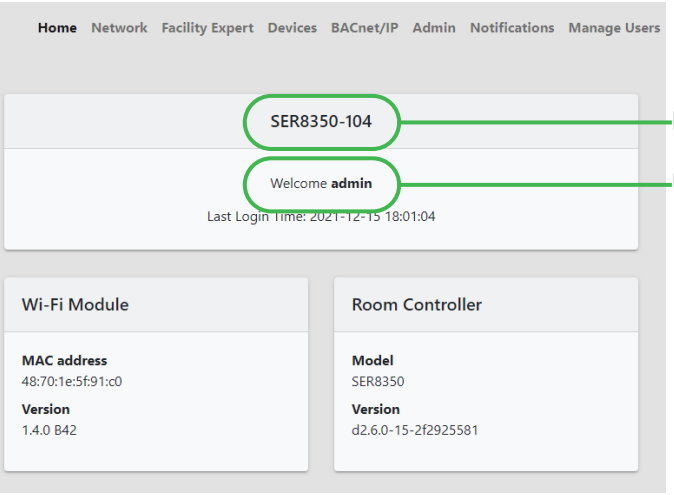
UNAUTHORIZED ACCESS

When commissioning is complete, it is recommended to disable USB Access on the Room Controller to minimize entry points to the system.

Failure to follow these instructions may lead to unauthorized users accessing the Wi-Fi Module or the Room Controller via USB.

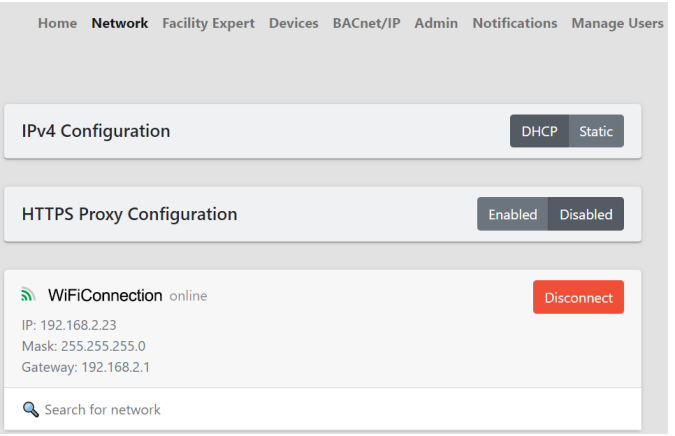
CONFIGURATION WEB PAGES

Home



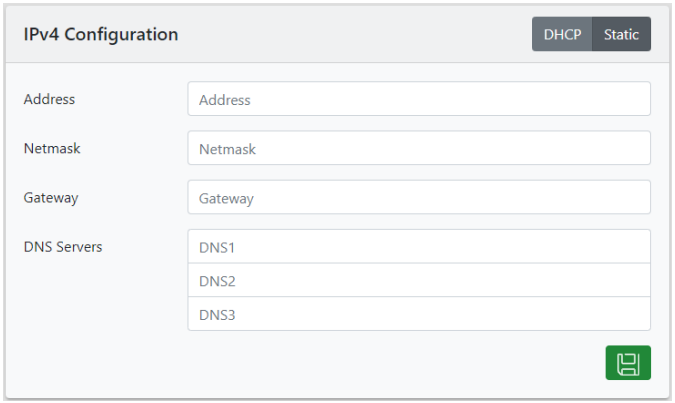
The Wi-Fi Module device name can be changed on the Admin page (refer to “Device Name” on page 11). It is used in email notifications and as the SSID for the module’s Wi-Fi Access Point. This name is different from the RC device name which is set by the BACnet front end.

Network



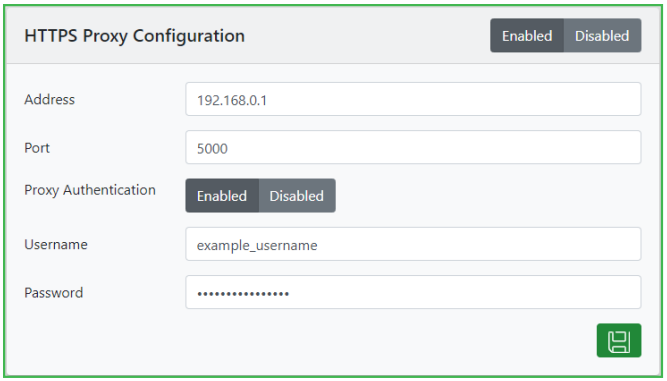
The Network page shows the IPv4 and HTTPS proxy configuration settings, and the building Wi-Fi network connection information. IPv4 and Wi-Fi can also be configured using the VT8000 Uploader Tool.

IPv4 Configuration



The default DHCP setting will automatically assign a valid IP address to your device. To set a Static IP configuration, please contact your network administrator for the correct values.

HTTPS Proxy Configuration



An HTTPS proxy may be configured for connection to Facility Expert. If configured, all traffic between the device and Facility Expert will pass through the proxy server.

When do I need to configure a proxy?

It is only necessary to configure a proxy server if:

- You are connecting your Wi-Fi Module to Facility Expert, and
- A proxy server is required for internet connectivity from the Wi-Fi network.

Configuration

Proxy servers are maintained by your Wi-Fi network administrator. Please contact your network administrator for proxy server configuration values required below.

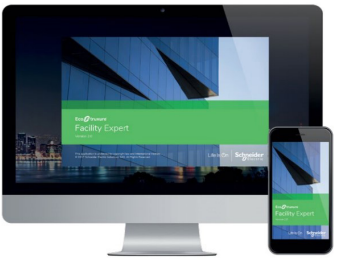
To configure the proxy, you need to specify:

- An address (e.g. 192.168.0.1 or proxy.my-domain.com)
- A port (e.g. 5000)
- If authentication is required to use the proxy:
  - A username
  - A password

Confirmation of Operation

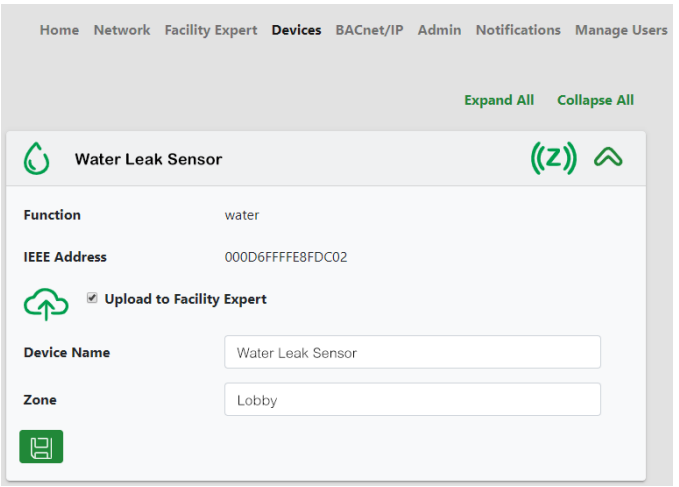
After configuring your proxy, go to the Facility Expert page and ensure Facility Expert is online.

Facility Expert



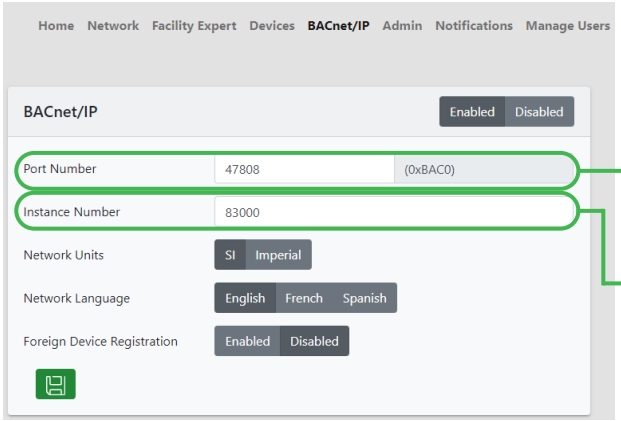
Refer to the Integration Guide for Connecting VT8000 to EcoStruxure Facility Expert.

Devices



The Devices page shows the paired wireless devices configuration settings. Make sure to configure the wireless devices before connecting to the Facility Expert platform.

BACnet/IP



This is the default BACnet/IP port, but it may be configured to use a different number if necessary.

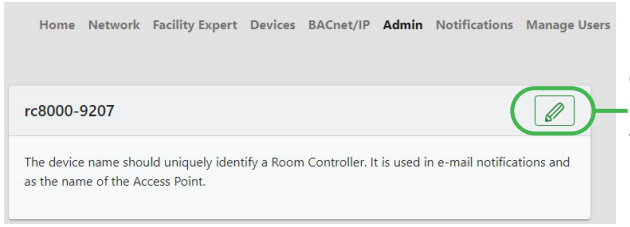
The BACnet instance number must be set uniquely for each device.

BACnet/IP can also be enabled and configured using the VT8000 Uploader Tool.

NOTE: The RC supports either BACnet/IP or BACnet/MSTP. If BACnet/IP is enabled, then BACnet/MSTP will be disabled.

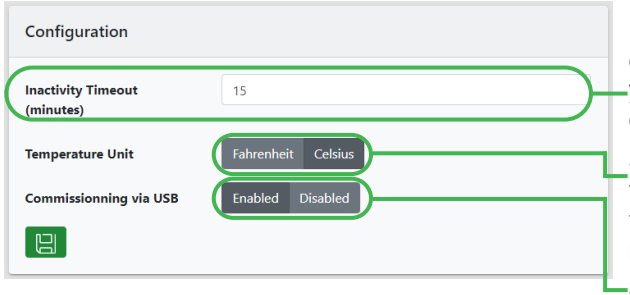
Admin

Device Name



Click the Edit button to change the device name.

Configuration

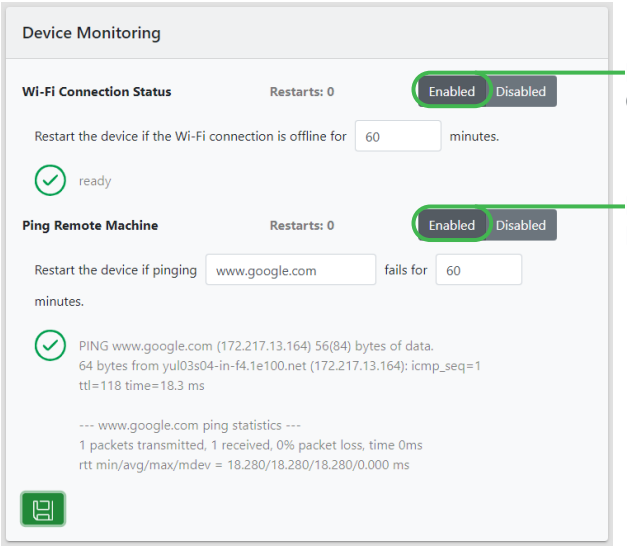


Number of minutes of inactivity before you are signed out of the web app.

Select the temperature unit to use in Email notifications.

Select to enable/ disable configuration via USB

Device Monitoring



The Wi-Fi Module provides configurable self-monitoring tools that can be used to monitor the device and recover in case of failure. When well configured, these tools add a layer of robustness to the system and reduce the need for human intervention if something unexpected happens.

The number of restarts caused by each monitor is counted and displayed, to aid in the diagnosis of unstable systems.

Configurable timeouts may be set with values between 10 minutes and 1440 minutes (1 day).

Monitors are prevented from restarting the system if the module Access Point is enabled.

Wi-Fi Connection Status

When enabled, the Wi-Fi connection status will be monitored and the module will restart if the Wi-Fi status is not Ready for the configured time.

This monitor is enabled by default, with a timeout of 60 minutes.

Ping Remote Machine

When enabled, the Wi-Fi Module will ping the configured IPv4 address or domain name every 5 minutes. If all pings fail for the configured time period, the module will restart. This monitor confirms the end-to-end network connectivity between the module and the configured remote machine.

NOTICE

PING REMOTE MACHINE FEATURE

Before enabling this feature, careful consideration must be given to the remote machine that will be pinged. If that machine is removed or changes address, the Wi-Fi Module will need to be reconfigured.

Failure to follow these instructions can result in having to reconfigure the Wi-Fi Module.

After enabling this feature, check that the ping has been performed successfully (Green checkmark icon is displayed).

Considerations for Remote Machines to ping:

- Consider the primary usage of your Wi-Fi Module when selecting what to ping.
- Only ping your BACnet client (BMS) or SMTP server directly if it uses a static IP address!
- If DHCP (automatic IP assignment) is used for the network, ping the DHCP server. Do not ping a device via its IP address if that IP address may change.
- Before using a domain name, consider the long-term availability of that domain. If it is changed or deactivated your Wi-Fi Module will need to be reconfigured.

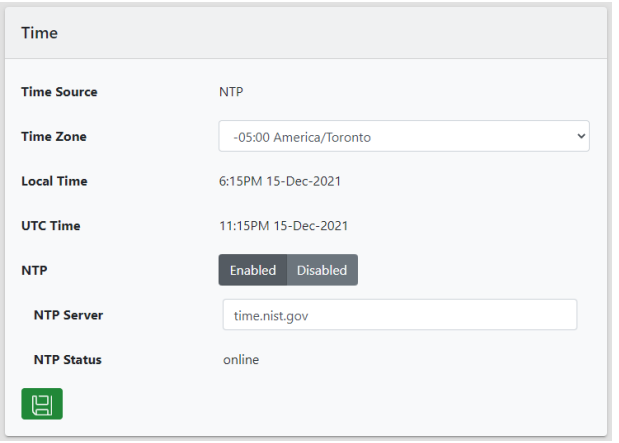
Example Remote Machine Addresses:

- IPv4 Address: 192.168.0.1
- Domain Name: www.se.com

This monitor is disabled by default.

NOTE: If your IT infrastructure allows the Room Controller to access the Internet, you can use a domain name. If Internet access is restricted by your IT administrator, you can use the network's gateway IP address (ask your IT administrator for those details).

Time



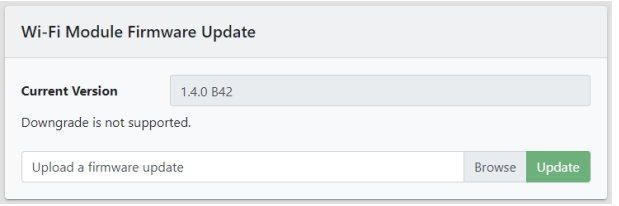
The RC and Wi-Fi Module support setting and maintenance of time via; the RC local display, BACnet, a Network Time Protocol (NTP) server, or the cloud. NTP time can also be enabled and configured using the VT8000 Uploader Tool.

To configure time:

- Always set the time zone on the Wi-Fi Module to allow it to convert between Coordinated Universal Time (UTC) and local time.
- BACnet: If time is received via BACnet, no further configuration is required.
- NTP: If available, it is recommended to configure an NTP server for accurate time.
- Facility Expert: The time zone and time must be correctly set for the Wi-Fi Module to successfully connect to the cloud. Time can be set via NTP (recommended) or locally on the RC display.

For more information, refer to the Wi-Fi Module FAQ.

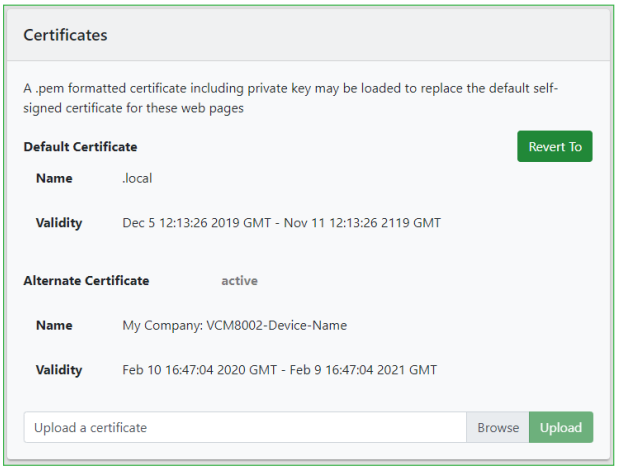
Wi-Fi Module Firmware Update



Upload the latest version SWU file. Only the administrator has permission to update firmware.

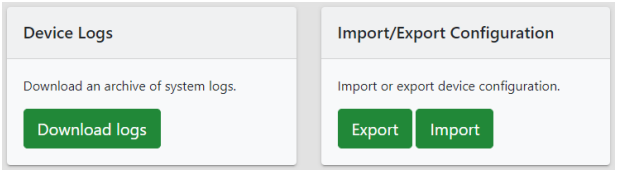
Certificates

The certificate must be in the ".pem" format and include the private key. Browser warnings can be avoided if this certificate is signed by a public or private Certificate Authority known to the browser.



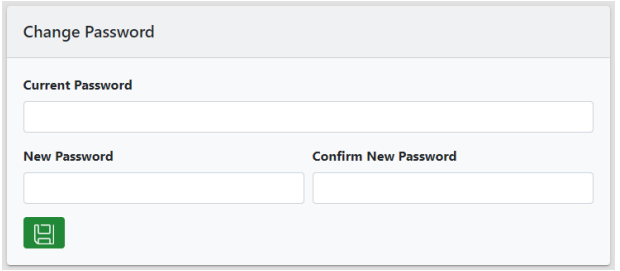
For more information, refer to the Wi-Fi Module FAQ.

Device Logs and Import/Export Configuration



Device logs can be downloaded for troubleshooting and auditing purposes. The Wi-Fi Module configuration can be exported to or imported from a JSON file.

Change Password

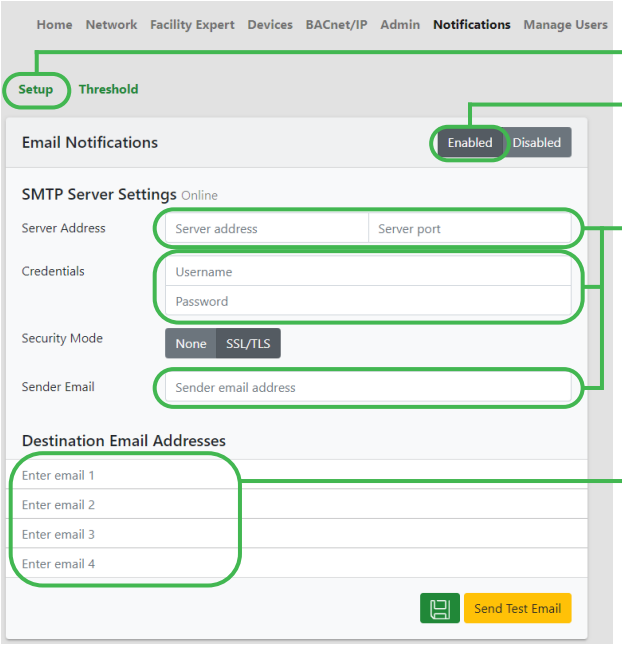


Users can change their current password to a new password.

NOTE: Passwords must have at least 8 characters, one uppercase character, one lowercase character, and one number or symbol.

Notifications

Setup



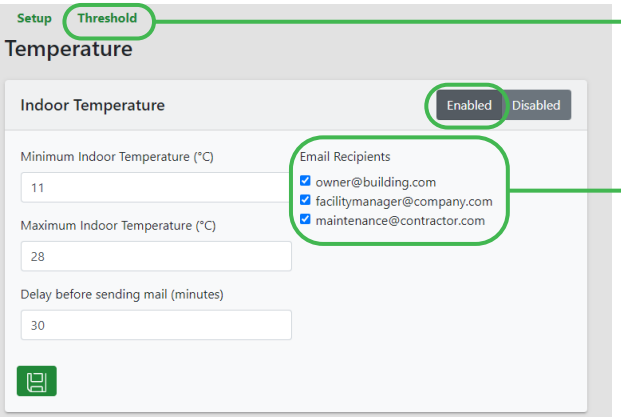
Setup tab

To set up email notifications, first enable them.

You may obtain this information from your IT service provider.

The RC may send notifications to a maximum of 4 email addresses.

Threshold



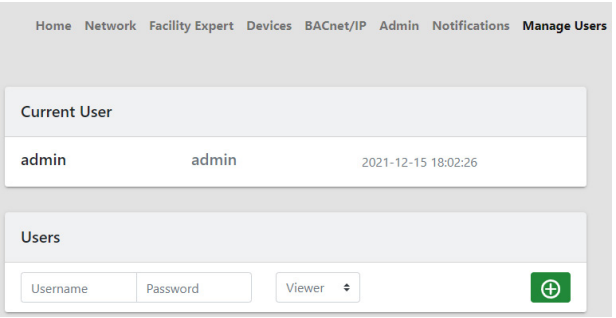
Threshold Tab

A list of registered emails is displayed here.

You can enable various notifications to be sent by email. For example, with the above configuration, the temperature must stay below 11°C or above 28°C for 30 minutes before an email is sent.

For more information, refer to the Wi-Fi Module FAQ.

Manage Users



Only the administrator has permission to add and delete users. Upon their first login, a new user is required to change the password given to them by the administrator.

NOTE: Passwords must have at least 8 characters, one uppercase character, one lowercase character, and one number or symbol.

Administrators cannot view or modify the password of an existing user. If a password reset is required, the user must be deleted and re-created.

Users are assigned one of three roles: Administrator, Manager or Viewer. Capabilities of the roles are shown in the table below:

Role	Administrator	Manager	Viewer
View configuration data	☑	☑	☑
Modify configuration data	☑	☑	☒
Import/export configuration files	☑	☑	☒
Download device log files	☑	☑	☒
Manage certificates	☑	☑	☒
Update firmware	☑	☒	☒
Manage users	☑	☒	☒

Cybersecurity and Auditability

It is strongly recommended to create individual accounts for each user needing to access the RC. Individual accounts increase cybersecurity by ensuring passwords are not shared among multiple people, and ensure auditability as log files can be inspected to see who was responsible for a change in the device configuration.

To ensure the secrecy of user passwords, user accounts are not included in exported or imported configuration files.

TROUBLESHOOTING

- If you lose or forget your admin password for the Configuration Web Page, you must do a Factory reset of the Wi-Fi Module directly on the Room Controller's screen 5/5 of the Wi-Fi Reinitialization menu.

  This action will restore the Wi-Fi Module to the factory settings, erase all configuration data and revert the Wi-Fi Module Firmware to the factory firmware version.

  NOTE: If the room controller had already been connected to Facility Expert, you will need to contact Technical Support once the factory reset is completed, in order to reset the Wi-Fi connection string.

- When decommissioning a Wi-Fi Module, a Factory Reset should be performed to erase all user data on the module
- If you cannot see the contents of the web pages after logging in, ensure JavaScript is enabled on your web browser. It is required to view the Configuration Web Page.

For more information, refer to the Wi-Fi Module FAQ.

GNU LESSER GENERAL PUBLIC LICENSE

For three years after the final factory shipment, you may request a copy of the source code for any portions of the product, which are licensed under the GNU Lesser General Public License by writing to the following address:

7262 Marconi Street
Third Floor
Montreal, QC, H2R 2Z5
Canada

NOTE: Viconics Technologies shall bear no responsibility whatsoever for the source code or its use.

The source code will be provided at no charge, however, we may require you to reimburse Viconics Technologies for the cost of delivering the source code to you.

CALIFORNIA PROPOSITION 65 WARNING STATEMENT FOR CALIFORNIA RESIDENTS

⚠ **WARNING**: This product can expose you to chemicals including Lead, which is known to the State of California to cause cancer and birth defects or other reproductive harm, and Bisphenol A (BPA), which is known to the State of California to cause birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.