VT8000 Room Controllers

Wi-Fi Module Frequently Asked Questions
VCM8002V5031

General

Q: Why is my VT8000 not detecting the Wi-Fi module?

A: Check the firmware version of the Room Controller. It must be version 2.4.0 or higher to detect the Wi-Fi module.

Room Controllers with firmware version 2.0 or higher may be upgraded to support the Wi-Fi module using the VT8000 Uploader Tool 3.x.

Older Room Controllers with firmware version 1.x.x do not support the Wi-Fi module.

Wi-Fi Networks

Q: What Wi-Fi networks can the Wi-Fi module connect to?

A: The Wi-Fi module can connect to networks with the following settings:

- Security:
  - WPA2-PSK (**Recommended**)
  - WPA-PSK (Not recommended)
  - WEP (No longer supported from version 1.4)
  - No security (Not recommended)
- Frequency:
  - 2.4GHz
  - 5GHz is **not supported**
- Protocol:
  - IEEE 802.11 b/g/n

Q: Can I connect the Wi-Fi module to a Wi-Fi network using WEP security?

A: WEP security is no longer supported from version 1.4, as it:

- Is no longer secure: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
- Was deprecated by the Wi-Fi Alliance in 2004
- Is actually very difficult to find a router that will even allow it
- Is recommended against by cybersecurity experts.
- If a network using WEP security is detected it will be shown as “Not supported”.

Q: What considerations should I take with my Wi-Fi network?

A: Ensure your Wi-Fi routers have enough capacity for the number of devices that will be connected to the network. If the Wi-Fi module is “dropped” by the router due to the router reaching its maximum device limit, connectivity can be lost.

Q: Can the Wi-Fi module be connected to hidden Wi-Fi networks?

A: Yes, the Wi-Fi module can connect to networks that do not broadcast their SSID.

IMPORTANT: Ensure the Wi-Fi network is in its desired configuration **before** connecting the Wi-Fi module to the network. The SSID must either be hidden or exposed (broadcast) and must **not** be changed after the Wi-Fi module has been connected.

Q: What common issues does someone using Wi-Fi run into?

A: The following is a list of typical issues that may occur:

- Network security needs to be considered, with strong and carefully-managed passwords.
- Configuration of devices can become complex – managing IP addresses, subnets, ports, etc.
- Wireless network performance can degrade in environments with many networks and heavy traffic loads.
- Performance can also be impacted by the distance between the Wi-Fi module and router, or its physical location (e.g. if you have concrete walls).

NOTE: In general, if a mobile device or personal computer has Wi-Fi access in the location of the Room Controller, the Controller will likely have the same Wi-Fi experience.

Q: Why are the web pages inaccessible after connecting my device to the Wi-Fi module's access point?

A: Check the IP address of your device for the wireless connection to the access point. It should be in the range of 192.168.71.x.

If it is not:

- Ensure that DHCP is enabled for your Wi-Fi client. The Wi-Fi module runs a DHCP server and will automatically assign a valid IP address to your device.
- Or, assign an IP in the range of 192.168.71.x to your Wi-Fi client. Do **not** use the same address as the Wi-Fi module.

NOTE: If the problem persists, refer to "Web Pages" on page 3.

Q: Why is my VT8000 not reconnecting automatically when connected to Tridium N4 built-in Wi-Fi?

A: Its Wi-Fi is not meant for a permanent connection (contact Tridium for more information). Use a standard Wi-Fi router instead.

Q: Why are the web pages inaccessible after connecting my Wi-Fi module to the building Wi-Fi network?

A: Make sure the IP address you are accessing is correct. The Wi-Fi module has different IP addresses for its access point and Building Wi-Fi network connections.

Your device must be connected to the same Wi-Fi network, or have another access to the subnet.

Q: My Wi-Fi module is indicating it has an Auto IP address. What does this mean?

A: If the Wi-Fi module is configured to receive an IP address via DHCP but does not receive one, it will assign one for itself automatically. Typically, this will happen if there is no DHCP server present on the network, it is not responding, or has run out of IP addresses.

Check your DHCP server or assign your Wi-Fi module a static IP address. Typically, a device with an automatically assigned IP address indicates the system has not been correctly configured and will not work as expected.

Q: Should I set up my VCM8002 via USB or its access point?

A: VCM8002 can be setup either way.

The Access Point is recommended when commissioning a few devices as it:

- Only requires a device that connects to Wi-Fi and an internet browser.
- Provides a rich, interactive user interface, for example listing available Wi-Fi networks.
- Supports all features of the VCM8002.

USB is recommended when commissioning large numbers of devices as:

- Connecting via USB is faster than connecting a device to the Access Point of each VCM8002 in turn.
- It handles repetitive commissioning information that is often the same for each VCM8002.
- It supports what is typically required for large projects; connect to the Wi-Fi network and enable BACnet/IP.

Q: What can I commission of my VCM8002 via USB and why?

A: The essential items to get the VCM8002 connected to the building's Wi-Fi network are supported via USB.

Advanced commissioning can then be continued via the VCM8002's configuration web pages, across the building Wi-Fi network, from any machine with access to the network. It is not necessary to connect to the Access Point of each VCM8002 or be physically close to it to complete advanced commissioning.

Advanced commissioning is limited to the VCM8002 web pages only as:

- VCM8002 firmware updates are large files, which can be transferred quicker over Wi-Fi than via the Room Controller.
- The configuration web pages offer a richer, more interactive user interface for complex items like User Management and Email Notifications.

VCM8002 USB commissioning supports:

- Wi-Fi network connection: With user provided network name (SSID)
- IP configuration: DHCP or Static
- BACnet/IP configuration
- NTP configuration

It does not support:

- VCM8002 firmware upgrade
- User management
- Facility Expert configuration
- Email notification configuration
- Time zone selection

Security

Q: Can someone hack into my Wi-Fi module?

A: Whilst it is impossible to guarantee against possible future vulnerabilities in Wi-Fi or embedded software components:

- The VCM8002 was developed within the guidelines of Schneider Electric's cybersecurity process.

- Possible threats were analyzed and rectified:
  - The Wi-Fi access point is secured with WPA2.
  - Web page communication is secured using HTTPS with unique self-signed certificates. Refer to “Certificates” on page 8 for more information.
  - Web page access is authenticated with a user name and password.
  - All features are disabled by default and must be individually enabled by the user based on their requirements.
  - Firmware updates are signed via Schneider Electric’s Public Key Infrastructure, ensuring only authentic software provided by Schneider Electric can be loaded onto the device.
- Penetration testing was performed to ensure the product is not vulnerable to common attacks known at the time of testing.

Q: Is my data freely available to anyone or is it protected?

A: The VCM8002 stores all user data in an encrypted file system.

Configuration data is only available via the configuration web pages, where users must authenticate with a user name and password, and sessions are protected via HTTPS.

All user data can be entirely removed by doing a factory reset of the module.

Q: When planning my network, what should I consider to protect data or equipment (router, firewall, etc.)?

A: There are no requirements on the infrastructure, as the VCM8002 is secure, with all ports closed by default.

Some recommendations should be followed:

- Security should be enabled on the Wi-Fi network:
  - WPA2 is recommended.
  - Strong and unique passwords should be used and carefully managed.
  - MAC white listing can be used to ensure only the intended devices can access the network.
- Updates should be done regularly to ensure devices are protected with the latest security features and patches.
- If email notifications are used, SSL or TLS security should be used to authenticate the SMTP server and encrypt messages.
- If BACnet/IP is to be used, network access should be carefully considered (see below for more details).

Q: Is there anything special I need to add to the project to protect the Building Management System (BMS)?

A: BACnet/IP may be enabled for integration with a Building Management System. If BACnet/IP is used, the following points should be considered:

- BACnet/IP opens a port on the VCM8002, which allows any device with access to the subnet (the Wi-Fi network) to discover and control the VT8000 using the BACnet/IP protocol.
- This means access to the network should be strictly managed, as any device on the network (even a smartphone with a BACnet app) can control the VT8000.

Q: I want to decommission my Wi-Fi module. What should I do to ensure all my data is erased?

A: Factory reset the Wi-Fi module via the “Wi-Fi Reinitialization” screen of the VT8000. 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.

Web Pages

Q: I lost the user name and password for the configuration web pages. What can I do?

A: There are no security backdoors in the Wi-Fi module. You will need to Factory Reset the Wi-Fi module and re-commission it.

NOTE: If the 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.

Q: My IP addresses are correct, but I cannot see anything on the web pages. What can I do?

A: Check the security configuration of your web browser. To access the configuration web pages, you must accept the self-signed certificate. Some browsers, particularly in corporate configurations, may not allow access to a web page with a self-signed certificate. In this case, contact your IT support department.

Q: Why does my web browser warn me the connection is insecure when I access the configuration web pages?

A: In fact, the connection to the web pages is secured with HTTPS, but the browser is warning you that it is unable to verify the identity of the Wi-Fi module. This occurs as the Wi-Fi module uses a self-signed certificate, which is not verified by a Certificate Authority (CA).

Q: When I access the configuration web pages, why do I only see some heading components, not the contents of the pages?

A: Make sure JavaScript is enabled in your web browser. It is required to view the configuration web pages.

Various websites can tell you if JavaScript is enabled. Try searching "is JavaScript enabled in my browser".

BACnet/IP

Q: My BACnet Building Management System (BMS) reports that VT8000s connected via Wi-Fi are going offline for short periods of time (e.g. 1 minute).

A: Wi-Fi devices sometimes need to reconnect to the Wi-Fi network. If a Wi-Fi reconnection coincides with a BACnet message from the BMS, the BMS may not get a response from the VT8000 and hence may report it as offline.

To resolve the issue, it is recommended to:

- Review the Wi-Fi signal to the VT8000, particularly if only some (not all) devices are affected:
  - If it is weak, consider installing more access points.
  - Consider if it is physically located where other devices may be interfering with the Wi-Fi signals?
- Review the Wi-Fi Access Point settings to try to reduce reconnections, particularly if the majority of devices are affected:
  - Consult recommendations from the Wi-Fi Access Point manufacturer.
  - Pay attention to configured timeouts for security keys or sessions. Try extending these and observe if the rate of issues decreases.
- If the above steps do not reduce or resolve the issue, try increasing the APDU Timeout of the BACnet client:
  - Typically, clients are configured with:
    - APDU Timeout = 3 seconds
    - APDU Retries = 3
  - This means a BMS will try a message 4 times, 3 seconds apart, for a total of 12 seconds, before it fails and considers the device offline.
  - If the Wi-Fi reconnection time of the device and access points exceeds 12 seconds (in the example above), BACnet messages may fail.
  - Extending the APDU timeout or retries causes the BACnet client to wait longer before failing a message, giving the Wi-Fi device more time to complete its reconnection

Consider all factors when extending APDU retries and timeouts, as other parts of the system may be affected.

For more information, refer to the "Guide to Industrial Wireless Systems Deployments" from the National Institute of Standards and Technology, U.S. Department of Commerce.

Q: Can my VT8000 access both BACnet/MSTP and BACnet/IP at the same time?

A: No. Only one BACnet protocol can be used at a time.

BACnet/IP will be used if:

- A Wi-Fi module is installed in the VT8000.
- BACnet/IP is enabled on the Wi-Fi module.

Otherwise, BACnet/MSTP is available.

Email Notification

Q: Why does the SMTP server not become "Online"?

A1: Check your SMTP server settings. Successfully reaching an online status requires the following settings to be correctly configured:

- Server Address
- Port
- Security

A2: Set the time on your VT8000. The VT8000 and Wi-Fi Module need a reasonably accurate time reference to validate security certificates for secured SMTP servers. If the time is not set, or significantly wrong, the certificate validation will fail as the certificate appears to have expired.

NOTE: Make sure you are using the correct value for AM/PM, as this may cause issues.

Q: Why is the SMTP server "Online", but the test email does not work?

A: "Online" confirms that the SMTP server address, port, and security are configured correctly. However, to successfully send an email, the following settings must also be configured correctly:

- User name.
- Password.
- Security settings of your SMTP server. For example, some web mail type service providers require account settings to be correctly configured for use as an SMTP server:

  Gmail: Make sure "Allow less secure apps" is enabled.
- Valid destination email addresses.

VT8000 Room Controllers

Wi-Fi Module Quick Start Guide
VCM8002V5031

Prerequisites

This quick start guide assumes the VCM8002V5045 is:

- Installed into a VT8000 Room Controller.
- Connected to a Wi-Fi network with an internet connection.

Application Guidelines

VT8000 supports BMS integration via:

- BACnet/IP over Wi-Fi using VCM8002
- BACnet/MSTP (wired RS-485)
- Modbus RTU (wired RS-485)

When considering the use of Wi-Fi while designing a system, the following points should be considered:

- Wi-Fi is a wireless technology and hence devices are more likely to experience temporary offline periods due to events such as:
  - Wireless interference.
  - Changes in the physical environment disrupting the signal to a device.
  - Wi-Fi Access Points restarting or updating.
  - Wi-Fi Access Points becoming overloaded and dropping devices, requiring them to reconnect.
  - Load balancing between access points.
  - Channel or key changes in the Wi-Fi network.
- Wi-Fi offline periods (while it is reconnecting) may cause devices to appear Offline in the BMS system.
- If it is critical for your system that the BMS always has access to the VT8000 then a wired connection may be more suitable than Wi-Fi.
- Wi-Fi is highly dependent on the configuration of the Access Points.
- Consult the manufacturer's guidelines for configuring the system.

For more information, refer to the "Guide to Industrial Wireless Systems Deployments" from the National Institute of Standards and Technology, U.S. Department of Commerce.

Time Configuration

WARNING: Time synchronization requires VT8000 firmware 2.4.0 or higher.

The VT8000 and VCM8002 support setting and maintenance of time via the VT8000 local display, BACnet, a Network Time Protocol (NTP) server, or Facility Expert.

The time zone must always be correctly configured on the VCM8002 to allow it to convert between local and UTC sources.

The active time source is displayed on the VT8000 "2/2 Clock" screen and the VCM8002 Admin tab. Time sources will be used based on the following priority (1 is highest), with fail-over from higher to lower priority sources when the higher priority source is disabled or offline.

1. Cloud: UTC is coming from Facility Expert. Local time is calculated by the VCM8002 and written to the attached VT8000.
2. NTP: UTC is coming from the configured NTP server. Local time is calculated by the VCM8002 and written to the attached VT8000.
3. BACnet: Local time is received via BACnet.
4. Local: Local time was set via the VT8000's touchscreen or resumed from its Real-Time Clock after powering on.

Whenever possible, the use of an NTP server is recommended for the VCM8002.

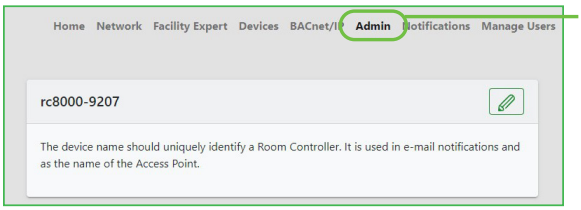
NTP Configuration

NTP may be enabled and configured with the IPv4 address or domain name of a local or remote (internet) NTP server.

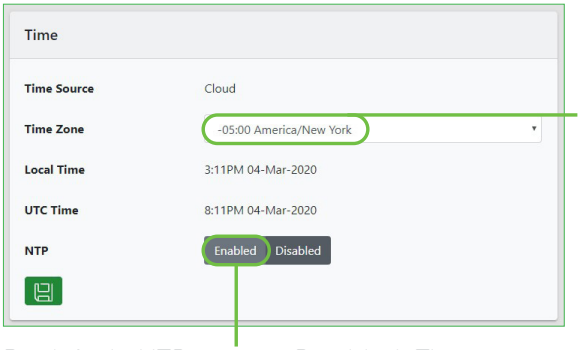
NTP best practice suggests using an NTP server as "close" (in network terms) to the device as possible, so a local server is preferable.

Using Local NTP servers requires a valid Wi-Fi connection. Remote servers require an internet connection and with the internet, we suggest Ping Device Monitoring. Check to ensure the "NTP Status" becomes "online" before completing commissioning.

The NTP option is disabled by default. When enabled, a default server of "time.nist.gov" is used.



Go to the Admin tab.



Select the Time Zone of the site.

By default, NTP is set to Disabled. This is not a problem, because the device will synchronize its time with the local time on the VT8000, BACnet or Facility Expert. However, you can choose to Enable NTP and configure a backup connection to ensure that time is still synchronized in the case where connectivity to Facility Expert is lost.

Email Notifications

This section explains how to use the VT8000 Room Controller email notifications with common webmail providers. All information is current as of the date of publication. No guarantees can be given on the future configuration of third-party email providers.

Configure the SMTP Server

Sending email requires an SMTP (Simple Mail Transfer Protocol) server to relay emails to the recipients.

1. Enable email notifications.
2. Enter the SMTP server address: smtp.myEmail.com.
3. Enter the port: 465.
4. Enter the user name of the webmail account. For example, "myUserName" if the account is myUserName@myEmail.com.
5. Enter the account password.
6. Select SSL/TLS security.
7. Set the sender address. This field is optional and can be left blank.
8. Set the destination addresses (recipients) who will receive the email notifications.

   NOTE: Each of these addresses can then be individually selected/deselected for each type of email notification.
9. Save your settings.

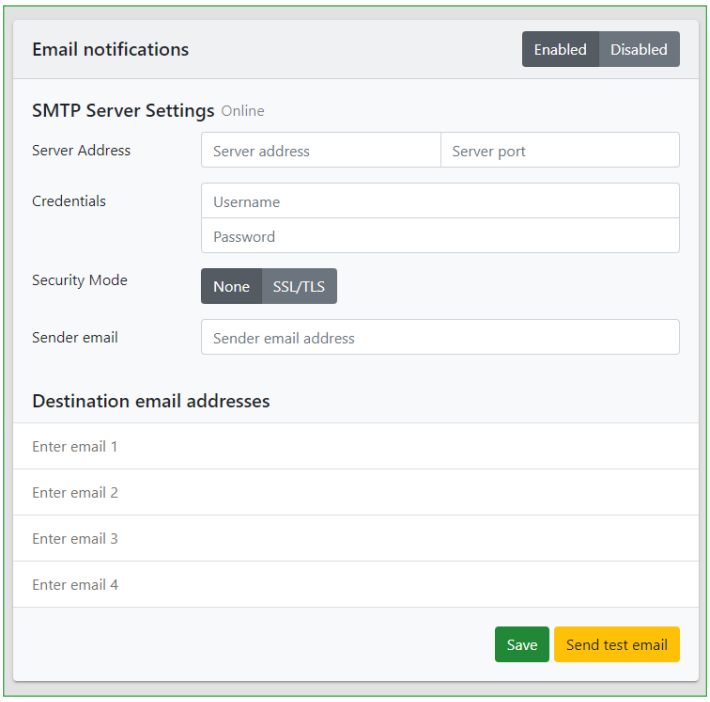


Figure 1: SMTP Server Configuration

Once saved:

- The status shown next to "SMTP Server Settings" should change to "Online", indicating the device can connect to the SMTP server.

  If not, check your SMTP server settings.
- The "Send test email" button can be used to send a test email to each destination and confirm that the configuration is working correctly.

  If not, check that the SMTP server is online, and the user name and password are valid.

Webmail

NOTICE
It is not recommended to use free webmail accounts for email notifications in a professional installation. Webmail providers may change their functionality or security settings at any time, and this may result in service disruption or failure. If you do use a webmail account for email notifications, **it is strongly recommended to create a dedicated account for each site** to contain security risks and limit the scope of devices affected by changes to the account settings or password. Do not use your personal email account. **Failure to follow these instructions can result in service disruption or failure.**

No guarantees are given for the future compatibility of third-party email providers; however, some options are listed below. To find guides for these email services, try searching for "using Gmail as an SMTP server" or similar.

- **Gmail** (as demonstrated in this guide) – Refer to "Use G Suite settings to set up a device or app to send email": https://support.google.com/a/answer/176600?hl=en
- **Yahoo Mail** – Refer to "POP access settings and instructions for Yahoo Mail": https://help.yahoo.com/kb/SLN4724.html
- **Outlook.com** – "POP, IMAP, and SMTP settings for Outlook.com": https://support.office.com/en-us/article/pop-imap-and-smtp-settings-for-outlook-com-d088b986-291d-42b8-9564-9c414e2aa040

The following table shows alternative webmail configurations:

Server Address	Port	Security Mode
smtp.gmail.com	465	SSL/TLS
smtp.gmail.com	587	SSL/TLS
smtp.mail.yahoo.com	465	SSL/TLS
smtp.mail.yahoo.com	587	SSL/TLS
smtp-mail.outlook.com	587	SSL/TLS

Create a Gmail Account

For reference only: The use of free webmail is not recommended for real sites.

Create an account for the Room Controller(s) of a site by following the procedure from Gmail: https://support.google.com/mail/answer/56256?hl=en

NOTE: To use Gmail, you MUST enable "Less Secure Apps" on the account.

Refer to "Allow or disallow less secure apps to access accounts": https://support.google.com/a/answer/6260879

Configure Notifications

An email notification may be configured for the following events:

- Temperature Out of Range:
  - Indoor
  - Outdoor
  - Supply
  - Remote
- CO2 Out of Range
- Humidity Out of Range
- Alarms:
  - Service Alarm
  - Water Leak Alarm
  - Dirty Filter Alarm
  - Wireless Sensor Low Battery
  - Wireless Sensor Communication Failure
  - Clock Alarm
  - Low Temperature Alarm (from wireless sensors)
  - Frost Protection Alarm
  - Fan Lock Alarm
  - Low Fresh Air Alarm

Below is an example of how to configure an out of range notification for the indoor (room) temperature:

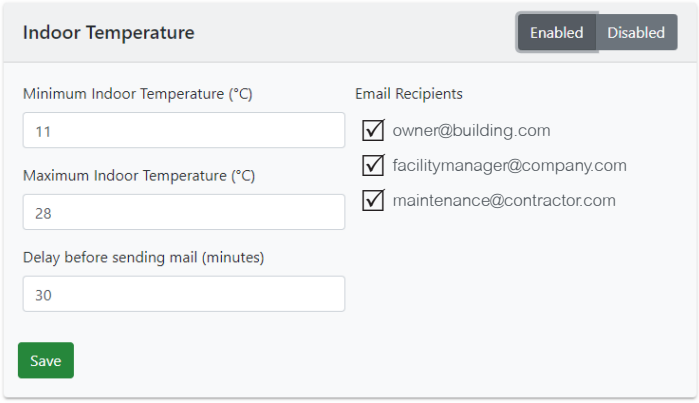


Figure 2: Indoor Temperature Notification

1. Enable the notification.
2. Specify the temperature below which an email notification will be sent.
3. Specify the temperature above which an email notification will be sent.
4. Specify the duration for which the temperature must stay continuously out of limits before an email notification is sent.
   - With the configuration above, the temperature must stay below 11°C (51.8°F) or above 28°C (82.4°F) for 30 minutes before an email is sent.
   - The delay is useful to avoid notifications being sent for short-term events such as when a door is left open.
   - The delay may be set to zero minutes if immediate notifications are required.
   - A notification will be sent immediately when the notification condition is cleared to inform the email recipients the issue is no longer present.
5. Select which of the (up to 4) previously configured email addresses will receive these email notifications.

Email Notification Contents

When an email notification event occurs, each selected recipient will receive an email similar to the example below:

> Subject: VT8000 - [DeviceName]: Indoor Temperature out of range (85.0F)
>
> [DeviceName] has detected the Indoor Temperature is out of range:
>
> - Current Indoor Temperature = 29.4C/85.0F
> - Minimum Indoor Temperature Threshold = 11.0C/51.8F
> - Maximum Indoor Temperature Threshold = 28.0C/82.4F
> - VT8000 Date = 05-Nov-2018
> - VT8000 Time = 11:31:04

When an email notification event clears, each selected recipient will receive an email similar to the example below:

> Subject: VT8000 - [DeviceName]: Indoor Temperature out of range - Cleared
>
> [DeviceName] has detected the Indoor Temperature is no longer out of range:
>
> - Current Indoor Temperature = 28.1C/82.5F
> - Minimum Indoor Temperature Threshold = 11.0C/51.8F
> - Maximum Indoor Temperature Threshold = 28.0C/82.4F
> - VT8000 Date = 05-Nov-2018
> - VT8000 Time = 11:54:38

Certificates

The VCM8002's configuration web pages are secured with HTTPS using, by default, a self-signed certificate. Whilst secure, this causes web browsers to warn users about a potential security issue as the browser is unable to validate the certificate with a known, trusted certificate authority.

The self-signed certificate can be replaced with a user-supplied certificate. 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.

WARNINGS:

- A unique certificate should be generated for each VCM8002. Do not re-use the same certificate on multiple devices.
- PEM files contain security-sensitive material and should be managed accordingly.

Certificates need to be configured. Go to the Admin tab to configure certificates.

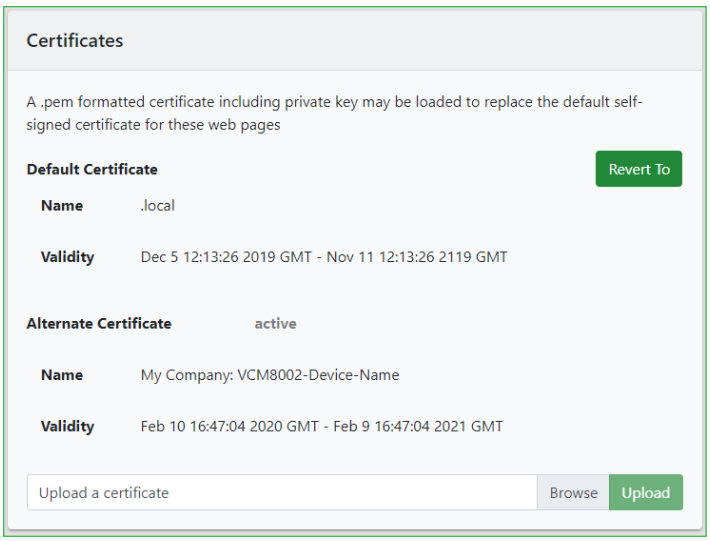


Figure 3: Certificates

Sample procedure for creating a certificate

The following example shows how to create a new self-signed certificate that can be loaded on a VCM8002.

Please note: This example does not include signing by either a public or private Certificate Authority. If required, please contact an IT professional with knowledge of Certificate generation and signing.

This example was written for OpenSSL 1.1.1b on Windows.

Prepare:

1. Install OpenSSL.
2. Open windows command prompt: Windows+R, then type "cmd"
3. Navigate to the folder where you want to create certificates, for example, cd c:\VCM8002\mySiteName

Generate Certificate and Key:

Execute command:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365
-out certificate.pem
```

This will generate a new x509 certificate with a 2048bit RSA key, valid for 365 days. The private key will be output into key.pem. The certificate will be output into certificate.pem.

OpenSSL will ask for some information to be entered:

Country Name (2 letter code) [AU]:

- The ISO-3166 2-character country code for the country the device is installed in. Refer to: https://www.iso.org/iso-3166-country-codes.html
- Examples:
  - Canada = CA
  - USA = US

State or Province Name (full name) [Some-State]:

- The state or province the device is installed in

Locality Name (e.g., city) []:

- The locality (city) the device is installed in

Organization Name (e.g., company) [Internet Widgits Pty Ltd]:

- The name of the organization to whom the device belongs

Organizational Unit Name (e.g., section) []:

- The unit within the organization to which the device belongs

Common Name (e.g. server FQDN or YOUR name) []:

- The Common name of the device.
- For VCM8002, it is recommended to use the Device Name (also the hostname) as configured on the Admin tab of the configuration web pages.

Email Address []:

- Contact email for the administrator of the device

NOTE: If generating multiple certificates, it is recommended to use an OpenSSL configuration for the above command to avoid needing to type information many times.

Combine Certificate and Key:

Execute command:

```
cat key.pem certificate.pem > VCM8002-Certificate.pem
```

The file "VCM8002-Certificate.pem" will now be created and can be loaded to your VCM8002 via the Admin tab of its configuration web pages.

Cleanup Cybersecurity Critical Files

Delete or otherwise secure key.pem, certificate.pem, and VCM8002-Certificate.pem. These files contain keys that are critical to the cybersecurity of your VCM8002.