



VIP STATUS MONITOR USER GUIDE

Version 4.2.0

Abstract

A guide to monitoring Valcom VoIP endpoints
with the VIP Status Monitor software.

Valcom, Inc.
Copyright © 2023

Table of Contents

Introduction	5
Installing the VIP Status Monitor	6
Getting Started with the VIP Status Monitor	11
Importing Devices from the VIP-102B Tool	11
Working with Configuration Files in the VSM	13
Starting a New Session	13
Saving the Current Session	13
Opening a Previous Session	13
Configuring Devices in the VIP Status Monitor	14
Adding a New Device	14
Entering Standard Fields	14
Selecting a Test Method	15
Configuring a Failover System	16
Adding a Range of Devices	16
Changing an Existing Device	17
Deleting an Existing Device	17
Changing the Test Method for Multiple Devices	17
Working with the VIP Status Monitor	19
Examining the State of Devices	19
Receiving Client Notifications	20
Viewing Device Details	20
Using the Device Context Menu	21
Customizing the Display	21
Views and Groupings	21
Showing the Summary View	24
The System Tray Context Menu	25
Controlling Network Ports	26
Fire Panel Supervision Details	27
External Supervision Details	28

Settings and Notification Options	29
General Client Settings.....	29
Test Control Settings.....	31
Standard Test Settings	31
VoIP Heartbeat Test Settings	32
Mail Settings	34
Syslog Settings.....	38
Relay Control Settings.....	40
V-Alert Settings	42
MQTT Settings.....	44
Network Interface Settings	46
Security and Remote Access	48
Protecting the VSM from Local Changes	48
Remote Access with the VSM	49
Enabling Remote Access	49
Connecting from a Remote Client.....	50
Advanced Topics and Troubleshooting.....	53
Controlling the Monitor Service.....	53
Windows Firewall Configuration.....	55
Storage Location of Data Files	56
Reverting to an Older Version of the VSM.....	59
Known Device Issues with the VSM	60
Using a Web Request with eLaunch.....	60
Using a Heartbeat Request with I/O Units.....	60
Supervising a UTM Router	60
Appendix A: VSM Syslog Messages.....	61
Emergency	62
Alert.....	62
Critical	63
Error	64
Warning.....	64
Notice.....	65

Info	66
Debug	67
Appendix B: Required Protocols and Ports	68

Introduction

The VIP Status Monitor is a powerful tool that can be used to monitor and supervise devices on an IP based network. The VIP Status Monitor, referred to as the VSM for the remainder of this document, was mainly designed to supervise endpoints in a Valcom VoIP based paging system and provide notifications when problems are detected. Monitoring is not limited to Valcom VoIP endpoints, however, and any device with a valid IP address on the network can be watched for network issues.

An advantage of using the VSM is that it does not rely on passive resources, such as syslog, to provide its information. Instead, the tool will periodically contact each configured device to verify that it receives a proper response. Valcom VoIP devices can typically be monitored using specialized protocols that were designed for communication between the devices. This helps to ensure that communications between them are working and will be successful. Other devices can be tested for basic network connectivity using protocols such as ping or http web requests.

The VSM can be configured to perform a variety of notifications when problems are detected. Simple notifications such as audio alarms and system tray messages will easily give noticeable warnings when the tool is running on a workstation that is attended by a user. The VSM can also be configured to send syslog or e-mail messages and control relay outputs for cases when it is running on a server based PC that is not typically interacted with on a daily basis.

Use of the VSM can be an essential part of keeping a watchful eye on your network based devices. If a problem occurs, the VSM can let you know about it in a timely manner so action can be taken on your time schedule instead of finding out about it during a critical situation.

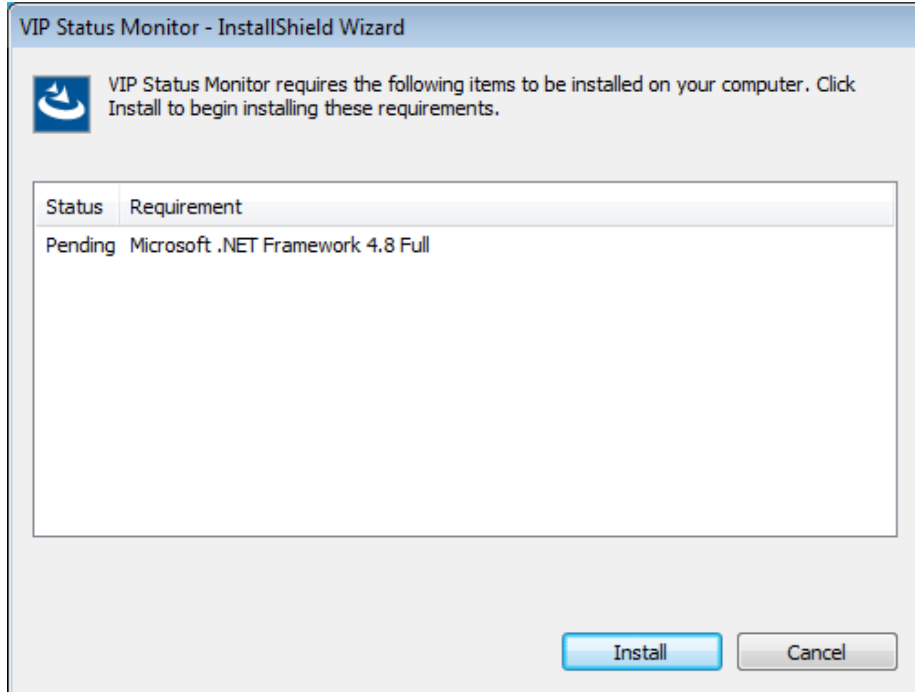
Installing the VIP Status Monitor

Installation of the VSM can be performed by obtaining the latest setup file from Valcom. There are typically two versions of the installation that are offered, a full setup and an upgrade setup. Despite their names, either setup file can be used to perform a new or upgraded installation. The download choice is simply affected by whether or not the required version of the Microsoft .NET Framework is already present and whether the PC has internet access. The Microsoft .NET Framework version 4.8 or greater is currently required to install and use the VSM.

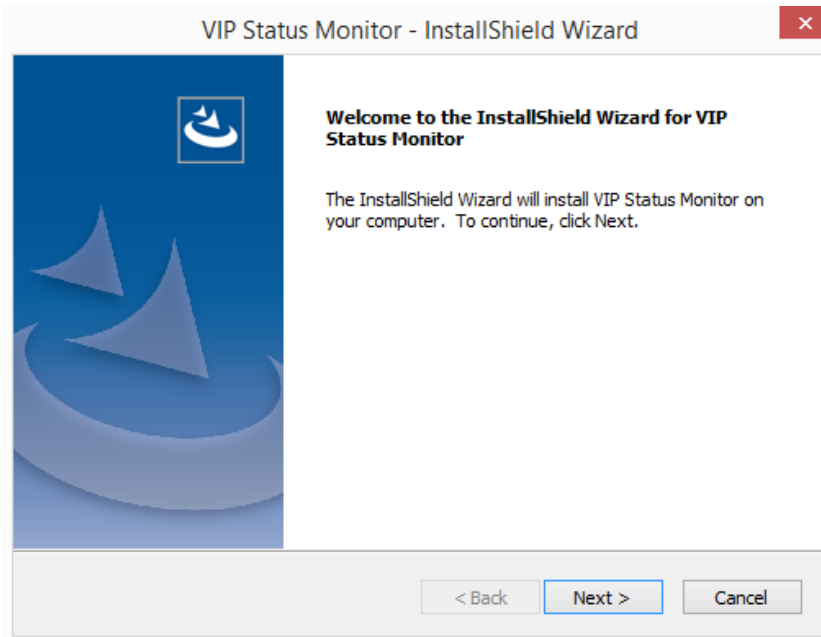
The full or complete setup file contains all the files and components needed to install the program, including the Microsoft .NET Framework. The full setup file is larger, but might be needed when installing the VSM on a PC without internet access that does not already have the .NET Framework installed.

If the .NET Framework is already present on the destination PC, the upgrade or web setup file can be used. This setup file is smaller in size and only contains the VSM runtime files and does not include the .NET Framework. This setup file can still be used, however, to install the .NET Framework if internet access is available. If the Framework is needed, it will be downloaded and installed by this setup file as necessary.

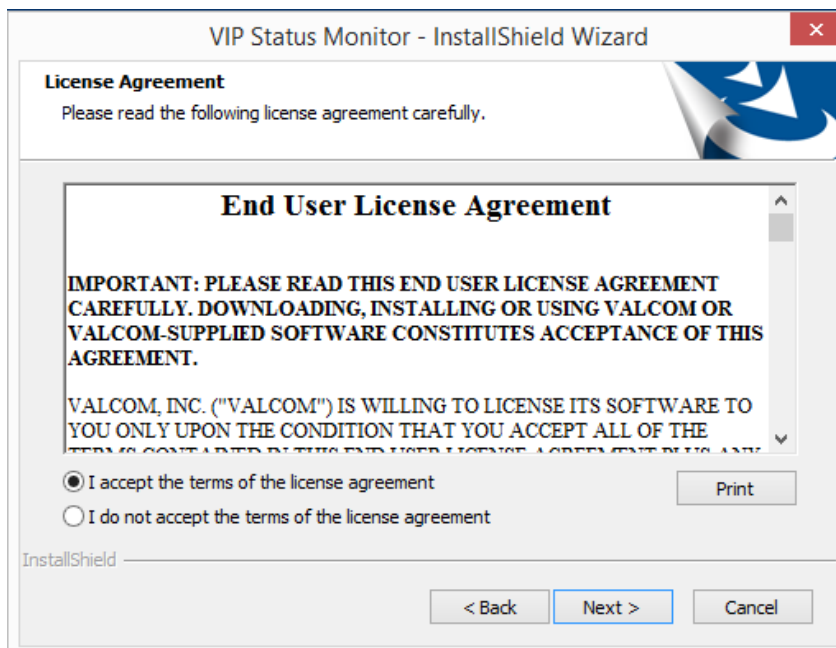
Once the setup file is downloaded, it can be launched by double-clicking on the file. If the .NET Framework needs to be installed, you will be prompted to install it. A reboot may be required.



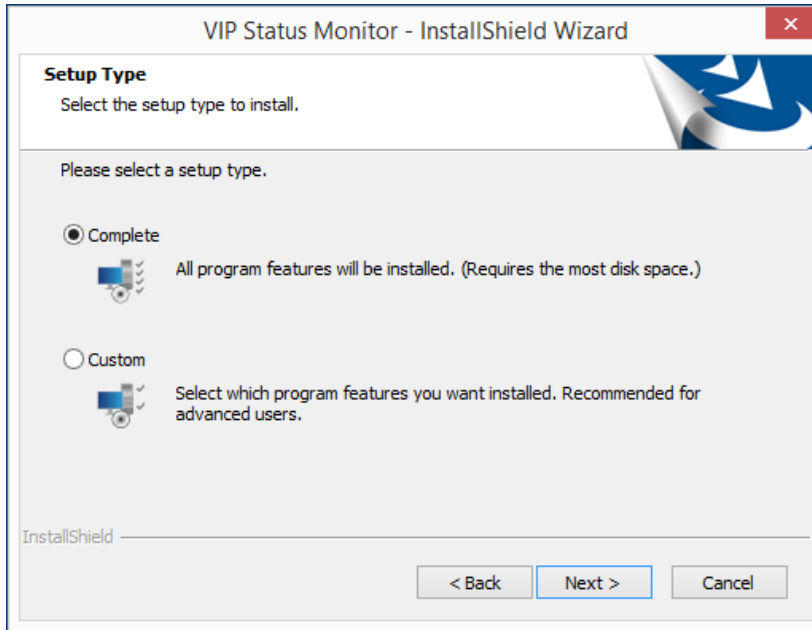
Once the .NET Framework setup is complete, the normal installation will begin.



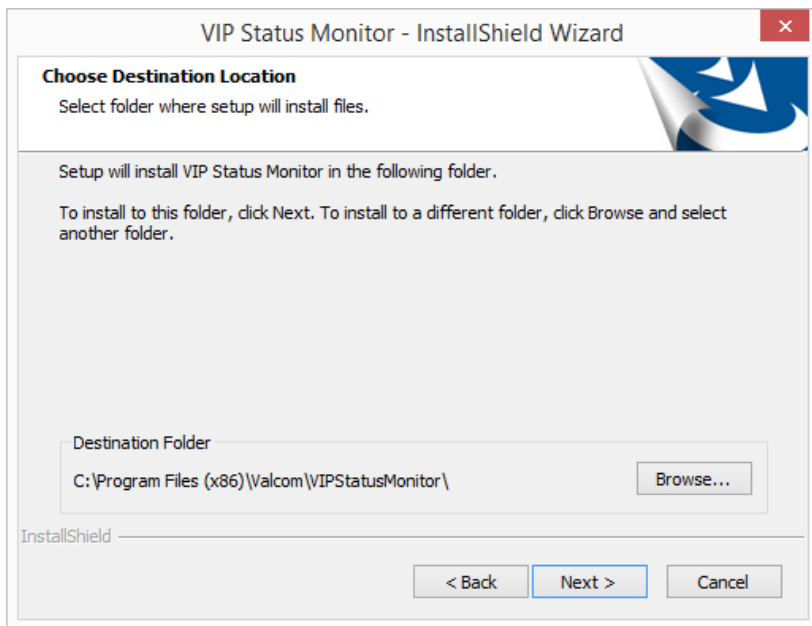
You will be presented with a license agreement for the VSM. The license agreement must be accepted before the installation can continue.



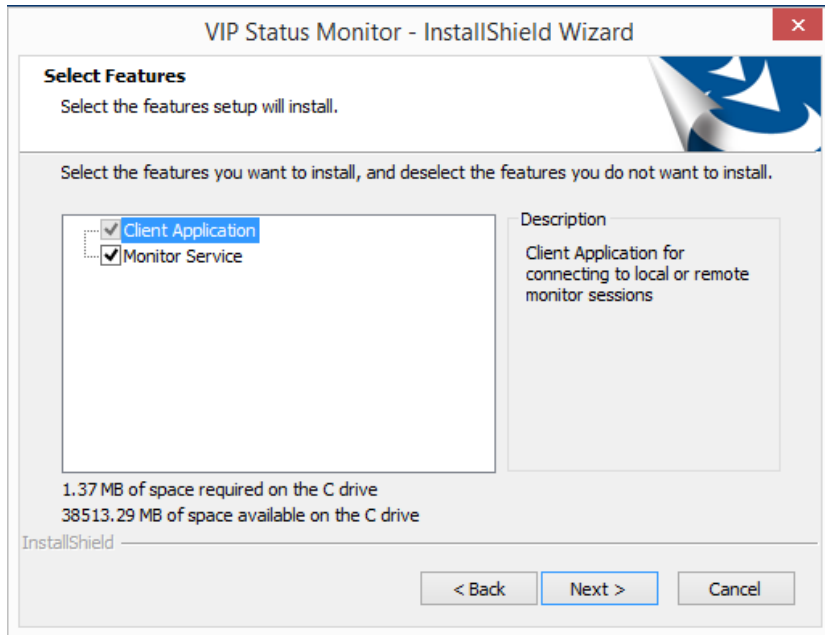
You will then be presented with a choice between two different methods of installation. A Complete install will install all possible features for the program. A Custom install will only install the features that you request and will allow the installation location to be changed. Please select the desired setup type and continue.



A Complete install does not require any further input, but the Custom install will require several additional choices. In this mode you will first be presented with a screen to allow you to select the location where you want the VSM to be installed. Either use the default location or change the location as desired and continue.



After selecting the installation location during a Custom installation, you will be given a choice for which features of the VSM you wish to install. There are two main features included, the Client Application and the Monitor Service.

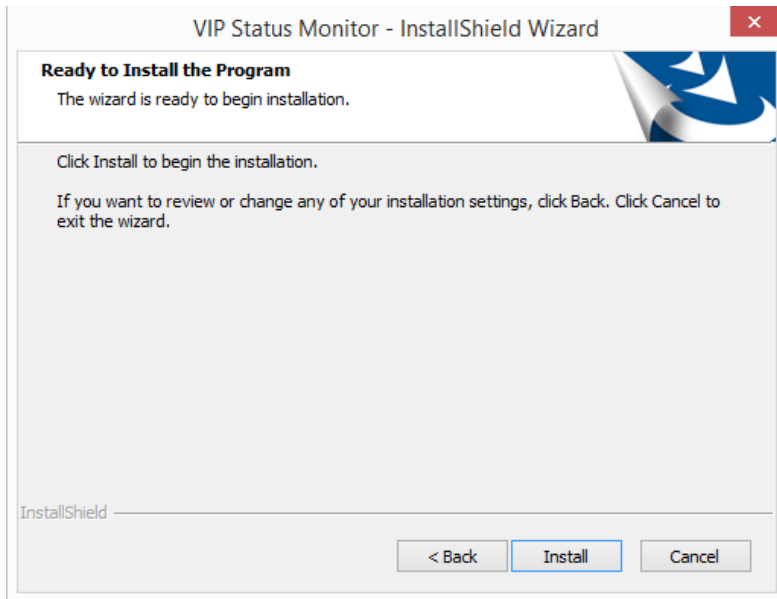


The Monitor Service is the portion of the VSM that actually performs the work of monitoring network devices and raising notifications, such as e-mail and syslog. This component will run as a Windows Service, even if a user is not logged into the PC.

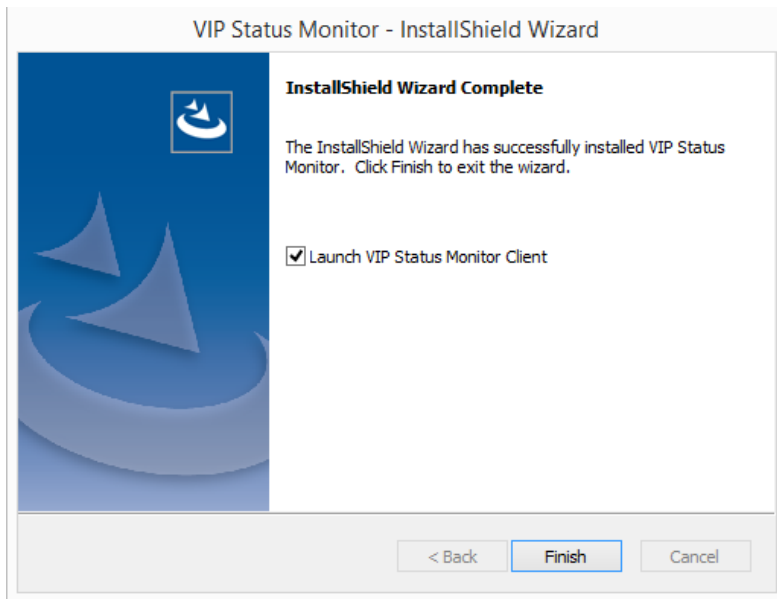
The Client Application is used to configure the Monitor Service and receive interactive notifications while logged in, such as system tray messages and audio alarms. It can also be used to configure the Monitor Service on a remote machine, as discussed later in this document.

The Client Application is required for every instance of the VSM, but the Monitor Service is optional. If you want this machine to actually perform monitoring, both options should remain checked. If you only want this machine to have the ability to connect to the VSM on a remote machine, however, the Monitor Service may be unchecked. The choices can always be changed at a later time by entering maintenance mode for the VSM through the Add / Remove Programs panel within Windows.

After the choices are made, you may continue with the installation.

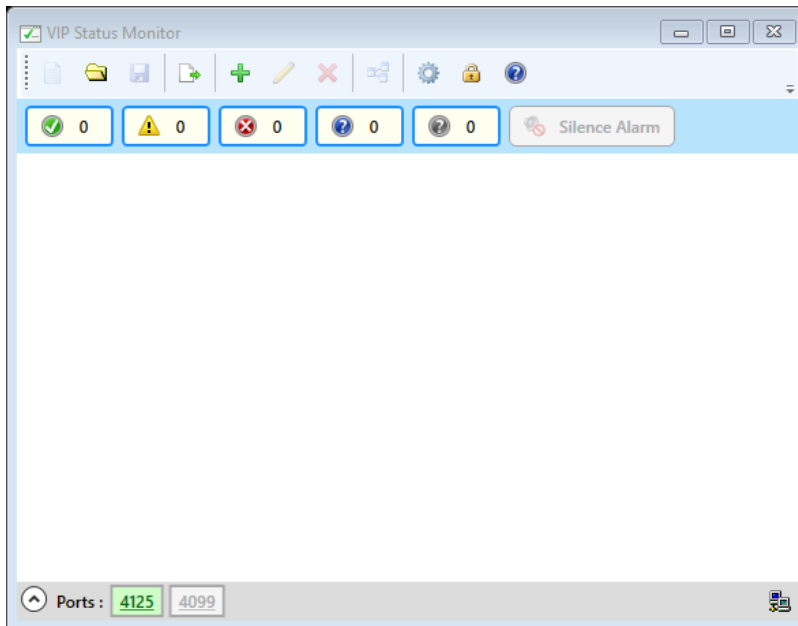



Once the installation is complete, the Monitor Service should start automatically if it was installed. The installation will give you the option of also launching the Client Application at this time if desired.



Getting Started with the VIP Status Monitor

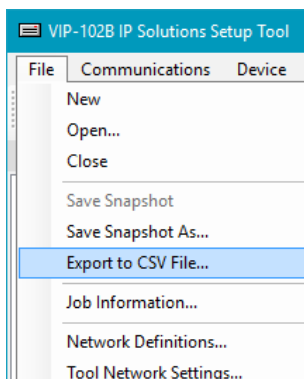
When the VSM client is launched, you will be presented with a screen for working with the program. This screen is the main place where interactions with the VSM will occur.




You will also notice a new icon in your system tray notification area that will display the overall state of the VSM.  Because no devices have been entered yet, it should display an unknown state.

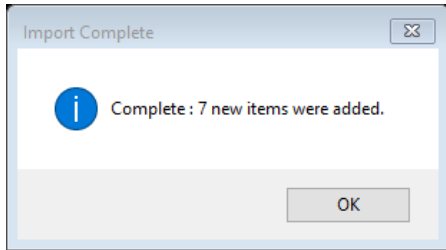
Importing Devices from the VIP-102B Tool

The quickest and easiest way to get started with using the VSM is to export a CSV file of your devices from the VIP-102B IP Solutions Setup Tool and then import that file into the VSM. The use of the VIP-102B tool is beyond the scope of this document, but the export option is typically found under the File menu in this tool.

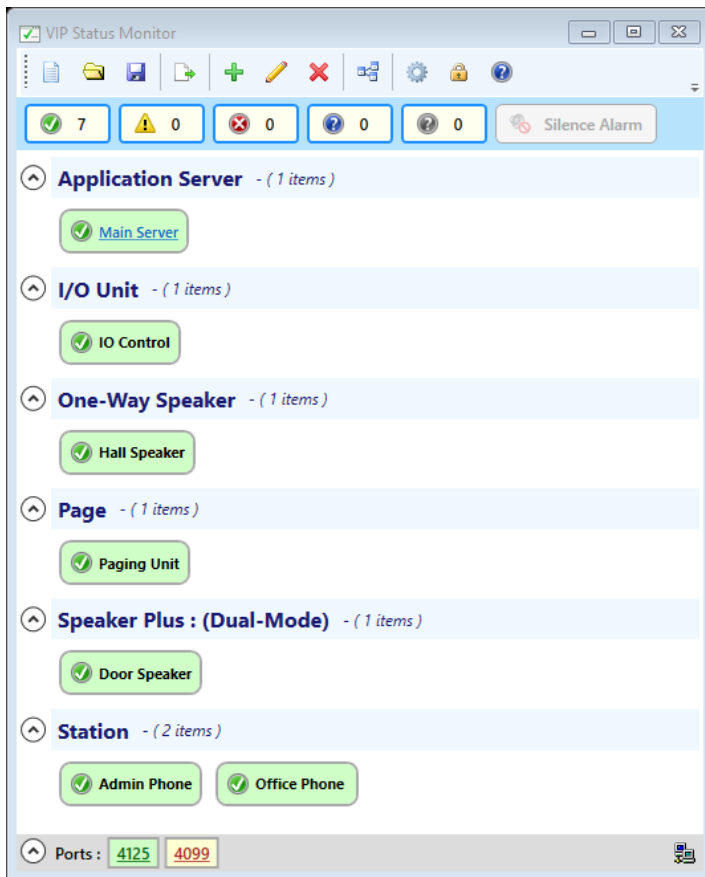


Once the CSV file has been exported from the VIP-102B tool, it may be imported into the VSM by clicking on the Import button in the main toolbar.  Clicking this button will open up a dialog that will

allow you to select the exported CSV file. Once the file is selected, it will be read into the VSM using the default options. You will be presented with a message that tells you how many devices were imported.



The devices will then appear in the main screen and monitoring will begin on each of them.




If new devices are added to your system in the future, a new CSV file can be imported into the VSM at any time. Any devices that are already present will remain unchanged, but new devices will be imported so they can also be monitored.

Please note that heartbeat testing, the preferred method for many imported devices, is initially disabled globally by default and might need to be enabled at this time for optimal testing if desired. Please refer to the sections of this document on heartbeat testing and tool settings for more details.


Working with Configuration Files in the VSM

The configuration for the VSM is stored in basic INI files that can easily be saved or opened from within the tool. This allows you to back up your configuration for safe keeping or to transfer the configuration from one instance of the VSM to an instance on another machine. There are several buttons for controlling the file used on the main toolbar of the VSM.


Starting a New Session

The New Session button  will delete all devices currently loaded into the VSM and allow you to start a new monitoring session from scratch. You will be asked for confirmation before starting a new session and this action cannot be undone unless you have saved a backup file.

Saving the Current Session

The Save button  will allow you to save your current configuration to an INI file that can be used as a backup or to transfer settings to another tool.


Opening a Previous Session

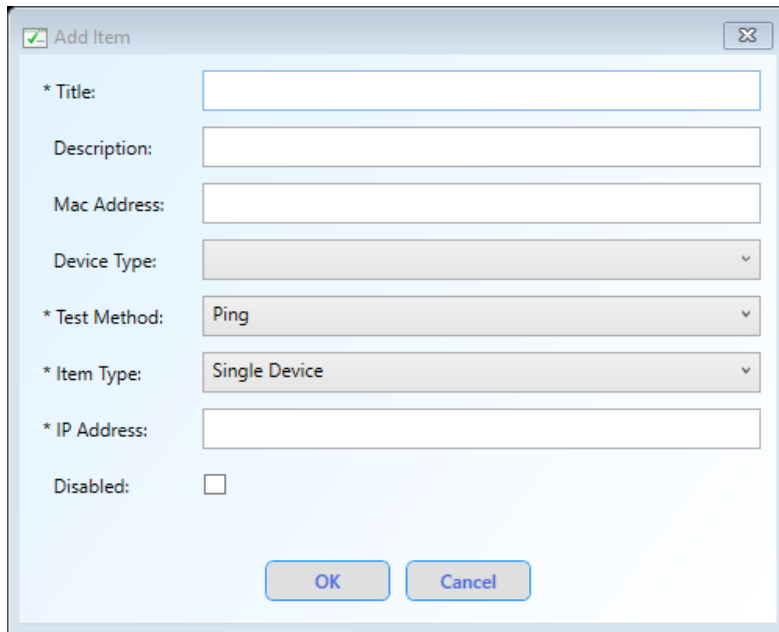
The Open button  will allow you to open a previously saved file and make it the active configuration. It should be noted that opening a file is very different from importing a CSV file from the VIP-102B tool. Whereas the Import function will add new devices to your existing configuration that are not currently present, the Open function will completely remove and replace all currently monitored devices with those stored in the saved INI file. Make sure you have saved a copy of your current configuration before opening an existing file.

Configuring Devices in the VIP Status Monitor

While importing a CSV file is certainly the easiest and quickest way to get started with monitoring your devices, it is certainly not the only way. The import also uses default settings, so you might want to change or tweak individual devices after the import has been completed. The settings for any device can be modified and devices can always be added or removed manually.

Adding a New Device

A device can be added manually by clicking on the Add button in the main toolbar.  Clicking on this button will open up a window where settings can be configured for the device.



The screenshot shows a dialog box titled "Add Item" with a close button in the top right corner. The dialog contains the following fields and controls:

- * Title: [Text input field]
- Description: [Text input field]
- Mac Address: [Text input field]
- Device Type: [Dropdown menu]
- * Test Method: [Dropdown menu with "Ping" selected]
- * Item Type: [Dropdown menu with "Single Device" selected]
- * IP Address: [Text input field]
- Disabled:

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Entering Standard Fields

Values should be entered for all of the standard fields, which are detailed as follows.

- Title – This field is required and is the main text used to identify the device. It is often the name assigned to the device in the VIP-102B tool.
- Description – This field can be used to enter additional information about the device, such as its physical location.
- Mac Address – The unique value used to identify this device on the network.
- Device Type - One of the known Valcom VoIP device types, such as speakers, clocks, etc. The Device Type is often used to group devices of a similar type together in the display and also controls the default Test Method that will be used during an import. If a type is not selected, the device will appear as a miscellaneous device in the main display.
- Test Method - An important field that controls how the device will actually be monitored. Many different test methods are available and different methods are recommended for different types of devices. When you select a Device Type, the Test Method field will automatically

default to the recommend method for that device, but this can always be changed if you want to use a different method and that method is actually supported by the device.

- Item Type – Indicates whether this item represents a single device or a group of devices that are working together in Failover or High Availability mode. Failover is typically only offered for Valcom server based devices, and some test methods cannot be used with a Failover system.
- IP Address – The IP address of the device that will be monitored.
- Port – Some test methods might require an additional port to be entered.
- Disabled – A flag used to temporarily disable testing on a device. This can be useful if you know there is a problem with the device so it can be disabled until repairs can be made.

Selecting a Test Method

The following test methods are available for a device and each one offers unique benefits.

- Ping – This is a standard ICMP request that can be used to determine if an IP Address is active on the network. It is the most basic type of test and provides the least amount of information in that it simply tells you if the device is powered up and has a valid IP address. This test can be useful, however, to monitor non-Valcom equipment.
- Web Request – This test is used to connect to devices that have a web interface, such as Application Servers, using an http request. It is more useful than a Ping in that it also helps to ensure that the web server is actually up and running on the device. Most Valcom server based devices should use this test method.
- Heartbeat Request – This test uses the same Valcom VoIP protocol that the devices use to communicate with each other in the paging system. A heartbeat request is sent by the VSM to the device and a response is received to indicate that the device is up and functioning. This is useful because it will tell you that the device is actually able to communicate with other VoIP equipment using Valcom protocol, whereas a Ping only tells you that the device is powered up. This is the recommended method for the majority of Valcom VoIP endpoints, such as speakers and clocks. Please note, however, that not all devices support this method, and a firmware upgrade could be required on some of them to use this method.
- External Supervision – This test can be used to communicate with devices, such as a Network Audio Port, that are used to drive analog speakers. This method will communicate with the device to determine if there are problems with the wiring of its external speakers. At the time of this writing, this method was still under development and might not be supported. A firmware upgrade might be required to use this method. This method also requires you to enter the port on the device that will receive the request from the VSM. This is typically the standard Control Port used by the device as defined in the VIP-102B tool.
- Status Monitor Request – This method can be used so the VSM can monitor other VSM tools on the network. This is a powerful feature that allows you to distribute the workload between multiple copies of the VSM. In a school district, for example, local VSMs could monitor VoIP hardware at each individual school and a top level VSM could monitor the other VSMs and be notified when there is a problem at any single location. This method also requires you to enter the port that the other VSM is listening for messages on.

- Fire Panel Supervision – This test method allows the VSM to monitor Potter fire alarm panels. When a fire panel is being monitored, not only will the VSM alert you to issues communicating with the panel, but it will also alert you to actual panel conditions such as alarms, troubles, and supervisory signals. Fire panels are not configured with or imported from the VIP-102B tool and must be entered manually into the VSM. By selecting a device type of Fire Alarm Panel and a test method of Fire Panel Supervision, your fire panel can be monitored by the VSM.

Configuring a Failover System

Some devices, such as Valcom server based devices, have the ability to work as a failover system, also known as high availability. In this type of system, there are 2 servers, a primary and a secondary. If a problem occurs on the primary server, the secondary server will seamlessly step in and take over. The web interface is accessed through a virtual IP address that is shared between both servers.

The VSM is powerful in that it has the ability to monitor all the network addresses in a failover system and will perform notifications if there is a problem with any of them. In fact, monitoring devices in a failover system was the original driving force behind the development of the VSM. In most cases, monitoring a failover system will use the Web Request test method.

To configure this type of system, the Item Type field should be changed to Failover System. Doing this will change the screen so that additional fields appear.

* Test Method:	Web Request
* Item Type:	Failover System
* Primary IP:	
* Secondary IP:	
* Virtual IP:	

In the new fields, you must enter the Primary IP, Secondary IP, and Virtual IP that all make up the components of the Failover System. The VSM will monitor these addresses and let you know when problems occur. It will even be able to tell you which address the problem is on and will classify the notifications as complete failures (meaning the system cannot be accessed at all) or warnings (meaning some component is down but the system might still be accessible because the other server has taken over).

Adding a Range of Devices

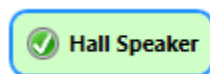
In some cases, you might have many similar devices within a range of IP address and you might want to quickly add multiple test items for all the devices in this range. Using this method, they might all have similar identifying properties (i.e. Hall Speaker for the Title), but each unique IP address can be monitored. To add a range of devices, you must select the Single Device Range option for the Item Type field. Please note that some test methods do not support adding a range of devices. Doing this will give


you two fields so you can enter the entire range of addresses and a test item will be created for every address within that range.

* Item Type:	Single Device Range
* Lower IP:	192.168.43.10
* Upper IP:	192.168.43.20


Changing an Existing Device

Once a device is present in the VSM, its settings can be modified at any time. Simply click on the item to select it. A blue border will appear around the item, like so:




You may then click the Edit button  in the main tool bar. The same screen that was used to add the device will appear and the fields will be populated with the current settings so they can be modified.

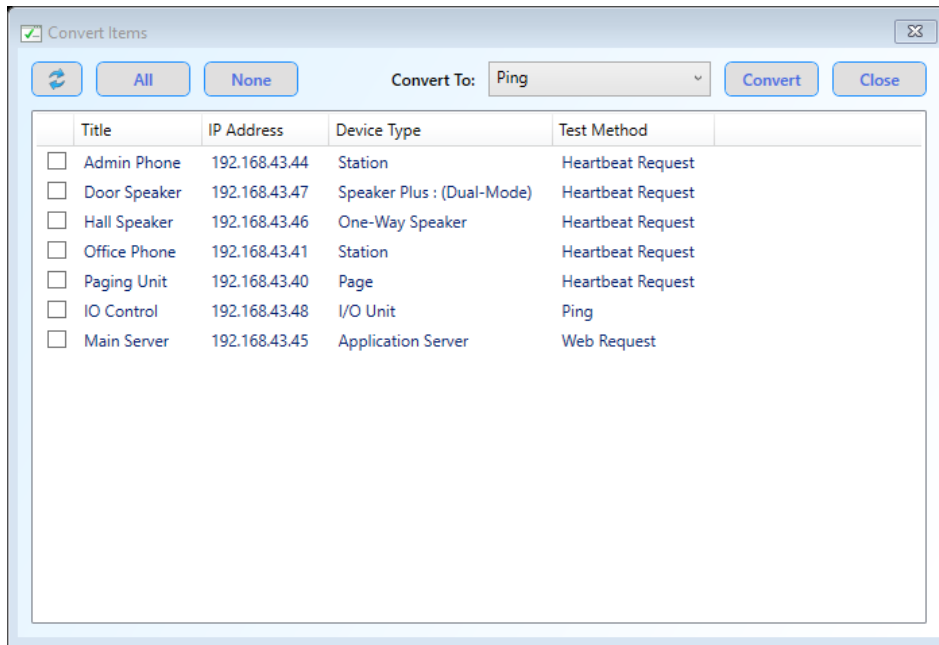
Deleting an Existing Device

Any device can be removed from the VSM by selecting it and clicking the Delete button  in the main toolbar. You will be asked to confirm the delete. Simply answer yes and the device will be removed from the VSM and will no longer be monitored.

Changing the Test Method for Multiple Devices

Occasionally, you might decide that you want to change the method being used to test the devices in your system. One example of this would be if you had an older copy of the VSM that only supported ping and you now want to switch the devices to use the Heartbeat Request method. If you have multiple devices that need this change, it could be very tedious to edit each one individually.

Fortunately, the VSM offers an easy solution. Simply click on the Convert Items button  in the main toolbar. A new screen will open that shows all the devices in your system and the current test method they are using.



Put a check mark beside each device that you want to change. There are buttons that can be used to quickly select multiple devices and a button to refresh the list if necessary. You can also highlight an item and use the standard Windows Shift or Ctrl keys to highlight multiple items with the mouse and then toggle all of them by clicking in the checkbox of any of the highlighted items.







Once the desired devices have been checked, select the new method that you want to convert the devices to use and click the Convert button. After confirming the conversion, the devices will be changed to use the new method. Please note that some of the less common methods, such as Status Monitor Request, cannot be converted to in mass because they might require additional settings like the port to use. Switching to these method will require a manual edit of the necessary devices. In addition, switching a device to a method that is not supported with a Failover system might cleanup some settings if they were previously entered, such as the Secondary or Virtual IP Address.

Working with the VIP Status Monitor

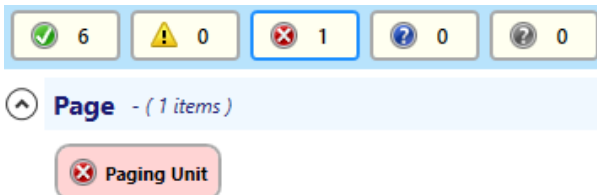
On a day to day basis, there are many features of the client application that can be used to keep track of the status of the devices on your network. It can be very easy to see at a glance which devices on your network need attention.

Examining the State of Devices

Each device in the VSM can be in one of several states. The state of each item will be indicated by its color and by an icon on the item. The states are as follows:

-  - Normal – This device is in a normal state. No errors have been detected.
-  - Warning – There is a problem with this device, but it might not be fatal.
-  - Failure – This device is in a failure state. There is a major problem detected.
-  - Alarm – This device is in an alarm state. This is an emergency.
-  - Disabled – This device is disabled and is not being tested at this time.
-  - Unknown – This device has not yet been tested so its state is unknown

Below the main toolbar is a series of buttons that will display how many devices are in each state. These buttons can also be used to filter devices in each state by toggling them on or off. For example, if you only wanted to view items in a Failure state, all other states could be toggled off. A blue border around a state will indicate that items in that state will be visible while a gray border indicates they will be hidden.



Note that the Alarm state button is only visible when a device in your system has been configured for Fire Panel Supervision or an alarm is detected on a remote VSM. In addition, since Alarms are a true emergency, you will not be able to hide items in this state by toggling the filter button. They must remain visible at all times.

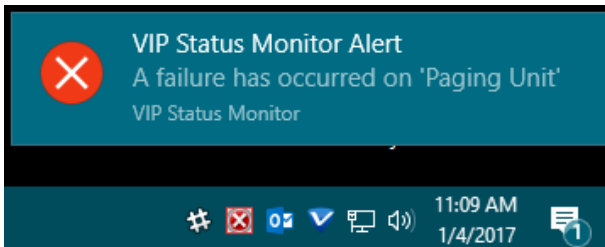


While each device has a state, there is also a main state for the VSM itself. The icon in the system tray will indicate the overall state of the VSM based on the state of the individual devices. If any devices are in a Failure state, the VSM will be in a Failure state. Likewise, the VSM will only be in a Normal state when all devices are in a Normal state.

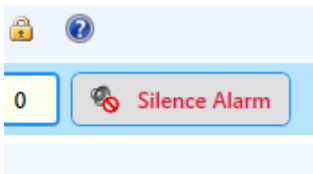


Receiving Client Notifications

When a problem occurs on a device, the client application will be notified in several ways. These notifications can be configured, and will be discussed later in this document during the topic on Settings. To begin with, when a problem occurs, the main client window will pop up and will appear above all other windows. A notification message will also appear in the system tray that details the problem that has occurred.

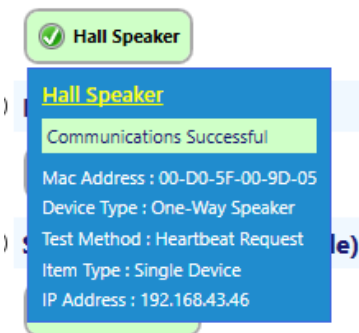


In addition, a chiming audio alarm will begin to sound and will continue until the device returns to a normal state or the alarm is silenced. The alarm may be silenced by clicking on the Silence Alarm button in the tool bar area. Note that this only silences the PC alarm played by the VSM and does NOT silence any actual fire panel alarms.



Viewing Device Details

Very often, you might want to know the details of a device without entering the edit screen. The VSM makes this very easy by offering a detailed tool tip for each item that is being monitored. Simply hover over any device with your mouse and you will see expanded details for each item. If the device is in a failure state, you will often see additional details as to why it has failed.

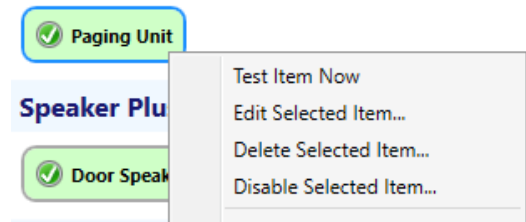


As a bonus, if the device is one that uses a Web Request for its test method, the title for the device will appear as link. Clicking on the link will open up a web browser to the home page for that device.



Using the Device Context Menu

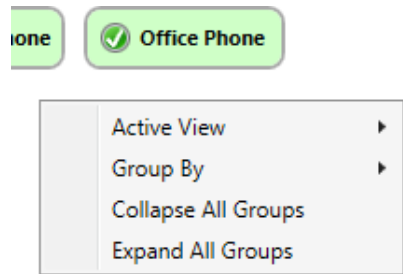
If you right click on a device in the VSM, a context menu will appear that will allow to you perform some of the more common functions on that device.



Several of these menus, such as Edit and Delete, are shortcuts to functions available on the toolbar. An additional menu item, labeled Test Item Now, will cause the device to be tested immediately instead of waiting until the next iteration.

Customizing the Display

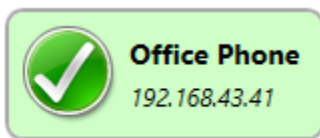
There are many different ways that the VSM can be customized to easily view the devices in the system. Many of these options are accessed by right clicking on a device or within any empty space in the main window.



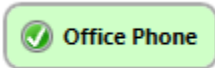
Views and Groupings

There are several active views that can be used to display the devices.

- Large Icons – A large icon will be displayed with the device Title and IP Address.



- Small Icons – A small icon will be displayed with only the device Title shown.

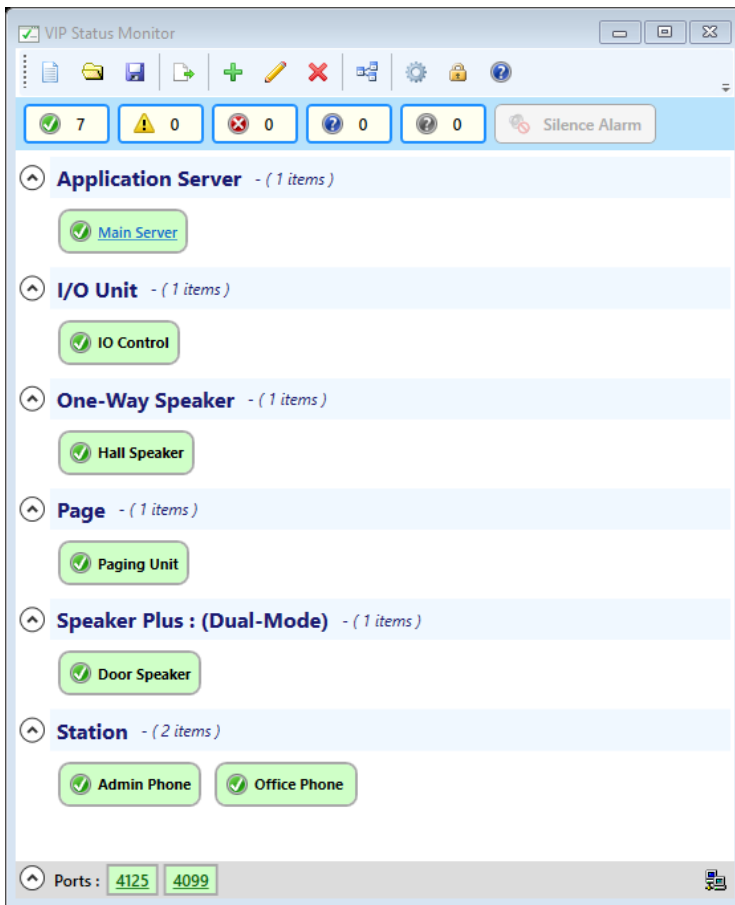


- Switchboard – A small icon will be shown with no text displayed. Details for an item can always be viewed by hovering over the item to view its tooltip. This view is useful if you have a large number of devices in your system and want to see many of them all at the same time.

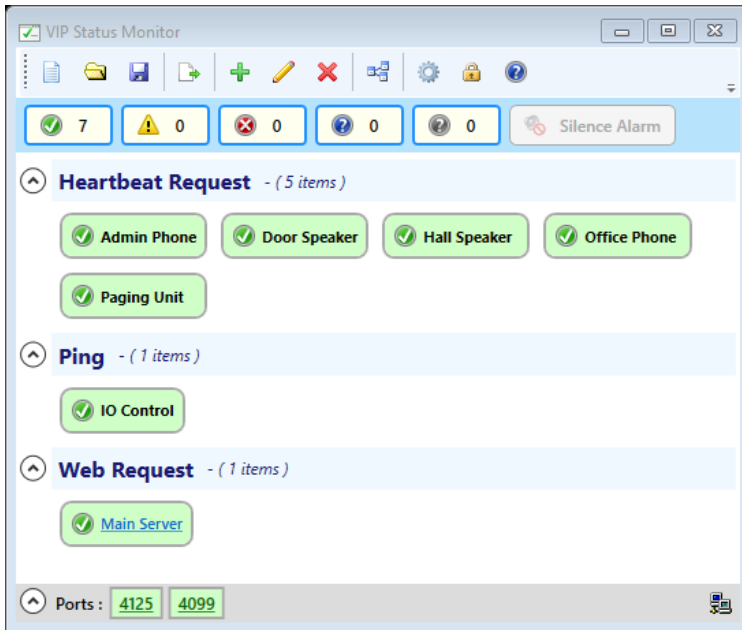


In addition, devices can be grouped together according to several different properties.

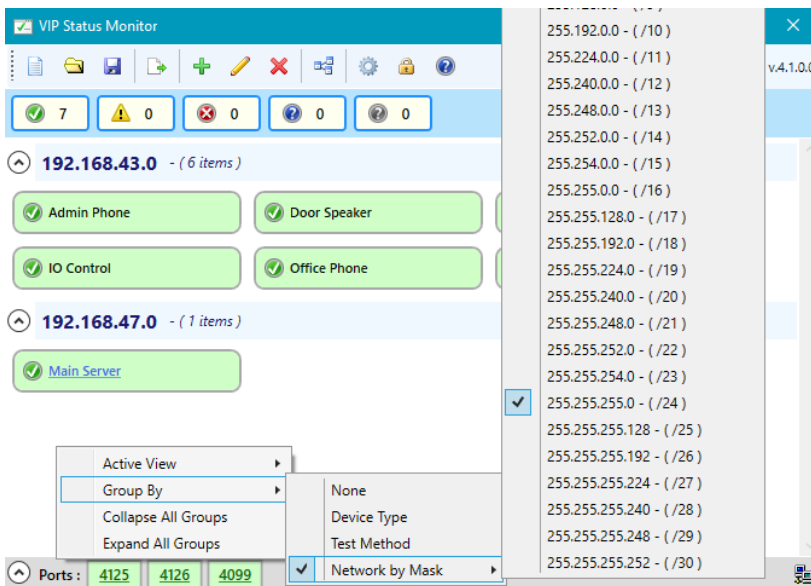
- Device Type – Devices will be grouped together based on their device type



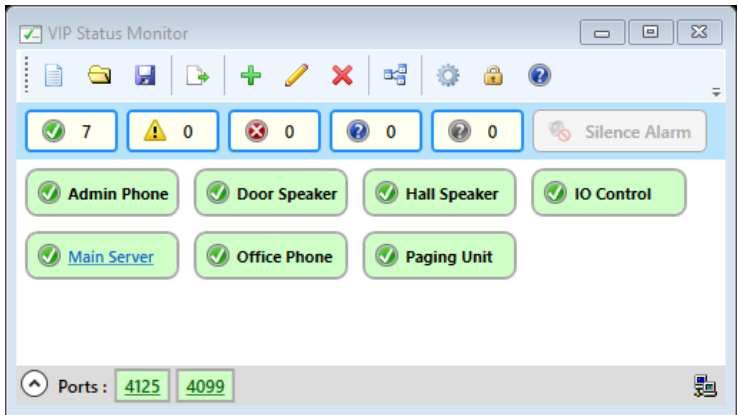
- Test Method – Devices will be grouped together based on their test method



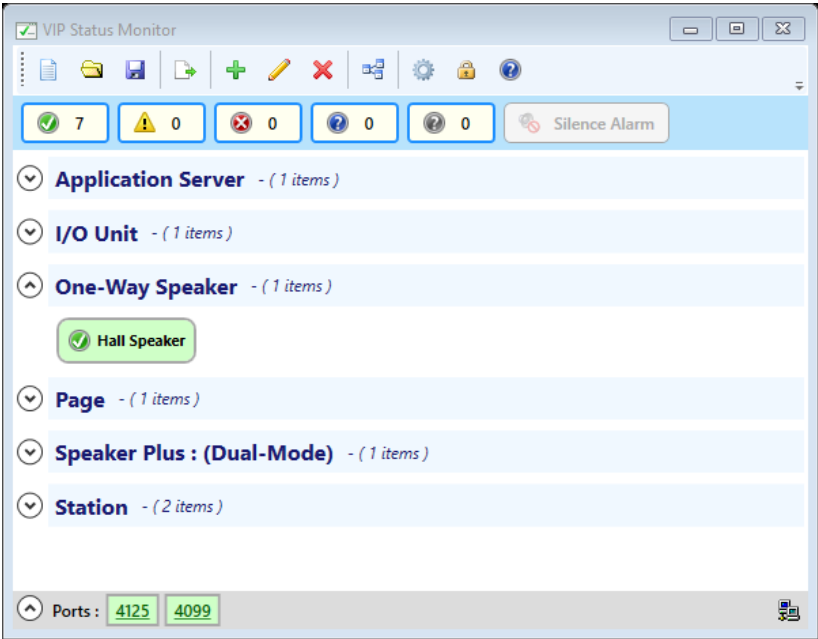
- Network by Mask – Devices will be grouped together in their respective network based on the Netmask that is selected from the submenu.



- None – Devices will not be grouped together



When grouping is being used, individual groups can be collapsed or expanded by clicking on the arrows to the left of each group. Multiple groups can be toggled all at once by using the context menus.



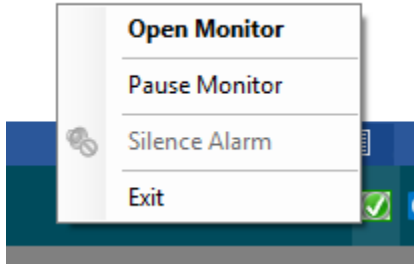
Showing the Summary View

If your goal is to let the VSM take up as little screen real-estate as possible, the client can be switched to the Summary Display mode. In the lower left corner of the main window, an arrow is present that can be used to collapse or expand the entire window. When collapsed, the window will display only the minimum information necessary to see an overview of the system.

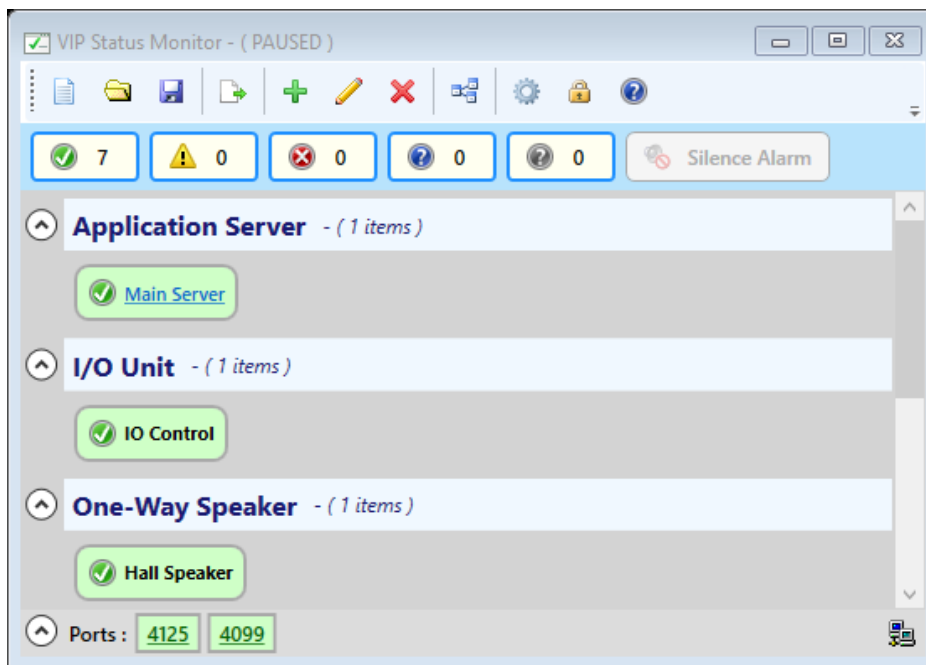



The System Tray Context Menu

Several functions of the client application can be controlled from the system tray icon. Simply right click on the icon and a context menu will appear.



- Open Monitor – This menu will open up the main VSM window if it has been minimized.
- Pause Monitor – This menu will cause the Monitor Service to pause until it is manually resumed or the PC is rebooted. This may be useful if you ever need to temporarily disable the network traffic that the VSM generates. It should be noted that pausing the VSM will also cause the service to stop sending Relay Control messages if they are being used, which will put the relay into a failure state. When the VSM is paused, the main window will appear grayed out.



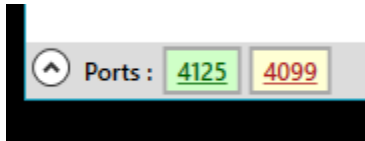
The system tray icon will also have a red line through it like so: 

- Silence Alarm – This menu is another way the audio alarm can be silenced when it is active
- Exit – This menu will completely exit the client application. In normal cases, closing the VSM window will not actually exit the program. It will only minimize it to the system tray. Clicking the Exit menu, however, will completely shut down the client application. The Monitor Service

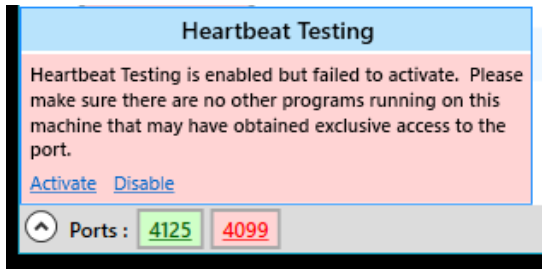
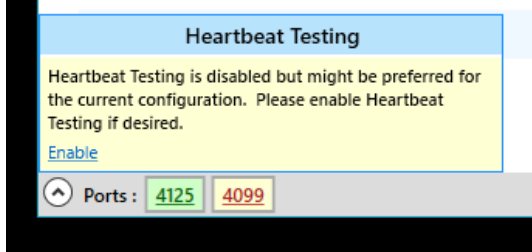
will still be running so that e-mails, syslog, etc. can be sent, but the client will not be active to receive client notifications. The client application will normally start by default when the user logs into the machine, but can always be restarted by clicking the appropriate shortcut in the Windows Start menu.

Controlling Network Ports

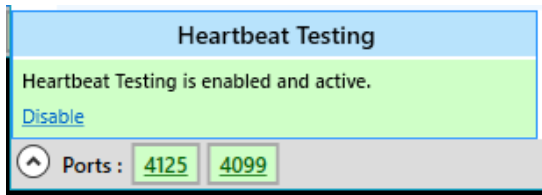
The VSM uses several ports for various network functions. The lower left corner of the main window will display a summary of many of the ports that are currently being used. If there is a problem with one of the ports or something that needs attention, it will often display in a color other than green.



Clicking on the port will give you additional details about the port and what actions can be attempted.



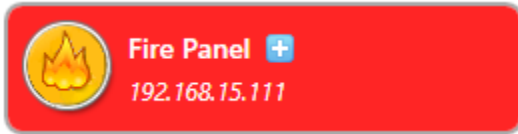
Links within the port details can be used to perform the necessary functions.



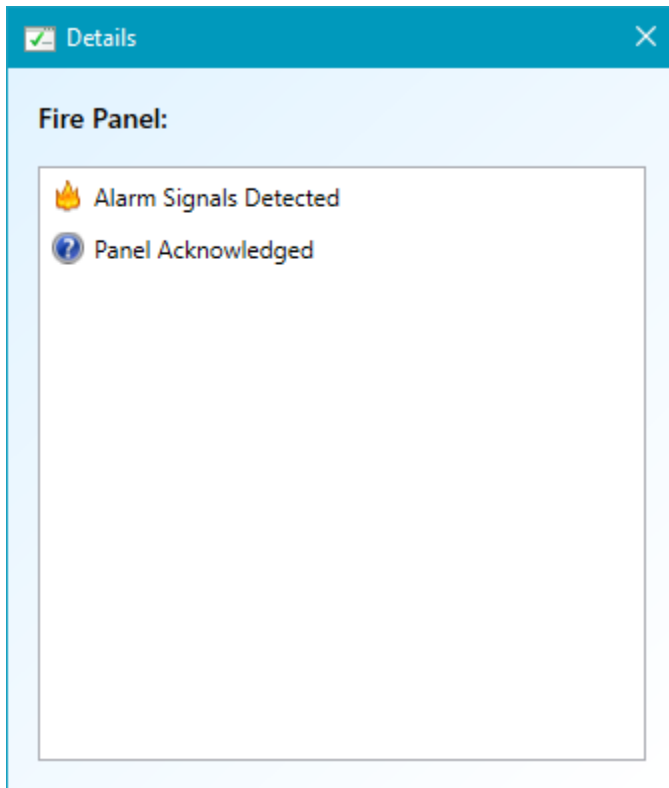
The ports that might be shown include the Local Monitor Port, the Heartbeat Control Port, and the Remote Access Port. More information on each of these ports can be found in the topics on the VSM Settings that follow.

Fire Panel Supervision Details

If a device is configured to use the Fire Panel Supervision test method, then additional details will be available for the device that give extra information about the device state. For example, the details may tell you whether a warning is due to a trouble or supervisory condition and whether the condition has been acknowledged on the panel. A blue plus mark will be visible on the device to view details.

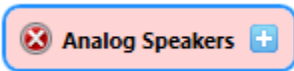


Clicking on this plus mark will open a window that shows the additional details. The window will update in real time as new states are detected on the device.

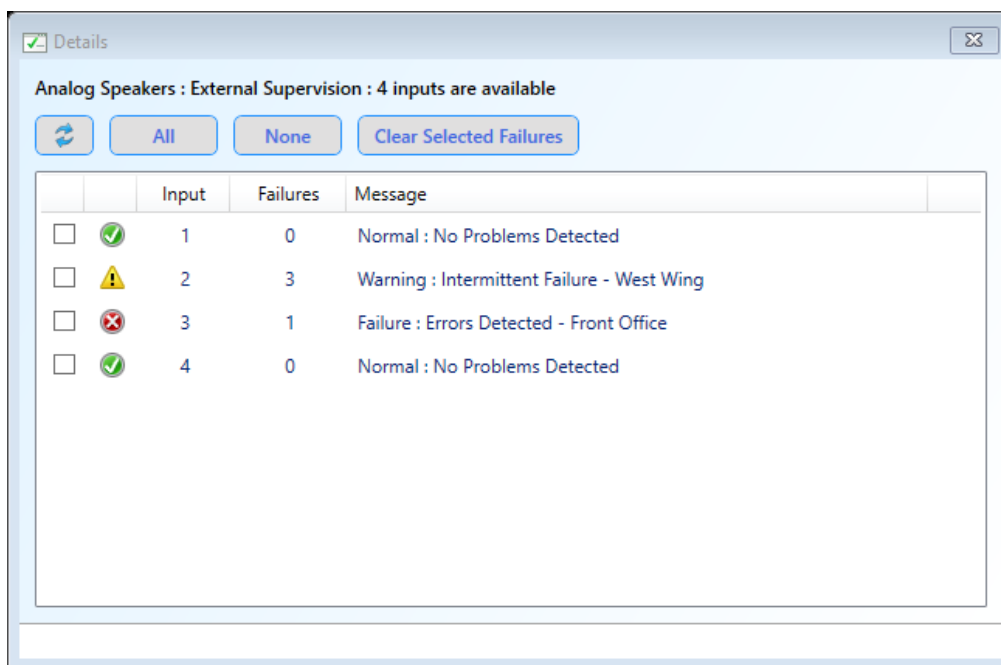


External Supervision Details

If a device is configured to use the External Supervision test method, additional details are often available for the device. As previously mentioned, at the time of this release, External Supervision was still under development and might not be available. If additional details are present, a blue plus mark will be visible on the device.




Clicking on this plus mark will open a window that shows additional details for the externally supervised speakers connected to the device. This window may also be opened by right clicking on the device and selecting the View Item Details option from the context menu.



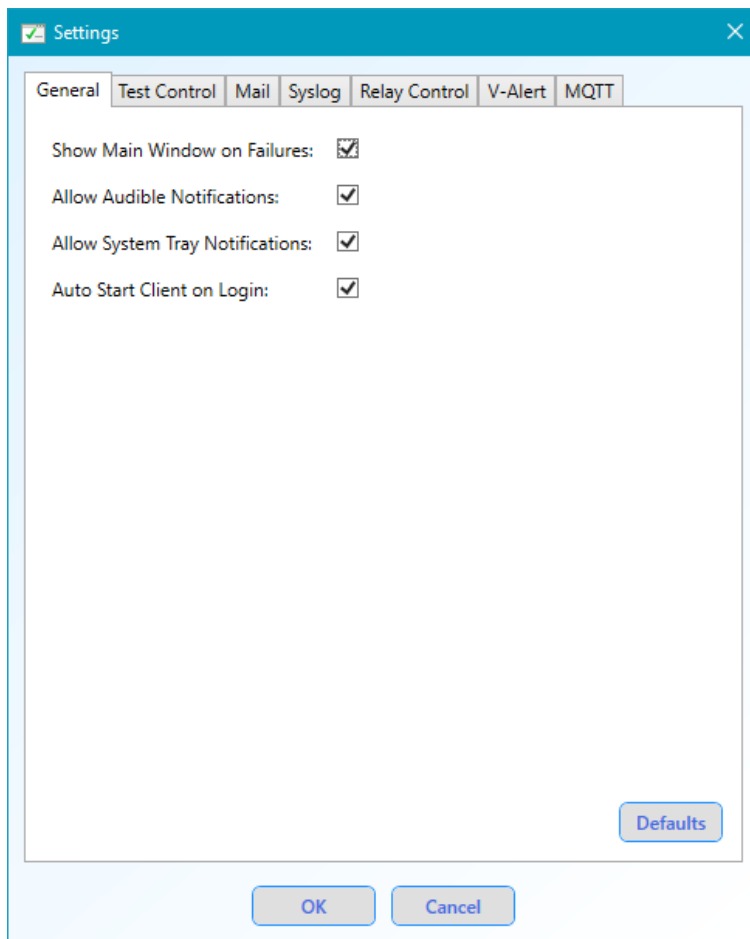
In the details window, you will see additional details for each of the inputs on the device that have been configured for external supervision from within the VIP-102B tool. Each input being supervised will show its current state and how many times it has failed or experienced a wiring fault. Intermittent failures will often show as warnings. A button is available to refresh the screen. You may select any of the problem inputs and clear the failures once the errors have actually been corrected. This will reset the failure counts on the selected inputs to zero and will restore the inputs to the normal state if the problems have indeed been fixed. All failures and warnings must be cleared before the device can return to a Normal state.

Settings and Notification Options

There are a variety of settings that can be used to control how the VSM functions and the notifications that are received. The settings can be accessed by clicking on the Settings button  from the main toolbar. Clicking this button will open a window with different tabs where settings can be adjusted. The default values can be restored for any single tab by clicking on the Defaults button on that tab. Once the settings have been changed, click the OK button to accept them. The settings that are available will be discussed in the following sections:

General Client Settings

Most of the settings in the General section pertain to how the client application handles notifications. These settings are typically on a per client basis and might be different for different user accounts.



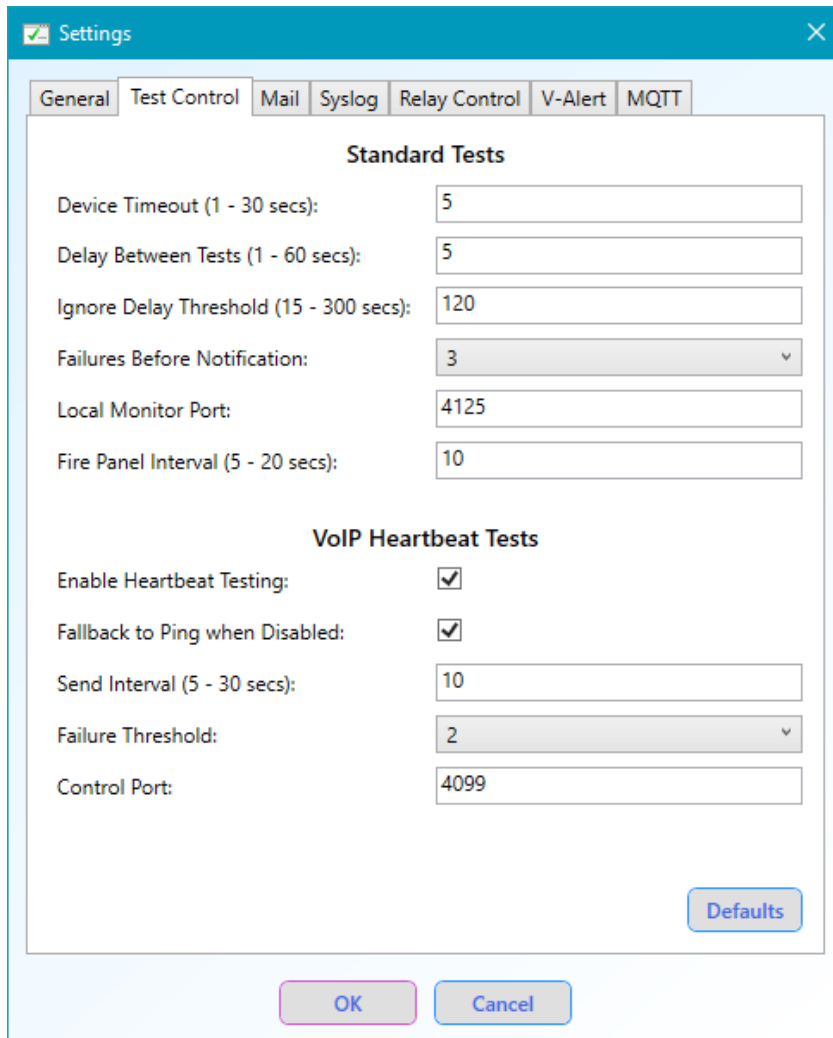
- Show Main Window on Failures – This setting controls whether or not the main VSM window should popup to the foreground when a failure is detected. If turned off, the window will not be displayed.
- Allow Audible Notifications – This setting controls whether or not an audible alarm is played through the PC speakers when a failure occurs. If turned off, the Silence Alarm button will also disappear from the main window since it is no longer applicable.

- Allow System Tray Notifications – This settings controls whether a popup notification will occur from the system tray when a failure occurs.
- Auto Start Client on Login – This setting controls whether or not the client application will automatically start when the user logs into the PC. The Monitor Service will always be running regardless of this setting. If this setting is turned off, however, the client application will not appear in the system tray and must be launched manually from the Windows Start menu.

If the notification settings in this section are all disabled, then the only client side indication that an error has occurred would be a changed icon in the system tray.

Test Control Settings

Settings in this section are used to control how the Monitor Service actually goes about performing tests. They can be used to adjust the timings so that testing and notifications occur on a more or less frequent basis. The two main sets of settings in this section are Standard Tests and VoIP Heartbeat Tests. The proper settings are used based on the Test Method that has been specified for each device.



The screenshot shows a 'Settings' window with a 'Test Control' tab selected. The window is divided into two sections: 'Standard Tests' and 'VoIP Heartbeat Tests'. The 'Standard Tests' section includes fields for 'Device Timeout (1 - 30 secs):' (5), 'Delay Between Tests (1 - 60 secs):' (5), 'Ignore Delay Threshold (15 - 300 secs):' (120), 'Failures Before Notification:' (3), 'Local Monitor Port:' (4125), and 'Fire Panel Interval (5 - 20 secs):' (10). The 'VoIP Heartbeat Tests' section includes checkboxes for 'Enable Heartbeat Testing:' (checked) and 'Fallback to Ping when Disabled:' (checked), and fields for 'Send Interval (5 - 30 secs):' (10), 'Failure Threshold:' (2), and 'Control Port:' (4099). A 'Defaults' button is located at the bottom right of the settings area, and 'OK' and 'Cancel' buttons are at the bottom of the window.

Standard Test Settings

Settings for Standard Tests are used by most of the test methods that are available for a device. Examples of standard tests are Ping, Web Request, and Status Monitor Request. These are the tests that were originally offered in the VSM and their presence is still used today. Settings for standard tests are as follows.

- Device Timeout – This value indicates the amount of time in seconds when trying to contact a device before an invalid or missed response should indicate a failure.
- Delay Between Tests – This value is a delay in seconds that is used to help balance system resources. Standard tests work by having several threads constantly going through a list of test

items and checking them as needed. Once a thread has been assigned to a test, it will pause for this amount of time before actually running the test. This helps to make sure that the threads are not constantly running tests and overloading the network with testing traffic. It should be noted that this value does NOT mean that every individual standard device will be tested at least once within this interval. It simply means that each available thread will pause for this amount of time before running a test on SOME device. If you have a large number of devices that use standard testing, it is possible that the VSM might not detect a device that rebooted if it was back up and running by the time a thread was assigned for testing that item. Using Heartbeat testing for the majority of your devices can help alleviate this issue, and will be discussed momentarily.

- **Ignore Delay Threshold** – This value indicates a time in seconds for which the Delay Between Tests should be ignored. Consider for example, if the Delay Between Tests is 5 seconds and the Ignore Delay Threshold is 120 seconds. If a thread prepares to test a device and it has been more than 120 seconds since that device was last tested, then the thread will NOT wait the 5 second delay before testing the device. It will test the device immediately and move to the next device as soon as it completes. As a result, there could be bursts of network activity from the VSM if it gets behind and tries to play catch up. Once caught up, the delays will again take effect to help balance the network traffic and system resources.
- **Failures before Notification** – This setting is used to control how many failures can occur on a single device before notifications actually occur. Regardless of this setting, a device will always change its state if a valid response is missed from a single test. The service and client will wait, however, until this many sequential failures occur on that device before performing actual notifications such as e-mail, syslog, audio alarms, system tray notifications, etc. A higher number here will help to prevent excess notifications due to temporary network issues that might not indicate actual failures while a lower number will increase the rate and speed at which notifications are raised.
- **Local Monitor Port** – This is the UDP Port that the VSM listens on for being monitored by other VSM tools. A Status Monitor Request from another VSM should be directed to this port. This port is also used to receive responses for test methods such as the Status Monitor Request and External Supervision. These test methods will include the port number in the request and the remote device will know to send their response to that port.
- **Fire Panel Interval** – When Fire Panel Supervision is being used, this setting indicates how often the panel will be polled for its status. For this type of test, the panel will always be polled at this interval and the Delay Between Tests is not applicable.

VoIP Heartbeat Test Settings

While standard tests are useful for sequentially monitoring items with specialized requirements, heartbeat testing was introduced to be much more responsive and has been optimized for performance. Heartbeat testing is better suited for detecting devices that may be rebooting and for ensuring that Valcom VoIP protocol is working correctly on your devices. Heartbeat testing is generally recommended for most devices when available. Standard tests should be reserved for the few devices that specifically need it, such as Web Requests for server based devices and Ping for devices that do not support

heartbeat testing. Using heartbeat testing for the majority of your devices also helps to reduce the number of devices in the standard test queue which allows them to be tested more frequently.

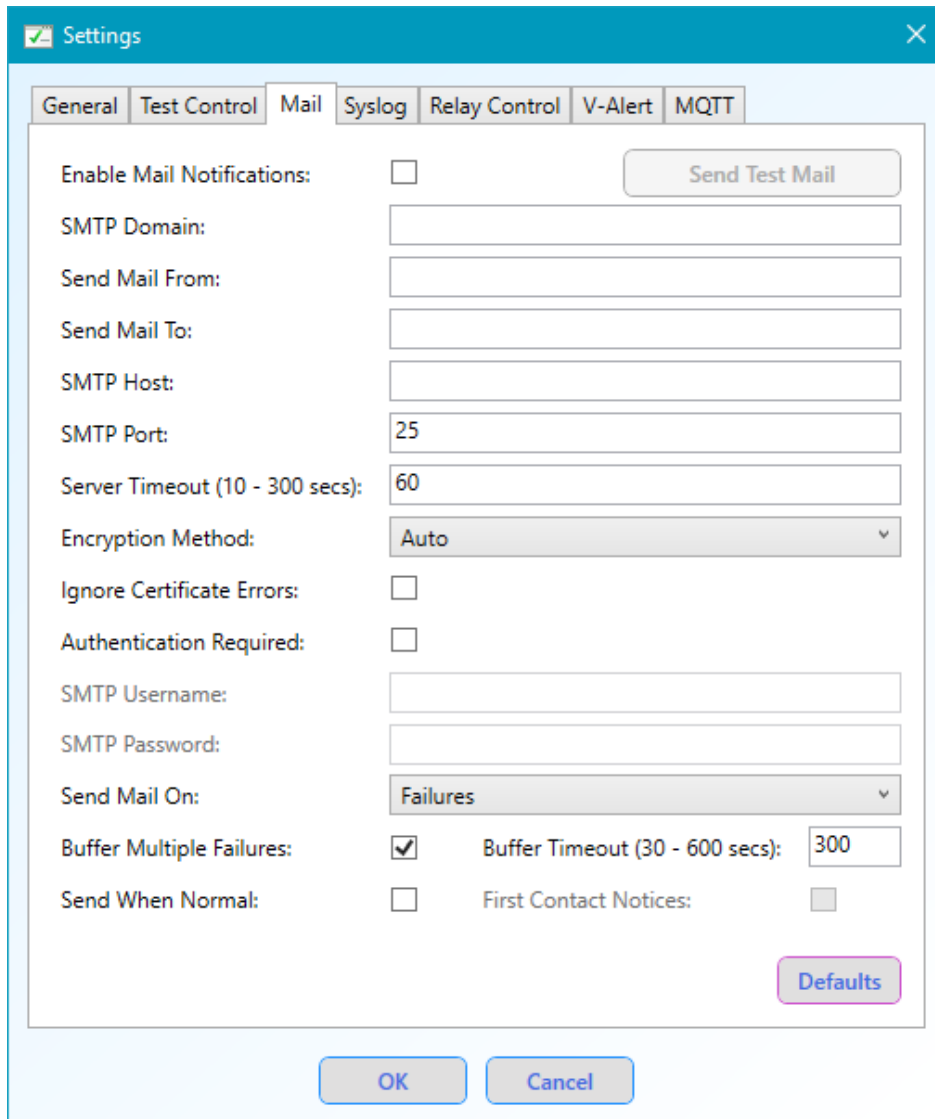
While heartbeat testing is often recommended, it is actually disabled globally by default. The reason for this is that heartbeat testing requires the sending and receiving of Valcom VoIP protocol messages on the standard Control Port. This port requires dedicated access by the monitor service and could cause conflicts with other Valcom tools that might be trying to communicate on this port. For example, the Paging Diagnostics feature of the VIP-102B tool listens for control messages and therefore cannot be run on a PC at the same time as heartbeat testing from the VSM. If you want to enable and use heartbeat testing, the VSM should be installed and run on a machine where you know that other Valcom products will not conflict. When you open a configuration file, import devices, or manually add a device that is configured to use heartbeat testing, you might be prompted at that time to enable heartbeat testing if it is disabled but recommended.

There are several settings that can be used to control heartbeat testing. They are as follows.

- Enable Heartbeat Testing – Used to enable or disable heartbeat testing. This value can also be toggled from the Ports section in the lower left corner of the status bar on the main window.
- Fallback to Ping when Disabled – If this value is enabled and heartbeat testing is disabled, then any device that is configured to use Heartbeat Requests will automatically revert to performing a standard Ping for as long as heartbeat testing is disabled. This can be useful if you need to temporarily disable heartbeat testing since standard testing can still be performed to keep the devices from entering a failure state. If this value is disabled and heartbeat testing is disabled, then any device that is configured to use Heartbeat Requests will appear as disabled because no tests are being performed on the device at that time.
- Send Interval – This is a value in seconds that indicates how often a heartbeat request will be sent to each device. For example, if the interval is 10 seconds, then each device will be sent a request every 10 seconds.
- Failure Threshold – This value indicates how many missed responses can occur from a single device before entering a failure state and performing notifications. Unlike with standard tests, as soon as the threshold is reached, the device will enter a failure state and notifications will occur immediately. Building on the previous example, if the Send Interval is 10 seconds and the Failure Threshold is 2, then a failure will be raised for a device if a response is not received from it every 20 seconds.
- Control Port – This is the port on which devices have been programmed in the VIP-102B to listen for control messages. Heartbeat requests will be sent to each device on this port and the response will be sent back to the VSM on this port. As mentioned previously, the monitor service must have exclusive access on the PC to listen for messages on this port. Otherwise, heartbeat testing cannot be used.

Mail Settings

The VSM has the ability to send e-mail messages when failures or problems occur. This allows users to be quickly notified of problems with the system, even if they are away from the office.



The screenshot shows the 'Mail' tab of the 'Settings' application. The dialog box has a title bar with a checkmark icon and a close button. Below the title bar are tabs for 'General', 'Test Control', 'Mail', 'Syslog', 'Relay Control', 'V-Alert', and 'MQTT'. The 'Mail' tab is active. The settings are as follows:

- Enable Mail Notifications: (Send Test Mail button)
- SMTP Domain:
- Send Mail From:
- Send Mail To:
- SMTP Host:
- SMTP Port:
- Server Timeout (10 - 300 secs):
- Encryption Method: (dropdown)
- Ignore Certificate Errors:
- Authentication Required:
- SMTP Username:
- SMTP Password:
- Send Mail On: (dropdown)
- Buffer Multiple Failures: Buffer Timeout (30 - 600 secs):
- Send When Normal: First Contact Notices:

Buttons: OK, Cancel, Defaults (highlighted in purple).

- Enable Mail Notifications – Used to enable e-mail notifications. When disabled, e-mail notifications will not be sent.
- SMTP Domain – The default domain that will be used to enter e-mail addresses. This field is optional and is not required. An example is valcom.com.
- Send Mail From – The e-mail address that messages will be sent from. The full address can be entered (such as user@valcom.com) or if a default SMTP Domain was entered, just the name can be entered (such as user).
- Send Mail To – Comma separated list of e-mail addresses to send notifications to. Like with the Send Mail From field, each address can include the full address or just the name if a default SMTP Domain was entered.

- SMTP Host – Name of the SMTP server host that will be used to send e-mail.
- SMTP Port – SMTP Server Port that is used to send e-mail.
- Server Timeout – Timeout in seconds for connecting to the mail server.
- Encryption Method – The type of encryption to use when connecting to the mail server.
- Ignore Certificate Errors – When this option is enabled, any errors that occur while validating the server certificate will be ignored. This might be necessary if the server certificate is out of date or improperly configured.
- Authentication Required – Indicates whether the mail server requires authentication. If authentication is required, then the SMTP Username and SMTP Password must be entered.
- SMTP Username – User name when Authentication is required by the server.
- SMTP Password – Password when Authentication is required by the server.
- Send Mail On – Indicates when mail notifications should be sent. The options are to send messages immediately when failures are detected or daily at scheduled times if there are active issues at that time. The default option is to send when failures are detected.
- Buffer Multiple Failures – When sending on failures and this option is enabled, multiple failures will be buffered and sent in a single e-mail once the Buffer Timeout expires. The first detected failure if there are no buffered items will be sent immediately so you can quickly know that something is wrong. Subsequent failures, however, will be buffered during the timeout period and sent in a single message. This helps to prevent multiple e-mail messages when there are many failures all at once, like when a router goes down. If this option is unchecked, then each device that fails will have a notification sent in its own separate e-mail.
- Buffer Timeout – When sending on failures and buffering messages this is the amount of time in seconds to buffer multiple failures before sending an e-mail.
- Send When Normal – When this option is enabled, a message will be sent when a device returns to the Normal state after a previous failure. These messages will also be buffered with the failure messages if the option to buffer has been enabled.
- First Contact Notices – When this option is enabled, a SUCCESS message will be sent for each device when it enters the Normal state after the VSM starts or contact is first made. Disabling this option will suppress these messages, and a SUCCESS will only be sent when devices actually return from a previously reported failure.

When mail is sent on a schedule, then a time must be provided when the message should be sent. If mail should be sent once a day, then the daily option should be selected and the desired time should be entered:

Send Mail On:

Daily Hourly

:

Send When Normal:

If messages are desired at multiple times during the day, then different hours can be selected when the messages should be sent:

Send Mail On: Schedule

Daily Hourly

Send When Normal:

7AM, 12PM, 5PM 🕒

Clicking on the clock button will allow you to select from a list of hourly times:

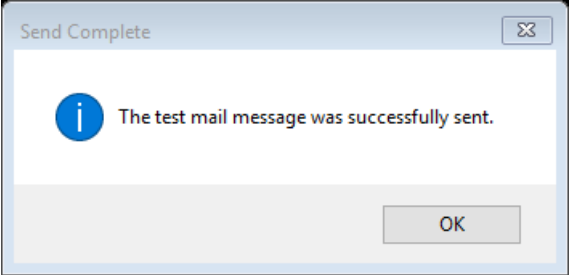
Mail Schedule
✕

<input type="checkbox"/> 12:00 AM	<input type="checkbox"/> 4:00 PM
<input type="checkbox"/> 1:00 AM	<input checked="" type="checkbox"/> 5:00 PM
<input type="checkbox"/> 2:00 AM	<input type="checkbox"/> 6:00 PM
<input type="checkbox"/> 3:00 AM	<input type="checkbox"/> 7:00 PM
<input type="checkbox"/> 4:00 AM	<input type="checkbox"/> 8:00 PM
<input type="checkbox"/> 5:00 AM	<input type="checkbox"/> 9:00 PM
<input type="checkbox"/> 6:00 AM	<input type="checkbox"/> 10:00 PM
<input checked="" type="checkbox"/> 7:00 AM	<input type="checkbox"/> 11:00 PM
<input type="checkbox"/> 8:00 AM	
<input type="checkbox"/> 9:00 AM	
<input type="checkbox"/> 10:00 AM	
<input type="checkbox"/> 11:00 AM	
<input checked="" type="checkbox"/> 12:00 PM	
<input type="checkbox"/> 1:00 PM	
<input type="checkbox"/> 2:00 PM	
<input type="checkbox"/> 3:00 PM	

All
None
OK
Cancel

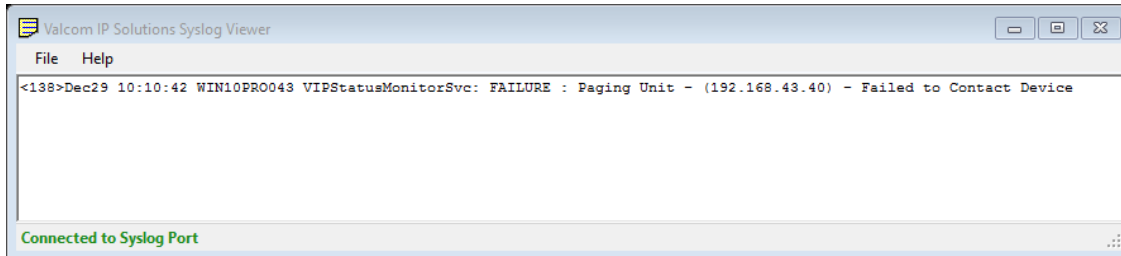
Whether mail is sent Daily or Hourly, a message will only be sent at the selected times if there are devices that are actually in a Warning of Failure state at that moment. The message will indicate which devices currently have issues. If all devices are currently in a Normal or Disabled state the message will not be sent. You may select the option to “Send When Normal” to still receive the message in this case. The message will simply contain a count of all the device states and a message indicating that no warnings or failures have been detected at the indicated time.

Once all the settings are entered, you may click the Send Test Mail button to test the entered settings. A test message will be sent to verify that the settings are valid and have been entered correctly.

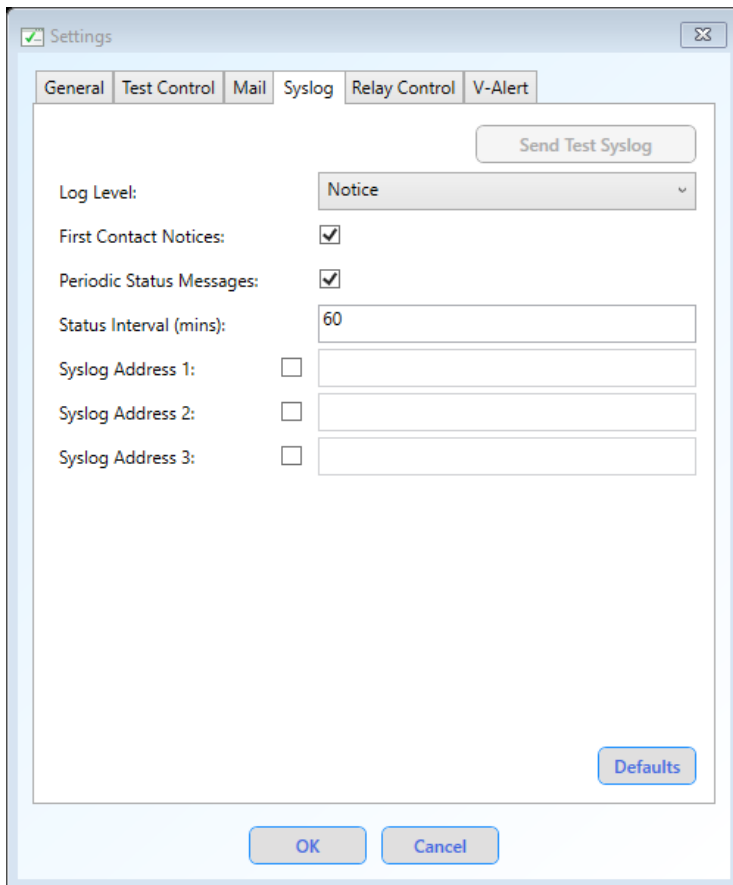


Syslog Settings

The VSM has the ability to send syslog messages when failures are detected. Syslog messages are sent to the standard syslog port 514. Messages can be received by any syslog viewer. A basic viewer is included with the VIP-102B tool.



Settings can be entered in the VSM for up to 3 different syslog addresses.



- Syslog Addresses – Each address should be the IP address of a machine that is running a syslog viewer. Addresses can be temporarily enabled or disabled by clicking the checkbox beside each address.
- Log Level - The Log Level can be used to control the amount of messages that are sent. Emergency is the highest level and will produce only a few critical messages. Debug is the lowest level and will produce the most number of messages. The default level is Notice and is

typically needed to receive failure and success notifications. Please see the Appendix for a detailed list of messages that are sent by the VSM and their associated levels.

The following options were added in a later version of the VSM, and might not be available in your particular system.

- **First Contact Notices** – A SUCCESS message is typically sent for each device when it's first contacted and enters the Normal state, provided the Log Level is set to Notice or lower. If you do not want to see these initial messages, the option can be disabled and they will not be sent. Disabling this option is useful if you do not want to be overwhelmed with messages when the VSM first boots or when a new file is opened in the tool. If the option is disabled, then the SUCCESS messages will only be sent when devices actually return from a previously reported failure.
- **Periodic Status Messages** – When this option is enabled, a STATUS message will periodically be sent from the VSM that provides counts of all the current states of the tested devices. This message is useful for ensuring that the VSM is still running and functioning properly. The message will also be sent once all devices have transitioned from the Unknown state, such as when initial testing is complete after a reboot of the VSM machine. While status messages are sent at the Notice level, they do not depend on the selected Log Level and will always be sent if this option is checked.
- **Status Interval** – This is the interval in minutes at which periodic status messages will be sent if the option is enabled. The default value is 60 minutes, so a message will be sent once an hour to provide an indication that monitoring is still active.

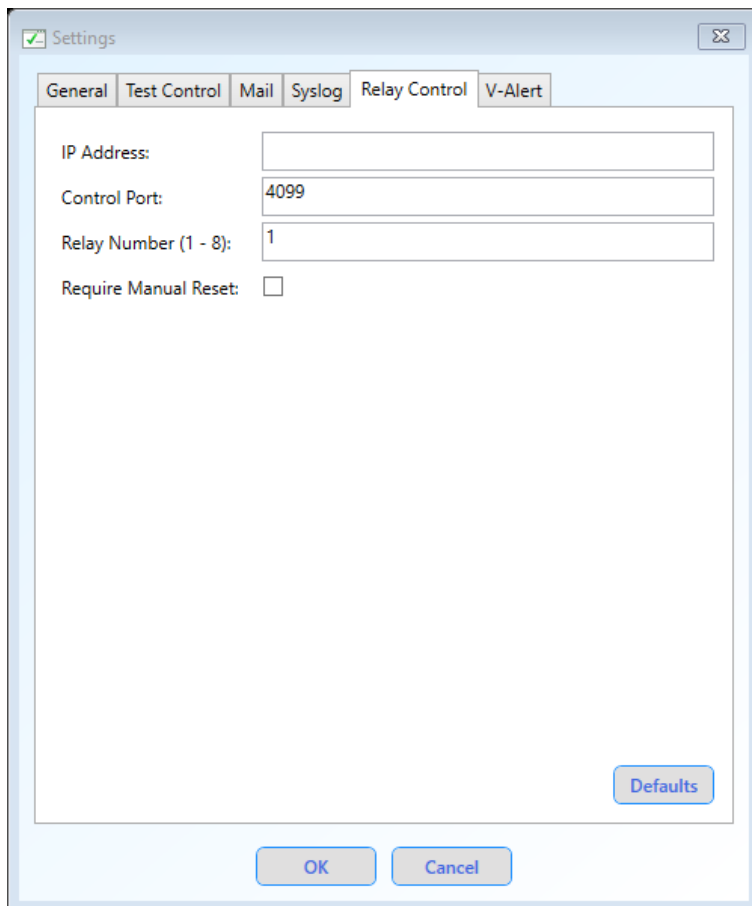
Once the settings are entered, the Send Test Syslog button can be used to send a test message.

Relay Control Settings

The VSM has the ability to control a relay output on a Valcom I/O Unit device. This relay can be used to control a variety of external equipment when the VSM enters a failure state. At this time, the VSM can only control a single relay on an I/O Unit. If multiple relays are needed, then the other relays can easily be programmed to follow the controlled relay from within the VIP-102B tool. When the controlled relay indicates a failure, all of the following relays will also indicate a failure.

In order for Relay Control to work properly, the controlled relay must be programmed in the VIP-102B so that its default state indicates a failure. For example, if an open relay is needed to indicate a failure, its default state should be programmed as open. Once the VSM successfully contacts all monitored devices, it will send a message to the controlled relay telling it to go to its non-default state, which in this case is closed. As long as the VSM is in a normal state with no failures, it will periodically send a message to the I/O Unit to keep the relay closed. If a failure is ever detected, it will send a message to the unit to tell the relay to return to its default state and a failure will be indicated. In addition, if the I/O Unit ever stops receiving control messages from the VSM, as when the PC running the VSM is shut down, the I/O Unit will eventually timeout and the relay will automatically revert to its default state to indicate a failure of the VSM itself. Pausing the VSM will also cause the relay to indicate a failure.

The settings used for Relay Control are shown below.

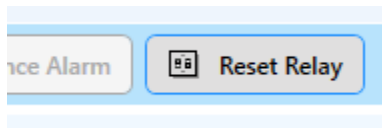


The screenshot shows a 'Settings' dialog box with the 'Relay Control' tab selected. The dialog has a title bar with a checkmark icon and a close button. Below the title bar are tabs for 'General', 'Test Control', 'Mail', 'Syslog', 'Relay Control', and 'V-Alert'. The 'Relay Control' tab contains the following fields:

- IP Address: [Empty text box]
- Control Port: 4099
- Relay Number (1 - 8): 1
- Require Manual Reset:

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Defaults'.

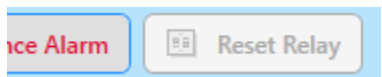
- IP Address – This is the IP address of the I/O Unit that is being controlled
- Control Port – This is the standard control port that the I/O Unit is listening for messages on. Messages will be sent to the unit from the VSM on this port to control the relay.
- Relay Number – This is the relay number that is being controlled on the unit. A Valcom I/O Unit typically offers 8 different relays that can be controlled.
- Require Manual Reset – When this option is disabled, the VSM will automatically send a message to the I/O Unit to put the relay in a normal state when all monitored devices have been successfully contacted. When this option is enabled, the relay will not be returned to a normal state automatically. A button will appear on the toolbar that must be used to manually reset the relay.



If the text on the button is black, then the relay is in a normal state and does not require a manual reset. If the text is red, however, it indicates that a failure was previously detected and the relay requires a manual reset.



It should be noted that the relay can only be reset once all monitored devices have returned to a normal state. If any devices are still in a failure state, the reset button will be disabled until all the devices are contacted successfully.



By requiring the relay to be manually reset, a history is effectively preserved so you can know if any devices have failed intermittently, even if they are all currently in a normal state.

V-Alert Settings

The V-Alert Server is a Valcom product that allows messages and alerts to be sent to a custom application on mobile devices. By configuring the VSM to interact with the V-Alert Server, mobile alerts can easily be sent whenever an issue is detected.

Note: Interaction with the V-Alert Server was added in version 3.3 of the VSM. If the VSM client is remotely connected to an older version of the service, the V-Alert settings will not be available.

The screenshot shows the 'V-Alert' settings window. It includes the following elements:

- Tabbed interface: General, Test Control, Mail, Syslog, Relay Control, **V-Alert**, MQTT
- Enable V-Alert: (Send Test Alert button)
- First Contact Alerts:
- Server Address: [Text Input]
- Token: [Text Input]
- Server Timeout: [10] (5 - 60 secs)
- Buffer Timeout: [60] (1 - 300 secs)
- Buffer Limit: [10] (1 - 10 alerts)
- Channels: [Text Input] (Add, Delete buttons)
- Defaults button
- OK, Cancel buttons

- Enable V-Alert – Used to enable or disable alert notifications.
- First Contact Alerts – When this option is enabled, a SUCCESS message will be sent for each device when it enters the Normal state after the VSM starts or contact is first made. Disabling this option will suppress these messages, and a SUCCESS will only be sent when devices actually return from a previously reported failure.
- Server Address – IP Address or host name of the V-Alert Server.
- Token – Security token required by the server for permission to send alerts.
- Server Timeout – Timeout in seconds for connecting to the server. If the server does not respond during this time, an error will be logged and the alert will be discarded.

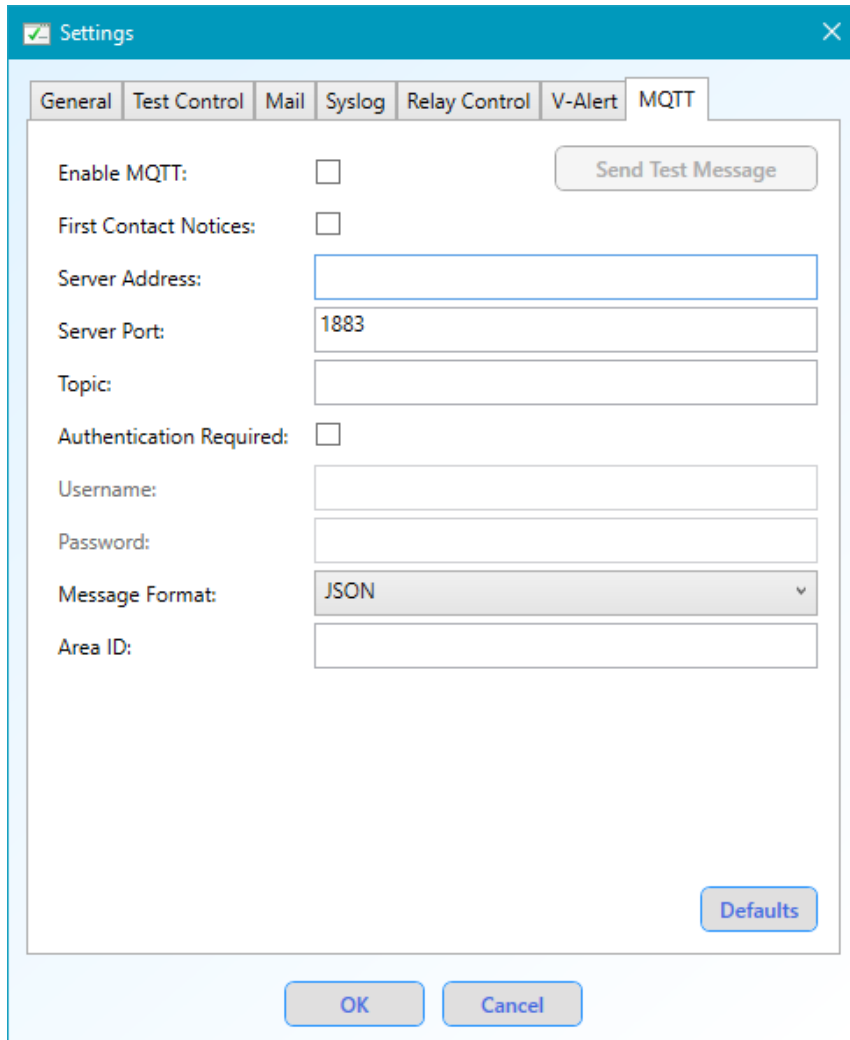
- Buffer Timeout - After an alert is sent, additional alerts will be buffered for this amount of time and sent as a single alert. If no additional alerts are buffered during this time, then buffering will be halted until after the next individual alert is sent. This option helps to prevent being overwhelmed with multiple alerts when a major problem occurs, such as a failing router. Please note, however, that events on Fire Panels will not be buffered and will be sent immediately when they occur.
- Buffer Limit - The max number of items that can be buffered before an alert is sent. If the limit is reached, a single alert will be sent with this number of items, even if the buffer timeout has not yet expired. Additional items will continue to be buffered until the timeout or limit is reached again. Setting this value to 1 will disable buffering and send every alert by itself.
- Channels – Each channel that is defined on the server can be subscribed to by mobile clients so that only the appropriate personnel will receive alerts about device failures. Channels can be added or deleted from the list and alerts will be sent to each channel that is provided. When entering a channel into the VSM list, the name is case sensitive and must be typed exactly as it appears on the server.

Once all the settings are entered, you may click the Send Test Alert button to test the entered settings. A test alert will be sent to verify that the settings are valid and have been entered correctly.

MQTT Settings

The VSM has the ability to publish messages to a MQTT server when failures are detected. Messages may then be viewed with any standard MQTT client.

Note: Support for MQTT was added in version 3.4 of the VSM. If the VSM client is remotely connected to an older version of the service, the MQTT settings will not be available.



The screenshot shows a 'Settings' dialog box with a tabbed interface. The 'MQTT' tab is selected. The dialog contains the following fields and controls:

- Enable MQTT:** A checkbox that is currently unchecked.
- Send Test Message:** A button located to the right of the 'Enable MQTT' checkbox.
- First Contact Notices:** A checkbox that is currently unchecked.
- Server Address:** An empty text input field.
- Server Port:** A text input field containing the value '1883'.
- Topic:** An empty text input field.
- Authentication Required:** A checkbox that is currently unchecked.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Message Format:** A dropdown menu currently set to 'JSON'.
- Area ID:** An empty text input field.
- Defaults:** A button located at the bottom right of the settings area.
- OK:** A button at the bottom center.
- Cancel:** A button at the bottom center, to the right of the OK button.

- Enable MQTT – Used to enable or disable MQTT notifications.
- First Contact Notices – When this option is enabled, a SUCCESS message will be sent for each device when it enters the Normal state after the VSM starts or contact if first made. Disabling this option will suppress these messages, and a SUCCESS will only be sent when devices actually return from a previously reported failure.
- Server Address – IP Address or host name of the MQTT Server.
- Server Port – Port used to communicate with the MQTT Server.
- Topic – The topic on the server that messages will be published to.

- Authentication Required – Indicates whether or not the server requires authentication. If authentication is required, then the Username and Password must be entered.
- Username – User name when Authentication is required by the server.
- Password – Password when Authentication is required by the server.
- Message Format – Format of messages that will be published. The JSON format contains expanded information that is parsed by other Valcom products.
- Area ID – A descriptive string used to identify the area that this VSM is monitoring.

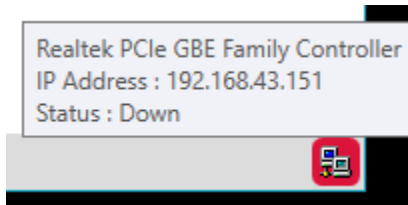
Network Interface Settings

One additional setting that can be useful is the ability to select the local network interface that should be used in a system that has multiple network adapters. This might be necessary for instance on a machine that has both a wired and a wireless adapter. Without selecting the adapter, the VSM might attempt to use the wrong adapter for communications and failures could occur. A machine with multiple adapters could also be helpful if other Valcom software tools need to be run on the same machine as the VSM.

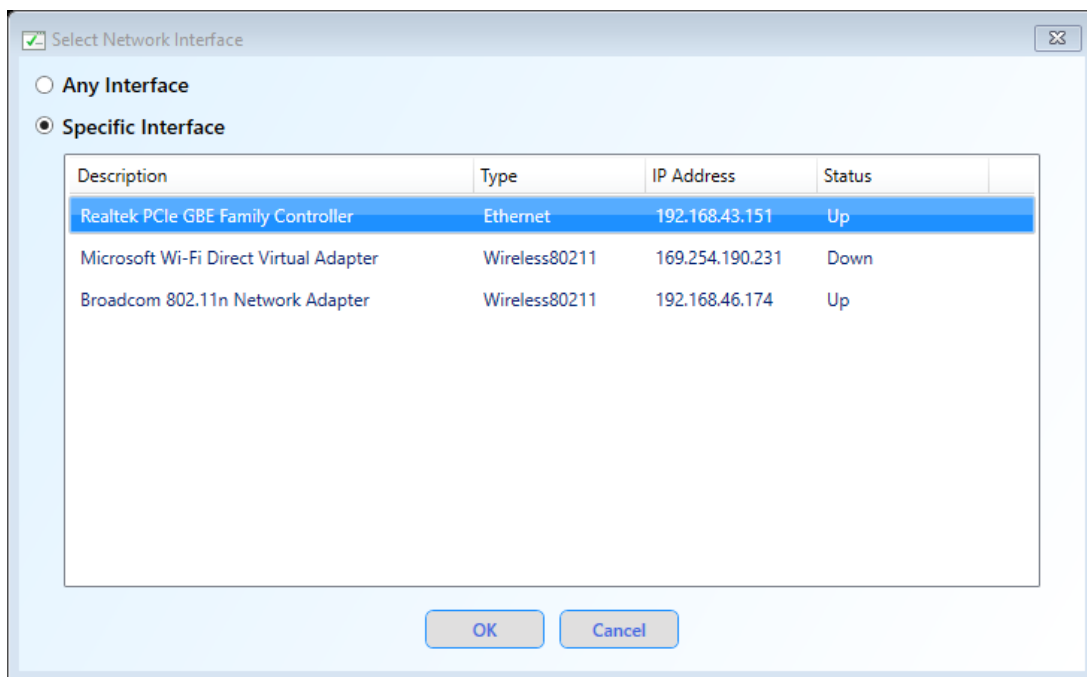
In order to select the network interface, you must click on the network icon in the lower right hand corner of the main window in the VSM.



This icon is also used to show when there are problems with the network connection, such as when a network cable has been unplugged.



Clicking this icon will open a window that displays all the network adapters that are enabled on your PC.




By default, the VSM will attempt to use Any Interface when performing communications. This causes network sockets to bind to the IP Address 0.0.0.0 and the best adapter will be selected by Windows on the fly. If you want to use a specific network interface, click the Specific Interface radio button, highlight the interface that you want to use, and click OK. At this point, the VSM will bind to that specific IP address for network communications. If the IP address of the PC is later changed through the Windows Control Panel, the VSM should detect this change and rebind its sockets as necessary. It should be noted that some communications, such as Ping, might still use a different interface, because that is what the protocol dictates.

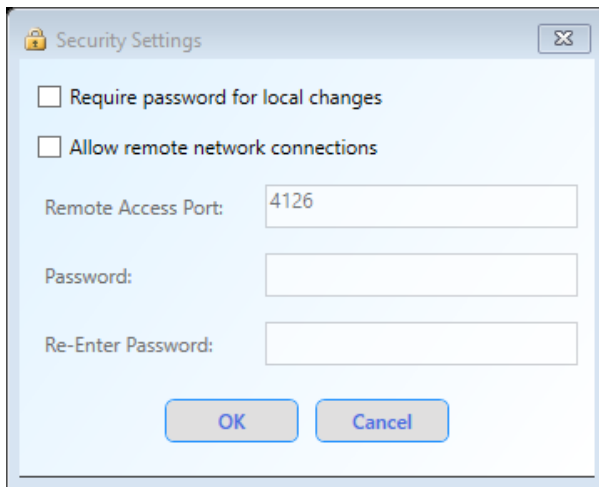
Using a specific network interface can be helpful in preventing hard to trace errors. It can also provide more control over obtaining exclusive access to required ports. For example, if using Any Interface with Heartbeat Testing, another program that uses a specific interface will still be able bind to the necessary network control port. This could cause the other program to inadvertently receive the heartbeat responses that are intended for the VSM and cause the VSM to produce failures. By using a specific interface in the VSM, the other program will receive an error if it tries to bind to same network control port. The VSM will obtain exclusive access to the responses and not the other program.

Security and Remote Access

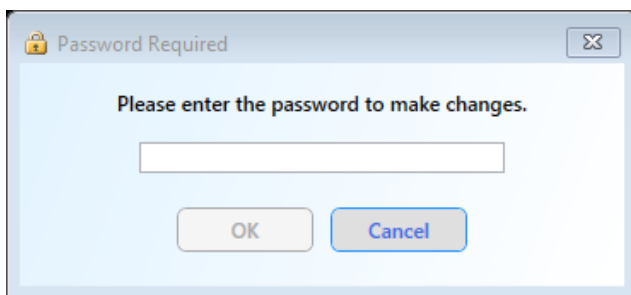
The VSM has the ability to password protect areas of the software that could be changed by the user. This might be helpful if installed by the administrator on a machine to which other people have access. Along similar lines, the same password can be used to allow remote access to the VSM service from another machine.

Protecting the VSM from Local Changes

In order to password protect the VSM, you must click on the Security Settings button  in the main toolbar. Clicking this button will open a window where you can specify that a password is required to make local changes.



Simply check the box to require a password for local changes and enter a password in the provided boxes. From this point on, when you try to make changes to the configuration or settings, you will be prompted for a password before continuing.



Some major changes, such as creating a new system or changing notification settings will always prompt for the password. Other changes such as adding a new device or editing the properties of an existing device might only prompt for the password the first time they are attempted from the main VSM window. The VSM recognizes that you might be making changes to multiple devices in a row and will only prompt for the password before making the first initial change. This keeps you from having to re-enter the password multiple times. After a short period of inactivity, however, the password will time

out and you will have to re-enter it if you try to make changes after too much time has passed. The password will also time out whenever the main VSM window is closed or minimized to the system tray.

Remote Access with the VSM

The VSM has the ability to allow access to the monitor service from a remote client on a different machine. When connected remotely, the client will still receive all the notifications that they would receive locally. This can be very useful if the monitor service is running on a server machine in a storage closet or even at an offsite location.

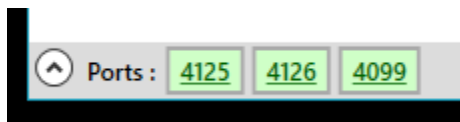
Enabling Remote Access

For security reasons, remote access is disabled by default and must be manually enabled by the user. Remote access can be enabled from the same screen where a password was entered for local changes. A password is required when using remote access and is not optional.

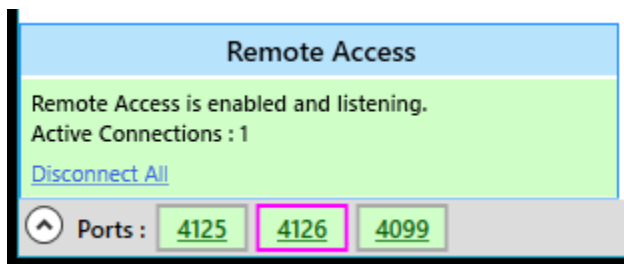
A Remote Access Port is also required that can be changed if necessary. In most cases, the default port should be fine. If another program on your PC is using this port it can be changed to some other value as needed.

Once remote access settings are changed, it might take several seconds while the monitor service is restarted to allow the changes. During this time, the local client application will disconnect from the service and will reconnect automatically.

Once remote access is enabled, a new port value should appear in the ports display for the remote access port.

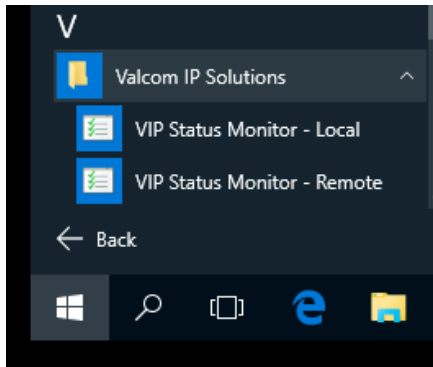


Clicking on the port will show details about remote access and the number of connections that are active to the local monitor service. When a remote client is connected, the port will have a pink border to draw attention to the fact that some other client is connected. There will also be a link that can be clicked on to force all remote clients to disconnect from the service. Note that if you are actually connected over a remote connection, this will also close your active connection.



Connecting from a Remote Client

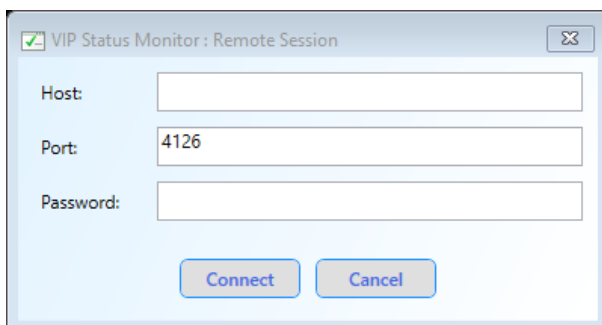
Once remote access has been enabled, the remote client can be used to connect to the monitor service from another PC. In a complete installation, the VSM setup will create two shortcuts in the Windows start menu. One shortcut is used to launch the local client for connecting to the service on the local machine. This client is typically automatically launched when the user logs in. The other shortcut can be used to launch an instance of the remote client. The only real difference in the shortcuts is that the remote client passes the `-remote` parameter to the client application so it knows to start in remote access mode.



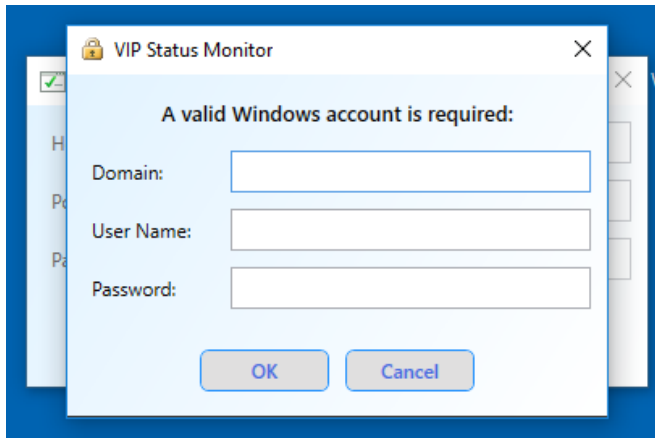
When using remote access, multiple different clients are allowed to connect to the same instance of the monitor service. In practice, however, this is discouraged in order to prevent multiple clients from trying to make changes at the same time.

From a client PC, only one instance of the remote client is allowed to be running. In other words, you cannot have multiple remote clients connected to multiple monitor services at the same time from a client PC.

Once you click on the shortcut to launch the remote client, you will be presented with a connection screen. You must enter the IP Address or host name of the remote monitor service, the port being used by the service for remote connections, and the password that was set for remote access.

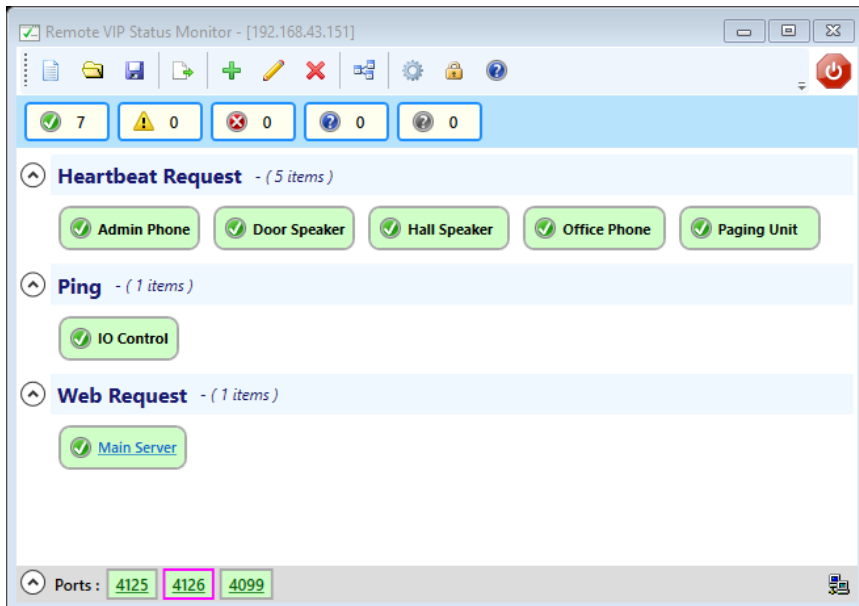


In most cases, when the remote machine and the client machine are on the same network domain, this is all the information that is necessary and the remote client will attempt to connect. Sometimes, however, if the machines are on different domains, an additional Windows user account will be prompted for.

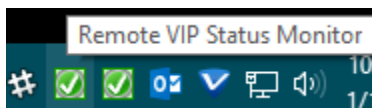


This account must be an account that has authority to login to the remote machine as if you were physically sitting at the keyboard trying to login to it. You should enter the appropriate Domain (or possibly the machine name) and a user and password that can be used to login to this machine.

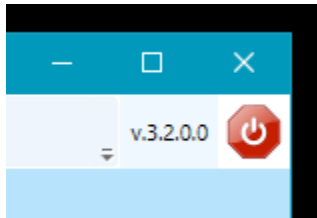
Once the proper credentials are provided, you will be connected to the remote service and the remote client will obtain the configuration so it can be displayed in the main VSM window. At this point, you can do anything to the remote service that you could do if you were connected locally.



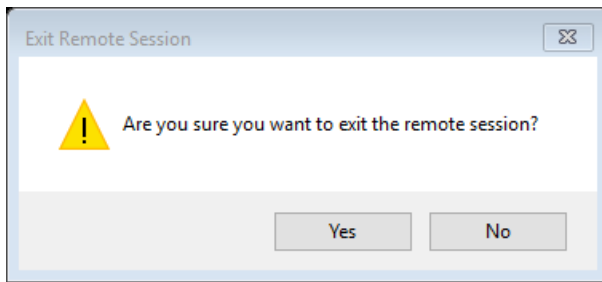
An additional icon will also appear in the system tray that is used for the remote client. If this machine is also running the local client and service, you will see 2 icons, one for the local client and one for the remote client. Hovering over each icon with the mouse will give you a tooltip that can be used to distinguish them from each other.



One additional thing you might notice is a version number and a new power button in the upper right hand corner of the main window of the remote client.



On systems that support it, the version number of the VSM service that the remote client is connected to will be displayed. This is the version of the actual service itself and not the version of the client application. Just like with the local client, closing the main window will minimize the remote client to the system tray. To completely shut down and end the connection, the new power button can be used to exit the remote session. You will be prompted to end the session and can continue.

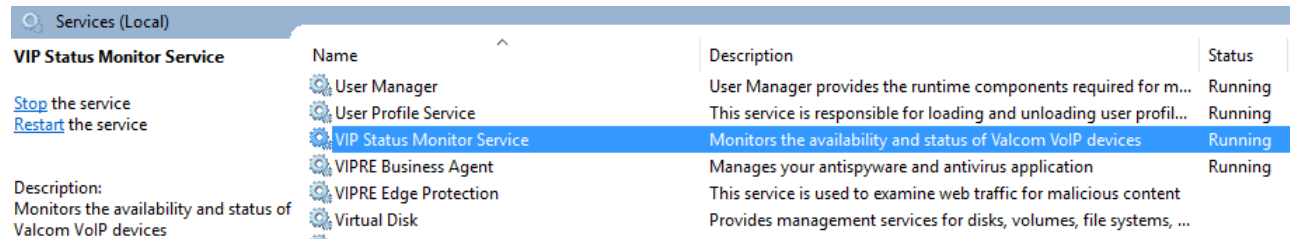


The remote session can also be terminated by clicking on the Exit Remote Session menu in the system tray icon, just like you would with the local client.

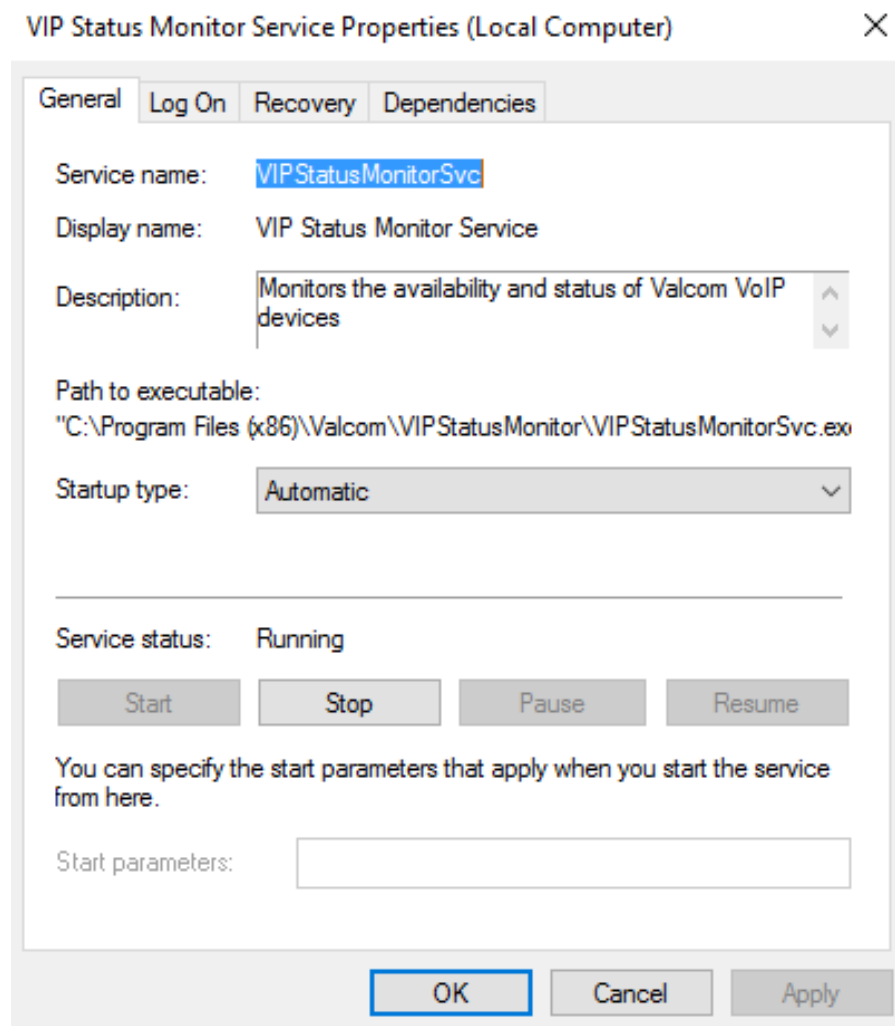
Advanced Topics and Troubleshooting

Controlling the Monitor Service

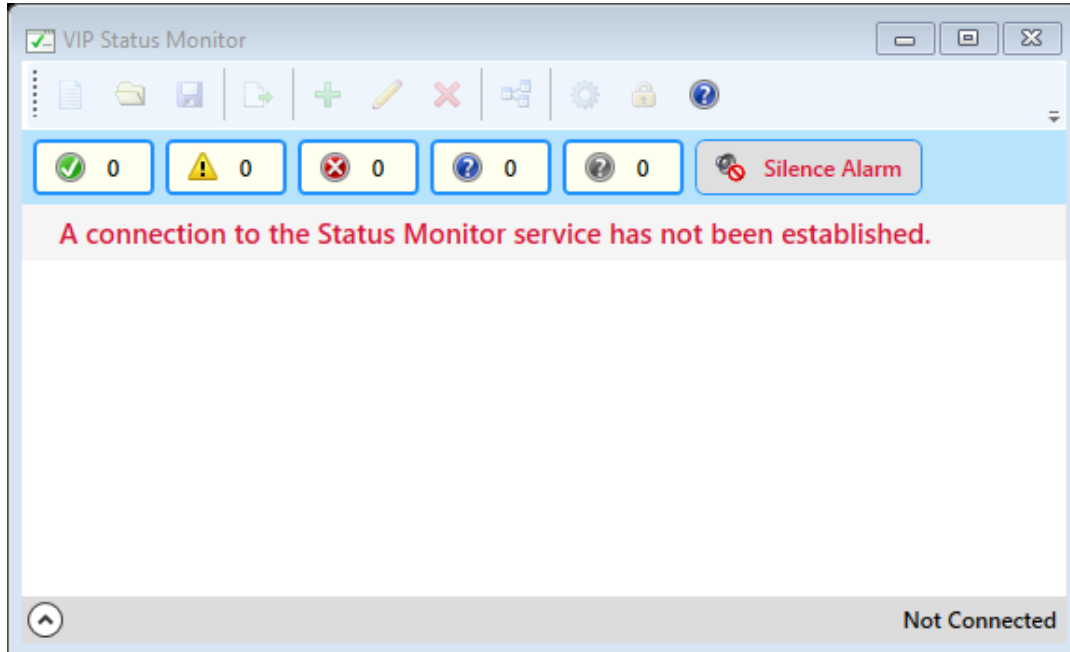
The VIP Status Monitor Service should be installed and registered with Windows during the program installation. You can view this service in the Windows Services control panel.



This service runs under the Local Service Windows account and should start automatically whenever the machine boots up. The properties of the service can be viewed from the Services control panel.

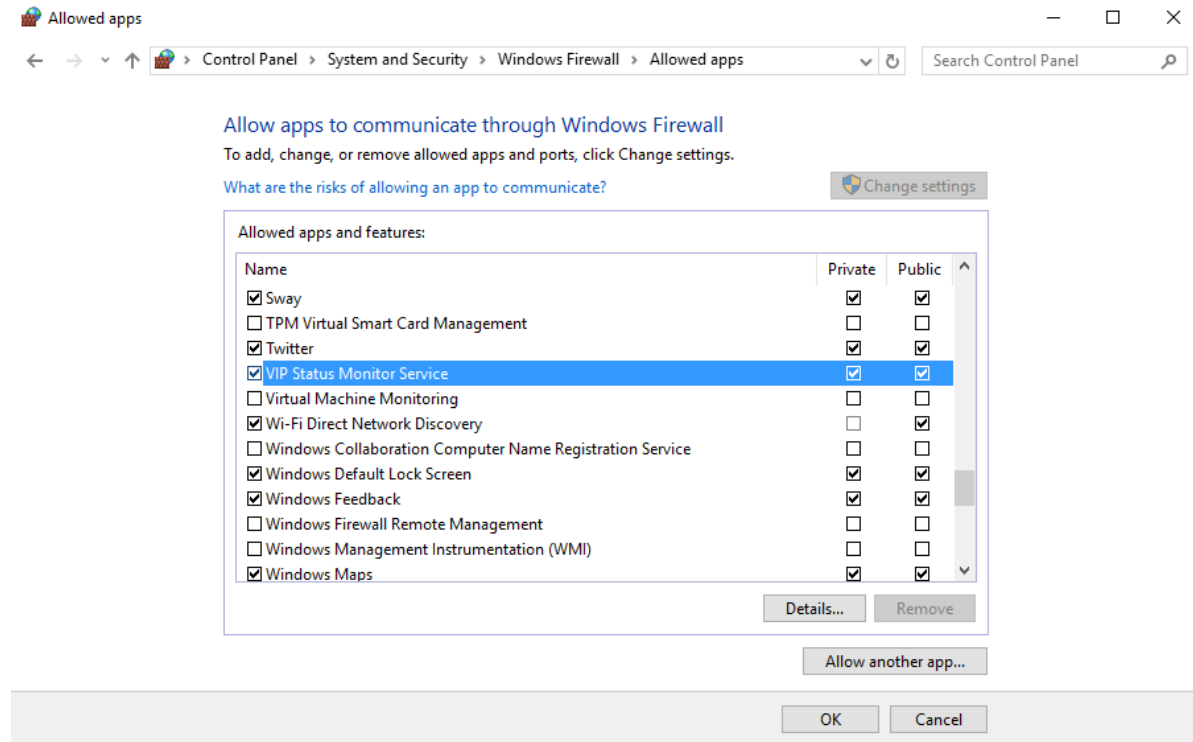


If the monitor service ever runs into a major problem and needs to be restarted, it can be done from this control panel. Simply stop and then restart the service. While the service is stopped, the client application will disconnect and might show an error if it is not able to reconnect within a short amount of time.



Windows Firewall Configuration

The VIP Status Monitor Service requires an exception in the Windows Firewall (or any other firewall software you are running) in order to allow network traffic to and from the service. This exception should be created by the setup program during installation. This can be verified by viewing the firewall exceptions in the Windows Control Panel.



Symptoms of a missing firewall exception sometimes include the failure of Heartbeat Request testing and not being able to connect from a remote client, even though remote access has been enabled.

If the exception is not present or has been removed, it might need to be added manually. You will need to click the button to Allow Another App and the browse to the location of the VIP Status Monitor Service file to add the exception.

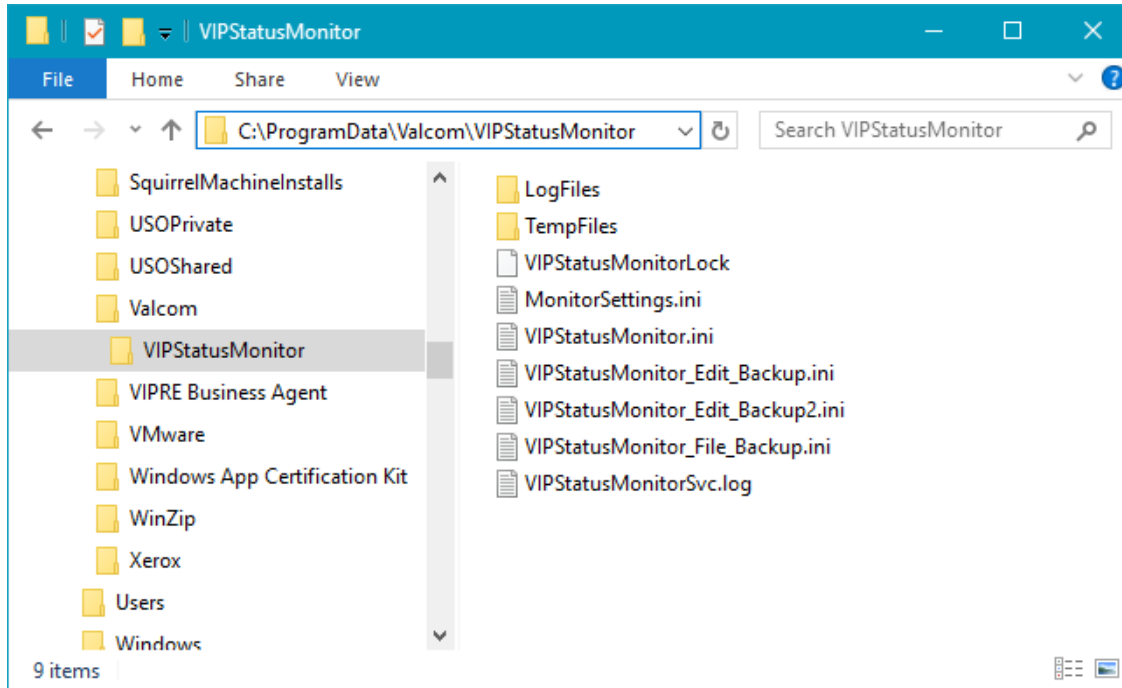
(Typically located at C:\Program Files (x86)\Valcom\VIPStatusMonitor\VIPStatusMonitorSvc.exe)

Storage Location of Data Files

The VSM Service creates and stores a variety of files on the local PC that are used to control the configuration and settings for the service. These files are typically stored in the following folder.

C:\ProgramData\Valcom\VIPStatusMonitor

Please note that the ProgramData folder is typically a hidden folder and might not be visible on your PC. You can either turn on the ability to view hidden files and folders in Windows or type the path in the address bar of Windows Explorer and hit Enter.

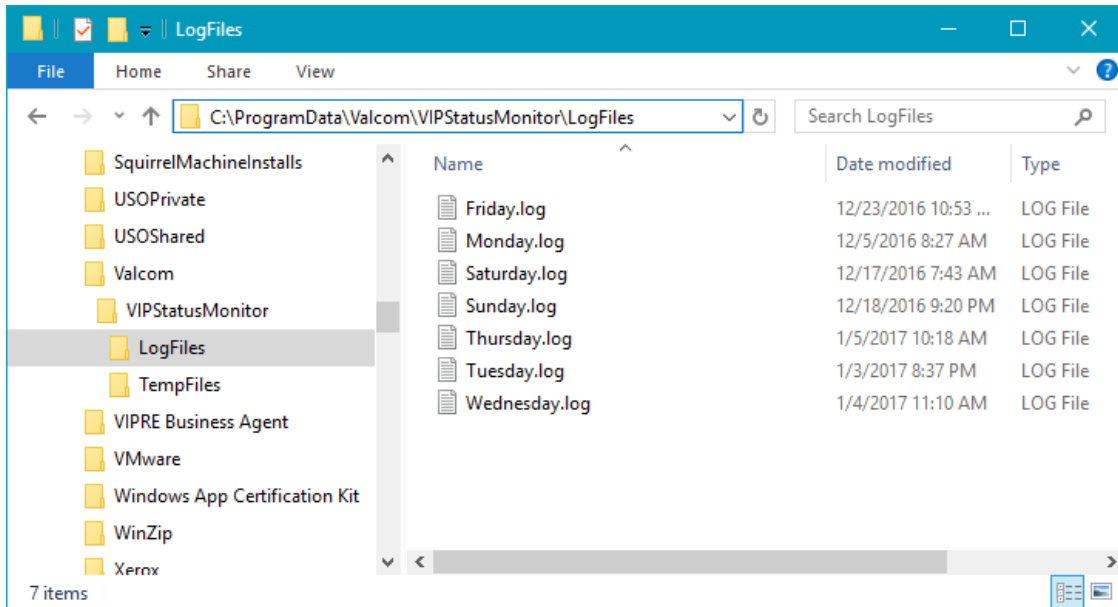


Several of the files in this folder might be useful when troubleshooting. The VIPStatusMonitorSvc.log file will often contain errors that occur with the actual monitor service itself. If contacting Tech Support, this file might be requested.

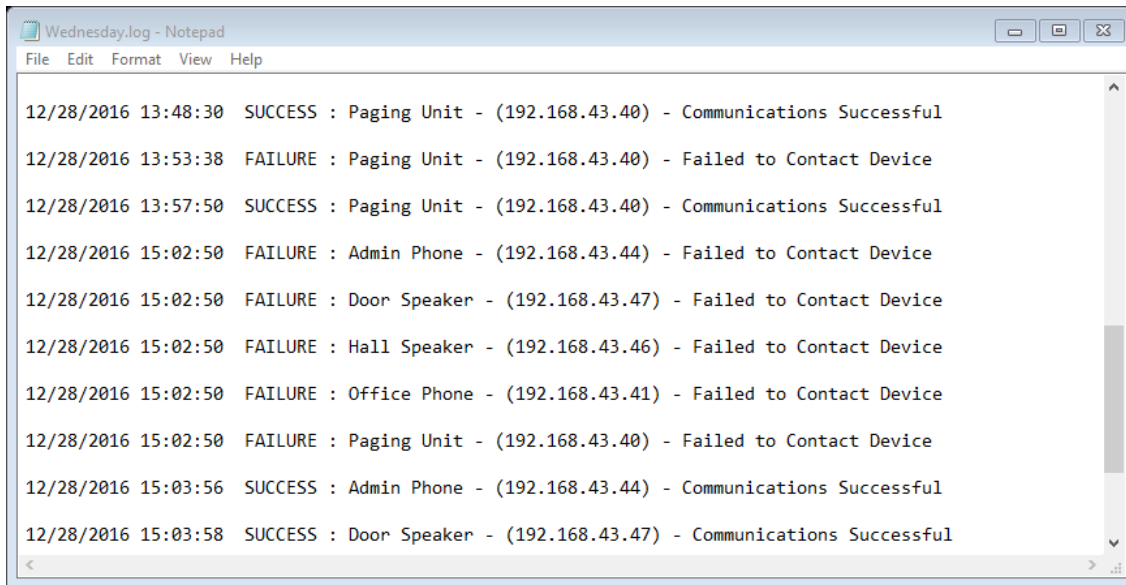
The VIPStatusMonitor.ini file contains the working configuration and is used to initialize the VSM when it first starts up. This file should not be modified directly. Always save or open files from the client application itself.

When modifying the configuration of the VSM, backup files are typically made before major changes, such as creating a new system, adding a device, deleting a device, etc. If you accidentally made a change without meaning to and you do not have a recent saved copy of the configuration, you might be able to revert your changes by loading one of these backup files if you catch it soon enough. Backups with the word File_Backup in then name are often created before making a major change, like creating a new system or opening a saved file. Backups with the word Edit_Backup in the name are often created before making individual device changes, like adding a new device or deleting an existing device.

The LogFiles folder in this directory will often contain logs of recent status changes to devices in the VSM. Log files are written on a daily basis when changes occur and are overwritten each week as necessary.

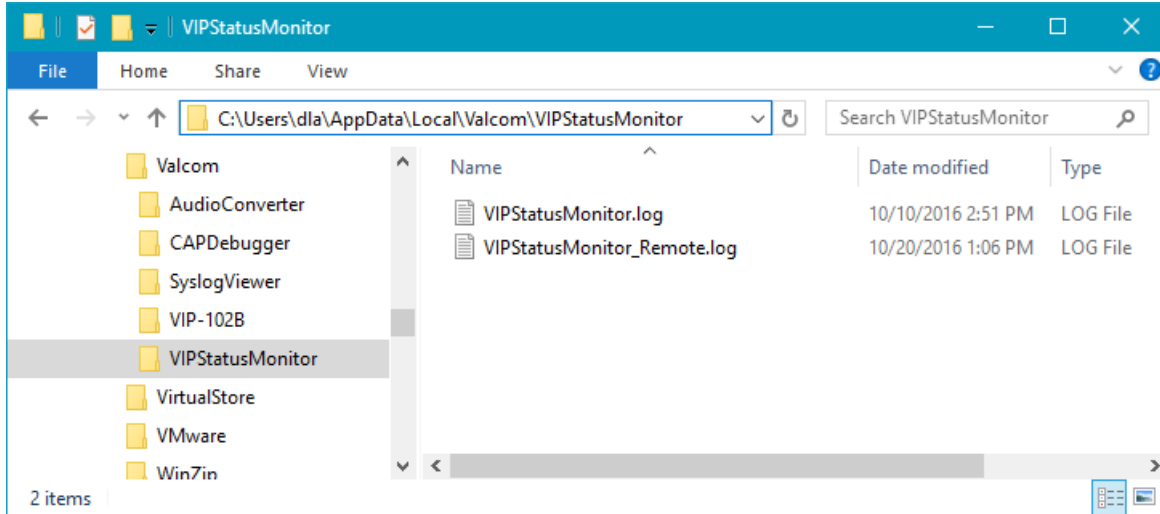


A sample log file is shown below.



If there is ever a problem with the VSM due to invalid or corrupted files that a re-install does not correct, then the local data files created in the ProgramData folder could be removed in an attempt to start from scratch. Note that doing this will remove all configuration options and customized settings that have been entered. Also note that you might have to uninstall the VSM, or at least stop the monitor service, before data files can be removed, since the service might have some files locked.

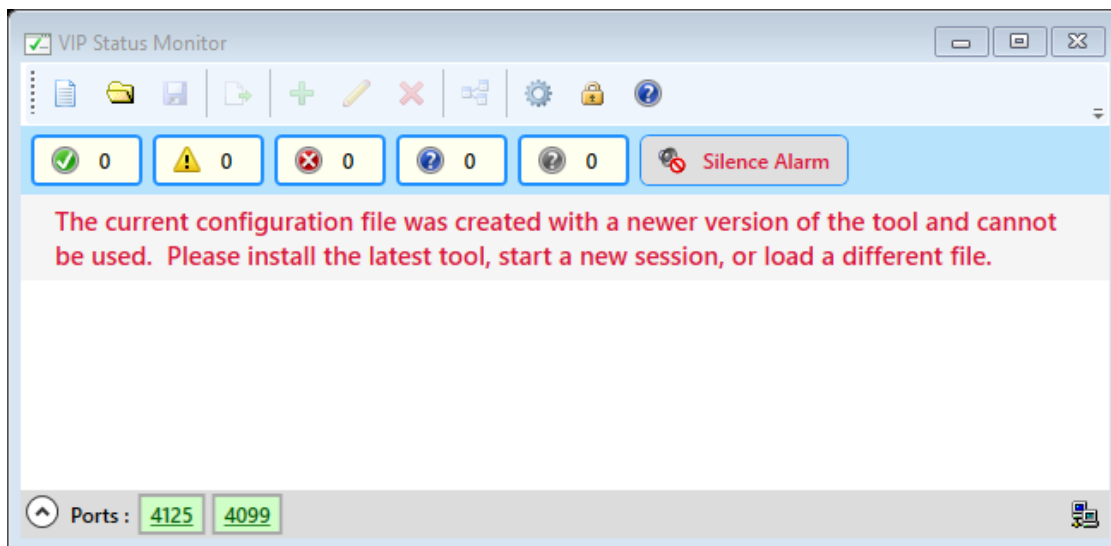
While these data files are created by the monitor service, the client application also creates its own data files, such as log files for client errors. Example of errors that could be found in these logs include problems with the client being able to connect to the monitor service. These files are stored in a separate location, typically under the logged in user's profile, and might also be requested if contacting Valcom Tech Support.



Reverting to an Older Version of the VSM

While everyone would love to write perfect code, it's a fact of the software world that bugs do sometimes occur. Since this is the case, you might find yourself at some point needing to revert to an older version of the VSM. Hopefully this will never be the case. But in order to make sure this is as easy as possible if the need ever arises, Valcom always recommends saving off a copy of your current configuration before performing any upgrade to the VSM. Newer versions of the VSM often change the structure of the configuration files and might not be read by an older version of the program. By saving a copy of your configuration before performing an upgrade, you will be making sure that you can easily revert to an old file if necessary.

If you do ever revert to an older version of the program, you could potentially see a message like the following from the client application.



If this is the case, you can start a new session or load the saved copy of your configuration that you made before performing the upgrade.

Known Device Issues with the VSM

Some Valcom VoIP devices have known issues when interacting the VSM. Devices with these issues may require firmware upgrades in order to be monitored properly. Otherwise, workarounds may be needed and are detailed below.

Using a Web Request with eLaunch

One known issue is when using the VSM to monitor an eLaunch server using the Web Request method. In versions of the eLaunch server earlier than 2.2, there is a bug where each iteration of the Web Request method creates a new user session in the eLaunch database. These sessions were not being disposed of properly by the eLaunch server and were causing the system database on the server to fill up. Once the database was filled, there would be problems with connecting to the server from a web browser and syslog errors would be generated by the server. This issue was fixed in version 2.2 of the eLaunch server and a firmware upgrade will be required if you want to use the VSM to supervise it using a Web Request. If a firmware upgrade cannot be performed, you will have to use the Ping method to supervise the eLaunch server instead of a Web Request. Importing devices into the VSM from a CSV file will typically select the appropriate method based on the version number of the device. Adding a device manually, however, will initially default to using a Ping since the version number is unknown.

Using a Heartbeat Request with I/O Units

Another issue concerns the use of the Heartbeat Request method with the I/O Unit. Earlier versions of this device did not support the Heartbeat Request. This feature was not added until version 3.0 of the device. Any I/O Unit earlier than this will be required to use the Ping method for supervision. If you have a version of the device that supports the preferred Heartbeat Request method, it can be used instead. Importing devices into the VSM from a CSV file will typically select the appropriate method based on the version number of the device. Adding a device manually, however, will initially default to using a Ping since the version number is unknown.

Supervising a UTM Router

The UTM router can only use the Ping method for supervision and cannot use the Heartbeat Request. The reason for this is that the router is designed to forward all packets sent to its control port to another address. This includes the Heartbeat Request. Because the device forwards the request packets instead of responding to them, messages sent to the control port cannot be used and the Ping method will be required. This is the default method used by the router, so special action should not be required.

Appendix A: VSM Syslog Messages

The VIP Status Monitor has the ability to send syslog messages when various events occur for monitored devices or within the monitor service itself. This appendix is intended to detail the different messages that might be encountered. All messages are sent to the standard syslog port of 514.

Syslog messages sent by the VSM will all have the following format:

```
<PRI>Mmm dd hh:mm:ss HOSTNAME VIPStatusMonitorSvc: MESSAGE
```

PRI = Numeric value that indicates the Facility and Severity of the message. All messages sent by the VSM are sent with a standard syslog Facility of local1 (which has a value of 17). This produces a base PRI value of 136. The Severity is based on the standard log levels that can be set in the VSM, and when combined with the Facility, will produce the following possible PRI values:

- 136 = Emergency (0)
- 137 = Alert (1)
- 138 = Critical (2)
- 139 = Error (3)
- 140 = Warning (4)
- 141 = Notice (5)
- 142 = Info (6)
- 143 = Debug (7)

Mmm dd hh:mm:ss = A timestamp that indicates when the syslog message was sent. For example:

```
Jan 15 08:30:45
```

HOSTNAME = The Hostname of the PC that the monitor service is running on.

VIPStatusMonitorSvc = Tag that indicates the message is from the VIP Status Monitor Service.

MESSAGE = This is the actual content of the syslog message. Specific messages that are sent by the VSM are detailed in the following sections. Messages will be sent based on the log level that is specified in the tool settings. For a certain level, the VSM will send all messages at that level and above. For example, the default level of Notice will cause the VSM to produce messages from every level except Info and Debug.

For the purpose of this document, when a message pertains to a specific device, a tag with the identifying information for that device will appear within angle brackets. For example, the name of a device will be listed as <DEVICE> and the IP address will be listed as <IPADDRESS>. The angle brackets will NOT appear in the actual message and the tag will be replaced with the actual value for that device.

Emergency

- A fire panel device being monitored has entered the Alarm state. Additional details as to the cause of the alarm will be reported at the end of the message if they are available.

```
ALARM : <DEVICE> - (<IPADDRESS>) - Panel Alarm - [Details]
```

Alert

- The VSM service has started and is beginning the initialization process. This message will be sent after the host machine boots. The version number of the service is reported.

```
Service Startup : Monitor startup, version=4.2.0.0
```

- The VSM Service is being stopped, likely because the PC is being powered off.

```
Service Shutdown : Shutdown in progress
```

- Initialization errors for various components of the VSM Service.

```
Service Error : Failed to initialize mail manager
Service Error : Failed to initialize relay manager
Service Error : Failed to initialize UDP communications
Service Error : Failed to initialize test manager
Service Error : Failed to initialize V-Alert manager
Service Error : Failed to initialize MQTT manager
Service Error : Failed to initialize heartbeat test manager
Service Error : Failed to initialize monitor server
Service Error : Failed to initialize service host
Service Error : Failed to initialize refresh timer
Service Error : Failed to initialize watchdog timer
Service Error : Unexpected errors creating test manager
Service Error : Unexpected errors creating heartbeat manager
Service Error : Unexpected errors creating fire panel manager
```

- Failure to re-initialize Relay Control after settings have been changed.

```
Service Error : Failed to initialize relay manager with new settings
```

- Errors when attempting to start Remote Access if it has been enabled. The monitor service might still be running, but access from a remote client will not be possible.

```
Service Error : Service host remote access could not be started
```

- Failure to start UDP based components. This is sometimes due to port conflicts with other applications running the same machine. The IP Address and Port that the component tried to start on should be included in the message.

```
Service Error : Failed to start UDP communications on 192.168.43.100:4125
Service Error : Failed to start heartbeat testing on 192.168.43.100:4099
```

- Security settings, such as the tool password, were changed by the user.
Service Control : Security settings have been changed
- Remote Access settings were changed by the user, which requires re-initialization.
Service Control : Remote Access was modified. Service host is restarting...
- Errors occurred when trying to read or load the configuration files when the service is starting. This could be due to files that are corrupted or left over from an incompatible version.
Initialization Error : Unable to load all configuration files
Initialization Error : The current configuration file is invalid or corrupt.
Initialization Error : The current configuration file was created with a newer version of the tool and cannot be used.
Initialization Error : Errors occurred while loading the current configuration file.
Initialization Error : The current configuration file has not been loaded.
Initialization Error : The state of the current configuration file could not be determined.

Critical

- A device being monitored has entered the Failure state. Contact with it could not be made and it is likely not functioning.
FAILURE : <DEVICE> - (<IPADDRESS>) - Failed to Contact Device
- Failed to contact the Virtual IP Address in a Failover system. Without the Virtual Address, the system cannot be used by clients and the web interface cannot be accessed.
FAILURE : <DEVICE> - (<IPADDRESS>) - Failed to Contact Virtual
- If a remote monitor is reporting a Failure state for some device, then a message will be sent for that service. The remote service likely sent its own message with more specific details.
FAILURE : <DEVICE> - (<IPADDRESS>) - Remote Monitor Reports Failures
- A fire panel being monitored has entered the Failure state. There were errors during communications or a panel has been reported as missing. Additional details as to the cause of the failure will be reported at the end of the message if they are available.
FAILURE : <DEVICE> - (<IPADDRESS>) - Panel Failure - [Details]

Error

- If there is a failure of the Primary or Secondary device in a Failover System, a message will be sent to indicate the failure. In this case, the system is likely still functioning because the peer device is working correctly, but the problem needs to be addressed.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Failed to Contact Primary  
WARNING : <DEVICE> - (<IPADDRESS>) - Failed to Contact Secondary
```

- If a remote monitor is reporting a Warning state for some device, then a message will be sent for that service. The remote service likely sent its own message with more specific details.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Remote Monitor Reports Warnings
```

- If a remote monitor is reporting that it has been paused, then a message will be sent to indicate that the remote service is not performing monitoring.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Remote Monitor is Paused
```

- The selected test method is not supported by the device. This is typically only seen with the External Supervision test method.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Test Method Not Supported
```

- A status reported by the device is not recognized. This is typically only seen with the External Supervision test method.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Unrecognized Status Detected
```

- A fire panel being monitored has entered the Warning state. Examples of items that can cause this state are trouble or supervisory conditions. Additional details as to the cause of the warning will be reported at the end of the message if they are available.

```
WARNING : <DEVICE> - (<IPADDRESS>) - Panel Warning - [Details]
```

Warning

- The monitor service has been paused by the user.

```
Service Control : Monitor paused
```

- If heartbeat testing is disabled, but is the preferred method for the current configuration, a message will be sent to indicate that it should be enabled for optimal monitoring.

```
Service Control : Heartbeat testing is disabled but might be required
```


- An error occurred while trying to send an e-mail. This could be due to incorrect mail settings or a mail server that is unreachable.

```
Mail Failure : An error occurred while sending a mail notification.
Mail Failure : Unable to send mail notification for Init Failure
Mail Failure : Unable to send mail notification for <DEVICE>
```

- An error occurred while trying to send a message to the V-Alert Server. This could be due to incorrect settings or a server that is unreachable.

```
V-Alert Failure : An error occurred while sending an alert.
V-Alert Failure : Unable to send notification for Init Failure
V-Alert Failure : Unable to send alert for <DEVICE>
```

- An error occurred while trying to publish a message to the MQTT Server. This could be due to incorrect settings or a server that is unreachable.

```
MQTT Failure : An error occurred while publishing.
MQTT Failure : Unable to publish message for Init Failure
MQTT Failure : Unable to publish message for <DEVICE>
```

- If a remote monitor is reporting a Disabled state for some device, then a message will be sent for that service. The remote service likely sent its own message with more specific details.

```
DISABLE : <DEVICE> - (<IPADDRESS>) - Remote Monitor Has Disabled Items
```

Notice

- Relay control settings were changed by the user and the new settings are active.

```
Service Control : Relay Control settings have been modified
```

- Heartbeat testing is disabled, but it is not required for the current configuration.

```
Service Control : Heartbeat testing is not active
```

- The IP Address of the active network interface was changed, typically by the user from the Windows Control Panel. This might also be seen when a new address is obtained via DHCP.

```
Service Control : Network address changed : 192.168.43.100
```

- The VSM has resumed after previously being paused by the user.

```
Service Control : Monitor resumed
```

- A new monitor session was created by the user in the client application.

```
Service Control : New monitor session created
```

- A new monitor session was loaded by the user in the client application from a saved file.

Service Control : New monitor session loaded from saved file

- A device being monitored has entered the Normal state. It is functioning properly and contact with the device was successful.

SUCCESS : <DEVICE> - (<IPADDRESS>) - Communications Successful

- A device being monitored has been disabled by the user. The device will not be monitored again until it is re-enabled.

DISABLE : <DEVICE> - (<IPADDRESS>) - Test Item Disabled

- A device entered the disabled state because it was set to use Heartbeat Testing, but Heartbeat Testing is disabled globally and Ping Fallback is not active.

DISABLE : <DEVICE> - (<IPADDRESS>) - Heartbeat Testing Disabled

- When using the External Supervision test method, a manual clear of faults was requested by the user through the client application.

CLEAR : <DEVICE> - (<IPADDRESS>) - Clear requested by user

- When Periodic Status Messages are enabled in the Syslog Settings, a message that shows the current states will be sent. The message will also be sent once all devices enter a known state (such as when all tests complete after a reboot). Status messages are always sent if they're enabled in the Settings, regardless of the selected Log Level.

STATUS : Total=7, Normal=6, Warning=0, Failure=1, Alarm=0, Disabled=0

Info

- The Service Host has started and is ready to accept connections from the client application. This message will also indicate whether or not Remote Access enabled.

Service Control : Service host has started. Remote access is enabled.
Service Control : Service host has started. Remote access is disabled.

- UDP based components have started with the IP Address and Port they were started on.

Service Control : UDP communications started on 192.168.43.100:4125
Service Control : Heartbeat testing started on 192.168.43.100:4099

- A syslog message was generated by the user to test the entered settings.

Service Control : Test syslog message requested by user

Debug

- There are currently no messages sent at this level

Appendix B: Required Protocols and Ports

VIP Status Monitor Feature	Required Protocol / Port
Ping Test Method	ICMP
Web Request Test Method	HTTP / Port 80
Heartbeat Request Test Method	UDP Port 4099 by default
Status Monitor Request Test Method	UDP Port 4125 by default
External Supervision Test Method and Control	UDP Ports 4099 and 4125 by default
Fire Panel Supervision Test Method	Modbus Protocol / TCP Port 502 by default
Remote Access Connections	TCP Port 4126 by default
Mail Notifications	SMTP / TCP Port 25 by default. Common ports with encryption include 465 or 587.
Syslog Notifications	Syslog Protocol / UDP Port 514
Relay Control	UDP Port 4099 by default
V-Alert Notifications	HTTPS / Port 443
MQTT Notifications	MQTT Protocol / TCP Port 1883 by default