



Viola Patrol User Guide

Firmware Version M2MGW 3.3.3-2503-88269563
Document Version 1
May 2013

Copyright and Trademark

Copyright © 2008-2013, Viola Systems Ltd. All rights to this manual are owned solely by Viola Systems Ltd. (referred elsewhere in this User's Manual as Viola Systems). All rights reserved. No part of this manual may be transmitted or reproduced in any form or by any means without a prior written permission from Viola Systems.

Viola Systems Ltd.

Lemminkäisenkatu 14-18 A

FI-20520 Turku

Finland

E-mail: info@violasystems.com

Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: <http://www.violasystems.com>

Disclaimer

Viola Systems reserves the right to change the technical specifications or functions of its products or to discontinue the manufacture of any of its products or to discontinue the support of any of its products without any written announcement and urges its customers to ensure that the information at their disposal is valid.

Viola software and programs are delivered "as is". The manufacturer does not grant any kind of warranty including guarantees on suitability and applicability to a certain application. Under no circumstance is the manufacturer or the developer of a program responsible for any damage possibly caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are the sole property of Viola Systems. Any transfer, licensing to a third party, leasing, renting, transportation, copying, editing, translating, modifying into another programming language or reverse engineering for any intent is forbidden without the written consent of Viola Systems.

Viola Systems has attempted to verify that the information in this manual is correct with regard to the state of products and software on the publication date of the manual. We assume no responsibility for possible errors which may appear in this manual. Information in this manual may change without prior notice from Viola Systems.

Revisions

Date	Document Version	M2MGW Version	Description of Changes
05/2013	1.0	3.3.3-2503-88269563	First version

Contents

COPYRIGHT AND TRADEMARK	2
DISCLAIMER.....	3
REVISIONS.....	4
1. VIOLA PATROL – TRAFFIC LIGHTS FOR REMOTE DEVICE MONITORING.....	6
1.1 Viola Patrol user interface.....	6
2. LOGGING IN TO VIOLA PATROL.....	7
3. SETTING UP REPORTING AND MONITORING.....	8
3.1 Configuring Viola Patrol.....	8
3.1.1 Configuration options.....	8
3.2 Adding a new device to Viola Patrol.....	9
3.3 Removing a device from Viola Patrol.....	10
3.4 Disabling viewing of reports from a device.....	11
4. MONITORING REMOTE DEVICES.....	12
4.1 Viewing status and other data about devices.....	12
4.1.1 The Devices view.....	12
4.2 Viewing an overview of VPN types and signal strengths.....	14
4.2.1 The Overview view.....	14
4.3 Viewing statistics on VPN and signal status.....	15
4.3.1 Statistics categories.....	15
4.4 Viewing details on an individual device.....	17
4.4.1 The Details view.....	18
TECHNICAL SUPPORT	19

1 Viola Patrol – traffic lights for remote device monitoring

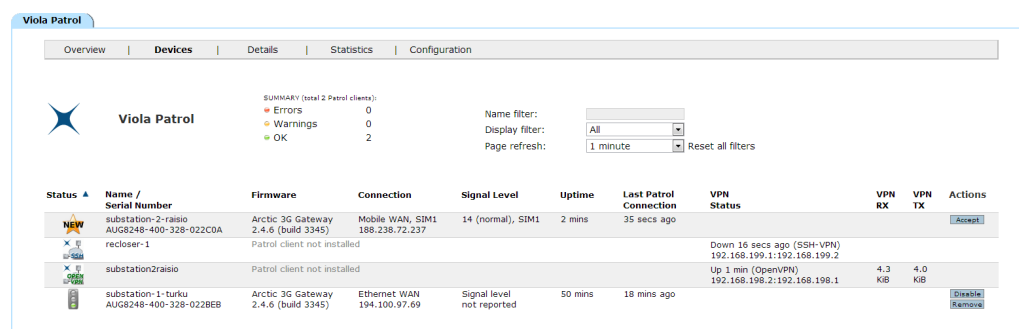
Viola Patrol is a graphical user interface for monitoring the status of remote Arctic device connections. You can view the reporting status of all connected devices as graphical traffic lights. You can also view details on any individual device or view history data as graphs. Furthermore, Viola Patrol can send automated alarms directly to the email. With these features you can quickly check the connection status and quality, locate possible fault situations, and ensure that all connections are working at all times.

No installation is required to start using Viola Patrol. It is pre-installed on the Viola M2M Gateway and may be used through a standard web browser.

1.1 Viola Patrol user interface

The user interface of Viola Patrol consists five different views which you can access through the tabs at the top. The currently selected view is shown in the display area below the tabs.


Figure 1. Viola Patrol user interface



Tab / View	Description
Overview	Shows the number of each VPN connection type, the number of connected devices with Patrol client and the number of devices divided into five categories according to their signal strength.
Devices	Shows the status of each device as traffic lights, and other data such as VPN status.
Details	Shows details about an individual device.
Statistics	You can view history graphs about data transfer through the VPN connection and signal strength.
Configuration	With the configuration options you can select the client device registration password, email alert options and how quickly device statuses change.

2 Logging in to Viola Patrol

1. In a web browser, enter the address `https://10.10.10.10:10000` to open the Viola M2M Gateway user interface.
2. Enter your username and password, and click **Login**.
The default username is `viola-adm` and default password is `violam2m`
The Viola M2M Gateway main menu opens.

3.  Click **(Viola Patrol)** to open the Viola Patrol application.

The Viola Patrol application opens.

3 Setting up reporting and monitoring

This chapter details all tasks related to setting up the Viola Patrol application and the client devices for reporting.

3.1 Configuring Viola Patrol

1. Click the **Configuration** tab to open it.
2. Click [**edit**] to activate the editing mode.
The table cells change into editable text fields and checkboxes.
3. Edit the values.
See [Configuration options](#) on page 8 for information on the configuration values.
4. When ready, click **Save** to save the changes.
The new configuration values are saved.
5. If you edited the email addresses, test the email settings by clicking **Send test email**.

Note!

With these settings, Viola Patrol is ready to start receiving reports, but before the client devices can start reporting, you must register them with Viola Patrol. See section [Adding a new device to Viola Patrol](#) on page 9 for instructions.

3.1.1 Configuration options

With the configuration options you can select the registration password for the client devices, email alert options and how quickly device statuses change.

Note!

The actual reporting interval must be configured in the Arctic client device. The configuration options below do not affect it. They only determine how soon a device status changes if reporting is unsuccessful, and how often Viola Patrol sends email alerts about devices with the warning or error status.

Table 1: Configuration options

Field	Description
Device registration password	The password with which remote Arctic devices with the Patrol client can be registered with the Viola Patrol, so that it can start reporting. For more information, see section Adding a new device to Viola Patrol on page 9.
Mail alert from address	The email address that appears as the sender when Viola Patrol sends automatic alerts.
Mail alert to addresses	The email address(es) to which Viola Patrol sends the alerts.

Field	Description
Mail alert minimum interval	The minimum amount of time that must pass before Viola Patrol sends a new alert. If multiple alerts happen before this time interval has passed, Viola Patrol sends all the alerts in the same email.
Mail alert statuses	The types of device statuses that cause alerts. You may configure Viola Patrol to send alerts about only warnings, only errors, both, or neither.
Device interval until warning	If a device cannot report successfully within the given amount of time, Viola Patrol starts showing it in the warning state (yellow light). The device goes back to OK state (green light) the next time it successfully reports to Viola Patrol.
Device internal until error	If a device cannot report successfully within the given amount of time, Viola Patrol starts showing it in the error state (red light). The device goes back to OK state (green light) the next time it successfully reports to Viola Patrol.

3.2 Adding a new device to Viola Patrol

You can add new connected devices for reporting and monitoring under Viola Patrol.

The following task involves actions in both Viola Patrol and a device with the Patrol client.

Note!
 The instructions below apply to Arctic 3G Gateway (2622), Arctic LTE Gateway (2625) and Arctic Substation Gateway (2651). If you are adding an Arctic device of different type, contact technical support at support@violasystems.com for more instructions.

Note!
 A device without the Patrol client can be added for monitoring, but some details are not available in the views.


1. In Viola Patrol, open the **Configuration** tab and write down the registration password or copy-paste it into a text file.
2. Log in to the Arctic device you want to add to Viola Patrol. See the Arctic device's own user manual for instructions.
3. Select **Applications > Viola Patrol**.

4. Configure the Arctic device:

Figure 2. Configuration example





Basic Information	
Enabled	Yes <input type="button" value="v"/> Enable Viola Patrol
Server	62.236.180.172 Server IP address
Connection interval	1500 How often to report to server.
Registration password	Password needed to register to server. Do not enter this password after registration has taken place unless you want to reregister.

- a) In the **Enabled** drop-down menu, select **Yes**.
 - b) In the **Server** field, enter the IP address of the M2M Gateway.
 - c) In the **Connection interval** field, enter the reporting interval as seconds.
 - d) In the Registration password field, enter the password that was copied in step 1.
5. Click **Submit**.
6. Reboot the Arctic device.
7. In Viola Patrol, open the **Devices** tab.

Each new device that is not enabled yet has the  icon in the status column. If the new device is not visible, wait for a minute and refresh the page. Registering the device with Viola Patrol may take some time.

8. Click **Accept**.

Figure 3. Example of adding a new device in the Devices view

Viola Patrol										
		SUMMARY (total 2 Patrol clients):		Name filter:		Display filter:		Page refresh:		Reset all filters
		Errors: 0				All		1 minute		
		Warnings: 0								
		OK: 2								
Status	Name / Serial Number	Firmware	Connection	Signal Level	Uptime	Last Patrol Connection	VPN Status	VPN RX	VPN TX	Actions
	substation-2-raiso AUG8248-400-328-022COA	Arctic 3G Gateway 2.4.6 (build 3345)	Mobile WAN, SIM1 188.236.72.237	14 (normal), SIM1	2 mins	35 secs ago				<input type="button" value="Accept"/>
	recloser-1	Patrol client not installed					Down 16 secs ago (SSH-VPN) 192.168.199.1:192.168.199.2			
	substation2raiso	Patrol client not installed					Up 1 min (OpenVPN) 192.168.198.2:192.168.198.1	4.3 KB	4.0 KB	<input type="button" value="Disable"/> <input type="button" value="Remove"/>
	substation-1-turku AUG8248-400-328-022BEB	Arctic 3G Gateway 2.4.6 (build 3345)	Ethernet WAN 194.100.97.69	Signal level not reported	50 mins	18 mins ago				<input type="button" value="Disable"/> <input type="button" value="Remove"/>

The new device is added to the **Enabled devices** table.

3.3 Removing a device from Viola Patrol

You can remove a device from all views and stop receiving reports from it.

Note!

When a device is removed from Viola Patrol it cannot be re-enabled with Viola Patrol or in M2M Gateway. It can only be added again as a new device as instructed in section [Adding a new device to Viola Patrol](#) on page 9. If you want to disable reporting from a device only temporarily, see section [Disabling viewing of reports from a device](#) on page 11.

1. Click the **Devices** tab to open it.
You can see all connected and currently enabled devices in the **Enabled devices** table.
2. Find the row describing the device you want to remove and click **Remove**.
3. Confirm the removal in the confirmation dialog.

The device is removed from all views and Viola Patrol stops receiving reports from it.

3.4 Disabling viewing of reports from a device

You can temporarily stop Viola Patrol from showing updated reports from a device by disabling it. You can re-enable the device easily when you want to continue viewing reports from it.

1. Click the **Devices** tab to open it.
You can see all connected and currently enabled devices in the **Enabled devices** table.
2. Find the row describing the device you want to disable and click **Disable**.

The device is moved to the **Disabled devices** table and Viola Patrol stops showing updated data on it.

Whenever you want to re-enable a disabled device, click **Enable**.

4 Monitoring remote devices

This chapter details tasks related to monitoring the status of connected devices.

4.1 Viewing status and other data about devices






1. Click the **Devices** tab to open it.
All connected devices and their statuses are listed in a table. If there are many connected devices, take the following steps to narrow down the number of devices displayed.
2. To show only devices with matching names, type a device name or part of a name in the **Display filter:** field and press enter.
To show all devices again, empty the **Display filter:** field and press enter.
3. To show only devices with a certain status, select a value in the **Display filter:** drop-down menu:
 - To display all devices regardless of status, click **All**.
 - To display only devices with the OK status (green light), click **OKs only**.
 - To display only devices with the warning status (yellow light), click **Warnings only**.
 - To display only devices with the error status (red light), click **Errors only**.
4. Set a page refresh rate by selecting a value in the **Page refresh:** drop-down list.

The status of the devices selected with the filters is updated at the selected intervals.

4.1.1 The Devices view

In the **Devices** view you can view the status of the connected devices as traffic lights, and to view other data about the connection.

Table 2: Values in the Devices view

Column	Possible values	Description
Status		The device is in the OK state.
		The device has the warning status, which means that it has not reported successfully within a given time frame.
		The device has the error status, which means that it has not reported successfully within a given time frame after it entered the warning status.
		A new device that has not been accepted for monitoring yet.
		The Arctic device does not have the Patrol client software or it has not been enabled for reporting. Only VPN data

Column	Possible values	Description
		is displayed for the device, and an icon indicating the VPN type is displayed instead of the traffic lights.
Name / Serial Number	(Device-specific value)	The name serial number of the connected device.
Firmware	(Device-specific value)	The firmware type, version and build present in the connected device.
Connection	Mobile WAN or Ethernet WAN	The network type through which the device is connected.
Signal level	Very good, Good, Normal, Weak or Very weak	These five categories and the numeric value indicate the strength of the signal. Note that the signal level refers to time shown in Last Patrol Connection and may therefore show a strong signal level even when the connection is down.
Uptime	<i>n</i> mins/hours/days	The amount of time the connection has been up since the last reboot.
Last Patrol Connection	<i>n</i> secs/mins/hours/days ago	The amount of time that has passed since the device has last reported to Viola Patrol.
VPN Status	Up <i>n</i> mins/hours/days	The VPN connection is currently up and has been up for the amount of time shown.
	Down <i>n</i> mins/hours/days	The VPN connection is currently down and has been down for the amount of time shown.
	(SSH VPN, L2TP-VPN or OpenVPN)	The VPN type used. The field is empty if no VPN has been installed.
VPN Rx	<i>n</i> KiB	Total amount of data received through the VPN connection since the last time the VPN was reconnected. History data on earlier data transfer is available in the Statistics view.
VPN Tx	<i>n</i> KiB	Total amount of data transmitted through the VPN connection since the last time the VPN was reconnected. History data on earlier data transfer is available in the Statistics view.
Actions	Disable	Temporarily disable a device. See section Disabling viewing of reports from a device on page 11.
	Remove	Remove a device from all views. See section Removing a device from Viola Patrol on page 10.
	Enable	Re-enable a disabled device. See section Disabling viewing of reports from a device on page 11.

Column	Possible values	Description
	Accept	Accept a new device. See section Adding a new device to Viola Patrol on page 9.

4.2 Viewing an overview of VPN types and signal strengths

Click the **Overview** tab to open it.

The page shows a summary of VPN types and signal strengths in the connected devices.

4.2.1 The Overview view

In the **Overview** tab you can view a summary of all connected devices categorized according to the VPN type used, and further below in the view, a summary of all devices with the Patrol client categorized according to their signal strength.

The following information is displayed in the view.

Category	Entry	Description
VPN	L2TP-VPN	The type of VPN application used for the connection. All connected devices are listed regardless of whether they have the Patrol client software.
	OpenVPN	The type of VPN application used for the connection. All connected devices are listed regardless of whether they have the Patrol client software.
	SSH-VPN	The type of VPN application used for the connection. All connected devices are listed regardless of whether they have the Patrol client software.
Patrol	Patrol clients	The total number of connected devices with the Patrol client software.
Mobile network signal levels reported by Patrol clients	Very good	The number of devices with the Patrol client software that have a very good signal strength.
	Good	The number of devices with the Patrol client software that have a good signal strength.
	Normal	The number of devices with the Patrol client software that have a normal signal strength.
	Weak	The number of devices with the Patrol client software that have a weak signal strength.
	Very weak	The number of devices with the Patrol client software that have a very weak signal strength.
	Mobile WAN not in use	The number of devices with the Patrol client software that are connected to a hardwired network instead of a wireless network and thus have no signal strength.

4.3 Viewing statistics on VPN and signal status

You can view history graphs on VPN connection and signal status on a selected scale.

1. Click the **Statistics** tab to open it.
2. Select a device to view in the **Device:** drop-down menu.
3. Select the scale of the graph:
 - **Month:** A 1-month graph starting from the beginning of the selected month until the last day of the month. Each interval (column) represents 6 hours.
 - **Day:** A 24-hour graph starting from midnight until the following midnight. Each interval (column) represents 15 minutes.
 - **Hour:** A 60-minute graph starting from the first minute of the hour until the sixtieth minute of the hour. Each interval (column) represents one minute.
4. Select the starting date and time for the graph by entering values in the **Year:**, **Month:**, **Day:** and **Hour:** fields.
If the scale is set at **Day** or **Month** in the previous step, the units smaller than the selected scale appear gray and do not affect the graphs displayed.
5. Click **Update**.

The view is updated, showing history graphs about the selected device.

4.3.1 Statistics categories

In the **Statistics** tab you can view history data on the VPN connection and signal strength of an individual device as graphs.

When a device is selected, the following general information is displayed, followed by the graphs as detailed below.

Table 3: General information

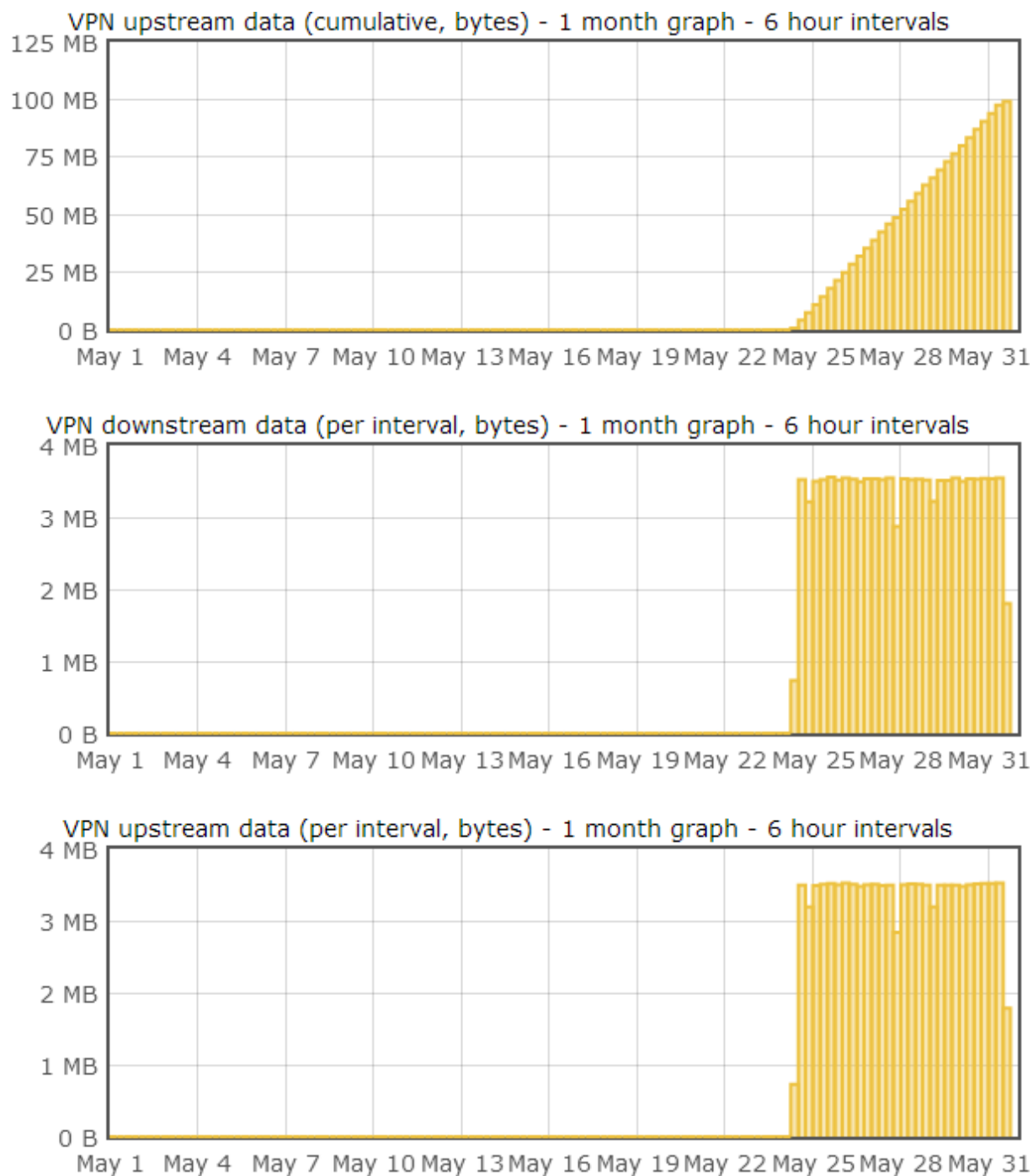
Table entry	Description
Device name	The name of the device
First VPN connection	The date, time and VPN application used for the first VPN connection established with the device.
Last VPN connection	The date, time and VPN application used for the most recent VPN connection established with the device.

Table 4: History data graphs

Graph title	Description
VPN downstream data (cumulative, bytes)	Cumulative amount of data received by the device through the VPN connection. Each column represents the total amount of data received since the selected starting date and time.
VPN upstream data (cumulative, bytes)	Cumulative amount of data transmitted from the device through the VPN connection. Each column represents the

Graph title	Description
	total amount of data transmitted since the selected starting date and time.
VPN downstream data (per interval, bytes)	Amount of data received by the device through the VPN connection. Each column represents the amount of data transmitted within a time interval. The length of the interval is shown in the graph title.
VPN upstream data (per interval, bytes)	Amount of data transmitted from the device through the VPN connection. Each column represents the amount of data transmitted within a time interval. The length of the interval is shown in the graph title.
Signal level	Average signal strength within the time interval shown in the graph title. On the 0–31 scale used, higher values indicate a stronger signal.
VPN received bytes/sec (RX)	Data transfer rate for data received by the device through the VPN connection.
VPN transmitted bytes/sec (TX)	Data transfer rate for data transmitted from the device through the VPN connection.
VPN connection status: up (1) / down (0)	Amount of uptime vs downtime in VPN connection within the time interval shown in the graph title. For example, 0.8 indicates that the connection was up 80% of the time and down 20% of the time.
Number of VPN reconnects	Number of times the VPN connection was re-established within the time interval shown in the graph title

Figure 4. Example graphs



4.4 Viewing details on an individual device

In the **Details** tab, you can view detailed information on an individual device.

1. Click the **Details** tab to open it.
2. In the **Selected device** drop-down menu, select the name of the device you want to view.

Information on the selected device is displayed.

4.4.1 The Details view

In the **Details** tab you can view device details and connection information.

Table	Entry	Description
Generic	Device name	The name of the currently selected device
	Serial number	The serial number of the currently selected device
	Firmware	The firmware type, version and build.
	Uptime	The time the device connection has been up since the last reboot. If the uptime value appears to be reset constantly, there may be a power outage or similar problem in the system.
Network	Connection type	The type of network connection used.
	Last Patrol connection	The date and time of the most recent report was received or the last time the device contacted Viola Patrol.
	Initial Patrol connection	The date and time of the first report was received or the first time the device contacted Viola Patrol.
VPN	Type	The type of the VPN application used.
	Status	The current status of the VPN (up/down) and the time it has been in that state.
	Rx	Current data transfer rate for data received through the VPN connection.
	Tx	Current data transfer rate for data transmitted through the VPN connection.
Mobile network	The Mobile Network table contains Mobile Network and Arctic radio-specific information. See the below image for an example.	

Figure 5. Example of the Mobile Network table

Mobile Network		
Signal level	14 (normal)	4 hours ago
Cell ID	"0005D6D2"	4 hours ago
GSM registration	registered to home network	4 hours ago
Location area code	"138D"	4 hours ago
IMEI number	355310030157196	4 hours ago
Modem manufacturer	Sierra Wireless, Incorporated	4 hours ago
Modem model	MC8795V	4 hours ago
Modem temperature	59 C (Normal)	4 hours ago
Mobile operator	FI SONERA	4 hours ago
Mobile operator selection	automatic	4 hours ago
Available services	UMTS,HSDPA/HSUPA	4 hours ago
Current service	HSDPA/HSUPA	4 hours ago
Modem service	GSM,GPRS,EDGE,UMTS,HSDPA/HSUPA	4 hours ago
SIM ID	244915471018288	4 hours ago
PIN attempts left	3	4 hours ago
PIN status	PIN not required	4 hours ago

Technical Support

Contacting Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: <http://www.violasystems.com>

Recording Arctic Information

Before contacting our Technical Support staff, please record (if possible) the following information about the Arctic product:

Product name:

Serial no:

Note the status of the Arctic in the space below before contacting technical support. Include information about error messages, diagnostic test results, and problems with specific applications.
