



# Viola M2M Gateway User's Manual



Version 2.0  
Modified Aug 13, 2004

## Copyright and Trademark

Copyright © 2004, Viola Systems Ltd. All rights to this manual are owned solely by Viola Systems Ltd. (referred in this manual as Viola Systems). All rights reserved. No part of the contents of this manual may be transmitted or reproduced in any form or by any means without the written permission of Viola Systems.

Ethernet is a trademark of XEROX Corporation. Windows and Internet Explorer are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communications Corporation. Linux is a Registered Trademark of Linus Torvalds. All other product names used in this manual are the properties of their respective owners and are acknowledged.

**Viola Systems Ltd.**  
Lemminkäisenkatu 32  
FIN-20520 Turku  
Finland

**Technical Support**  
Phone: +358 (0)20 1226 226  
Fax: +358 (0)20 1226 220  
E-mail: [support@violasystems.com](mailto:support@violasystems.com)  
On-line: <http://www.violasystems.com/>

## Disclaimer and Revisions

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 circumstances is the manufacturer or the developer of a program responsible for any possible damages caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are 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 all information in this manual as of the publication date. We assume no responsibility for any errors that may appear in this guide. Information in this manual may change without prior notice from Viola Systems.

### Revision History:

05/2004 Manual released, version 1.0

08/2004 Version 2.0

## Warranty and Safety Instructions

Read these safety instructions carefully before using the product:

Warranty will be void, if the product is used in any way, which is in contradiction with the instructions given in this manual, or if the product has been tampered with.

The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.

To prevent damage both the product and any terminal devices must always be switched OFF before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. Before connecting any power cables the output voltage of the power supply should be checked.

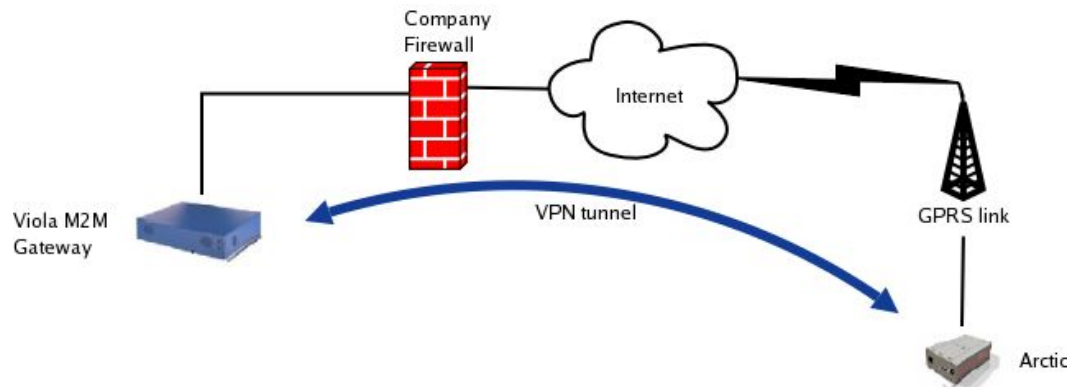
This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of our hardware or software could lead directly to death, personal injury, or severe physical or environmental damage.

## Table of Contents

1. Introduction.....	6
1.1. Features.....	7
2. Network Requirements.....	8
2.1. Connection Principle.....	8
2.2. Minimal Requirements for Network.....	8
2.3. Routing Setup.....	9
2.4. HTTP Server for SSH key exchange.....	9
2.5. Other Network Services.....	9
2.6. Recommended Network Setup.....	10
2.7. Using the Second Ethernet Port.....	11
3. Physical Interfaces.....	12
3.1. Front Panel.....	12
3.2. Back Panel.....	12
3.3. Power Switch and Connector.....	13
3.4. Product Label.....	13
4. Getting started.....	14
4.1. Configuring the IP address.....	14
4.2. Using Webmin.....	16
5. VPN Configuration for Arctic.....	17
5.1. VPN Client Settings.....	17
5.2. Key Management.....	18
5.3. Routing mode.....	18
5.4. Checking VPN Status from Arctic.....	19
6. VPN Configuration for M2M Gateway.....	20
6.1. Adding Peer.....	21
6.2. Checking VPN Status from M2M Gateway.....	21
7. VPN Setup Examples.....	22
7.1. Example 1. Basic VPN Tunnel.....	22
7.2. Example 2. Tunneling Network.....	26
7.3. Example 3. Proxy ARP.....	27
8. Troubleshooting.....	28
9. Technical Specifications.....	29
10. Limited Warranty.....	30
10.1. Coverage.....	30
10.2. Excluded Products and Problems.....	30
10.3. Remedies.....	30
10.4. Obtaining Warranty Service.....	30
11. Technical Support.....	31
11.1. Contacting Technical Support.....	31
11.2. Recording Product Information.....	31

# 1. Introduction

The Viola M2M Gateway is a network device that enables VPN connection between company network and remote Arctic devices. It can also be used to control and monitor Arctic devices in local or remote networks. Concept of the Viola M2M Gateway is described in the following picture.



Only a computer with network connection and a HTML browser is required to configure the Viola M2M Gateway. Using the Viola M2M Gateway Webmin user interface you can configure and view the status of the remote Arctic devices and configure the VPN connection between Viola M2M Gateway and Arctic device. Arctics have a WWW user interface which can be used to configure them using a HTML browser.

**Note:** Before setting up Viola M2M Gateway, read at least chapters 2 and 3.

For the rest of this documentation, the Viola M2M Gateway is referred as M2M Gateway.

## 1.1. Features

The M2M Gateway offers different advanced features for network usage. In most simple usage only VPN feature is used, but M2M Gateway makes possible to make complex network configurations.

### Routing

M2M Gateway can forward packets to local Ethernet (eth0) which it is connected to company network. Also it is possible to route packets to second Ethernet (eth1) of M2M Gateway. More complex routing solutions can be made but they need consultation of your local network administrator.

### Firewall

The M2M Gateway has internal firewall with graphical user interface. It is possible to connect M2M Gateway directly to the Internet and filter unwanted connections without external firewall. The recommend method is to use a dedicated firewall and install M2M Gateway behind it.

### VPN

VPN is used to connect remote Arctic devices to local network. Connection is started by Arctic and the M2M Gateway decides based on it's configuration does it allow remote Arctic start VPN connection. VPN connection can be disabled from M2M Gateway. If connection is for some reason terminated, it comes automatically back up. If routing is not needed, Proxy ARP can be used to access Arctic devices like in local network.

### Remote Management

M2M Gateway offers full remote management. Also traditional console access is available using SSH.

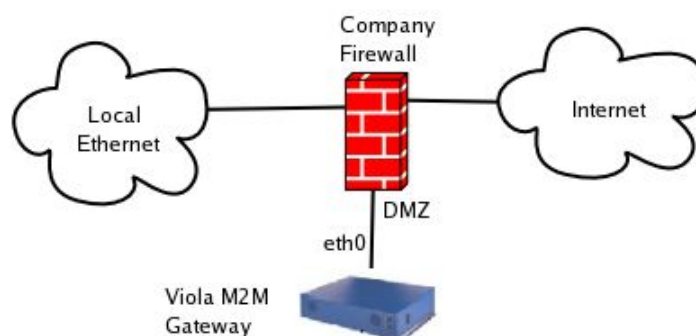
## 2. Network Requirements

To work properly M2M Gateway requires the parameters described in this chapter to be configured. For your network settings contact your local network administrator.

**Note:** Misconfiguration of the M2M Gateway can seriously hinder your network. Make sure you verify your network configuration with local network administrator.

### 2.1. Connection Principle

Company Intranet is normally connected to Internet via firewall. The following picture shows the M2M Gateway connected to the Demilitarized Zone (DMZ) of the firewall. This configuration allows hosts from Company Intranet to connect via firewall to the M2M Gateway. Other configurations are also possible. E.g. subnets and proxy ARP can be used.



**Note:** It is possible that internal routing in company intranet may require configuration in order to integrate M2M Gateway to an existing network.

### 2.2. Minimal Requirements for Network

At it's minimum the M2M Gateway requires these settings

- One public IP address for M2M Gateway
- SSH port (22) unblocked for incoming connections to M2M Gateway from the remote network.



Although this configuration is minimal it can be used for testing and evaluating more complex systems. It is always recommended to consult local network administrator when installing new servers to public network.

## 2.3. Routing Setup

When the M2M Gateway is installed to existing network some configuration require adding route to M2M Gateway and devices behind it. This means that for example local firewall to router needs to be aware of routes going via the M2M Gateway. Routing can be complex to setup in large networks and it is recommend to consult local network administrator also about routing.

## 2.4. HTTP Server for SSH key exchange

If a server key is needed to be received (default method is copy&paste) from the M2M Gateway HTTP port (80) has to be opened from firewall. By default HTTP server is enabled in the M2M Gateway and keys can be received with Arctic Web Configurator user interface. Chapter 5 describes briefly Arctic configuration.

If HTTP server is not needed, it is recommended to disable it by issuing the following commands in the shell of M2M Gateway. Server will be disabled after reboot.

```
[root@m2m-gw]# chkconfig --level 3 httpd off
[root@m2m-gw]# /etc/init.d/httpd stop
Stopping httpd:                                     [ OK ]
[root@m2m-gw]#
```

## 2.5. Other Network Services

M2M Gateway network services are listed in Table 1. The only mandatory service is Secure Shell (SSH). SSH server listens for incoming connections from Arctic devices in port 22. This port must not be blocked by any firewall otherwise the remote Arctic devices are not able to open VPN connections to the M2M Gateway.

Arctic uses ICMP ECHO (ping) messages to check it's network connection to the M2M Gateway. By default the private IP address of the VPN peer is used as the target for the network connection status check. I.e. the M2M Gateway is not required to accept ICMP ECHO messages.

The network connection status check can also be made using some public IP address (e.g. the public IP address of the M2M Gateway). In this case the target host of the network connection check is required to accept ICMP ECHO messages and that they are not blocked by any firewall.

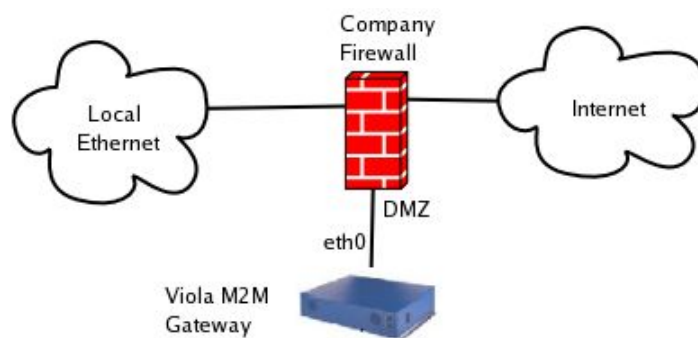
Service	Port	Description	
SSH	22	VPN authentication and data transfer	mandatory
HTTP	80	Server key exchange	optional
ICMP ECHO	-	Network connection checking	optional

*Table 1. Network services*

## 2.6. Recommended Network Setup

The M2M Gateway is recommended to be connected to a DMZ of a firewall. This way the M2M Gateway can have public or private IP address depending on the firewall configuration. When placed in DMZ the firewall protects efficiently against any unauthorized access to the M2M Gateway. Only incoming SSH connections are required to have access to DMZ zone. Services other than SSH are optional.

If the M2M Gateway is located in the DMZ and it has a private IP address the firewall has to support port forwarding or destination network address translation (DNAT). For firewall configuration please refer to your firewall documentation or to your local network administrator.

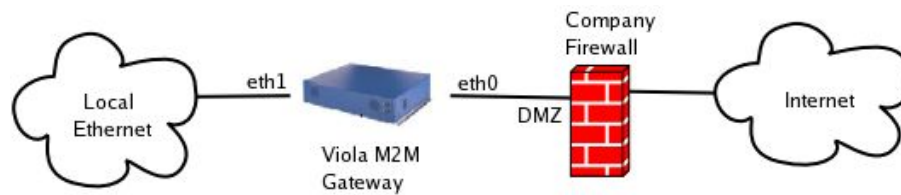


*Figure 1. Recommended network setup*

## 2.7. Using the Second Ethernet Port

If a firewall or network configuration does not allow the use of a DMZ or only few host has to have access to the M2M Gateway, the second Ethernet can be used. The second Ethernet of the M2M Gateway can be enabled from the Webmin configuration interface. The IP address of the second Ethernet of the M2M Gateway is then used as the default gateway for the devices connected to the second Ethernet port. This configuration is relatively easy to setup and it is the easiest way of setting up the M2M Gateway.

Look at Example 2 in Chapter 7 for further details.



*Figure 2 Second Ethernet port in use*

## 3. Physical Interfaces

In this chapter, the hardware interfaces used with the M2M Gateway are described. The M2M Gateway needs only Ethernet and power connection for full operation.

### 3.1. Front Panel

Led Color	Name	Description
Green	Power	Lit when power is on
Yellow	HDD	Lit when IDE hard drive is accessed



Figure 3. M2M Gateway front panel

### 3.2. Back Panel

The M2M Gateway has power connector on the right side of the back panel. Ethernet interfaces are located in the left side of the back panel. See Figure 4 for connector locations. Depending on the network configuration only one of them or both are used. The first Ethernet port (eth0) is always used and it is the left most Ethernet connector located to right from USB connectors.



Figure 4. M2M Gateway back panel

### 3.3. Power Switch and Connector

Power connector is standard 3 pin IEC inlet. Nominal input voltage is 110-230V. Power switch is lit when power is on. To turn off the M2M Gateway, change switch position from 1 to 0.

**Note:** Always remember to shut down the operating system before switching off the power, as data losses or corruption might occur if the system is not shut down properly.

Shutting down the operating system is done by from Webmin user interface by selecting *System->Bootup* and *Shutdown->Shutdown* system at the bottom of the screen. See Chapter 4 for more information about Webmin.

### 3.4. Product Label

Product label is found on the bottom of the device and it contains the basic information about the unit such as product name, serial number and MAC addresses of Ethernet ports.

## 4. Getting started

This chapter aims to give the necessary information to get the M2M Gateway device to fully working condition. It is assumed that you have already gathered up the necessary networking parameters for your specific networking environment, such as IP addressing and firewall issues. Look at the chapter 2 for network requirements and Chapter 7 for examples how the device could be connected and what would be the best configuration for your specific case.

### 4.1. Configuring the IP address

Because networks are different, you have to set a correct IP address for our device in order to get it work properly. There are two ways to do this, configuring it locally or remotely.

**Note:** The default IP address for M2M Gateway is 10.10.10.10

#### Configuring the IP address locally

This means we will connect the display and keyboard directly to the device and log on it locally. After logging on and being in the shell, there are several ways to change the network settings. One simple method is using a specific tool, called netconfig.

```
[root@m2m-gw root]# netconfig
```

Configure the parameters the way your networking scheme requires and exit the program. Then restart the network service by issuing the following command.

```
[root@m2m-gw root]# /etc/init.d/network restart
Shutting down interface eth0: [ OK ]
Shutting down interface eth1: [ OK ]
Shutting down loopback interface: [ OK ]
Setting network parameters: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
Bringing up interface eth1: [ OK ]
[root@m2m-gw root]#
```

Now you should be able to log in to Webmin from remote computer using previously configured IP address and port 10000. Take a look at the next discussion to find out how to connect to Webmin user interface.

## Configuring the IP remotely

The recommended way to do initial remote configuration is to use crossover Ethernet cable between M2M Gateway and workstation. This way the initial configuration of M2M Gateway is done in isolated network and there is no risk to mess up with any existing network.

The default IP address for M2M Gateway is 10.10.10.10 so your remote network machine should know a working route there. You could ping the address and see if it replies.

```
[anon@ymous anon]$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=0 ttl=64 time=0.202 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.172 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.193 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.240 ms

--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3020ms
rtt min/avg/max/mdev = 0.172/0.201/0.240/0.030 ms, pipe 2
[anon@ymous anon]$
```

If necessary, adjust your network settings so that the address 10.10.10.10 is accessible.

After you have a working connection to M2M Gateway, use your favorite HTML browser to connect to Webmin configuration interface by entering address <http://10.10.10.10:10000> to address bar. After entering the address, a login screen should appear. Login by entering username and password. Default login name is root and password is m2m.

Now you should be logged to Webmin. Select *Networking* from the top navigation bar. Then select *Network Configuration->Network Interfaces* and configure the interfaces properly. The user interface is quite clear and it should be quite easy task to configure the settings. If you feel not to be able to configure the settings, then it might be helpful to refer to some books about general TCP/IP networking.

For more information about Webmin, read the next section.

## 4.2. Using Webmin

By now you should have IP addresses set properly and you should be able to log in to Webmin. If this is not the case, please have a look at the previous section.

To connect to M2M Gateway, use HTML browser and address `http://<ip_address>:10000` to log in to M2M Gateway. Webmin uses port 10000 so it is necessary to include it to the address while connecting. If port number is omitted, the browser will try the default port 80 and won't be able to connect.

If you cannot access port 10000 please check that firewall allows connections to the M2M Gateway port 10000. Also if WWW proxy is used, this can cause problems. If proxy is used, disable WWW proxy for M2M Gateway's IP address.

After entering the proper address, a login screen should appear. Login by entering username and password. After login with correct username and password you see the main configuration window of M2M Gateway.

**Note:** Default login name is root and password is m2m. Remember to change these before connecting the M2M Gateway to existing network.



Webmin user interface has quite large collection of different web pages that each configure different functionality. In this manual, only relevant parameters for normal M2M Gateway operation, are described.

Closing the Webmin connection is done by clicking the “Log Out” button on the top right corner of the screen.

For more comprehensive documentation about Webmin, please refer to projects web page at [www.webmin.com](http://www.webmin.com).



## 5. VPN Configuration for Arctic

This chapter describes the settings on Arctic side that are relevant to get the VPN connection work properly. Configuration of GPRS connection is described in Arctic User's Manual and therefore it is not included in this document.

### 5.1. VPN Client Settings

Arctic needs few settings to be configured before VPN will be operational. These setting are listed in Table 2. All settings are located in *Network->VPN* menu except parameter hostname which is located in *Network->Ethernet* menu and ICMP Echo which is located in *Network->GPRS* menu.

The screenshot shows the Arctic Configurator web interface. The top navigation bar includes 'System', 'Network', 'Services', and 'Tools'. The left sidebar lists menu items: Summary, Ethernet, GPRS, VPN, Proxies, E-Mail, and Firewall. The main content area is divided into two sections: 'VPN Settings' and 'Key management'. The 'VPN Settings' section includes fields for 'Use SSH-VPN?' (set to Yes), 'Tunnel server IP' (172.16.4.11), 'Routing mode' (set to None), 'Remote network IP' (192.168.1.0), and 'Remote network mask' (255.255.255.0). There are 'Apply' and 'Reset' buttons. The 'Key management' section includes fields for 'Local SSH public key' and 'Server SSH key entry', both containing long alphanumeric strings. It also has 'Retrieve' and 'Insert' buttons. At the bottom right, it says 'Version 1.0.2, © 2004 Viola Systems Ltd'.

Parameter	Description	Mandatory
Hostname	Name used for authentication, must be unique, case-sensitive	Yes
ICMP Echo	ICMP echo	No
Use SSH-VPN	Enables and disables the VPN operation of Arctic	Yes
Tunnel Server IP	The M2M Gateway public IP Address for eth0 interface where Arctic makes the VPN connection	Yes
Routing Mode	Selects the type of routing none, network or Proxy ARP	No
Remote Network IP	IP address of remote network to be routed	If "Routing Mode" is set
Remote Network Netmask	Network mask of remote network to be routed	If "Routing Mode" is set

Table 2. VPN Client settings

When parameter *"Use SSH-VPN"* is enabled, the Arctic device tries to connect to the M2M Gateway. If the connection fails, Arctic tries it again in an endless loop.

Before VPN connection will be able to established, the VPN keys has to be exchanged between the Arctic and M2M Gateway. Note also that the connection has to be enabled from the M2M Gateway.

## 5.2. Key Management

The M2M Gateway uses public keys to control access from Arctic devices to the M2M Gateway.

Parameter	Description	Direction
Local SSH Public Key	Public key for accessing VPN Server	From Arctic to M2M Gateway
Server SSH Key Entry	Server key	From M2M Gateway to Arctic

Both of these keys can be copy&pasted from WWW user interface. The *"Server SSH Key Entry"* can also be received via HTTP protocol if the M2M Gateway HTTP server is not blocked by firewall or it has not been disabled from the M2M Gateway.

## 5.3. Routing mode

The M2M Gateway supports three routing modes. Examples of all three modes could be found in Chapter 7.

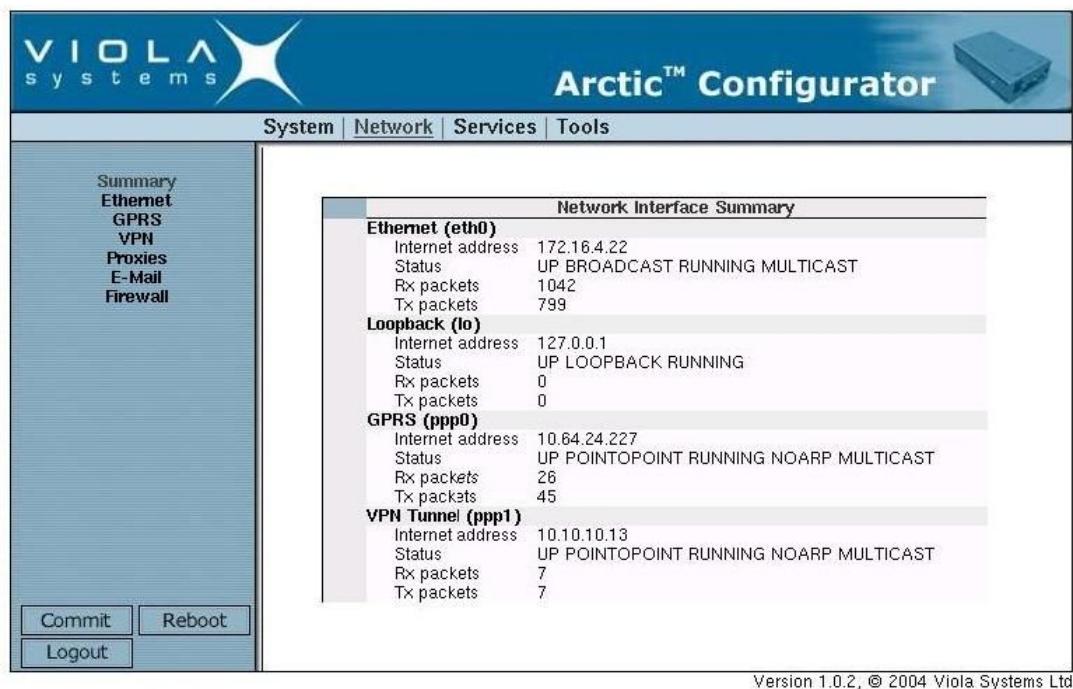
**"None"** – This is used when only Arctic VPN peer IP pair address is used to access. Ethernet of Arctic GPRS device and other devices connected to it cannot be used. Usually this is used when the devices connected to remote Arctic are connected via serial port.

**"Tunnel the following network"** - Used when Ethernet subnet of remote Arctic GPRS device is used. This is used when the devices connected to remote Arctic are connected via Ethernet. When this routing mode is used, both VPN ends need ip\_forward set to 1.

**"Proxy ARP"** - This option is used if remote Arctic device needs to look like it is connected to local network. Arctic Ethernet interface is configured with IP from same network than M2M Gateway. With this option, only Arctic device is visible to M2M Gateway side and any network behind the Arctic will not be available for routing.

## 5.4. Checking VPN Status from Arctic

After setting VPN settings and rebooting Arctic the VPN status can be checked from *Network -> Summary* page. When VPN is connected, user interface looks like in the following picture. VPN connection is up and running if VPN Tunnel device is present in the network interface listing.



The screenshot displays the Arctic Configurator interface. The top header includes the Viola Systems logo and the title 'Arctic™ Configurator'. Below the header is a navigation bar with tabs for 'System', 'Network', 'Services', and 'Tools'. The 'Network' tab is selected, and the 'Summary' sub-tab is active. The main content area shows a 'Network Interface Summary' table with four sections: Ethernet (eth0), Loopback (lo), GPRS (ppp0), and VPN Tunnel (ppp1). Each section lists the Internet address, Status, Rx packets, and Tx packets. The VPN Tunnel (ppp1) interface is shown as 'UP POINTOPOINT RUNNING NOARP MULTICAST' with 7 Rx and 7 Tx packets. On the left side of the interface, there is a sidebar menu with links for Summary, Ethernet, GPRS, VPN, Proxies, E-Mail, and Firewall. At the bottom left, there are buttons for 'Commit', 'Reboot', and 'Logout'. The bottom right corner of the window displays the version 'Version 1.0.2, © 2004 Viola Systems Ltd'.

Network Interface Summary	
<b>Ethernet (eth0)</b>	
Internet address	172.16.4.22
Status	UP BROADCAST RUNNING MULTICAST
Rx packets	1042
Tx packets	799
<b>Loopback (lo)</b>	
Internet address	127.0.0.1
Status	UP LOOPBACK RUNNING
Rx packets	0
Tx packets	0
<b>GPRS (ppp0)</b>	
Internet address	10.64.24.227
Status	UP POINTOPOINT RUNNING NOARP MULTICAST
Rx packets	26
Tx packets	45
<b>VPN Tunnel (ppp1)</b>	
Internet address	10.10.10.13
Status	UP POINTOPOINT RUNNING NOARP MULTICAST
Rx packets	7
Tx packets	7

## 6. VPN Configuration for M2M Gateway

After configuration has been made to remote Arctic device the VPN server (M2M Gateway) has to be configured properly. To access VPN configuration on M2M Gateway, login to Webmin and select *SSH-VPN configuration* from the main Webmin window.

**SSH-VPN configuration**

Peer	Interface	IP pair	Routing	Remote IP	Netmask	Status	Check			
Router	(no IF)	10.10.10.10 : 10.10.10.11	Tunnel	192.168.1.0	255.255.255.0	Active	n/a	Disable	Edit	Remove
gateway	(no IF)	10.10.10.20 : 10.10.10.21	Tunnel	192.168.2.0	255.255.255.0	Active	n/a	Disable	Edit	Remove

**Key management**

Server public key: 1024 35 1019961034048671407358895546623997411664925314

Add key for peer:

- Key

Version 1.0.0 (c)2003 Viola Systems Ltd

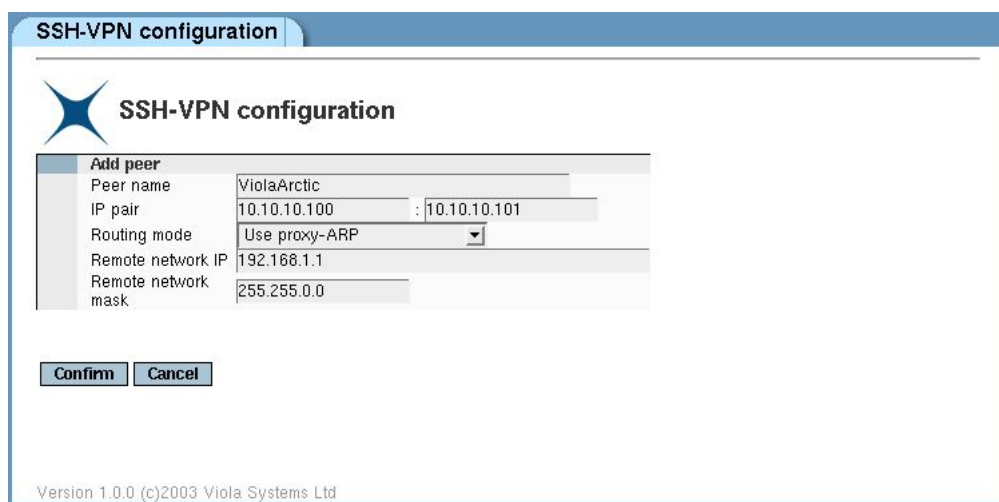
The VPN configuration screen is like in the picture above. First the page lists the existing peers and their status on the top of the page. The bottom of the page contains the SSH key management section.

The parameters for VPN tunneling on M2M Gateway side are listed in table below. These are visible on the peer listing and they are asked when a new peer is added. They could be modified by pressing the Edit button on appropriate peer.

Parameter	Description	Mandatory
Peer	Name used to authentication (Arctic hostname)	Yes
IP Pair	VPN IP pair address	Yes
Routing Mode	Selects if routing is used	No
Remote Network IP	IP address of remote network to be routed	If "Routing Mode" is set
Remote Network Netmask	Network mask of remote network to be routed	If "Routing Mode" is set

## 6.1. Adding Peer

Adding a new peer to M2M Gateway is done by pressing the *Add peer* button on the SSH-VPN configuration screen. The following window will appear. The parameters are listed in previous section. The configuration examples in Chapter 7 show generic guidelines how the configuration could be done.



The screenshot shows the 'SSH-VPN configuration' window. It has a title bar and a logo. Below the logo is the title 'SSH-VPN configuration'. There is a tab labeled 'Add peer'. The form contains the following fields:

Peer name	ViolaArctic		
IP pair	10.10.10.100	:	10.10.10.101
Routing mode	Use proxy-ARP		
Remote network IP	192.168.1.1		
Remote network mask	255.255.0.0		

At the bottom of the form are two buttons: 'Confirm' and 'Cancel'. At the very bottom of the window, it says 'Version 1.0.0 (c)2003 Viola Systems Ltd'.




## 6.2. Checking VPN Status from M2M Gateway

After setting the VPN properties from both Arctic and M2M Gateway, it is possible to check the status of configured connections from the SSH-VPN screen on the M2M Gateway.

When the connection is functioning properly, the peers have PPP interface as their interface and OK mark and key symbols next to their peer names. The key symbol means that the SSH keys are exchanged properly.

If there is no interface on the entry, there is something wrong in the configuration of that entry. See troubleshooting Chapter 8 for details.

Below are examples about different entries that are in working condition.

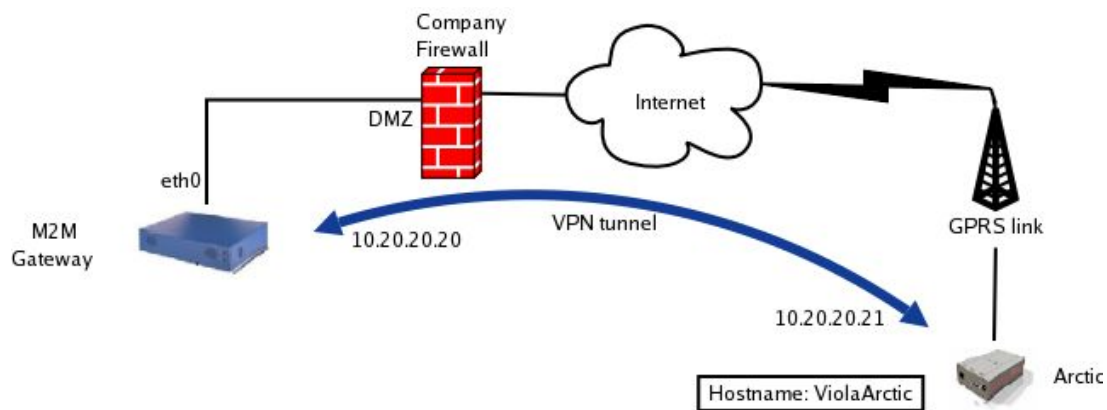
	ViolaArctic	ppp0	10.10.10.100 : 10.10.10.101	None		Active	OK	Disable	Edit	Remove
	ViolaArctic	ppp0(routed)	10.10.10.100 : 10.10.10.101	Tunnel	172.16.18.0 255.255.255.0	Active	OK	Disable	Edit	Remove
	ViolaArctic	ppp0	10.10.10.100 : 10.10.10.101	Proxy-ARP	172.16.200.50 255.255.255.0	Active	OK	Disable	Edit	Remove

## 7. VPN Setup Examples

As the VPN setup can be rather complex subject to learn, some example configurations are described here for your convenience. All these examples require that you have a static IP address for your M2M Gateway which is accessible from outside the firewall by Arctic devices.

### 7.1. Example 1. Basic VPN Tunnel

Configuring VPN tunnel between M2M Gateway and Arctic GPRS device. The network configuration for this example is following.



In order to make VPN tunnel operating both ends of the tunnel must be configured properly.

Lets begin by configuring the Arctic first. Log in to Arctic via its Ethernet port using appropriate cabling and IP addresses. Once you have logged to Web Configurator, enter *Network* menu and from there navigate to *VPN* submenu.

The screenshot shows the Arctic Configurator web interface. The top navigation bar includes 'System', 'Network', 'Services', 'Applications', and 'Tools'. The left sidebar lists 'Summary', 'Ethernet', 'GPRS', 'VPN', 'Proxies', 'E-Mail', and 'Firewall'. The main content area is divided into two sections: 'VPN Settings' and 'Key management'.

**VPN Settings**

Use SSH-VPN?	Yes
Tunnel server IP	212.182.218.91
Routing mode	None
Remote network IP	10.10.10.0
Remote network mask	255.255.255.0

Buttons: Apply, Reset

**Key management**

Local SSH public key	1024 35 1320760615343921745082007778:
Server SSH key entry	212.182.218.91 1024 35 10199610340486714...

Retrieve SSH server key for 212.182.218.91 [Retrieve]

Insert SSH server key for 212.182.218.91 [Insert]

Buttons: Commit, Reboot, Logout

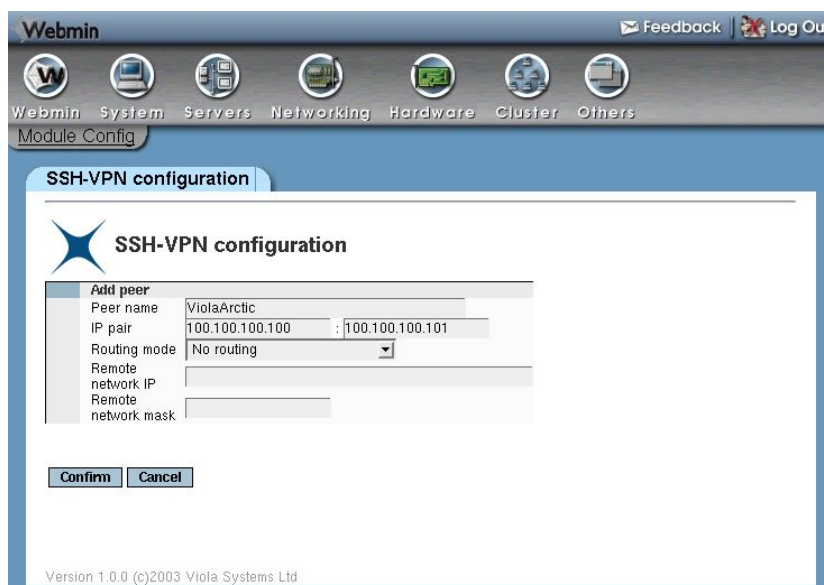
Version 1.0.5, © 2004 Viola Systems Ltd

Enable VPN tunneling by saying "Yes" to "Use SSH-VPN?" option. Then enter the IP address of M2M Gateway to "Tunnel server IP" field to configure the tunnel endpoint. M2M Gateway must have an IP address that is accessible from the outside network where the Arctic is located. If Arctic cannot ping the address, VPN tunneling will not be possible. IP Address of M2M depends on your network configuration and we could not give any recommendations. Your local network administrator should be able to help you on that.

Then click Apply and Commit to save settings.

Then Key management field below the settings complains the keys could not be found. Now we have to open a connection to M2M Gateway to configure the other endpoint of the tunnel. Do not close the Arctic Configurator as we will need it again very soon.

Log in to M2M Gateway. Connection details could be found earlier on this very manual. Select "SSH-VPN configuration" from the main Webmin screen.



The screenshot shows the Webmin interface for SSH-VPN configuration. The top navigation bar includes links for Webmin, System, Servers, Networking, Hardware, Cluster, and Others. The 'Module Config' tab is selected. The main content area is titled 'SSH-VPN configuration' and contains an 'Add peer' form. The form fields are as follows:

Add peer	
Peer name	ViolaArctic
IP pair	100.100.100.100 : 100.100.100.101
Routing mode	No routing
Remote network IP	
Remote network mask	

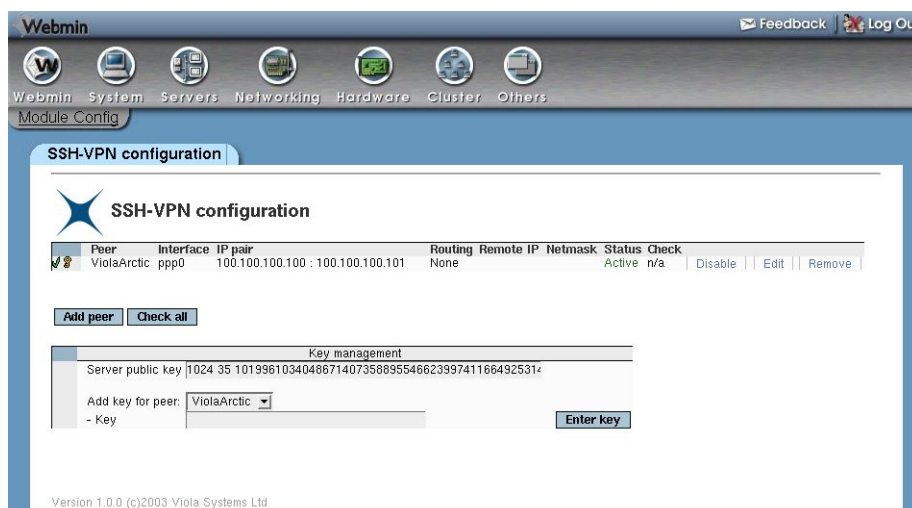
At the bottom of the form are 'Confirm' and 'Cancel' buttons. The footer of the interface reads 'Version 1.0.0 (c)2003 Viola Systems Ltd'.

*Peer name* is same as the hostname of Arctic device. Hostname is case sensitive and has to be same in both ends (Arctic and M2M Gateway). *IP pair* could be any pair of IP addresses as long as they don't conflict with existing ones. For example, first Arctic device IP pair could be 10.10.10.10:10.10.10.11, second could be 10.10.10.12:10.10.10.13 and so on. For IP pairs it is recommended to use private IP address space. Select "no routing" as *Routing mode*.

Addresses are assigned to VPN tunnel and the first one is M2M Gateway side and the second one is Arctic endpoint.

Select *Confirm* to save settings. Now you are returned to main SSH-VPN configuration screen.





Now we have to exchange the SSH keys. This is done by copying the key from “Server public key” field and paste it to Arctic Configurator where there is a field named “*Insert SSH server key for <your\_public\_ip\_address>*” If you have wrong server IP address in there, make sure you have the correct address entered to Tunnel server IP and you have pressed the *Apply* button on the same screen.

Paste the key from server and press *Insert* button. Now that just pasted key is shown in Server SSH key entry among its IP address. Now copy the Local SSH key from its field and paste it to M2M configuration screen. Remember to select the correct peer from the drop-down list if you have more than one Arctic configured.

**Note:** Every Arctic device must have unique hostname (case sensitive) as the identification is based to it.

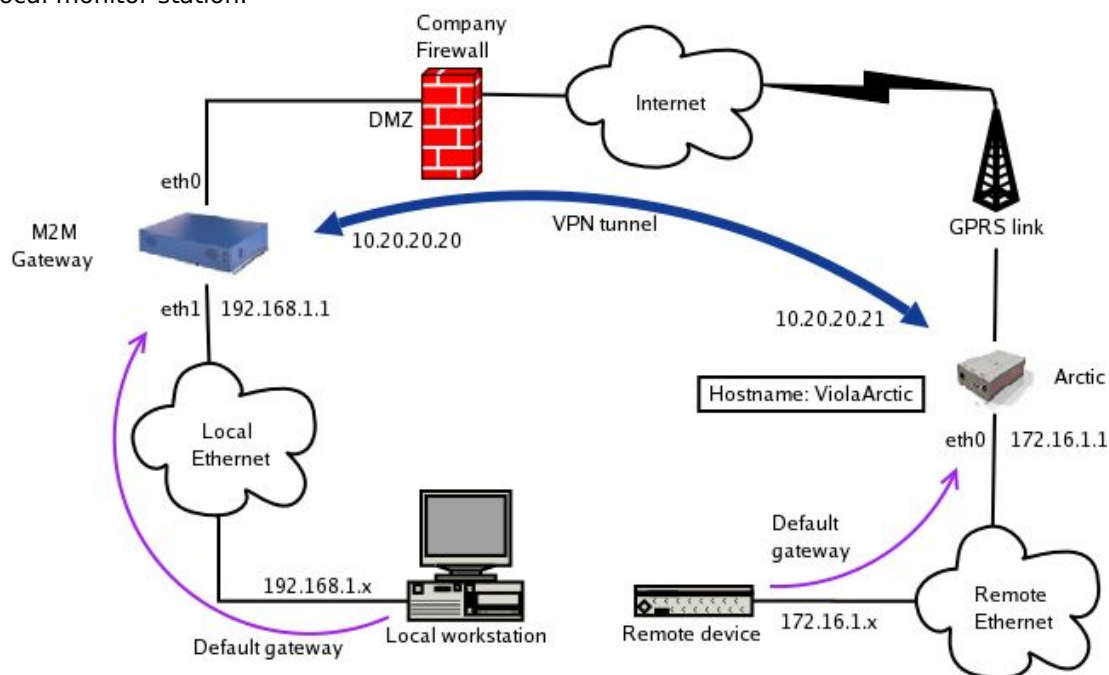
After the keys are exchanged properly, a key symbol will appear to the list on SSH-VPN configuration screen right next to the hostname. Entries should have ppp0 as their interface. You can use Check all button to check the tunnels are up and running.

Testing connection can be done by logging to Arctic via telnet or by pinging it.

```
telnet <ip_address>
ping <ip_address>
```

## 7.2. Example 2. Tunneling Network

This example shows a little larger system. This common setup is practical in connecting remote networks to as a part of local network. This could be used to connect isolated remote stations to local monitor station.



As the previous example explained some of the basic operations, this example assumes that those are clear at the time of reading this. If this is not the case, please take some time and browse the user interfaces of both M2M Gateway and Arctic. This will make the settings more familiar to you.

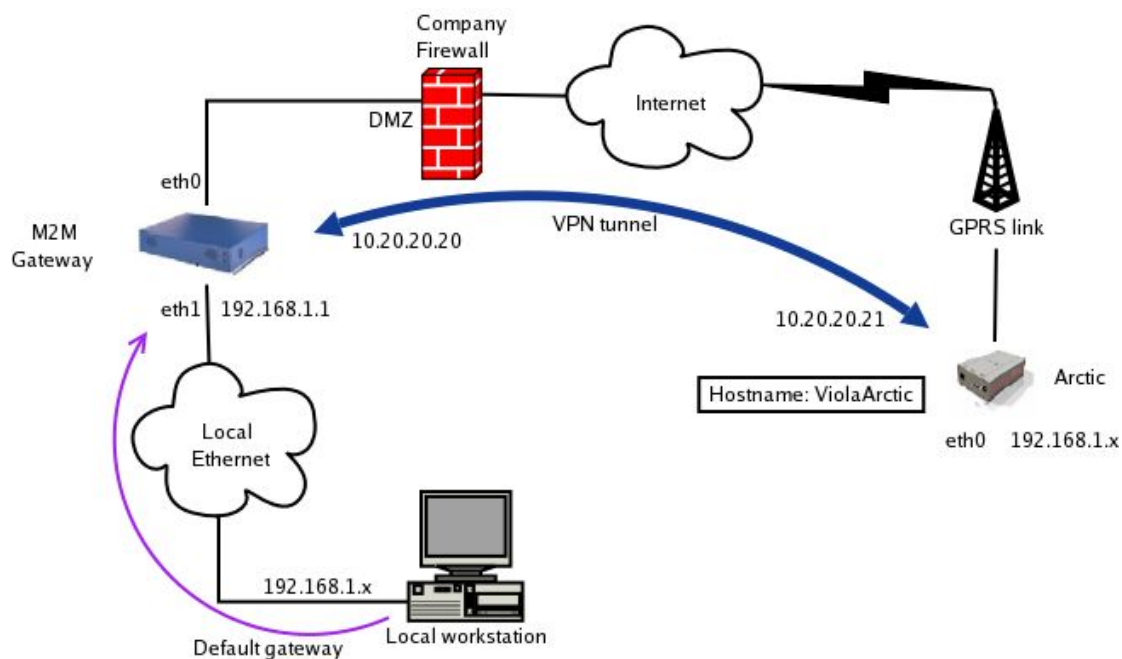
Select routing mode to "Tunnel the following network". IP address and netmask is the address that is located in the opposite side of the tunnel. For example, on Arctic set IP address to be the address that is assigned to the eth1 of M2M Gateway and vice versa.

Testing connection can be done by logging to Arctic via telnet or by ping it.

```
telnet <ip_address>
ping <ip_address>
```

### 7.3. Example 3. Proxy ARP

This example describes how the M2M Gateway can make remote Arctic GPRS device to have IP address from same (eth0 or eth1) network. This is done by using routing mode “Proxy ARP” from user interface.



**Note:** Arctic Ethernet interface has to have IP address from a local network. If this is not configured, Proxy ARP won't work and remote connections to Arctic cannot be made.

Select routing mode to “Proxy ARP”. IP address and netmask is the address that is located in the opposite side of the tunnel. For example, on Arctic set IP address to be the address that is assigned to the eth1 of M2M Gateway and vice versa.

Testing connection can be done by logging to Arctic via telnet or by pinging it.

```
telnet <ip_address>
ping <ip_address>
```

## 8. Troubleshooting

### Problem One

Q: When setting up routing mode "tunnel the following network", routing to M2M Gateway eth1 does not work?

A: Check that IP forwarding has been enabled and internal firewall does not block packets.

### Problem Two

Q: From Arctic Ethernet connection to M2M Gateway Ethernet is not working?

A: Check that IP forwarding has been enabled on Arctic.

### Problem Three

Q: If only one public IP is available, can the M2M Gateway be used?

A: Yes, if firewall connected to public IP can forward incoming ssh connections to the M2M Gateway.

## 9. Technical Specifications

Processor	x86 400MHz
Memory	256 MB RAM 30GB HDD
Network Interface	10/100 Base-T. Shielded RJ45 2x Ethernet (IEEE 802.3) 1.5 kV isolation transformer
Serial Device Interface	4 x Male DB9 connector DTE,
Power Requirements	100 – 240 VAC (65W max power consumption)
Temperature Range	Operating: XX to XX °C Storage: XX to XX °C
Relative Humidity	Operating: 5 to 85 % RH non-condensing
Dimensions and Weight	Size: 320 mm ´ 235 mm ´ 60 mm (W´L´H) Weight: 2.8 kg

## 10. Limited Warranty

### 10.1. Coverage

Viola Systems warrants this hardware product to be free from defects in materials and workmanship for the warranty period. This non-transferable, limited warranty is only to you, the first end-user purchaser. The warranty begins on the date of purchase and lasts for the period specified below:

Viola M2M Gateway      one (1) year

### 10.2. Excluded Products and Problems

This warranty does not apply to: (a) Viola Systems software products; (b) expendable components such as cables and connectors; or (c) third party products, hardware or software, supplied with the warranted product. Viola Systems makes no warranty of any kind on such products which, if included, are provided "AS IS." Excluded is damage caused by accident, misuse, abuse, unusually heavy use, or external environmental causes.

### 10.3. Remedies

Your sole and exclusive remedy for a covered defect is repair or replacement of the defective product, at Viola Systems' sole option and expense, and Viola Systems may use new or refurbished parts or products to do so. If Viola Systems is unable to repair or replace a defective product, your alternate exclusive remedy shall be a refund of the original purchase price.

The above is Viola Systems' entire obligation to you under this warranty. IN NO EVENT SHALL VIOLA SYSTEMS BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, USE, OR PROFITS EVEN IF VIOLA SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Viola Systems' liability exceed the original purchase price of the device server. Some states or countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

### 10.4. Obtaining Warranty Service

You must notify Viola Systems within the warranty period to receive warranty service. During the warranty period, Viola Systems will repair or replace, at its option, any defective products or parts at no additional charge, provided that the product is returned, shipping prepaid, to Viola Systems. All replaced parts and products become the property of Viola Systems. Before returning any product for repair, customers are required to contact the Viola Systems.

## 11. Technical Support

### 11.1. Contacting Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: [support@violasystems.com](mailto:support@violasystems.com)

On-line <http://www.violasystems.com>

### 11.2. Recording Product Information

Before contacting our Technical Support staff, record the following information about your product:

**Product name.:** \_\_\_\_\_

**Serial no.:** \_\_\_\_\_

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

---

---

---

---

---

---

---

---

---

---