Viola Systems Ltd.
Lemminkäisenkatu 14-18 A
FIN-20520, Turku
FINLAND

tel +358-(0)201-226 226
fax +358-(0)201-226 220
e-mail support@violasystems.com
web www.violasystems.com

TECHNICAL DOCUMENT TD-12-3-1.2

VIOLA SYSTEMS
VIOLA CLOUD M2M PILOT KIT
USER MANUAL

Version history:

1.2 Added DHCP client instructions
1.1 Added login instructions, minor corrections
1.0 Published by LaH

Date: Jul-05-2013
Version: 1.2
Author: LaH

Copyright and Trademarks

Ethernet™ is a trademark of Xerox Corporation. Windows™, Windows XP™ and Internet Explorer™ are trademarks of Microsoft Corporation. Netscape™ is a trademark of Netscape Communications Corporation. Mozilla® and Firefox® are registered trademarks of Mozilla Foundation. Linux™ is a trademark of Linus Torvalds. Cisco® is a registered trademark of Cisco Systems Corporation. All other product names mentioned in this document are the property of their respective owners, whose rights regarding the trademarks are acknowledged.

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

Contents

1. General

This document is the user's manual for Viola Systems Viola Cloud M2M Pilot Kit, product code 4000.

1.1. Introduction

Congratulations for ordering the Viola Cloud M2M Pilot Kit from Viola Systems Ltd.

The pilot kit is designed for smooth pilot execution, where the devices are delivered pre-configured and the Viola Cloud M2M Gateway is hosted by Viola Systems Ltd. The pilot configuration may later on be transferred to the actual production system.

The pre-configured set of devices with Viola Cloud M2M Gateway server removes most of the configuration work, leaving time and resources for the actual system tests.

1.2. The content of Viola cloud M2M Pilot Kit

The Viola Cloud M2M Pilot Kit consists of the following:

- Viola Cloud M2M Gateway service
- 2 pcs. Viola Arctic devices
- Accessory kits for the Arctic devices (Cables, power supplies, antennas)
- Preconfiguration for the devices
- User's guide (this manual)
- Usernames and passwords for the devices (may be provided by email)
- Technical support for the pilot kit

1.3. Conventions

The following conventions may be used in this document:

- The menu items in graphical user interface are denoted with ***bolded italic*** font and the sequence of mouse clicks, while configuring the devices in menus is separated with an arrow, e.g. "Click ***Tools*** → ***System log***"
- The console or command line output is printed with courier font and user input is printed with **`bold courier`** font. Example:

```
[viola-adm@m2mgw ~]#  date
 Fri Jul 5 08:52:00 CET 2013
```

- References to other documentation and figure/table captions are denoted with *italic* font
- Usernames, passwords and parameter-value pairs are denoted with `courier` font

1.4. Pre-requisites

- There is a PC running Microsoft Windows™ Vista, 7 or 8. Other operating systems can be used, but they're not supported by these instructions. The PC is used for the following
  - Running OpenVPN client for connecting to Viola Cloud M2M Gateway
  - Running a control/monitor/reading software (SCADA, etc.) for connecting to devices (Arctics, RTUs, PLCs, etc.) in remote sites
- The PC has internet connection, preferably a fixed line ADSL or similar

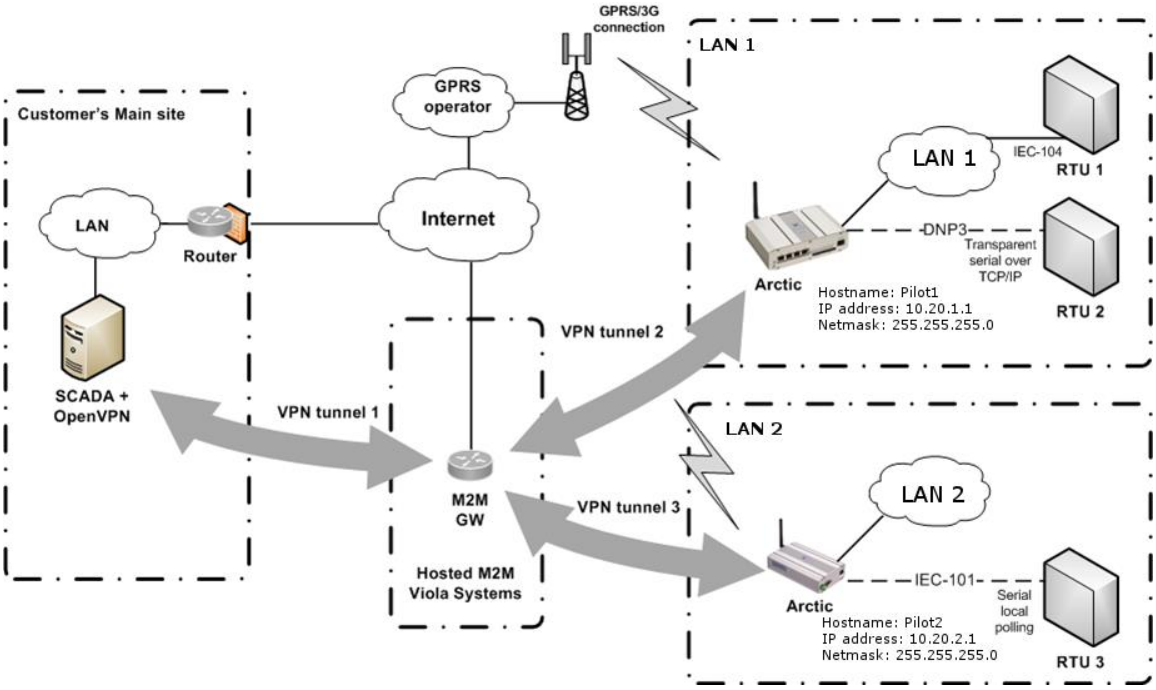
- There are available SIM cards for each Arctic. The SIM cards need to have data plan (GPRS data, etc.) enabled and 3G SIM functionality is needed with Arctic 3G Gateway for accessing 3G cellular network

2. Architecture

The Viola Cloud M2M Pilot Kit consists of selected Arctic devices, a Viola Cloud M2M Gateway, accessory kit, an OpenVPN client and ready-made configuration for communication between Arctic devices and Viola Cloud M2M gateway.

2.1. Overall Architecture

This is an example of the Viola Cloud M2M Pilot Kit Architecture.

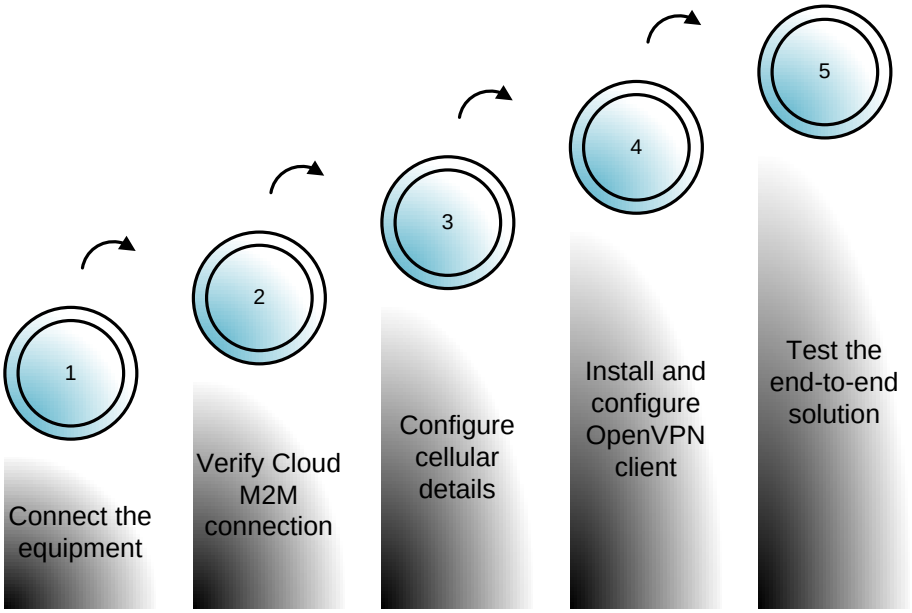


2.2. IP addressing example

- Customer's LAN: Freely selectable (shouldn't overlap other networks)
- LAN1: 10.20.1.0/255.255.255.0
- LAN2: 10.20.2.0/255.255.255.0
- Arctic 1, hostname: pilot1, IP address: 10.20.1.1
- Arctic 2, hostname: pilot2, IP address: 10.20.2.1
- SCADA is equipped with OpenVPN client
- Routing between tunnels is allowed
- SCADA is connecting RTU1 with IP 10.20.1.2 (in LAN1)
- SCADA is connecting RTU2 with IP 10.20.1.1 (behind serial GW of LAN1 Arctic)
- SCADA is connecting RTU3 with IP 10.20.2.1 (behind serial GW of LAN2 Arctic)
- The hosted M2M GW's own LAN is configured not to overlap any other LAN

3. Deployment

The deployment consists of the following high-level tasks.



There are some settings in Arctics that are needed for taking the system into use. Taking the Viola Cloud M2M Pilot Kit into use consist of the following steps.

1. Connecting cables
2. Viola Cloud M2M Gateway login
3. Verifying the initial connection
4. Configuring Arctics in DCHP client mode
5. Configuring cellular settings
6. Inserting SIM card
7. Installing the OpenVPN client to a PC
8. Configuring OpenVPN
9. Using OpenVPN
10. Configuring the monitoring application
11. Testing the solution

3.1. Connecting cables

The necessary cables and power supplies (i.e. accessory kits) are supplied with the Arctics.
The Arctics, depending on the model, have the following connectors:

- DC in (12…30 volts DC, positive pin on the left)
- Shared console/RS1 9 pin sub-D male connector (2G model) or separate RS1 port and Cisco® type RJ-45 serial console port (3G/LTE models)
- Dedicated configurable RS-232/422/485 port (RS1 or RS2, depending on the model)
- LAN Ethernet connector (2G model), 3 switched LAN ports, 1 WAN port (3G/LTE model)
- Antenna connector, type FME male in Arctic, female in antenna/antenna connector

"2G" Arctic

"3G/LTE" Arctic

1. Connect the power supply to Arctic. Verify that the power switch is in OFF position.
2. Connect the possible serial cable. If other than RS-232, verify the DIP switches as according to the user's manual. The default position of the switches is RS-232.
3. Insert the Ethernet cable to the LAN port. The cable is provided with the accessory kit. Generally, use unshielded twisted pair, CAT5(e) Ethernet cables.
4. Insert the antenna or antenna cable to Arctic's FME antenna connector.
5. When the power is switched on in the Arctic:
    a. 3G/LTE Gateway: The RUN LED should start blinking after a while from restart. The *Error* LED should turn off soon after starting.
    b. 2G Gateway: The *Power/Error* LED is lit and the *Function* LED should start blinking soon after starting.

3.2. Viola Cloud M2M Gateway login

Use the following login details when logging in to the Viola Cloud M2M Gateway.

- URL: https://<IP_address>:10000 for example, if the provided cloud M2M Gateway would reside at IP 10.20.30.40, the browser URL would be: https://10.20.30.40:10000 (The real IP addresses are public addresses)
- Username: `viola-adm`
- Password: The password is delivered with the actual devices or in a separate email.

Viola Cloud M2M Gateway login screen

3.3. Verifying the initial connection

The Arctics have DHCP client enabled and they're pre-configured for connecting Viola Cloud M2M Gateway automatically, once connected to an internet router.

Notes:

- The "2G" Arctics are having only one Ethernet interface, which has DHCP client enabled. Thus they are not initially available in the IP addresses 10.20.x.1. After verifying the initial connection according to this chapter, the "2G" Arctics can be configured to fixed IP rather than using DHCP.

- The "3G" and "LTE" Arctics are having "WAN" and "LAN" Ethernet interfaces. The Ethernet WAN interface is configured as DHCP client and is used for verifying the initial connection, whereas the LAN interface (switched, three ports) can be used for locally connecting to Arctic using IP address 10.20.1.1 (Pilot1) or 10.20.2.1 (Pilot2).

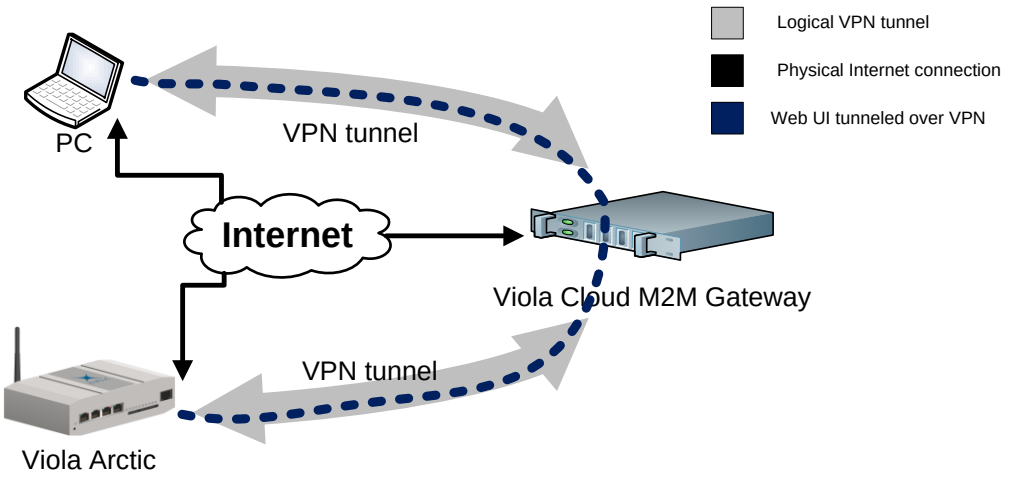
Perform the following steps for verifying that the Arctics are able to connect to Viola Cloud M2M Gateway.

1. Verify that all cables and antenna are connected
2. The Arctic's Ethernet cable must be connected to an internet router providing IP address and default gateway via DHCP. With Arctic 3G/LTE GW, connect the "WAN" Ethernet port. You can additionally verify the internet connectivity with a PC
3. Power on the Arctics
4. Wait approx. a minute for the Arctics to boot and to establish the connection to Viola Cloud M2M Gateway
5. Log in to the cloud M2M gateway. See chapter *Viola Cloud M2M Gateway login* for details
6. Click ***Viola Patrol → Devices***. You should soon see the Arctics appearing as new devices. You may want to cycle the Arctics' power OFF and back ON if they've been on a long time. This will speed up their appearing to Viola Patrol
7. The "traffic lights" for Arctics should go green
8. Accept the devices once they appear as *new* in Patrol by clicking ***Accept*** button

3.4. Configuring Arctics in DCHP client mode

Once it is checked that the Arctics are able to connect the Viola Cloud M2M Gateway, they can be configured through Viola Cloud M2M Gateway. You can alternatively contact Viola Systems Ltd. Technical Support (support@violasystems.com) for remote support or configure the Arctics by your own.

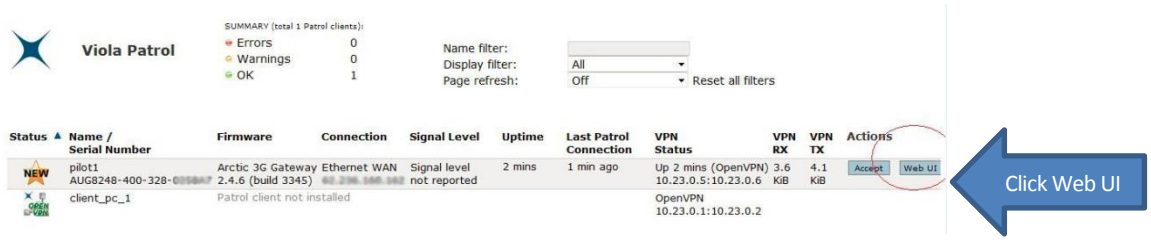
The following picture illustrates the connection from a PC through Viola Cloud M2M Gateway to Viola Arctic. Even though the Arctic may be connected to the same physical LAN as the configuration PC, the connection goes through the Viola Cloud M2M Gateway.



3.4.1. Logging in remotely to Arctic

1. Verify that the Arctic is connected to the internet router that assigns IP address to Arctic via DHCP. Power on the Arctic and wait a minute for the VPN tunnel to establish.

2. Use Viola Cloud M2M Gateway's link ***Patrol → web UI*** for connecting the Arctic's graphical user interface (Web UI).

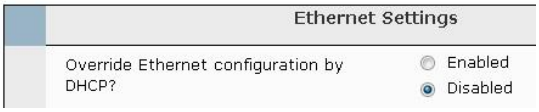


3. Configure the settings depending on the Arctic model, as described in next chapters.

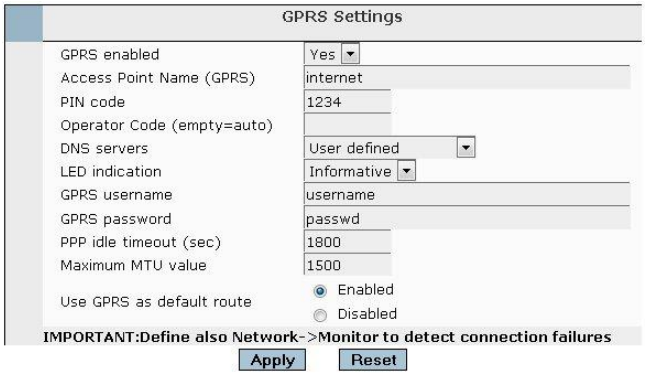
3.5. Configuring cellular settings

3.5.1. 2G Arctic (GPRS /EDGE)

1. After clicking the ***WebUI*** button, login to Arctic as `root` user via Viola Cloud M2M Gateway.
2. Disable the Ethernet DHCP client from Arctic. Click ***Network → Ethernet***. Change the ***Override Ethernet configuration by DHCP*** radio button to ***Disabled***. Click **Apply** button and wait for acknowledgement "***Operations completed successfully***".



3. Click ***GPRS*** from left vertical menu bar. The following screen opens.



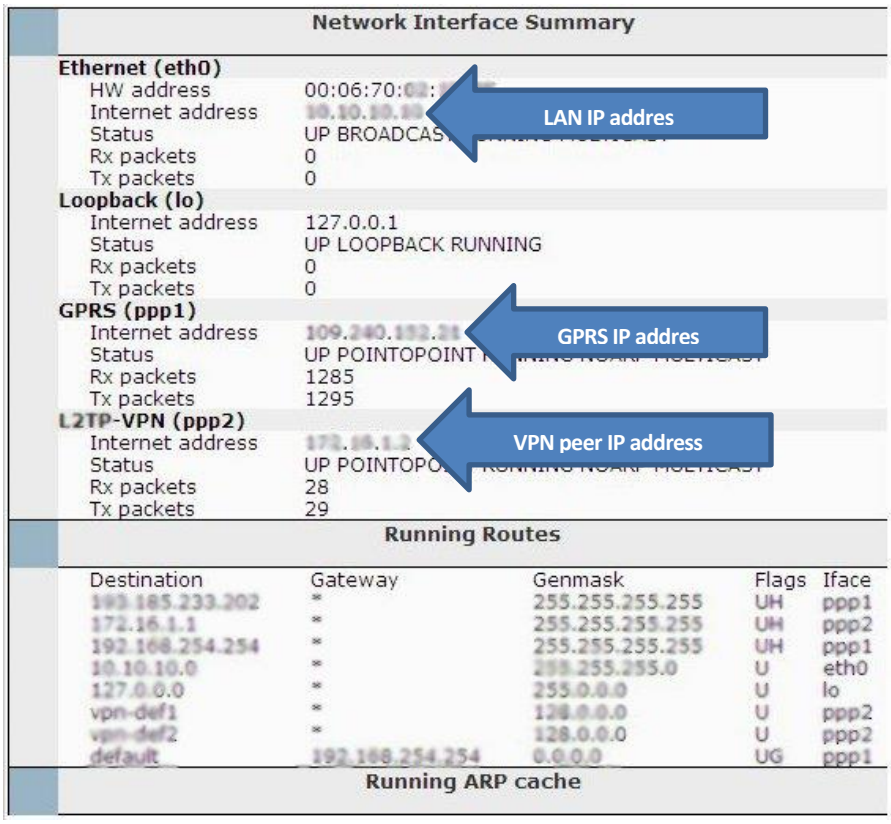
Fill in the following values according to the instructions from cellular operator:

> **Warning:** Do not enter empty Access Point Name value. The Access point name is a required parameter. Empty access point name is a difficult value to correct later on. Obtain the correct settings from your cellular network provider.

- ***Access Point Name (GPRS)***
- ***PIN code*** (leave ***NoPin*** or empty if the SIM card doesn't need one)
- ***GPRS username***
- ***GPRS password***

> **Note:** Some operators are instructing leaving the Access Point credentials (GPRS username and GPRS password) empty. However, if the GPRS network is requiring authentication (but not verifying the actual username and password), some values need to be set in Arctic. In this case, you can use "dummy" username and password, e.g. ***username***: username, ***password***: password.

4. Click ***Apply*** for applying the changes. Wait for acknowledgement "***Operations completed successfully***".
5. Click ***Commit*** from the lower left corner of the screen. This will write the changes to non-volatile memory. Wait for acknowledgement "***Data files successfully saved***".
6. Reboot the Arctic by clicking the ***Reboot*** button or cycling the power button.
7. Take off the Ethernet cable that connects the Arctic to the internet router.
8. Wait a minute for Arctic booting up and login as in chapter *Configuring Arctics in fixed IP mode*.
9. Click Network from the upper horizontal menu bar. In the ***Status*** screen, you will see the active interfaces. Verify that the GPRS interface appears to the status screen. This may take a minute and the browser screen needs to be refreshed in order to see the GPRS coming up.
10. Check that the SSH-VPN interface appears to the status screen. This will require refreshing the browser page as well.

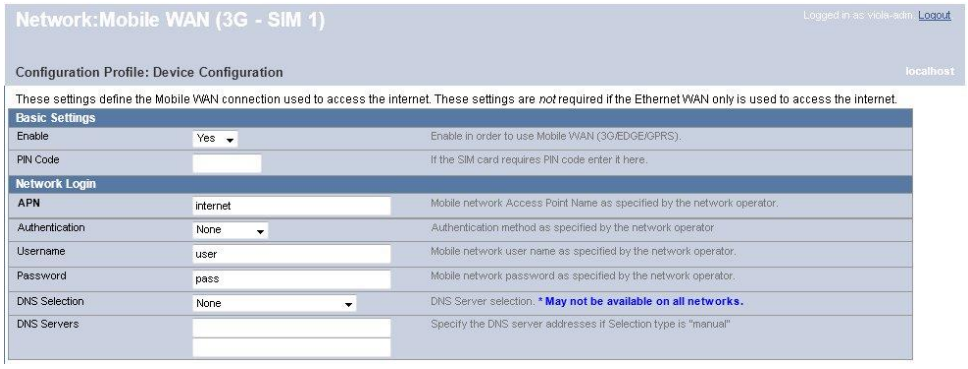


11. If the GPRS and/or VPN interface doesn't appear in the Network Interface Summary page, see the troubleshooting chapter *10.2, Cellular data connection*.

3.5.2. 3G/LTE Arctic

The parameters are entered similarly as in 2G Arctics but the Web UI's outlook is slightly different.

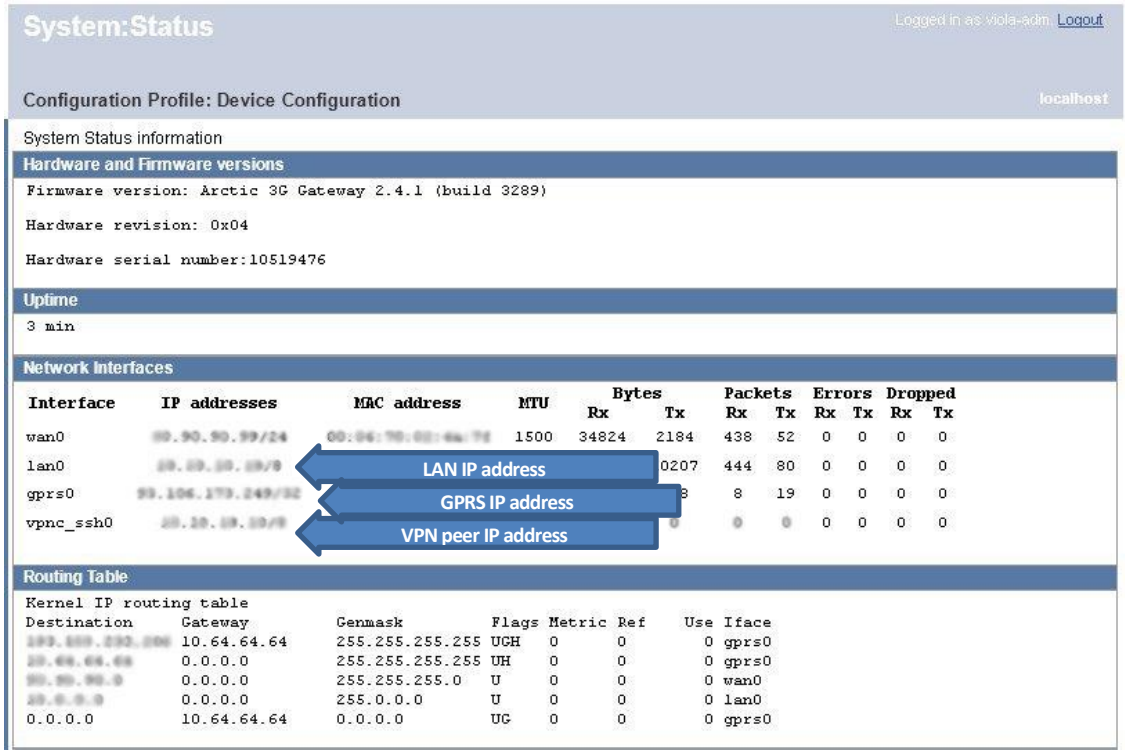
1. Login as `viola-adm` user as previously instructed (via Viola Cloud M2M Gateway, using ***Web UI*** button)
2. Click ***Mobile WAN (3G SIM 1)*** and fill in the following values according to the instructions from cellular operator:
   - ***PIN code*** (leave empty if the SIM card doesn't need one)
   - ***APN (Access Point Name)***
   - ***Authentication (None, PAP, CHAP or PAP/CHAP,*** *verify from operator****).***
   - ***GPRS username and GPRS password***



Note: Some operators are instructing leaving the Access Point credentials (GPRS username and GPRS password) empty. However, if the GPRS network is requiring authentication, some values need to be set in Arctic. In this case, you can use "dummy" username and password, e.g. ***username***: username, ***password***: password. In this case, use *pap/chap* authentication setting.

3. Click ***Submit*** button.
4. Take off the Ethernet cable from ***WAN*** Ethernet interface of Arctic.
5. Click ***Reboot*** from the left vertical menu bar. Confirm the reboot and wait approx. one minute for reboot.
6. Log in as in chapter *Configuring Arctics in fixed IP mode* and click Status from the left vertical menu bar. Check the **Network Interfaces** section. The gprs0 and vpnc_ssh0 interfaces should be seen. If not, see chapter *10, Troubleshooting.*

   See the picture below for verifying the cellular and VPN interfaces. With 3G/LTE Gateway, the OpenVPN is used as the VPN tunnel.



3.6. Inserting SIM card

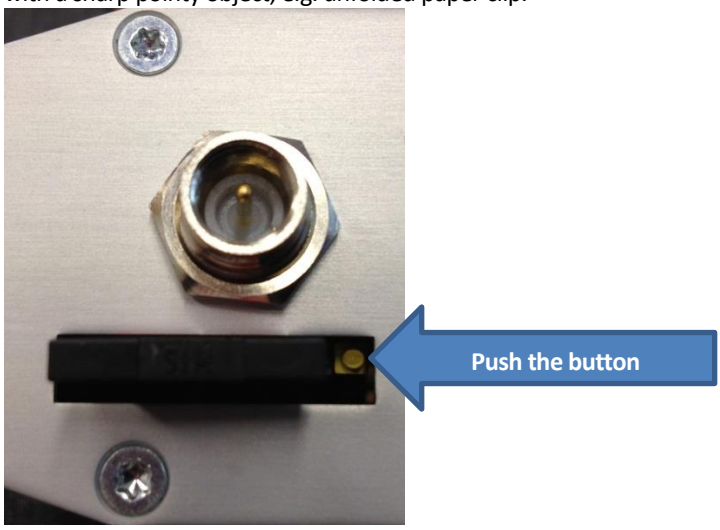
Make sure that the SIM card has cellular data plan enabled. You may test the SIM in a smartphone in order to verify the data transfer capability of the subscription.

If the SIM card requires PIN number, you will need to configure the PIN number in Arctic prior to inserting the SIM card. In case of a wrong PIN in Arctic, correct the PIN and insert SIM card to a cellular phone and enter the correct PIN. The Arctic tries PIN only once for avoiding SIM lockup.

Always use standard mini SIM card. A micro SIM card is not compatible unless a separate adapter is used. Nano SIM card is not compatible with Arctic devices.

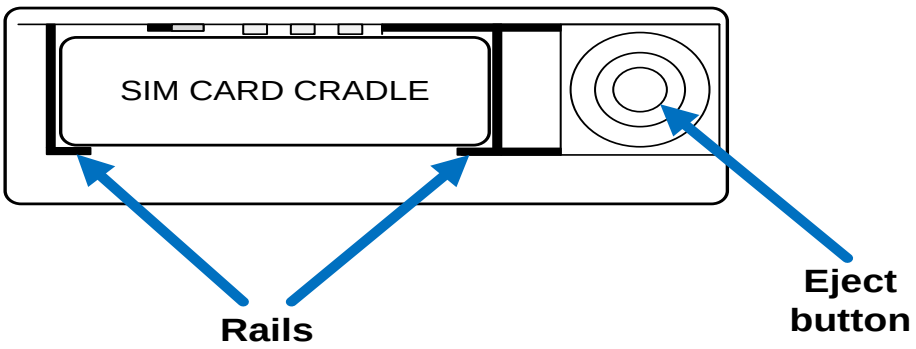
When the SIM card is inserted and the Arctic is powered on, the SIM LED should be lit after approx. a minute from starting. The SIG LED indicates strong signal (LED lit), weak signal (LED blinking) or no signal (LED not lit).

1) Eject the SIM card cradle from the Arctic device by pushing the green/yellow eject button in the SIM holder with a sharp pointy object, e.g. unfolded paper clip.



2. Insert the SIM card to the cradle so that the clipped notch aligns with the notch in the cradle and the electrical contacts of the SIM card are facing upwards.

3. Insert the cradle to the Arctic. Make sure the cradle slides to the rails in the connector. Push the cradle all the way in until it stops.



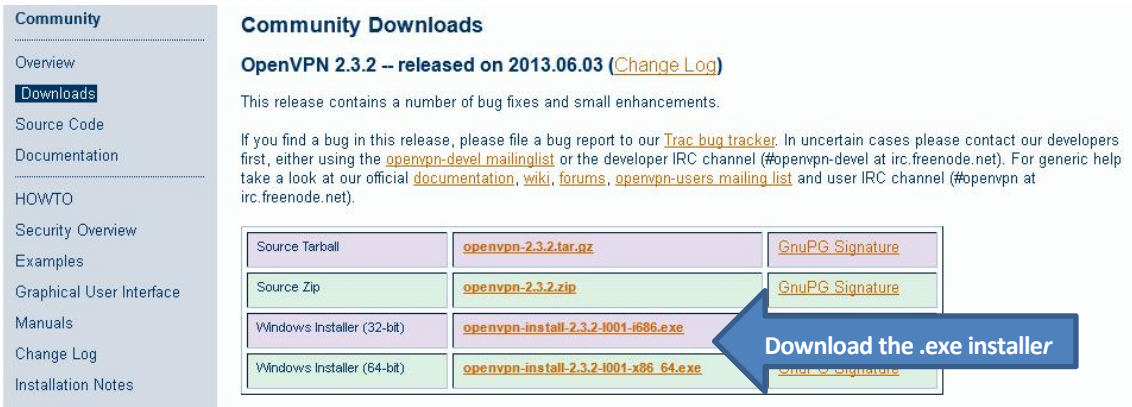
4. Installing the OpenVPN client to a PC

For safe connection from pilot SCADA or other supervisory/control application to Viola Cloud M2M Gateway over the internet, the VPN tunnel is used. OpenVPN provides safe, encrypted and relatively light-weight VPN tunnel, which supports routing between the client PC, Viola Cloud M2M Gateway and remote Arctics' LANs.

For installing an OpenVPN client to your PC, where the SCADA application is located, perform the following steps.

1. Obtain the OpenVPN client software. The newest version can be downloaded from the internet from the following URL: http://openvpn.net/index.php/open-source/downloads.html. In case the link changes, you may navigate to the correct location by opening http://openvpn.net page and going to ***Community*** and from there to ***Downloads***.

   The correct package is called "Windows installer" and the filename is in form of "openvpn-install-n.n.n-Ix.x.x-<architecture>.exe", where the n.n.n represents the current version (at the time of writing this document, the filenames are):
   - openvpn-install-2.3.2-I001-i686.exe (32-bit)
   - openvpn-install-2.3.2-I001-x86_64.exe (64-bit)



Click the file suitable for your Windows and the download will start. Save the file to the PC to a directory, where you can easily locate it. If you're unsure whether you're running 32 or 64 bit version

of Windows, verify it from ***Control Panel → System and Security → System → System Type***.

2. Once the installer file is downloaded, you will need to install the OpenVPN client. Go to the folder, where you have downloaded the OpenVPN installer and double-click the installer file.

   You may get a warning screen similar to as follows.

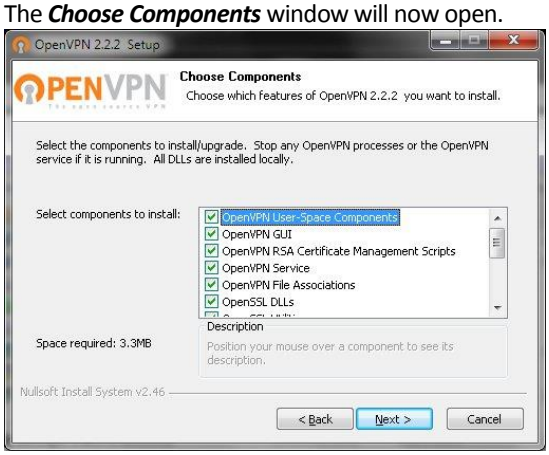
   Allow the OpenVPN to make changes to the computer by clicking the ***Yes*** button.

3. The Setup Wizard opens.

   Click ***Next*** to proceed.

4. Agree the "GNU general public license" by clicking ***I agree*** button. Alternatively, you can read the license first by scrolling the text down with the scroll bar.

5. The ***Choose Components*** window will now open.



   All components are needed and already selected. Click ***Next***, (do not unselect any components).

6. The OpenVPN will ask the location where to save program files.

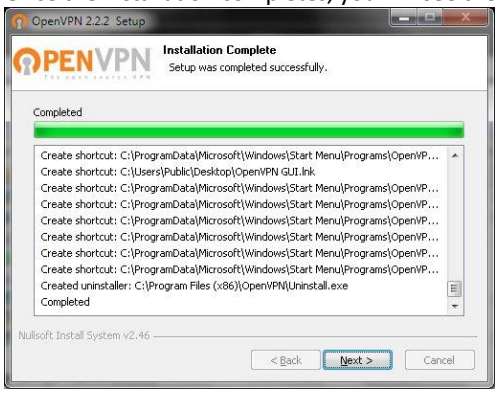
7. Accept the default location by clicking ***Install*** button.

8. The OpenVPN is being installed.

During the installation, the following window will open.

The Windows may warn about installing a device driver with the following details.
Name: TAP-Win32 Provider v9 Network adapters
Publisher: OpenVPN Technologies, Inc.
You can safely let the OpenVPN install a device driver, click ***Install*** button.

9. Once the installation completes, you will see the following windows.



Click ***Next*** when you'll see that the OpenVPN has been installed and click ***Finish*** in Setup Wizard screen.

Now the OpenVPN client is installed to the PC. However, before it can be used for connecting to Viola Cloud M2M Gateway, the OpenVPN certificates must be put to proper place in the OpenVPN folder. See the next chapter for details.

5. Configuring OpenVPN

The OpenVPN uses secure cryptographic certificates (easy VPN) for ensuring that:

- The Client (PC) is authorized to connect to the server (Viola Cloud M2M Gateway)
- The server is really the server it states to be
- The certificates are really coming from the stated authority (Viola Systems Ltd.)

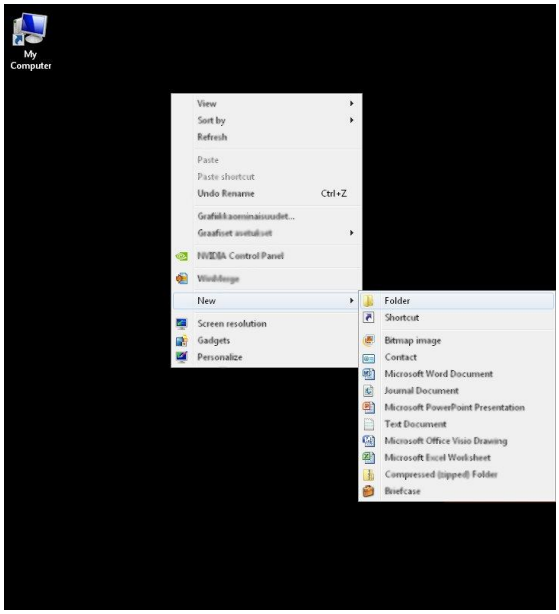
The certificates are received from Viola Systems in form of a file, which is compressed (Zip file for easy VPN).

Proceed as follows.

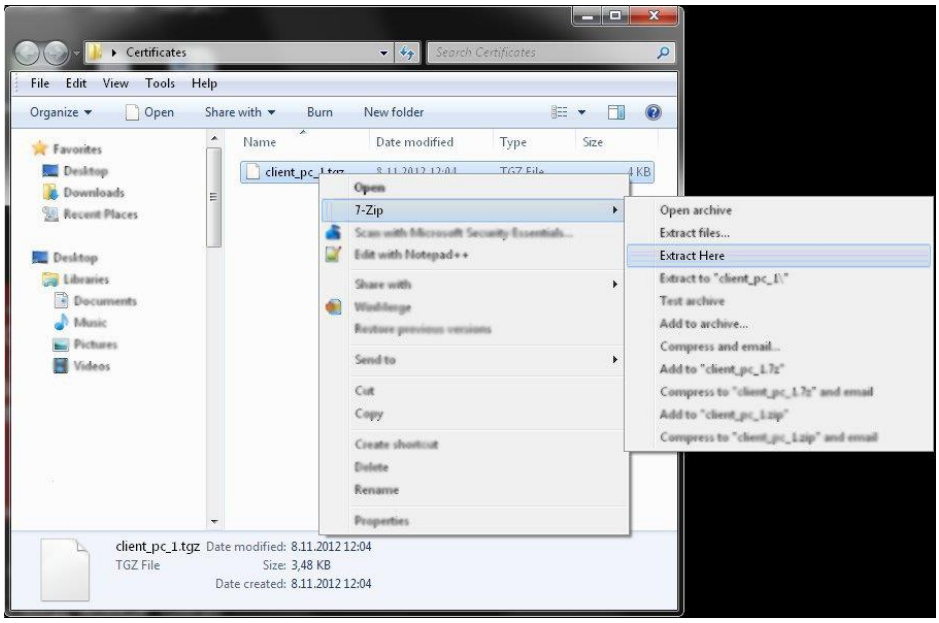
1. You have received a file containing the needed client certificates from Viola Systems Ltd. In case you're missing the file, please contact Technical Support at support@violasystems.com email address.

   Place the file to a directory, where you will easily find it (do not place it under OpenVPN directory yet). In this example, a directory (folder) is created at Windows desktop and we will name it as "Certificates".

   Right-click the empty space of desktop and select New from context-menu and then select Folder. Name the folder as Certificates.

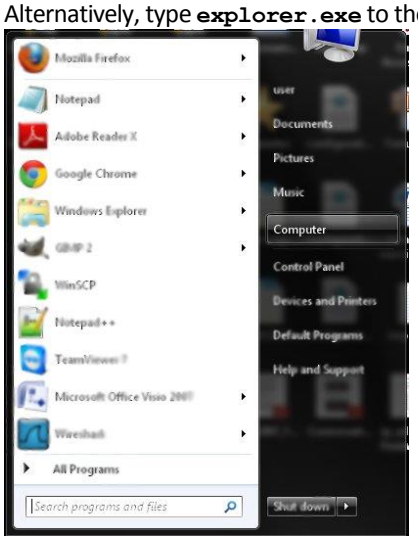


2. Copy the received file to the Certificates folder. In the folder, right-click the file and from the opening context menu, select ***Extract all.*** You may have different zip file managing software.
   Note that the Windows 7 or newer has native support for unzipping the file.

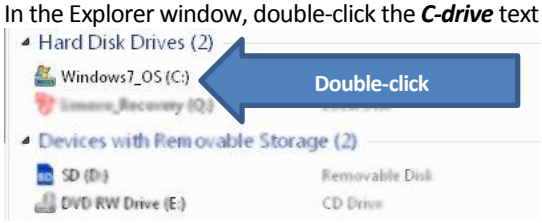


3. You will now see plenty of files. All of the files need to be copied to proper folder in OpenVPN directory structure. Leave this window open on your desktop and see the next steps for details.

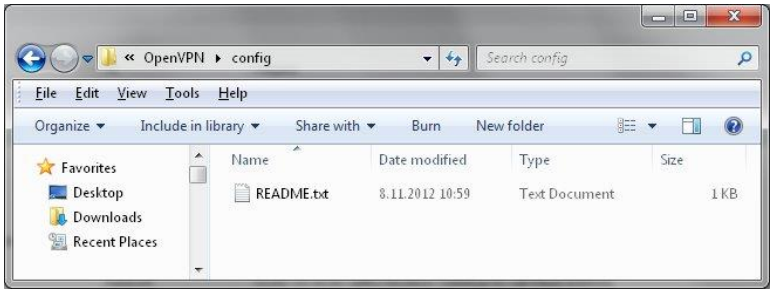
4. Click the start button (Windows logo) and select ***Computer*** from the right-side vertical menu bar. Alternatively, type **`explorer.exe`** to the search row and press enter.



In the Explorer window, double-click the ***C-drive*** text (showing as ***Windows7_OS (C:)*** in the next picture).



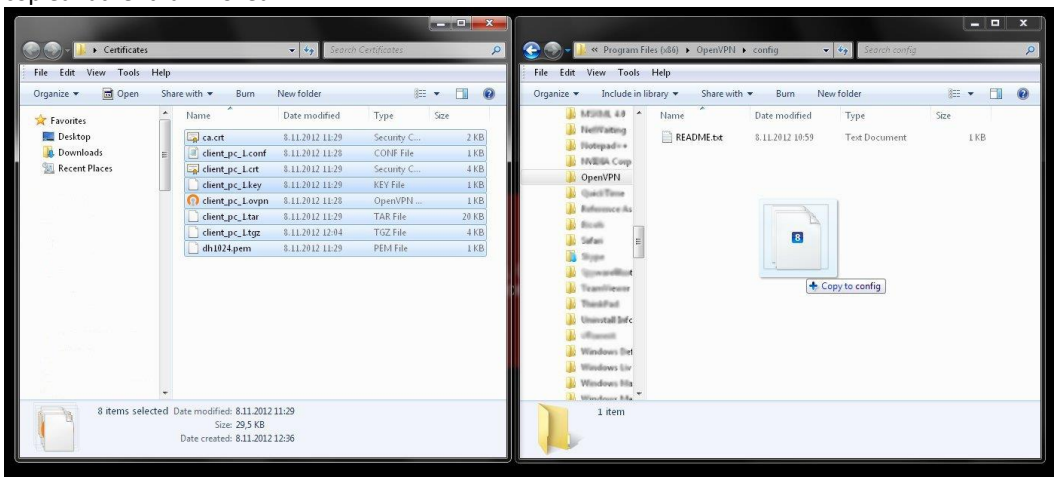
Scroll down the list of folders until you see the folder ***Program Files (x86)*** (the "x86" suffix is only in 64-bit Windows, select ***Program files*** folder in 32-bit Windows). Again, scroll down until you see a folder named **OpenVPN**. Double-click the ***OpenVPN*** folder. Now you see several folders, double-click the ***config*** folder.



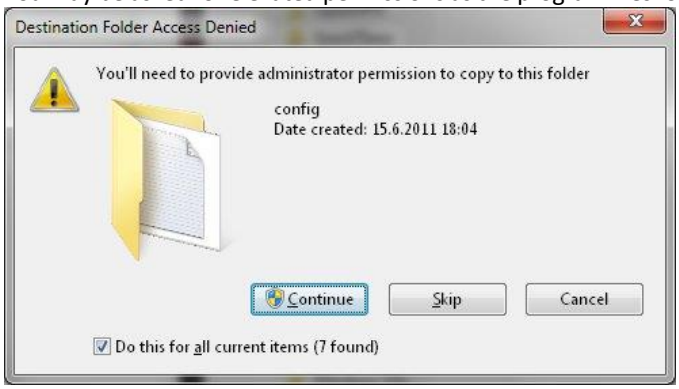
This is the folder you will need to copy the certificate files from your desktop's Certificates folder. Leave the original files to the Certificates folder as a backup. See the next step for copying the files.

5. You should now have two Explorer windows open; the `Desktop\Certificates` folder and `C:\Program Files (x86)\OpenVPN\config` folder.

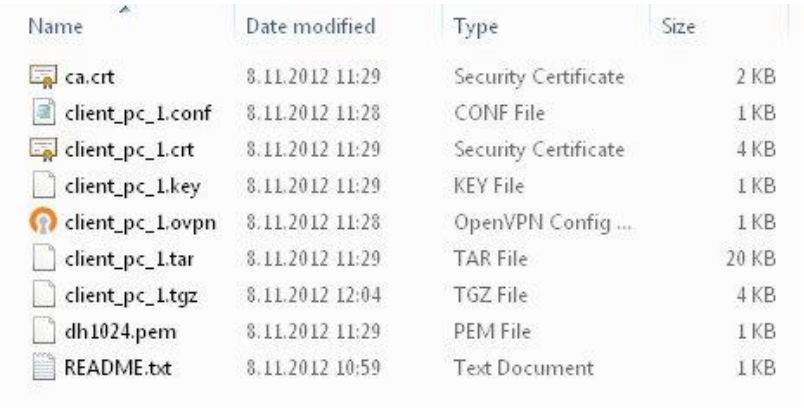
   Select all files in Certificates directory (you can press **`ctrl + a`** for selecting all files), then drag them to the OpenVPN's config folder. Press **`ctrl`** key, while you drag the files to config folder so that the files are copied rather than moved.



You may be asked for elevated permissions as the program files folder is protected by Windows.



Click ***Continue*** button to continue the copying. Now the ***config*** folder should look as follows.



Name	Date modified	Type	Size
ca.crt	8.11.2012 11:29	Security Certificate	2 KB
client_pc_1.conf	8.11.2012 11:28	CONF File	1 KB
client_pc_1.crt	8.11.2012 11:29	Security Certificate	4 KB
client_pc_1.key	8.11.2012 11:29	KEY File	1 KB
client_pc_1.ovpn	8.11.2012 11:28	OpenVPN Config ...	1 KB
client_pc_1.tar	8.11.2012 11:29	TAR File	20 KB
client_pc_1.tgz	8.11.2012 12:04	TGZ File	4 KB
dh1024.pem	8.11.2012 11:29	PEM File	1 KB
README.txt	8.11.2012 10:59	Text Document	1 KB

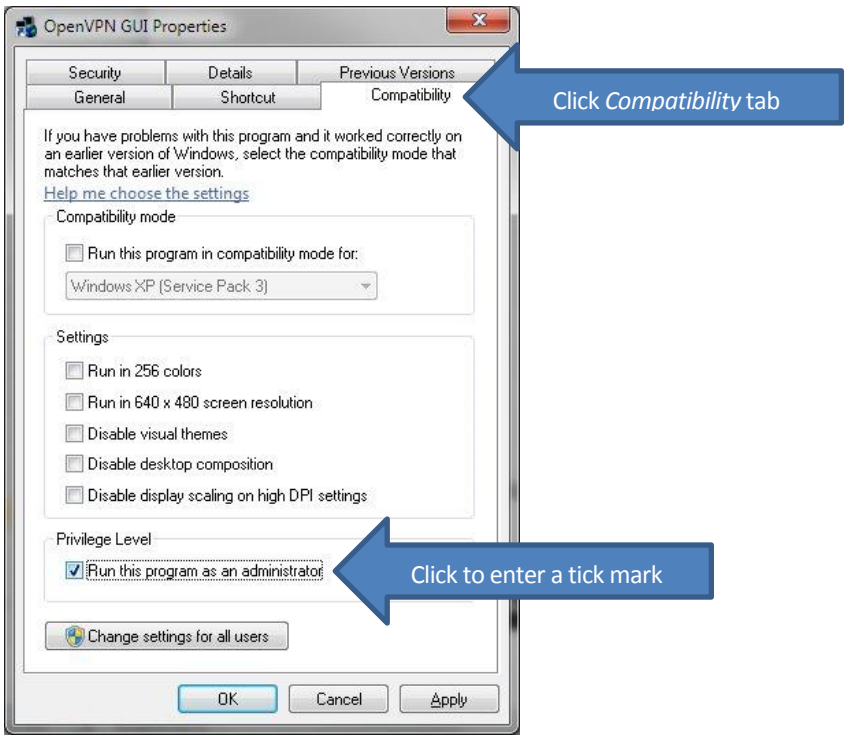
6. You have now copied the client certificate files to the OpenVPN directory. You may now start using the OpenVPN, as instructed in the next chapter.

6. Using OpenVPN

In a Windows PC, the OpenVPN is managed by the OpenVPN GUI, which can be started as any other program. When started, the OpenVPN places an icon to the notification area in Windows taskbar. You can select whether the icon is always shown or hidden until ***Show hidden icons*** button is pressed.

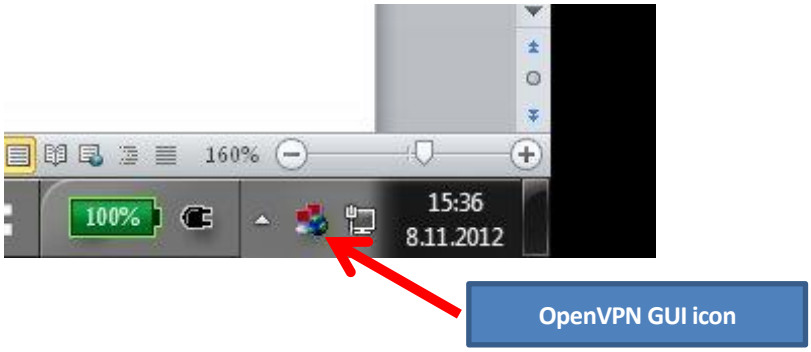
In contemporary Windows versions, the programs are not run with Administrator privileges, unless there's a need for that. The OpenVPN needs to be run with administrator rights as it needs to push routing entries to Windows' routing table. The following steps are instructing how to run the OpenVPN permanently as Administrator.

1. Start the OpenVPN by clicking Windows ***start button*** (Windows logo) and click ***All programs*** and scroll down to ***OpenVPN***, then click the ***OpenVPN*** text to see the ***OpenVPN GUI*** menu option. Do not click it yet. With right mouse button, click the ***OpenVPN GUI*** menu option, and then from the context menu, select ***Properties*** (at the bottom of the context menu). The following window opens. Click ***Compatibility*** tab.



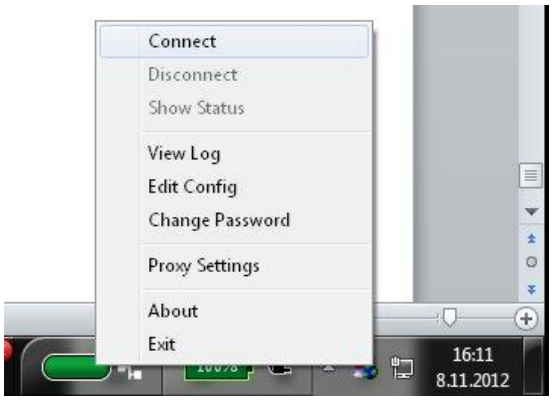
Place a tick to the checkbox ***Run this program as an administrator*** and press ***OK*** button.
Again, click Windows ***start button*** (Windows logo), click ***All programs*** and scroll down to ***OpenVPN***, then click the ***OpenVPN*** text and click ***OpenVPN GUI.*** If asked, allow changes to be made to computer.

2. Now the OpenVPN client is started, but it hasn't established a VPN tunnel yet. You can see the OpenVPN icon in the notification area of Windows taskbar.

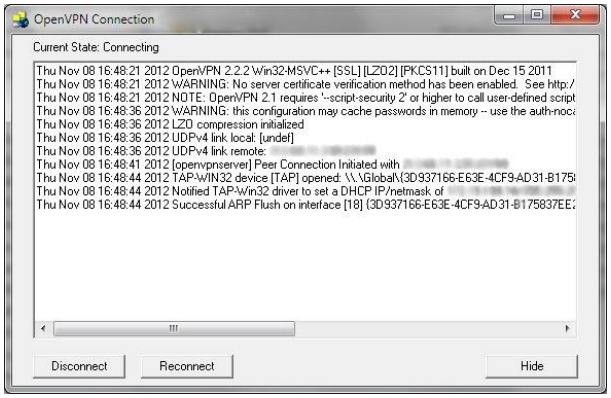


3. When the OpenVPN is running, the OpenVPN GUI icon is seen, either directly in the taskbar or by clicking ***Show hidden icons*** button (triangle-shaped button in the picture above). You can customize the visibility of the OpenVPN GUI icon, see Windows help for *selecting which icons and notifications appear on the taskbar*.
4. Click the ***OpenVPN GUI*** icon with right mouse button. A context menu opens.

Note: For this step, you need to have an active internet connection in the PC.



Click ***Connect*** for establishing a VPN tunnel to the OpenVPN server (Viola Cloud M2M Gateway). You will momentarily see the connection screen similar to as picture below, which disappears once the connection is established.



Once the connection screen disappears, the VPN connection to Viola Cloud M2M Gateway is established. The state of the VPN connection can be checked by hovering the mouse pointer over the OpenVPN icon.

5. For shutting down the VPN tunnel, right-click the OpenVPN icon and select ***Disconnect*** from the context menu.

In case of a problem, see chapter *10.4, OpenVPN.*

7. Configuring the monitoring application

The end device, being it RTU, PLC or other is connected to Arctic.

- For Ethernet devices, configure the RTUs IP address from Arctic's LAN, e.g. 10.20.x.10, where x=1 (Pilot1 LAN) or x=2 (Pilot2 LAN)
- Set the default gateway IP address in RTU as Arctic's IP address
- In case of serial device, set the Arctic's serial settings according to the serial device (set the speed, number of data bits, number of stop bits, parity and flow control from Arctic's Web UI and RS-232, 422 or 485 setting by DIP switches in Arctic)
- In case of IEC-101 to IEC-104 converter models, set the Arctic's IEC-101 settings as according to RTU's and IEC-104 settings as according to SCADA's.

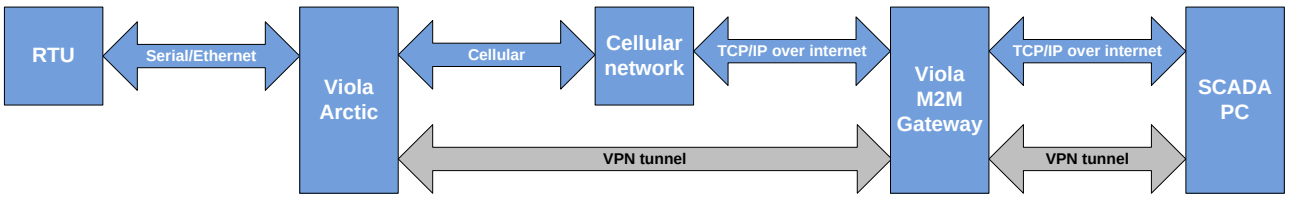
The monitoring application can be a SCADA or other control/monitor application, e.g. PLC reader, power quality meter reader or similar. Typically such applications are using TCP or UDP protocol as the information bearer.

When the IP addresses are configured to the monitoring application, use the following.

- Arctic's LAN IP (and Arctic's serial gateway port) for serial device that is read transparently over TCP/IP via Arctic's serial gateway.
- RTU's/PLC's LAN IP address for Ethernet devices that are read through VPN tunnel using Arctic as an IP router.

8. Testing the solution

At first, test each leg of the connection path separately, and then perform the end-to-end testing. Follow the instructions in next sub-chapters.



8.1. Arctic local Ethernet

If the RTU, PLC or other device is connected to Arctic via Ethernet, check the Ethernet LED in Arctic. If the Ethernet LED is lit, you can be sure that the Ethernet-layer connectivity is in place.

8.2. Cellular data connection

Verify that the Arctic has received an IP address from cellular network. With this test, you'll know that the SIM card is working and that the cellular network registration and cellular data connection initialization has been successfully performed.

See the chapter *3.5.1* step *9* (2G Arctic) or chapter *3.5.2,* step *6* (3G/LTE Arctic) for details. If the GPRS IP address is seen in status screen, the cellular data connection has been properly established.

8.3. VPN tunnel

After clicking ***Connect*** in OpenVPN context menu, the connection window is opened momentarily, and then it should disappear. After that, verify that the ***Connect*** text in OpenVPN's context menu is greyed out. Furthermore, by hovering the mouse pointer over OpenVPN icon, the text ***Connected to:*** should appear.

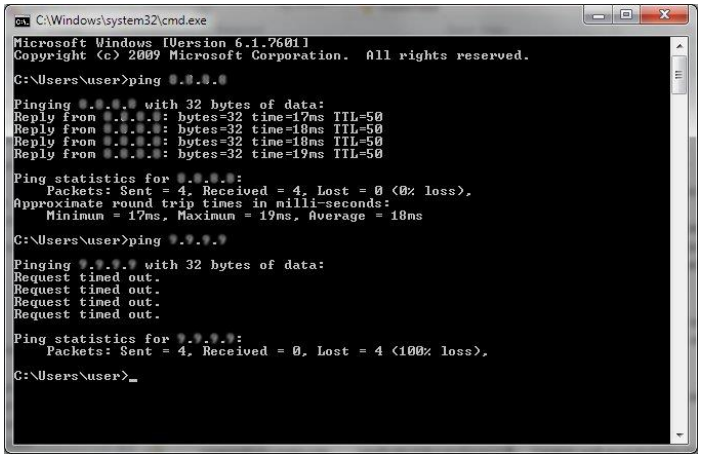
The text box also shows how long the connection has persisted and what is the VPN peer IP (10.23.0.x) received from Viola Cloud M2M Gateway.

8.4. ICMP Ping

Try pinging the remote device (RTU, PLC or PC) from the PC running OpenVPN client. Make sure that the remote device is answering to ICMP ping messages. Usually PC's firewall is blocking ping messages.

Note: The remote device (RTU, PLC, etc.) should be configured so that it belongs to the same network as Arctic. For example, if Arctic is configured as 10.20.1.1/255.255.255.0, the RTU can be 10.20.1.2/255.255.255.0. Furthermore, the remote device must be configured to use Arctic (i.e. 10.20.1.1 in this example) as remote device's default gateway.

1. Click ***Start*** button (Windows logo) and to the search bar, write the command `cmd`. The command prompt opens. Try to ping the Arctic's LAN IP and RTU's LAN IP (if the RTU is Ethernet connected)
2. Successful ping attempt shows with details, such as *time*= (which value is the round-trip time of the ping messages). Unsuccessful ping is seen by `Request timed out` message.



- The round-trip times for GPRS/3G/LTE over VPN tunnel are varying, typically the GPRS being from 1000 ms to 2000 ms, 3G around 1000 ms and LTE is considerably faster
- However, if your PC is also connected via GPRS, be aware that the round trip times may be longer

8.5. Application

- Try connecting and sending the read or control messages to the remote device. Is the sending successful?

9. Configuring Arctics in fixed IP mode

Once the "2G" Arctic is switched over from connecting via DHCP to connecting via cellular network, it can be connected via local LAN IP address 10.20.1.1 (pilot1) or 10.20.2.1 (pilot2). The URL is in form of http://10.20.1.1 or http://10.20.2.1

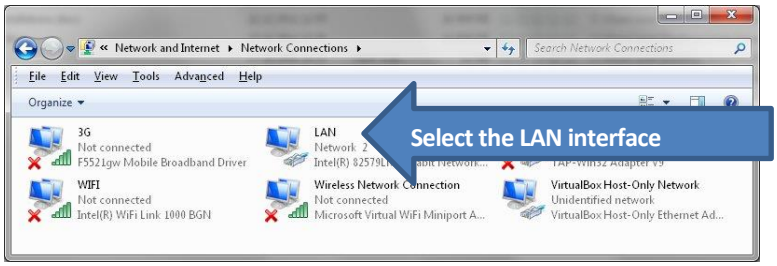
The "3G" or "LTE" Arctic can always be connected via LAN port. The URL is in form of https://10.20.1.1 or https://10.20.2.1. See the details below.

9.1. Configuring a PC for local connection to Arctic

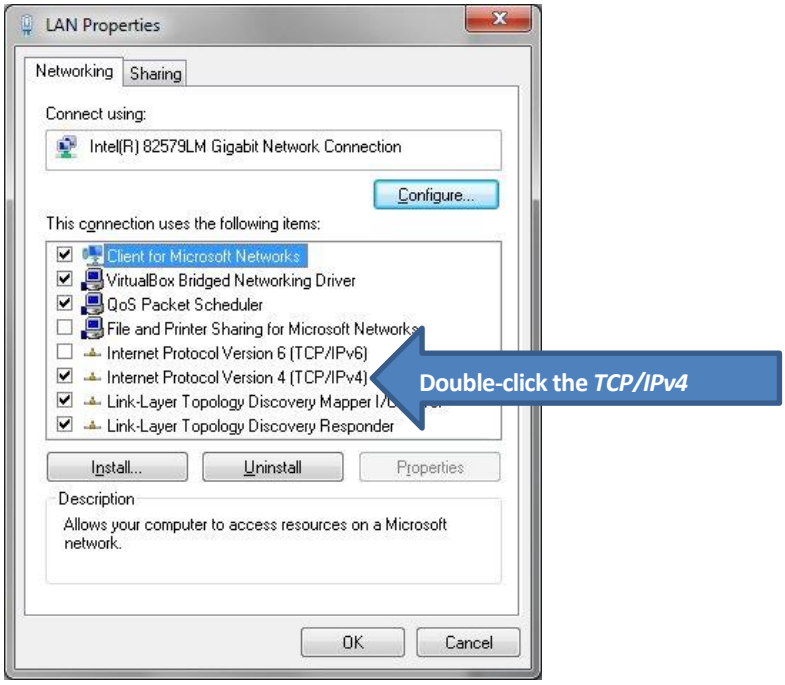
Apart from configuration, the Arctic's management user interface can be also used for troubleshooting and system verification purposes. The configuration and end-to-end testing should be done in a central place before the Arctics are deployed to the field or to customer's site.

1. Open the PC, which is used in configuring the Arctic. This can be the same PC, which is used for control/monitor software connecting to remote assets using Arctics.
2. Click ***Start → Control panel → Network and Sharing Center → Change Adapter settings*** and right-click the *LAN interface* of your computer with mouse and select ***Properties***.

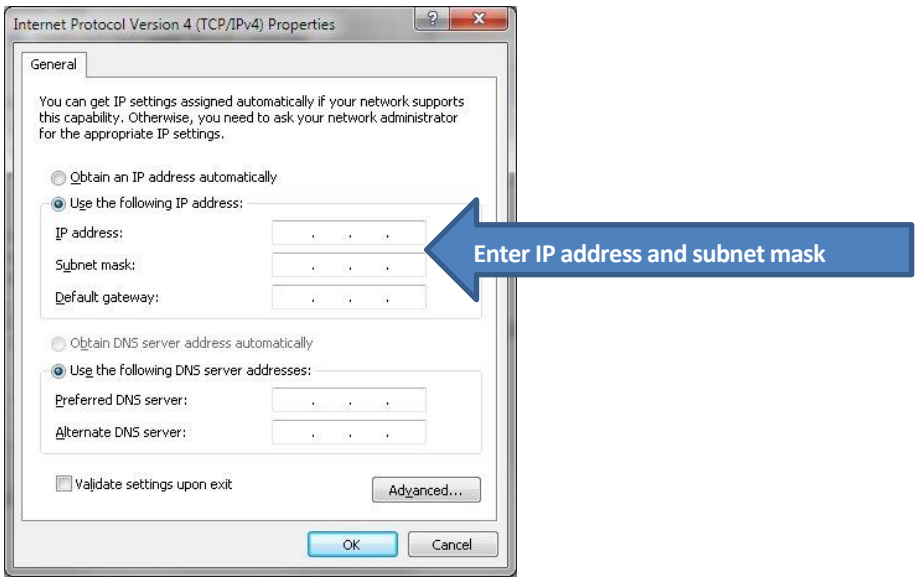
Note: Your LAN interface may be named differently, e.g. Gigabit Ethernet, etc.



3. Double-click the Internet Protocol Version 4 (TCP/IPv4) text so that the TCP/IP settings are opening.



4. The settings window will open. Click the Use the following IP address radio-button to set the IP address manually.



In the settings of LAN adapter's TCP/IP properties, set the details as follows
in "Pilot1" Arctic case:
IP address: 10.20.1.11
Subnet mask: 255.255.255.0

in "Pilot2" Arctic case:
IP address: 10.20.2.11
Subnet mask: 255.255.255.0

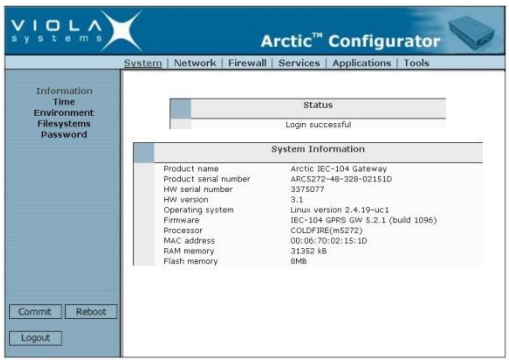
At this point, you don't need to define ***Default gateway*** or ***DNS server addresses***.

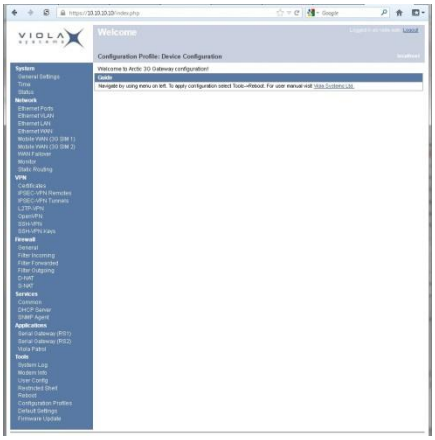
5. Click ***OK*** to get back to LAN interface's properties and ***OK*** again to save the settings.

9.2. Logging in to Arctic

1. Verify that Arctic is connected via cross-connected Ethernet cable to the PC's LAN interface and power on the Arctic. If the PC is supporting *MDI-X* (i.e. sensing the cable type), you can use direct cable as well.
2. Open a browser (e.g. Google Chrome or Mozilla Firefox). Enter the address of the Arctic's management interface as follows:
    a. 2G (GPRS/EDGE) Arctics: **http**://<IP address>, e.g. `http://10.20.1.1`
    b. 3G or LTE Arctics: **https**://<IP address>, e.g. `https://10.20.1.1`

Enter the user credentials (`root` user in 2G Arctic, `viola-adm` user in 3G/LTE Arctic) and the management user interface should now open. In case of a problem, see *chapter* *10.1, Arctic local Ethernet* for troubleshooting.





Welcome screens of 1) 2G Arctic, 2) 3G or LTE Arctic

3. You can now perform needed actions in Arctics Web UI.

10. Troubleshooting

If you're encountering problems with some area of Viola Cloud M2M Pilot Kit functionality, perform the troubleshooting steps as described in the next sub-chapters.

10.1. Arctic local Ethernet

If the Ethernet LED is not lit when the cable is connected, check the following.

- Is the Arctic still in DHCP mode ("2G" Arctic)?
- Verify that you're using "LAN" Ethernet port ("3G" Arctic)
- The cable is type of CAT5(e) Ethernet (unshielded twisted pair preferred)
- The cable is a direct cable between RTU and Arctic
- The cable is cross-connected between a PC and Arctic (or MDI-X is supported by PC)
- Try placing a simple switch between Arctic and problematic device
- With PC, try setting Auto-negotiation off and manually selecting 100 Mbit/s full duplex

10.2. Cellular data connection

If the cellular packet data connection is not established, check the following.

- The SIM card has an enabled data plan and it is proven active with e.g. a cellular phone
- Verify the Access Point Name, username and password. If unsure, ask from the cellular operator or search "worldwide APN list" from internet
- Try "dummy" names in APN username and password if the cellular operator is not providing them
- Try with another operator's SIM card
- Verify the PIN number if it is required. If the wrong ping number is set, you may need to put the SIM card to a cellular phone for entering a correct PIN. (Arctic will try only 2 times with a wrong ping number to avoid SIM locking)
- Check that the cellular field strength is sufficient enough (check from Arctic's GUI → ***Tools*** → ***Modeminfo*** in 2G Arctic or Arctic's GUI → ***Modeminfo*** in 3G/LTE Arctic). If the signal is weak, consider an external antenna

10.3. VPN tunnel

There isn't much to do in troubleshooting VPN as it is pre-configured in Viola Systems M2M Gateway.

In a DHCP client use case, verify first that the internet connectivity is OK (check with a PC). If Arctic is configured to use cellular connection, verify first that the cellular connection is working.

Do not make changes to Arctic's VPN configuration. Double-check the OpenVPN settings and if the problem persists, contact Viola Systems Technical Support (support@violasystems.com).

10.4. OpenVPN

If you suspect a problem in OpenVPN, perform the following checks.

- Is the OpenVPN run as administrator? Follow the instructions in *chapter 6, step 1*
- Is the internet connection working?
- Is the OpenVPN tunnel established? Check by hovering mouse pointer over OpenVPN icon. If the VPN tunnel is established and the OpenVPN is run as administrator, the problem may be in Viola Cloud M2M gateway's configuration. Contact Viola Systems Technical Support (support@violasystems.com)
- If the OpenVPN tunnel is not establishing, verify that the certificates are put to correct folder, see chapter *4, Installing the OpenVPN client to a PC* for details. Do not try to extract the files directly to the OpenVPN's config directory
- The OpenVPN writes a log, which can be seen by right-clicking the OpenVPN icon and selecting ***View Log***. If the problem persists, send the log file to Viola Systems Technical Support for analysis.

10.5. SCADA, etc. application

- Try increasing the timeouts if the application is designed to work inside one LAN or using circuit switched data
- Check applications log and Arctic's log for incoming/outgoing connections
- Disable or re-configure firewall in a target PC

10.6. Other problems

If encountering other problems related to Viola Cloud M2M Pilot Kit, don't hesitate contacting to Viola Systems Technical Support (support@violasystems.com).

11. References

See the following link for documentation: http://www.violasystems.com/docs

The following documents are useful for Viola Cloud M2M Pilot Kit user.

- Arctic *GPRS/IEC-104/Modbus* Gateway User's Manual
- Arctic 3G Gateway User's Manual
- Arctic LTE Gateway User's Manual
- Viola M2M Gateway User's Manual