

Trouble Shooting

SiteManager to GateManager access



If you are unsure if a SiteManager will be able to access the GateManager through the corporate firewall, or you experience connection issues, this document will assist you in verifying from a PC that the conditions for obtaining GateManager access is available.

Version: 1.4, February 2011



Table of Contents

1. introduction.....	3
2. Basic things to check.....	3
2.1.1. Ethernet cables	3
2.1.2. Check Uplink IP address.....	3
2.1.3. ping test from sitemanager.....	4
2.1.4. Ping test from a PC.....	5
3. Telnet test from command line.....	7
4. Test GateManager access from a PC with a browser.....	9
4.1. Web Proxy issues.....	10
4.1.1. how to check if PC use a proxy for surfing internet.....	10
4.1.2. Web Proxy automatically configured.....	10
4.1.3. Web Proxy NOT automatically configured.....	11
5. PC connect to internet but SiteManager does not.....	13
5.1.1. Web proxy TLS issue.....	13
5.1.2. NTLM proxy.....	13
5.1.3. Content filtering.....	13
6. summary table of possible cases.....	14
6.1. How to get more info for technical support.....	15
6.2. Final things to Check.....	16
7. Appendix A: how to enable telnet on window 7.....	18
8. Notices.....	19

1. introduction

The purpose of the guide is to solve internet connection issue. Typically you read this guide when you have the error led blinking that means, **sitemanager** can not connect to **gatemanager (to internet)**

2. Basic things to check

2.1.1. Ethernet cables

First of all check the cable is inserted in the uplink port and that both the Ethernet led on the uplink port of the sitemanager are lighting. The left one should be green (the status led) and the other should blink yellow when there is traffic. If both led are off. Please also check the cable is good and it's of correct type (straight or crossed).

Please note: **sitemanager port doesn't support autocrossing** so the right cable has to used (a **straight cable**).

If you are not sure, try to connect a PC to the same port with same cable and check if it can connect to internet. If it works, means that the port is working correctly but it doesn't prove the cable is **correct for the sitemanager**. Most of PC has **autocrossing feature** so it doesn't matter if the cable is **crossed** or **straight**, while the **sitemanager does not**. So a straight cable **must** be used for the **sitemanager uplink port**.

2.1.2. Check Uplink IP address

Check that the SiteManager has an IP address matching the network through which it should obtain Internet Access either via DHCP or statically.

If the Uplink IP address is DHCP assigned, check that an address has been assigned, if you see **169.xxx.yyy.zzz** this means that a valid address has not been assigned by DHCP.

In order to verify uplink address of *sitemanager*, you have to connect a PC to the DEV network and use the **Secomea Appliance Launcher** to browse the *SiteManager* and verify the *Uplink IP address*. Alternatively check on the DHCP server's lease table, what IP was given for the SiteManager. Another good test is **trying to ping this IP address** from another PC connected to network on uplink side (from customer network).

TIPS: You can ask customer to ping the *Sitemanager uplink ip* address from one of his PC. If you can't reach *sitemanager* via ping it means it didn't got a valid ip address or the cabling is wrong

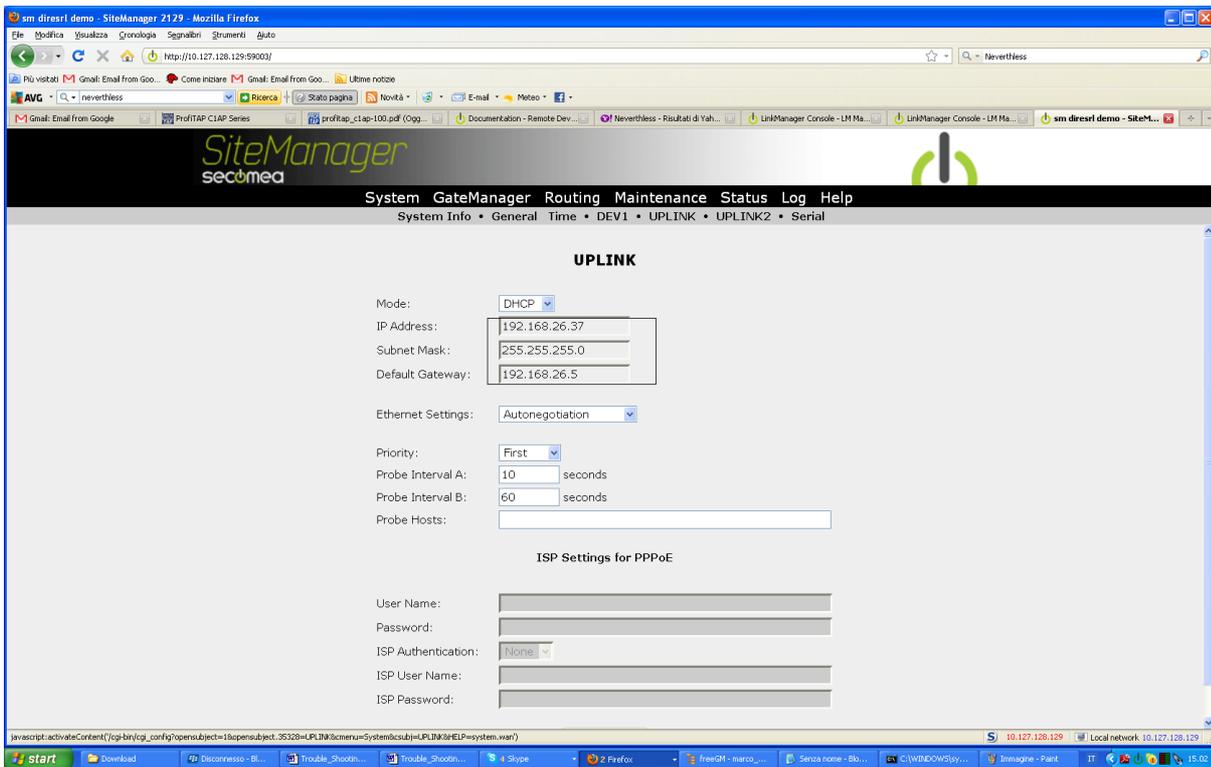
If the *Uplink IP* address is statically configured, you should check that it matches the subnet of the network it is connected to. Also check that the subnet mask matches the subnet class, and that the default Gateway is set to the router that provides Internet access

Please note that *dev1 network (automation network) should be different than uplink network* (customer network) and the network doesn't **overlap** each other or with other network reachable on uplink side (i.e. internal routing). **Pay attention to netmask value!**

Please note, that this is a potentially dangerous situation and it should be always avoided.

Solution: If dev1 use same ip address family as uplink does, change ip address of dev1 network the **advice** is to choose for dev1 network uncommon private ip family and to avoid 192.168.0.X or 192.168.1.x or 10.0.0.x cause everybody use that.

You can check **the sitemanager ip address on uplink side** in the *gatemanager* gui. Choosing **system** → **dev1** in the *sitemanager* gui.



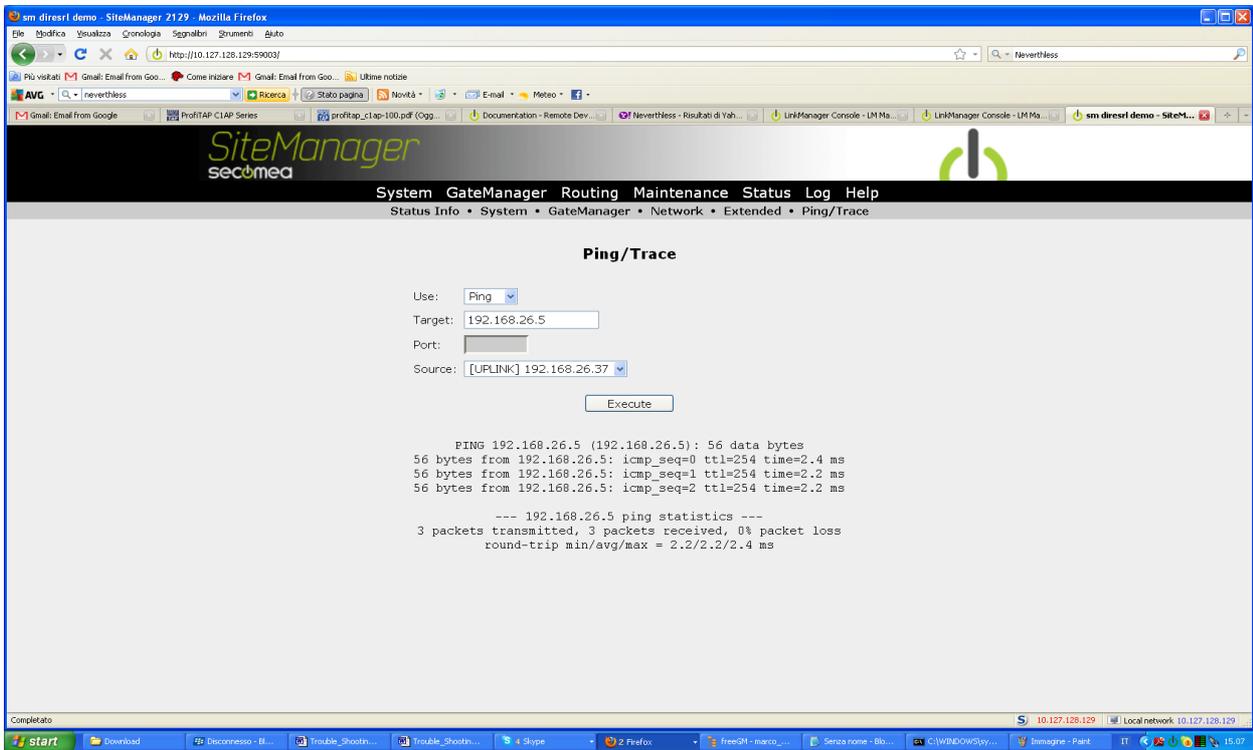
2.1.3. ping test from sitemanager

A good test is to enter the SiteManager Web GUI from the DEV side, and use the **ping** function under menu **Status** → **ping/trace** to ping the gatemanager ip address as in the picture below. If you get an answer it means that *sitemanager* can reach the *gatemanager*, at least via **ping (ICMP protocol)**.



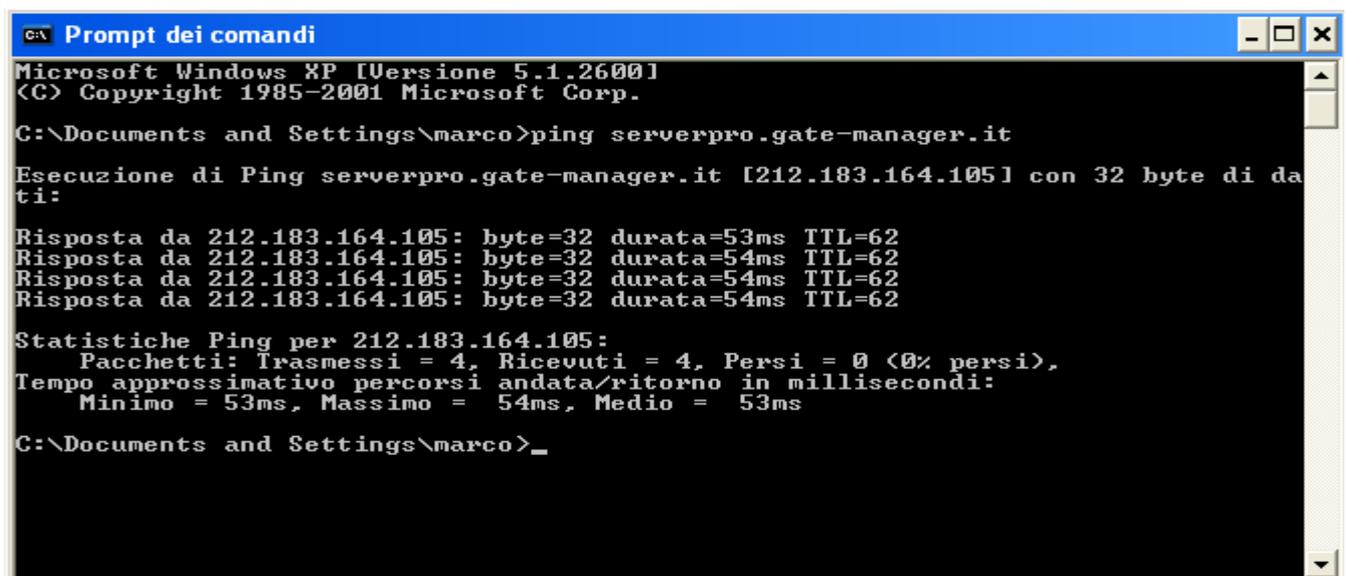
if it fails try to ping the **default gateway**. As in the next picture. **Result:** If *sitemanager* can not ping the *default gateway*, it means that **there is something wrong in the network cabling**. **So you must ask the customer IT to check the networking cabling and switching from sitemanager**. Note: If a proxy is used, try also to ping the proxy

Result: if you can reach the default gateway, but not the gatemanager it means that *sitemanager* is connected to network, but there are some **firewall /proxy blocking internet access** of sitemanager

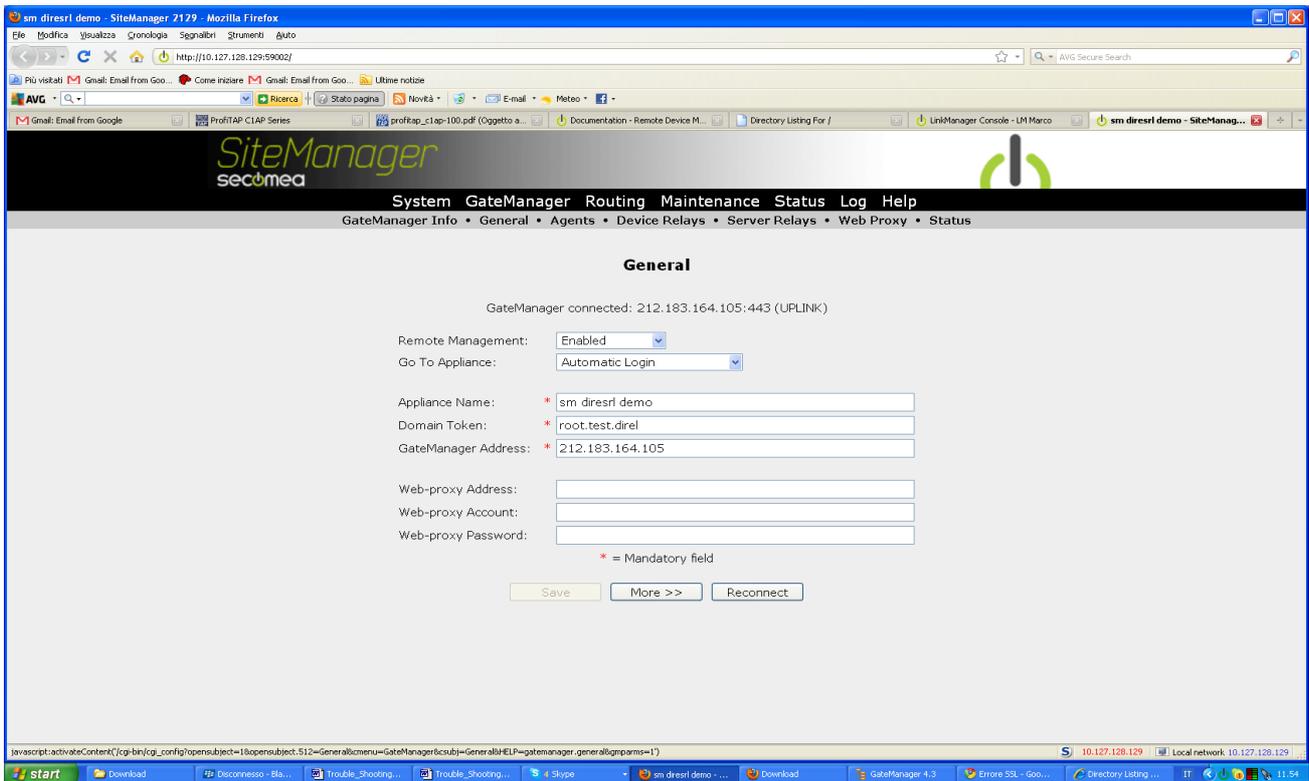


2.1.4. Ping test from a PC

It's useful to repeat the "ping test" from PC connected to the same port where uplink port of is connected. If you are using the DNS name of the *GateManager* server e.g. "**serverpro.gate-manager.it**" in the *SiteManager* configuration it may not be resolved correctly to the IP address (or DNS can not be set on the site manager), and you could try to change it to the IP address. If you don't know the ip address of the server, open a command prompt and ping the DNS name of the *GateManager*, and it will resolve the IP address (212.183.164.105):



Then, you can try to use the **gatemanager ip address** instead of the name, as shown in the picture from the page **gatemanager->general**.

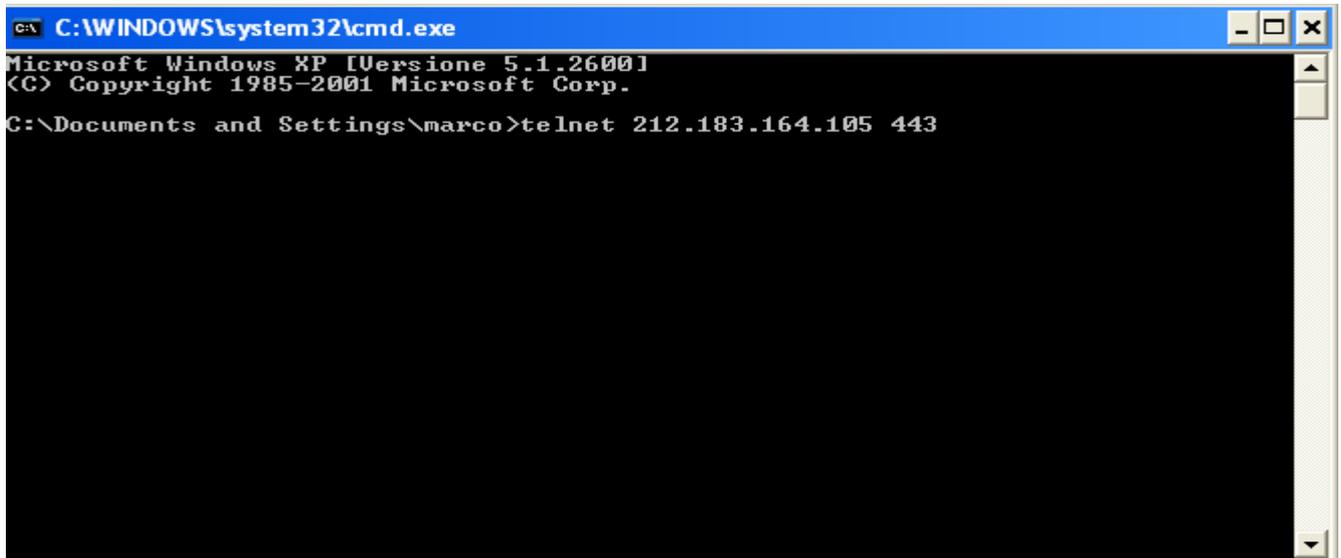


3. Telnet test from command line

In order to test internet access with a PC, please connect the PC to the same ethernet port with same cable as **sitemanager uplink port was** connected. You can disconnect temporary the *sitemanager* and connect your PC. A basic and useful test that can be done with a PC is the **telnet** test.

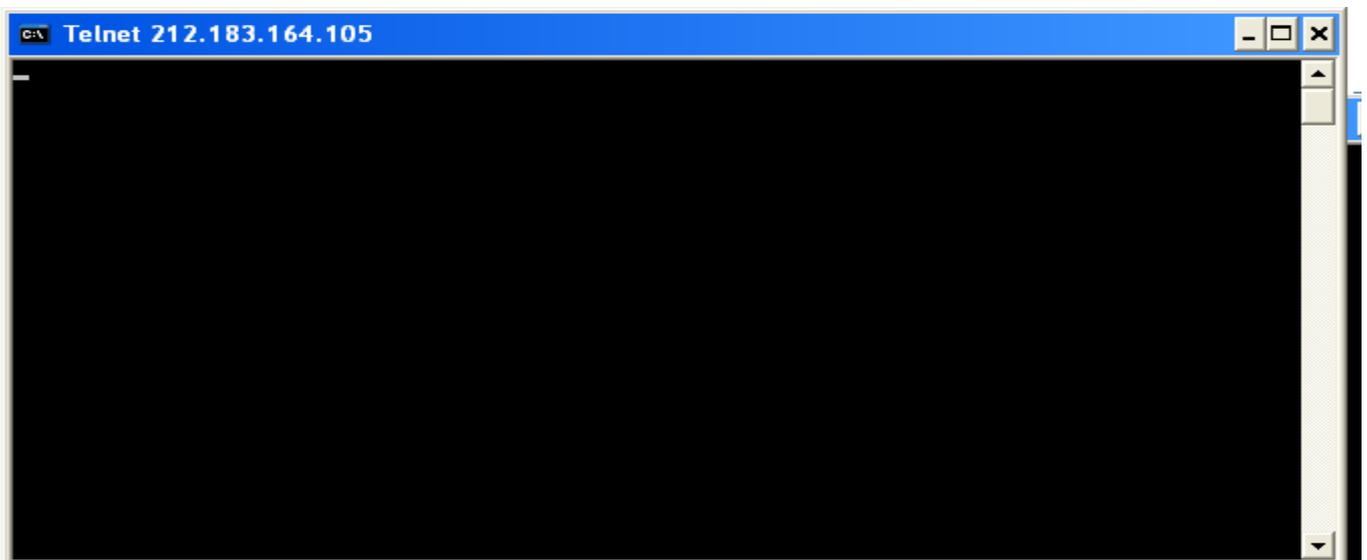
Note: on window 7 telnet is not installed by default and has to be enabled. See appendix A (page 18)

Try open a command prompt and typing the following command



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\marco>telnet 212.183.164.105 443
```

if the test is successful, you should get a black screen like the following



repeat the test 3 times using port 443, 80,11444 as above

result: if the test is successful at least with one port this means that port is open for an outgoing connection to *gatemanager server without using a proxy*. A *sitemanager* should not have any problem in connecting in this case

result: if the test with telnet is not successful in any case, it means that a proxy is in use and you have to configure it for the sitemanager. if you don't have the **proxy parameters** ask the customer IT for proxy configuration data.

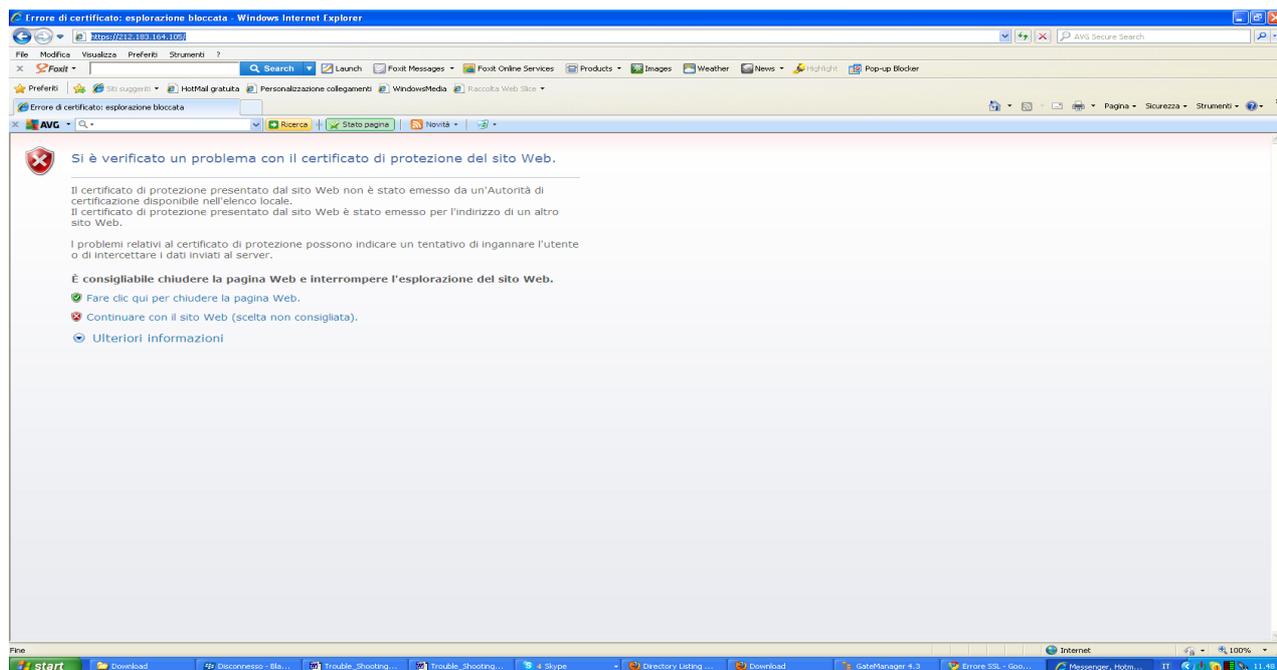
4. Test GateManager access from a PC with a browser

If the *telnet* test failed it's likely the a proxy is in use at customer site. In some case, a PC might auto-detect a proxy get automatically configured.

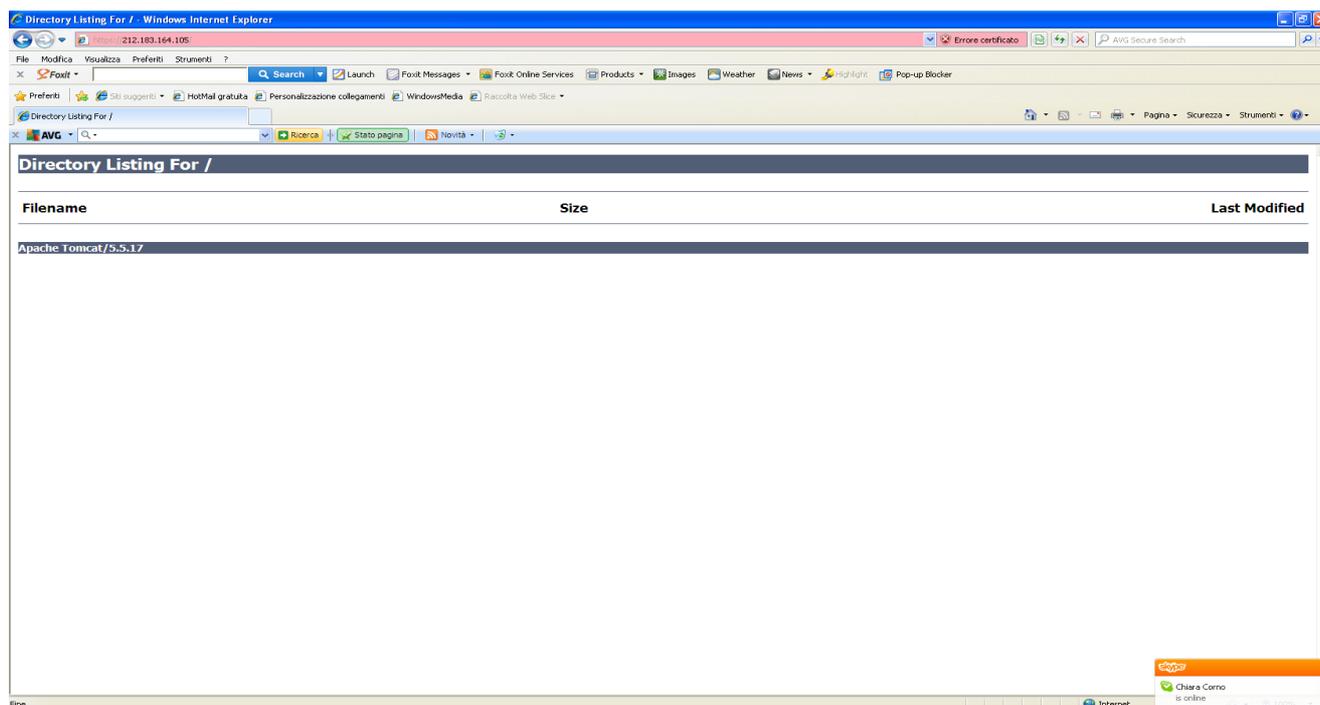
The *SiteManager* attempts to access the Internet by trying the following connection methods:

1. Port 11444 (verification: open <https://212.183.164.105:11444> in your favorite browser)
2. Port 443 with HTTPS/TLS (verification: open <https://212.183.164.105> in your favorite browser)
3. Port 80 with TLS over HTTP (verification: open <https://212.183.164.105:80> in your favorite browser)

So, open a browser and copy the link above (1,2,3) in your favorite browser. At least one should work:



Select **“Continue to this website”**, and you should get this screen:



If none of the links resulted in the above screens, it may be due to:

1. A **Web proxy is required for Internet access** and is not configured on the PC you are attempting to connect from. Typically this will be distributed from the DHCP server, but may also need to be manually configured (On MS Internet Explorer this is configured under: Tools → Internet Options → Connections → LAN Settings → Proxy server. See page 10)

The next chapter is all about situation where a proxy is used for internet access

2. **The customer firewall block the TLS session allowing only plain text HTML** access or a more complex firewall issue prevent access to gatemanager site (see page 10). in this case, you probably have to talk with customer IT and showing the issue.

If all the above is verified, and you still do not get the screen with the **Directory Listing**, you will not have much luck with the *SiteManager* either. As explained above, the only thing is to contact your IT administrator

Remember, that first step is always getting a PC connecting to internet. If the PC does not connect to internet, you would not *sitemanager* working either.

4.1. Web Proxy issues

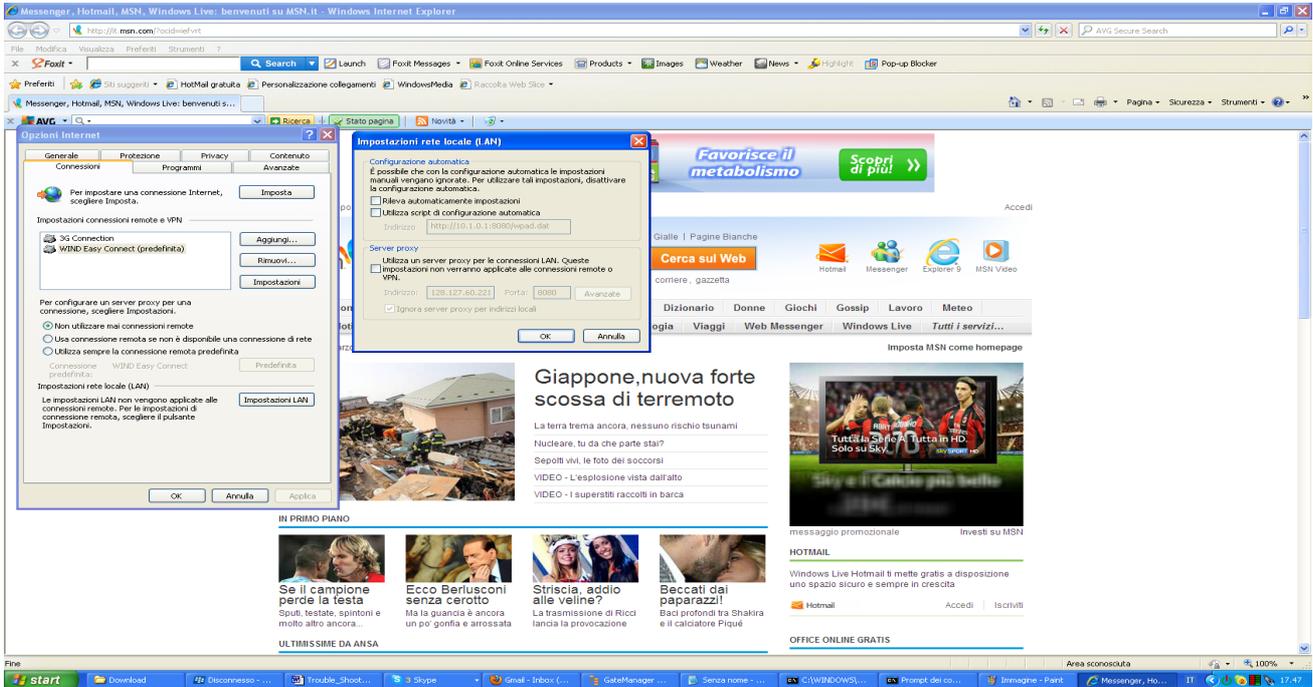
A Web proxy is often used to validate Internet access. SiteManager is designed to be able to access the Internet and the GateManager via a Web Proxy.

4.1.1. how to check if PC use a proxy for surfing internet

Open internet explorer, if it can surf the web then go to **tools->internet options->connections->lan options**. If the automatic configuration is checked and the address is filled it means the PC might detect automatically a proxy. If use server proxy is checked and address and port are specified it means the a proxy is in use. If a username/password are requested when internet explorer is opened it means the proxy requires an **authentication**, so go to the section "**web proxy not automatically configured**"

4.1.2. Web Proxy automatically configured

If the SiteManager receives its Uplink IP address via DHCP, it will automatically try to use the default gateway as a web proxy including WPAD as the pc does. So it automatically extracts the information from the PAC file distributed from the DHCP server (This "Auto Web proxy" functionality is supported from SiteManager firmware vxx_10405)



4.1.3. Web Proxy NOT automatically configured

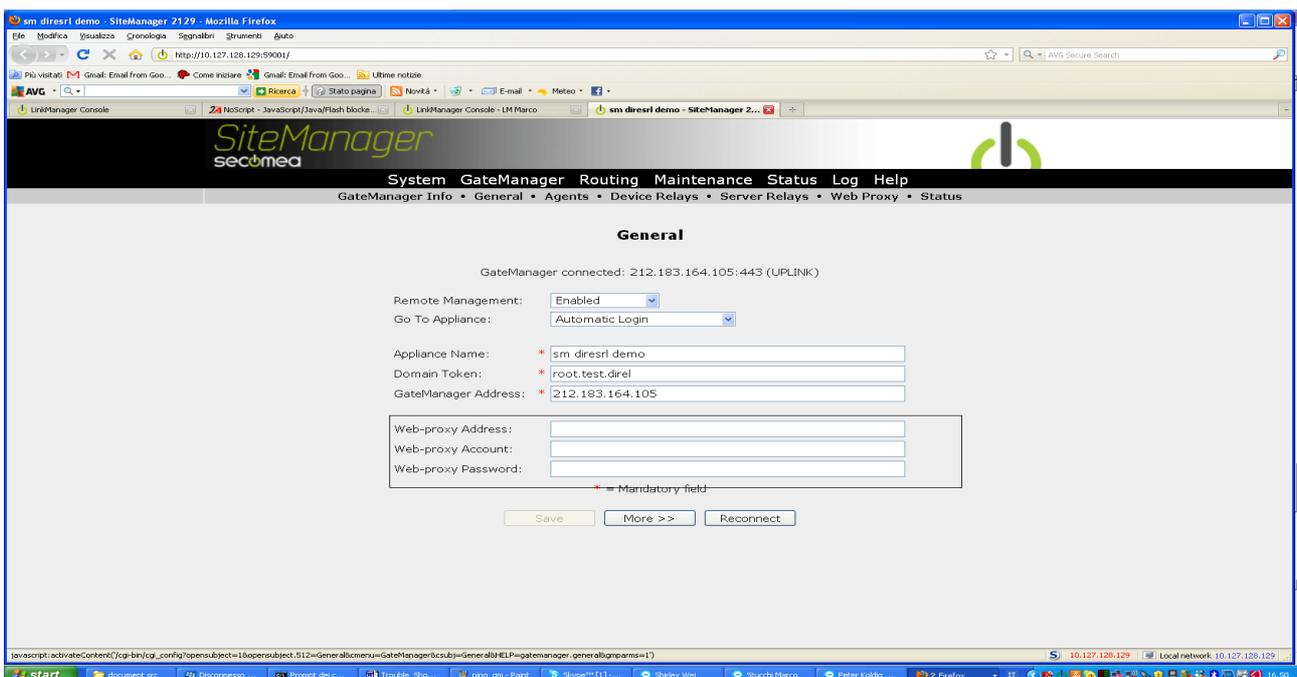
Two scenarios exist that require manual configuration of the Web Proxy into the SiteManager configuration menu:

1. If the **SiteManager does receive its IP address via DHCP**, but the Web Proxy require a **username and password** to be entered. If you have been asked for *username/password* the first time you open a browser you are in this case

note: there are a few case in which proxy authentication is done together with windows logon. This is called "integrated authentication or NTLM authentication". (see page 13)

2. If the **SiteManager does not receive its Uplink IP address via DHCP**, but is statically configured, the SiteManager will not detect the web proxy settings automatically, so the settings has to be entered manually

These settings therefore have to be entered manually into the SM GUI under GateManager → General



You may need to ask the local IT administrator for these values:

1. Proxy ip address :port es. 192.168.0.1:8080

Note: insert the ip address and not the name. .The port is usually 8080 but it can different es. 3128)

2. Username

Note: the username might include the domain **es. Ufficio\user**. In this case insert the full **username** has to be insterted

3. Password (the customer will insert the password or they might create a dedicate account for site manager).

4.

5. PC connect to internet but SiteManager does not

If the *browser* test from PC was successful but *sitemanager* can not connect to internet it means that you fall on some advanced case. It's a good idea, trying to connect to the same port where *sitemanager* is connected to verify if internet access is available or not for a PC. A good test is **skype**, if skype could connect generally *sitemanager* does too. Nevertheless there case in which a laptop can connect and *sitemanager* does not. The section describe the most common case and the reasons for that

5.1.1. Web proxy TLS issue

Even if port 443 is allowed, the company firewall might be blocking for TLS access (only allow plain text html). You may need to get special rules applied in the firewall for your PC; either approval on IP address, MAC address, the PC's DNS name, or the PC may need to be trusted on a local MS Directory Services server.

Result: ask customer IT to allow TLS traffic from sitemanager

5.1.2. NTLM proxy

NTLM is an old and legacy system that even microsoft doesn't recommend anymore. Even if, if you could still find it in the ms environment. (i.e. typically where ISA server is used)

Please note the NTLM proxy is not supported and only basic authentication can be used with *sitemanager*

*In this case, it's easier to get an ip address that bypass a proxy for reaching a single ip address of gatemanager (212.183.164.105), rather than asking to modify the rule of the proxy or the kind of authentication. Always remember, the sitemanager **doesn't need to access the whole internet but only the Gatemanager ip address (212.183.164.105).***

So, it's generally more reasonable to ask the IT **an exception for the sitemanager ip address for reaching a single ip address.** This is a good choice cause it's very secure for the customer and it's enough for the *sitemanager*.

This is explained by the module "internet prerequierelements" that you should already have. If not, you can find it on www.gate-manager.it in the "application notes section"

5.1.3. Content filtering

Please also note, **that some proxy applies content filtering policy that means they do a strict selection of allowed web site that can be reached via proxy.**

skype is a good test. If skype work, there are good chance that sitemanager could work too.

If a strict content filtering is applied, *skype* on normal PC would not connect

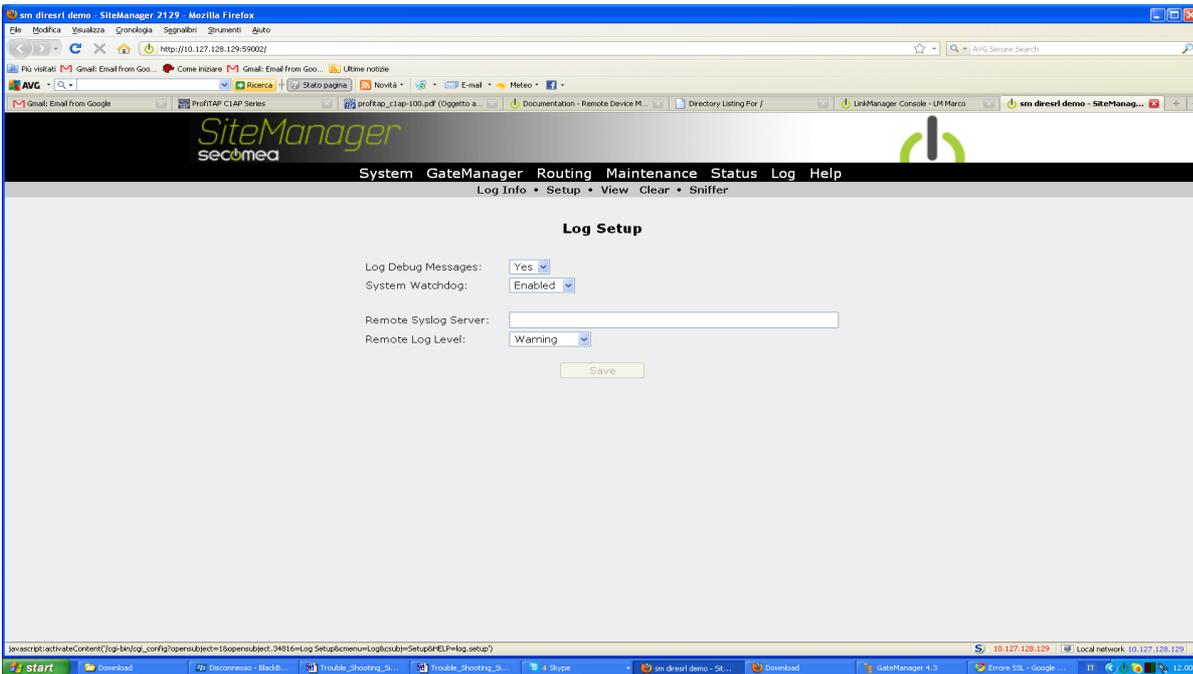
6. summary table of possible cases

If you have all the test explained in the previous section, you should be now able to follow this table and see in which case you are. The provided information are useful for explaining customer IT issue and for showing what is working and what is not working

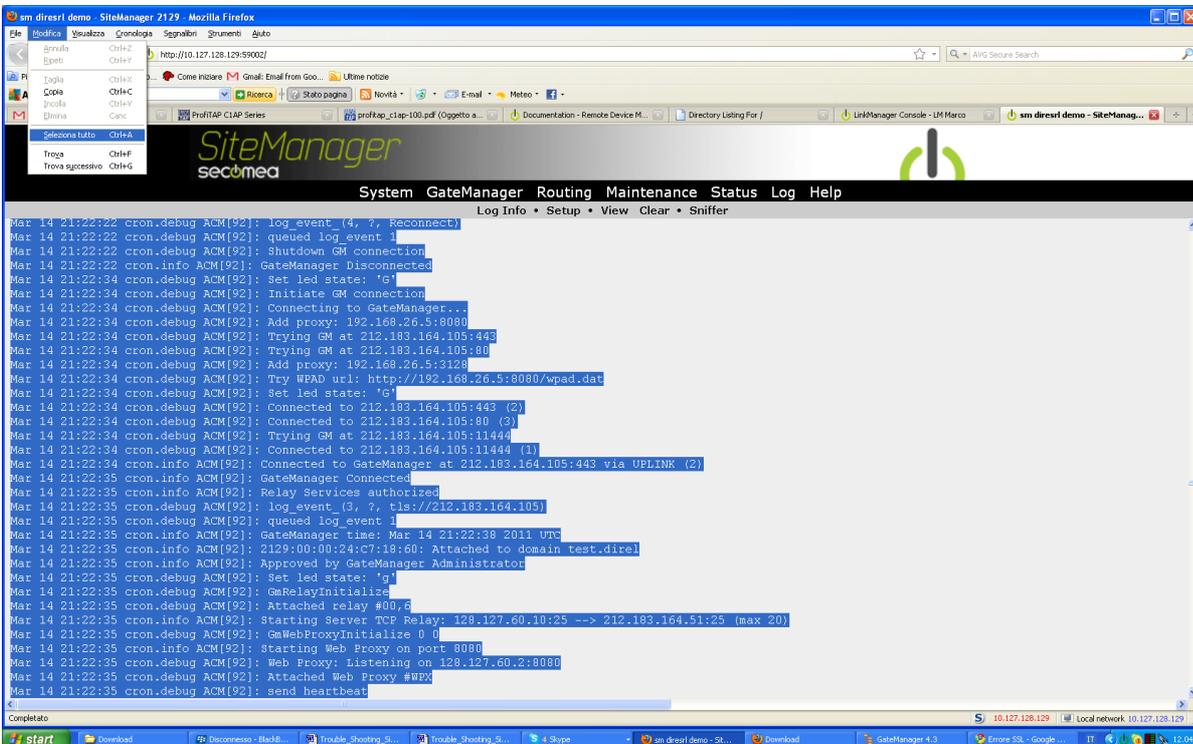
	Result from SM	result from PC	What do to/result
Ping from SiteManger to default gateway (see page 4)	It Work		Network cabling is correct and a local ip address has been assigned, <i>sitemanager</i> can connect to local network.
	It doesn't work		Check if the uplink ip address is correct or if DHCP has assigned one. Check also for the network cabling. <i>sitemanager</i> should be always able to reach at least the default <i>gateway/proxy</i> .
Ping test to gatemanager (see page 4)	It doesn't work	It doesn't work	PC can't connect to <i>gatemanager</i> . ask customer IT to allow PC to reach <i>gatemanager</i> and get internet access
	It doesn't work	It work	Network cabling is correct, <i>sitemanager</i> can connect local net but it can't connect outside while PC does. A proxy might be used and not be configured customer (see page 10) or customer firewall might block the ping from <i>sitemanager</i> . Ask customer IT for proxy parameters and to allow <i>sitemanager</i> to connect to <i>gatemanager</i> ip address.
	It work	It work	Network cabling is correct, <i>sitemanager</i> can connect to local net and it can ping GM. You fall in the advanced case (see page 13). Ask customer to allow <i>sitemanager</i> to connect to <i>gatemanager</i> ip address
telnet test (see page 7)	It Work from PC on at least on port (80,443,11444)		PC can reach the <i>gatemanager</i> ip address, without using a proxy. Site manager should work well in this situation
	It doesn't work		A proxy might be used. Ask customer for proxy parameters and configure it for <i>sitemanager</i> . See page 10 or to allow his firewall connection to <i>gatemanager</i> ip address
Web browser test (see page9)	It Work from PC		<i>Sitemanager</i> might not detect proxy automatically (See page 10to check if a proxy is used). Check with IT if NTLM (see page 13) proxy it is used or if firewall might blocks the <i>sitemanager</i> TLS connection (see page 13) or if content filtering is applied (see page 13)
	It doesn't work		customer firewall block the TLS connection to <i>gatemanager</i> . You must ask customer to allow internet access to <i>gatemanager</i> ip address
Skype test		It doesn't work	It's likely the PC can't access internet
	It works		SM would likelywork in this case

6.1. How to get more info for technical support

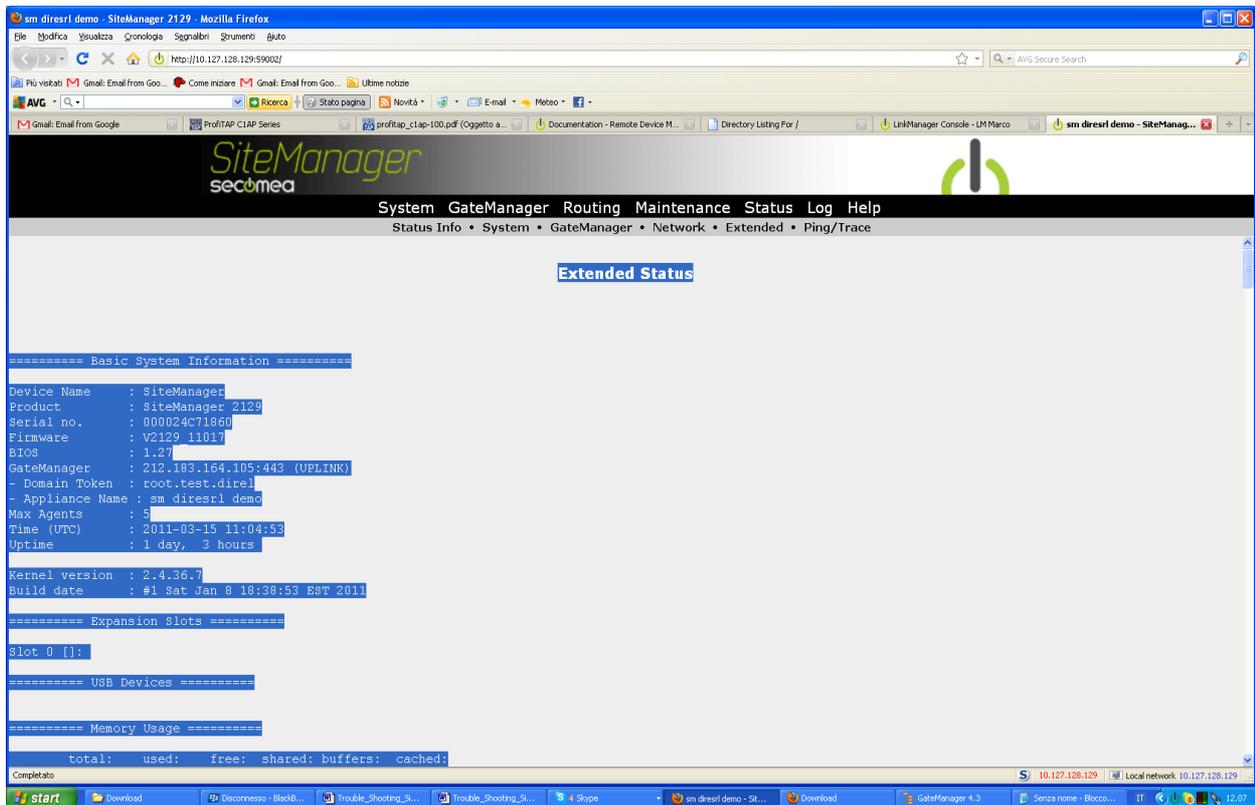
If none of the above test helped, it's a good idea to collect more info. In order to get more info, it's useful to enable the log in the *sitemanager* as shown in this picture. Enter the **log** section than choose **setup**, and set **yes**



then, after you have done some connection tests enter the **log** section again than choose **view** as in the picture below. **Select all** and **copy** in a text file and send it to tecnico@gate-manager.it as attachment together with a support request for "internet connection issue with sitemanager"



Copy also the data in the page **status**-and then choose **extended status** as in the the next picture



Save **all the data** in the page with select **all in a text file** and send it the file to **gatemanager** technical support at tecnico@gate-manager.it

Don't forget to add the result of all tests you have previously done (ping, telnet, browser)

6.2. Final things to Check

If the SiteManager is configured correctly, check the following further thing in the network.

These things will typically involve the local IT administrator to verify, and will definitely require this person to change:

1. Does the firewall require an exception for the source IP of an unknown IP device to be entered into the firewall in order to access the Internet?

Solution: ask the IT manager of the customer.

2. Does the firewall require an exception for the MAC address of a device to be entered in the firewall in order to access the Internet?
Note that the *Uplink MAC address* is typically one (or two) higher than the DEV1 MAC address, which is also the *SiteManager serial number*. So if the Appliance Launcher detects e.g. 00:00:24:00:97:6C, the Uplink MAC address will be 00:00:24:00:97:6D for 2129 (two ports) and . 00:00:24:00:97:6D for 2134 (three ports). You can double check the MAC address by checking the networks DHCP lease table, or ping Uplink and check the ARP cache.

Note: **In some company, the DHCP may apply a filter on MAC address base and every foreign device has to be approved**

Solution: ask the IT manager of the customer for adding the MAC of *sitemanager uplink port*

3. Does the *firewall or Proxy* require the DNS of a device to be trusted (e.g. checked by reverse lookup)? Since SiteManager is not a Windows PC, a special exception may need to be made.

Solution: ask the IT manager of the customer to add the needed exception

4. Does the firewall require an exception for the destination IP that a device tries to access to be entered into the firewall? Enter the IP address of the GateManager server.

Solution: ask the IT manager of the customer to add the needed exception

5. Does the firewall require using DNS names that resolves locally?

In that case the DNS name of the GateManager must be applied to the DNS server (e.g. **“serverpro.gate-manager.it”**, must be applied with its IP address 212.183.164.105). Subsequently it must be ensured that the SiteManager is configured with the IP of the DNS server. This will typically automatically be distributed via DHCP, but must manually be entered for the Uplink interface if the SiteManager has a fixed IP.

Solution: ask the IT manager of the customer

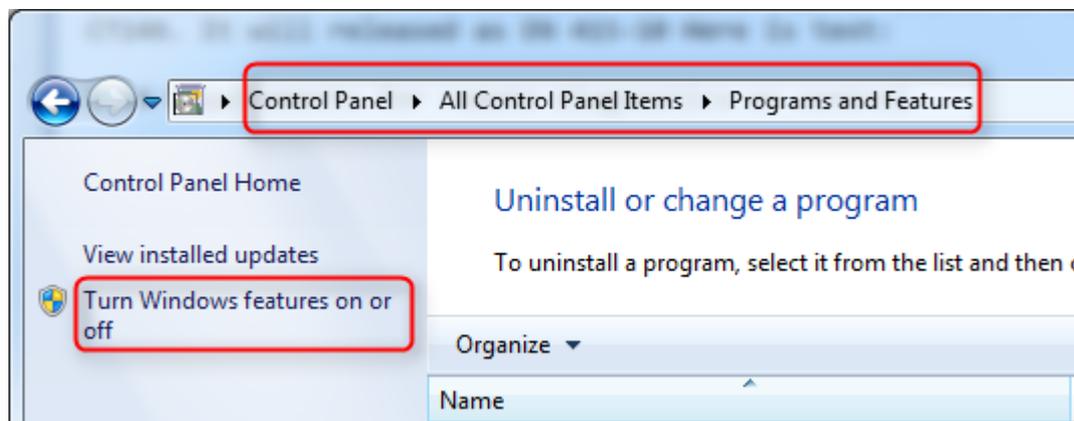
6. If the firewall is configured to NOT tolerate "rekey" on a TLS session for which it has not seen the original session be created, the SiteManager will possibly be rejected. This is due to the SiteManager using re-keying for starting the connection, and subsequently the firewall will not be able to use a cached session ID. You may need to add some exception in the firewall to allow the SiteManager to bypass this check.

Solution: ask the IT manager of the customer

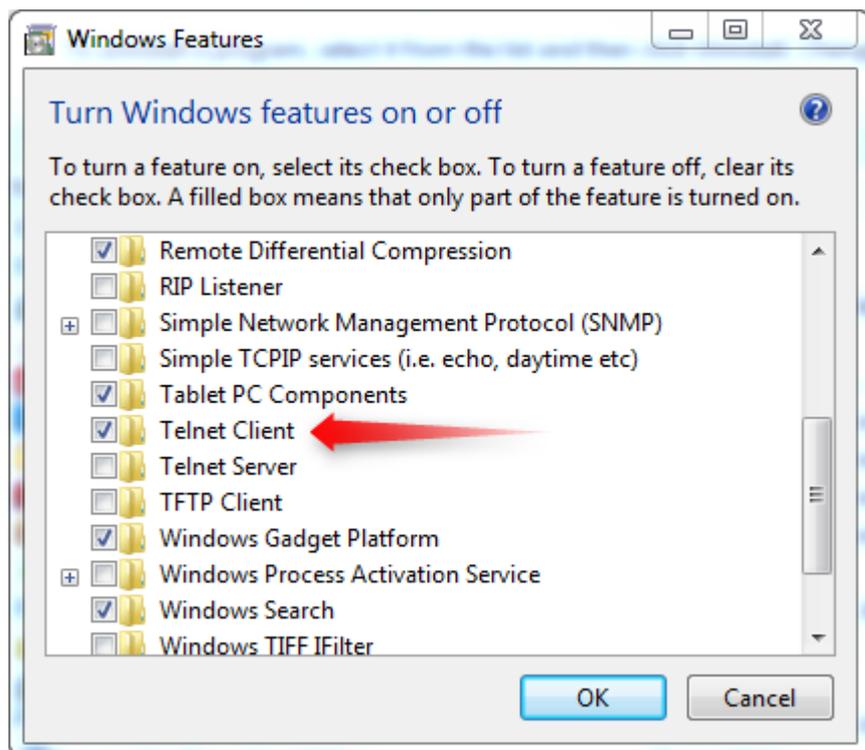
7. Appendix A: how to enable telnet on window 7

Telnet client is not default enabled in Windows7.

To enable it, enter control panel and Programs and Features, and select "Turn Windows features on or off"



Check mark the Telnet Client and press OK.



Telnet is now available in a command prompt

8. Notices

Publication and copyright

© **Copyright Secomea A/S 2011.** All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

SiteManger™ and GateManager™ are a trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.