Trouble Shooting
SiteManager to GateManager access via a corporate Intranet

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: 2.0, June 2013

secomea

Table of Contents

1. Test GateManager access from a PC 3

2. PC can connect, but SiteManager cannot 5

2.1. Basic issues 5
2.1.1. Ethernet cables not connected correctly 5
2.1.2. Uplink1 IP address configuration issues 5
2.1.3. DNS issue 5

2.2. Web-Proxy issues 6

2.3. Other things to Check 7

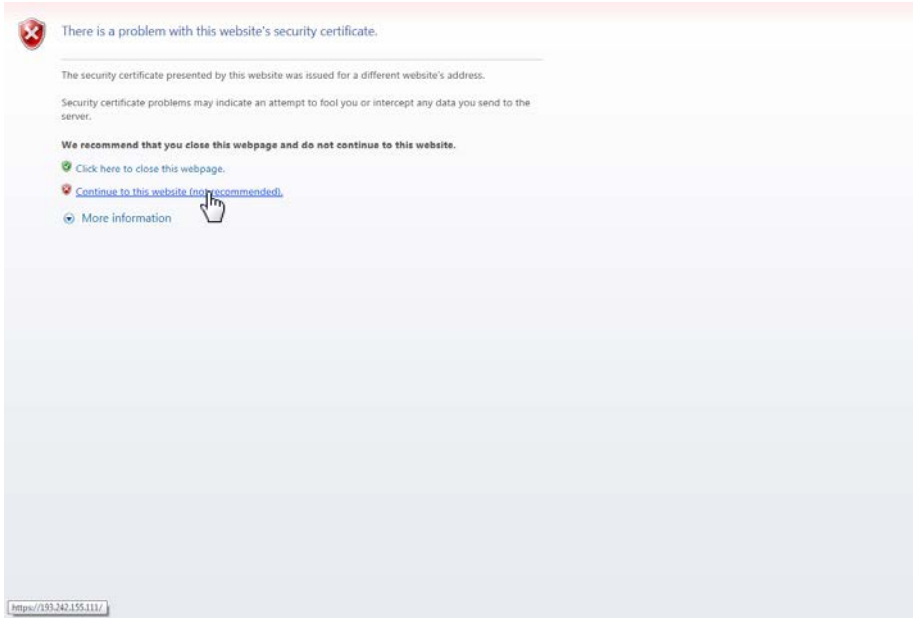
Notices 9

1. Test GateManager access from a PC

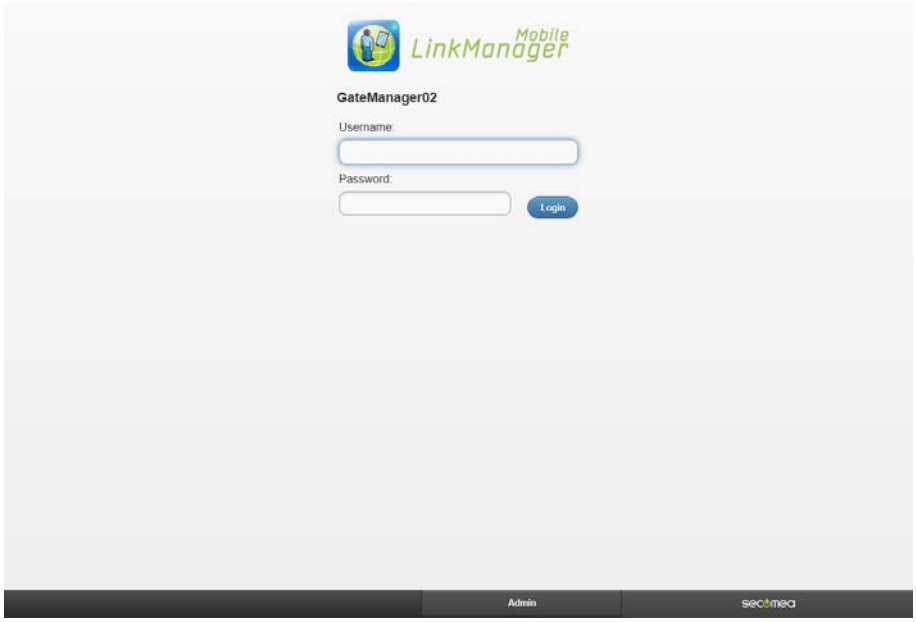
The SiteManager attempts to access the Internet by trying the following connection methods one by one from its Uplink port:

1. Port 11444 (verification: https://193.242.155.112:11444)
2. Port 443 with HTTPS/TLS (verification: https://193.242.155.112)
3. Port 80 with TLS over HTTP (verification: https://193.242.155.112:80)
4. TLS via Web Proxy

By clicking, or entering the above verification links in a web browser, at least one of the links should give you this result:



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 firewall is blocking for TLS access and only allows plain text/html (i.e. http://.. is supported while https://.. is not). You may need to get special rules applied in the firewall for your PC. This may be solved by approval of the IP address, the MAC address, the PC's DNS name, or the PC itself on a local MS Directory Services server.
2. 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.)

If all the above is verified, and you still do not get the LinkManager Mobile login screen on your PC, you will not have much luck with the SiteManager either. You should then contact your IT administrator.

2. PC can connect, but SiteManager cannot

2.1. Basic issues

2.1.1. Ethernet cables not connected correctly

Regardless how obvious this may sound, it is not un-common that the cables are not connected correctly. Check that the network, through which the SiteManager should obtain Internet access, is connected to the SiteManager Uplink port, and also check that there is link on the Ethernet port (the green /yellow LEDs on the Ethernet connector itself are lit)

2.1.2. Uplink1 IP address configuration issues

Check that the SiteManager has an IP address matching the network through which it should obtain Internet access.

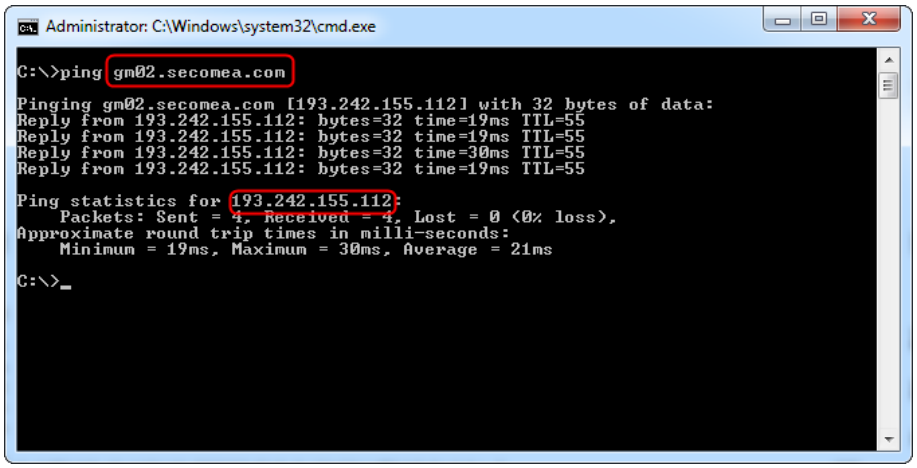
If the Uplink1 IP address is DHCP assigned, check that an address has actually been assigned. Connect a PC to the DEV network and use the Secomea Appliance Launcher to search for the SiteManager and verify the assigned Uplink IP address. Alternatively check the DHCP server's lease table. Try to ping this IP address from a PC on the same network.

If the Uplink1 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 defined to be the router that provides Internet access. Try to ping the IP address from a PC on the same network. A good test is to access the SiteManager Web GUI from the Uplink1 og DEV side (specify https:// in your web browser in front of the IP address. Default login/password is admin/admin), and use the ping function under the SiteManager menu **Status → ping/trace** to ping the Internet Gateway).

2.1.3. DNS issue

If you are using the DNS name of the GateManager server e.g. "gm02.secomea.com" in the SiteManager configuration it may not be resolved correctly to the IP address, and you should change it to the IP address (Menu GateManager → General)

Open a command prompt and ping the DNS name of the GateManager, and it will resolve the IP address (193.242.155.112):



The SiteManager does support using a DNS name as GateManager server target, but it is recommend using the IP address in order not to be dependent on a DNS server in the network.

2.2. Web-Proxy issues

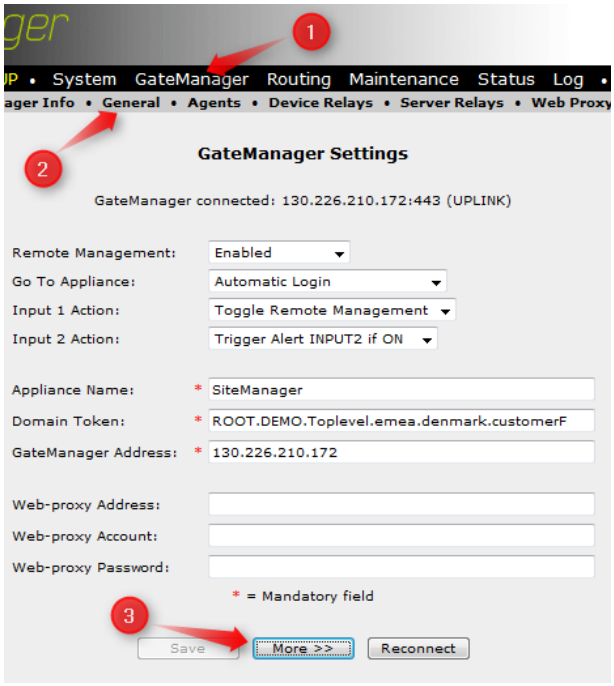
A Web-Proxy is often used to validate Internet access. SiteManager is designed to be able to access the Internet and the GateManager via a Web-Proxy.

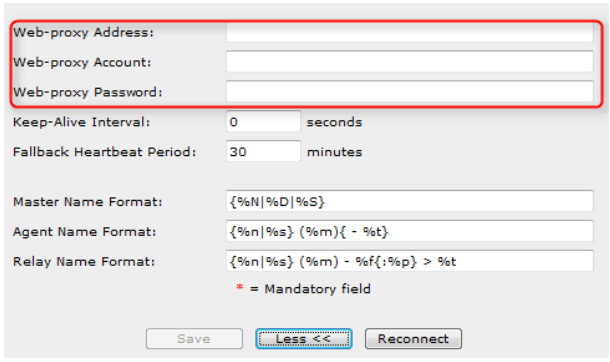
If the SiteManager receives its Uplink IP address via DHCP, it will automatically regard the default gateway as a web proxy including Web-Proxy Auto-Detect (WPAD). So it automatically extracts the information from the PAC file distributed from the DHCP server.

Two scenarios exist, however, 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 requires a password to be entered.
2. If the SiteManager does not receive its Uplink IP address via DHCP (but is statically configured), the SiteManager will not be able to detect the Web-Proxy settings automatically.

These settings therefore have to be entered manually into the SiteManager GUI under **GateManager → General → More>>**





Consult the online help of the SiteManager for detailed info about configuring the Web-Proxy settings.

For instance note that you can manually define the URL path to the WPAD file in the Web-proxy address field, which is useful if you do not receive Web-Proxy info from a DHCP server.

Also if you are using a **NTLM-based web-proxy**, you can enter the account into the Web-Proxy Account field in the format "DOMAIN\USER".

NOTE: You may experience that LinkManager does get GateManager access despite of the NTLM account not being configured in the LinkManager. This may be due to the PC itself already being approved by the proxy.

2.3. Other things to Check

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

These things will typically involve the local IT administration to verify, and will definitely require a person from the IT department 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?

   If so, enter the IP address of the SiteManager Uplink1 port.

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?

   If, so enter the MAC address of the SiteManager's Uplink1 port. Note that the Uplink1 MAC address is typically one higher than the DEV1 MAC address, which is also the SiteManager serial number. So if the Appliance Launcher detects e.g. 00:05:B6:00:97:6**C** on the DEV port, the Uplink MAC address will be 00:05:B6:00:97:6**D**. You can double check the MAC address by checking the networks DHCP lease table, or ping Uplink1 and check the ARP cache.

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.

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.

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. "gm02.secomea.com", and specified with its IP address 193.242.155.112). Subsequently it must be ensured that the SiteManager is configured with the IP address of the DNS server. This will typically automatically be distributed via DHCP, but must manually be entered for the Uplink1 interface if it is configured with a fixed IP address.

6. NOTE: The following is not a problem for GateManager 5, ONLY SiteManagers connecting to GateManager 4x servers:

   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 may be rejected. This is due to the SiteManager using re-keying for starting the connection when connecting to a GateManager 4x server, and subsequently the firewall will not be able to use a cached session

ID.

You can also verify the log messages on the firewall (if enabled). E.g. on a Fortinet firewall the message would say ""*The SSL session was blocked because the session ID was unknown*".

You would need to add some exception in the firewall to allow the SiteManager to bypass this check.

Notices

Publication and copyright

Trademarks

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.