

New in Release: Secomea Release 7.4

- This document shows the changes from 7.3 to current 7.4.

Version: 1.2, 2017

Table of Contents

Change log	3
1. Release 7.4	3
2. GateManager	4
2.1. SiteManager Embedded with EWF	4
2.2. Using Wildcard Certificates	4
2.3. Enforce GTA secret	5
2.4. Username/Password in USB configuration	6
2.5. Configuring static IP without a DHCP server	6
2.6. Log - extended target information	6
2.7. Basic Admin and Usage Tab	7
2.8. Raspberry Pie and BeagleBone added to GM	7
3. SiteManager Hardware	8
3.1. SiteManager and GateManager shows modem IMEI	8
4. SiteManager Embedded	10
4.1. Support for external USB modem	10
4.2. Support for WiFi Adapter ONLY setup	10
4.3. User Mode support (Linux)	10
4.4. Separate status and log folders	11
5. SiteManager General	12
5.1. SM GateManager Settings page	12
5.2. Agents updates and additions	12
6. LinkManager	13
6.1. Spectre/Meltdown fix for 64-bit Windows 8 and 10	13
7. LinkManager Mobile	14
8. License Portal	14
9. Advanced Tech topics	15
9.1. LMM API: Incl. IMEI/IMSI in Appliance Details	15
9.2. LMM API: Serial number instead of Appliance ID	15
10. Documentation	16

Change log

Version	Change log
1.0	Initial version
1.1	Added main topics
1.2	Finalized for public release

1. Release 7.4

Information

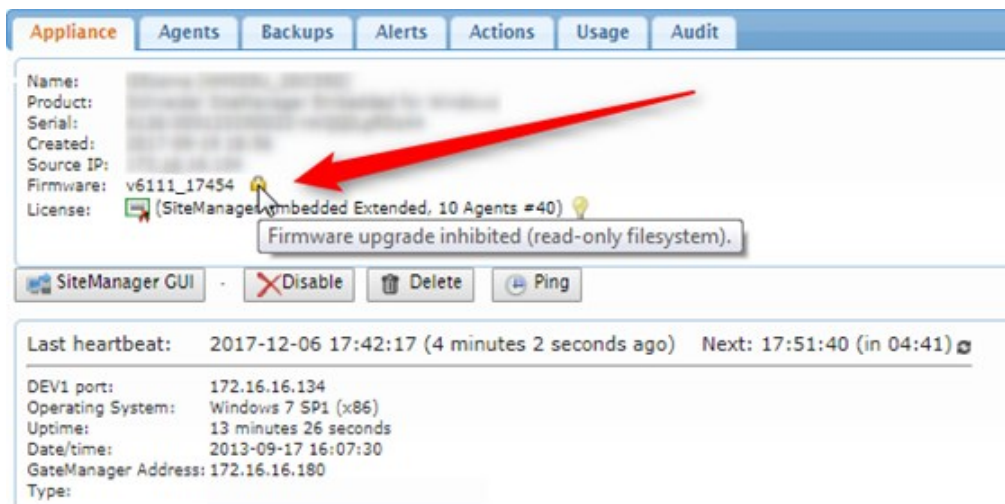
- Quick description of the new features and changes in product.
- Product: SM, SME, LM and GM
- **Current firmware build 7.4.18052 (LinkManager build 18025)**

2. GateManager

New in GateManager updates and fixes.

2.1. SiteManager Embedded with EWF

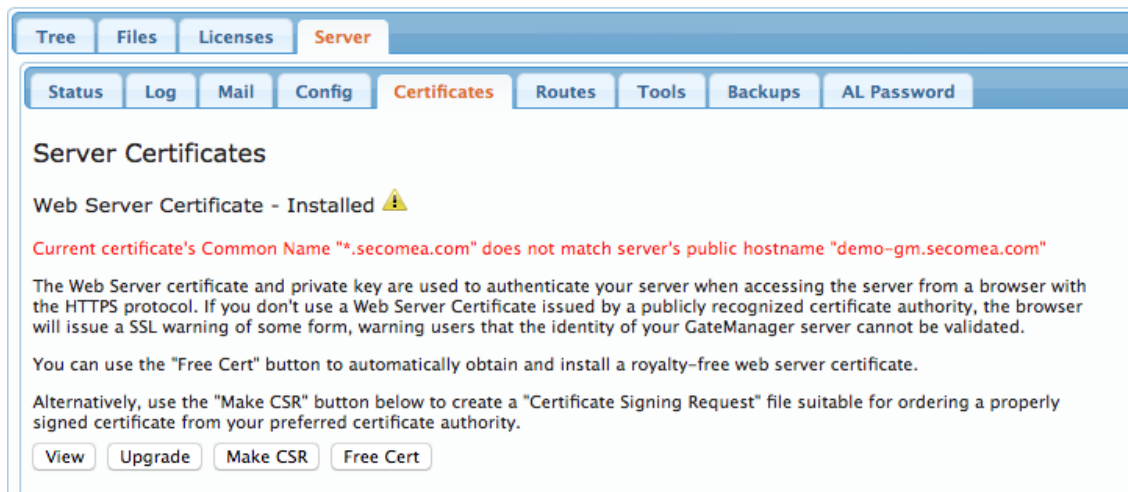
EWF (Enhanced Write Filter) has been supported by SME for a while, from 7.4 you will also be able to see on the GateManager Portal if the SiteManager Embedded has EWF protection enabled. If it is enabled, it will **not** be able up- or down-grade the firmware, just like configuration changes will not be restored after a device reboot.



The screenshot shows the GateManager portal interface. At the top, there are tabs for Appliance, Agents, Backups, Alerts, Actions, Usage, and Audit. Below the tabs, the 'Appliance' tab is selected, displaying details for a device. The details include Name, Product, Serial, Created, Source IP, Firmware (v6111_17454), and License (SiteManager Embedded Extended, 10 Agents #40). A red arrow points to a warning icon next to the firmware version. Below the details, there are buttons for SiteManager GUI, Disable, Delete, and Ping. At the bottom, there is a section for heartbeat and system information, including DEV1 port, Operating System (Windows 7 SP1 (x86)), Uptime, Date/time, GateManager Address, and Type.

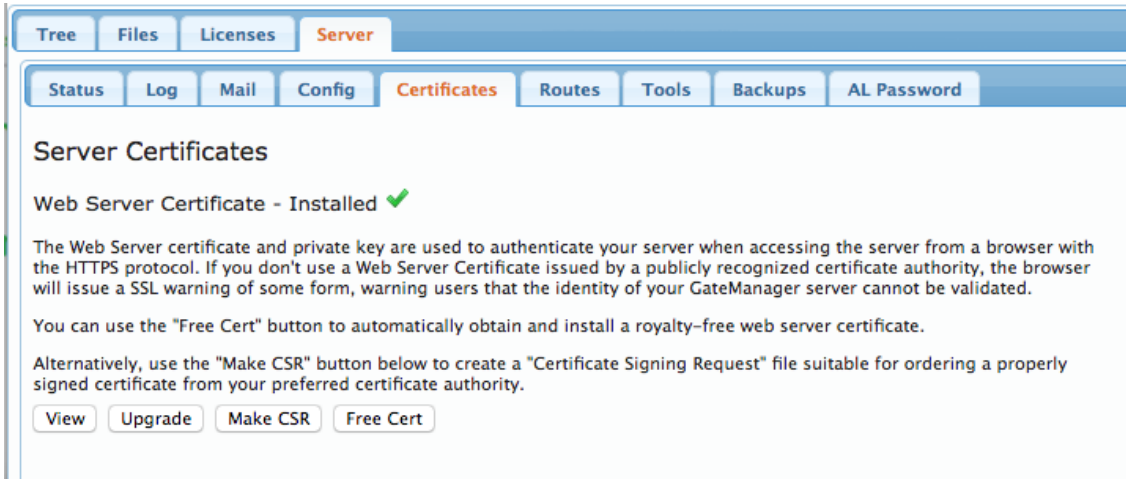
2.2. Using Wildcard Certificates

Previously a wildcard web certificate would be detected as not matching the hostname. That was only a false positive, as the certificate was installed correctly anyway.



The screenshot shows the GateManager portal interface for the 'Server' section. The 'Certificates' tab is selected, displaying the 'Server Certificates' page. The page shows a 'Web Server Certificate - Installed' with a warning icon. Below this, there is a red warning message: 'Current certificate's Common Name "*.secomea.com" does not match server's public hostname "demo-gm.secomea.com"'. The text explains that the Web Server certificate and private key are used to authenticate the server when accessed from a browser with the HTTPS protocol. It notes that if a publicly recognized certificate authority is not used, the browser will issue an SSL warning. There are buttons for 'View', 'Upgrade', 'Make CSR', and 'Free Cert' at the bottom.

Release 7.4 will accept the wildcard certificate without warnings.



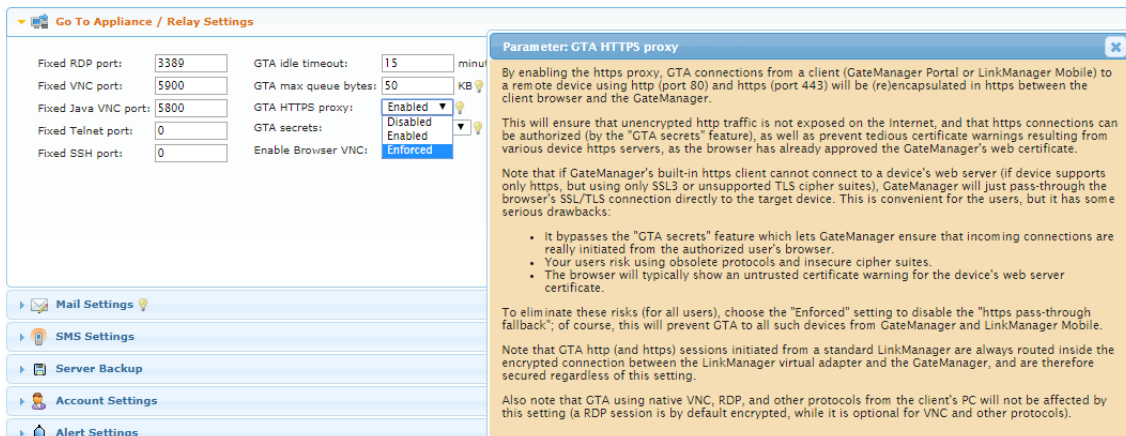
2.3. Enforce GTA secret

In Release 7.4 we have added an option to “Enforce GTA secret”. If set to “Enforced” any attempt to make a GTA to a remote device that do not support the GateManager minimum HTTPS-proxy level will be rejected.

Supported ciphers in the GateManager HTTPS -> HTTPS proxy:

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

The light bulb text below provides more details:

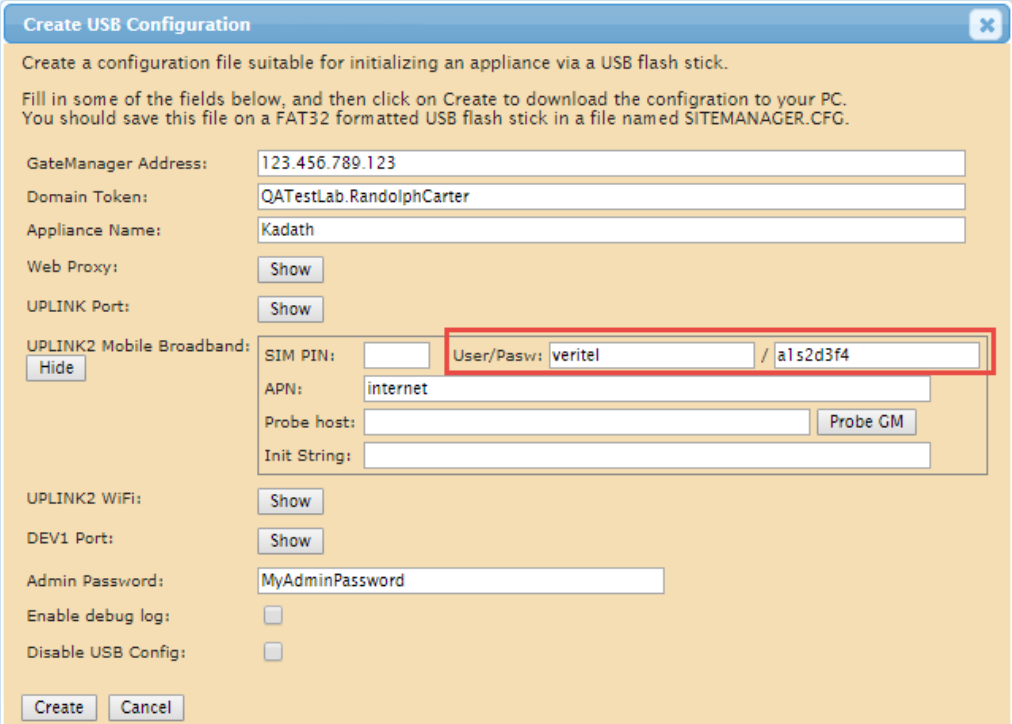


The above graphic shows the new “Enforced GTA HTTPS proxy” option, where no GTA will be possible to older WEB server interfaces using obsolete encryption protocols.

2.4. Username/Password in USB configuration

A feature has been added to the USB Configuration in the GateManager.

Clicking the USB icon () in the “Domain Overview” will produce the USB Configuration form below.



Here you can now add a username and password to the Mobile configuration.

In some countries, like Japan, they typically do not use SIM PIN code, but rather username/password. Also, it is possible to use the same username/password for multiple SIM's. Which makes the addition to the USB configuration helpful in these countries.

2.5. Configuring static IP without a DHCP server

When installing a new 9250 GateManager, it can be configured with a DHCP or Static IP address. But if it was installed without a DHCP server present, the NIC driver would announce that it was missing an IP address too often.

This could make it troublesome to enter the static IP address.

In version 7.4 the logging will be more limited, and there are no issues with entering the Static IP Address.

2.6. Log - extended target information

On the GateManager, some log information can be difficult to troubleshoot when there is no indication of who is generating the error.

When a relay tries to access an invalid target like:

```
Oct 23 07:25:17 gm78 ap-126: Unknown target name: Mail
```

It would be useful to know who caused the error.

In version 7.4 the appliance serial is included in the syslog messages. This applies to datagram, relay and webproxy target names:

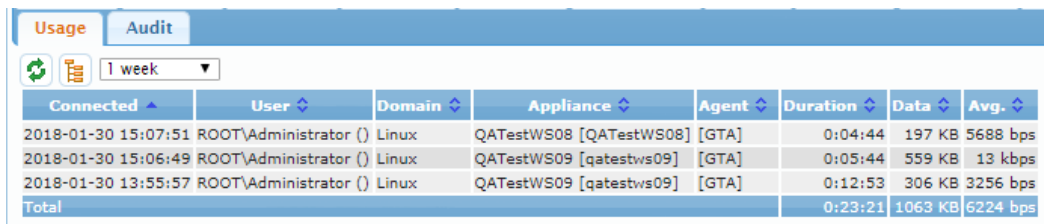
```
<190>ap-14: Unknown relay target Mail from 00C0A2555575#00
```

Then the target can easily be searched from the GUI.

2.7. Basic Admin and Usage Tab

In release 7.3, only a Domain Administrator could view the “Usage” tab on a domain.

From release 7.4, also Basic Administrators will be able to view this tab.



Connected	User	Domain	Appliance	Agent	Duration	Data	Avg.
2018-01-30 15:07:51	ROOT\Administrator ()	Linux	QATestWS08 [QATestWS08]	[GTA]	0:04:44	197 KB	5688 bps
2018-01-30 15:06:49	ROOT\Administrator ()	Linux	QATestWS09 [qatestws09]	[GTA]	0:05:44	559 KB	13 kbps
2018-01-30 13:55:57	ROOT\Administrator ()	Linux	QATestWS09 [qatestws09]	[GTA]	0:12:53	306 KB	3256 bps
Total					0:23:21	1063 KB	6224 bps

2.8. Raspberry Pie and BeagleBone added to GM

The GateManager now has support for Raspberry Pie (v6122) and BeagleBone (v6123) SiteManager Embedded in the GateManager GUI (Alerts, actions, etc.).

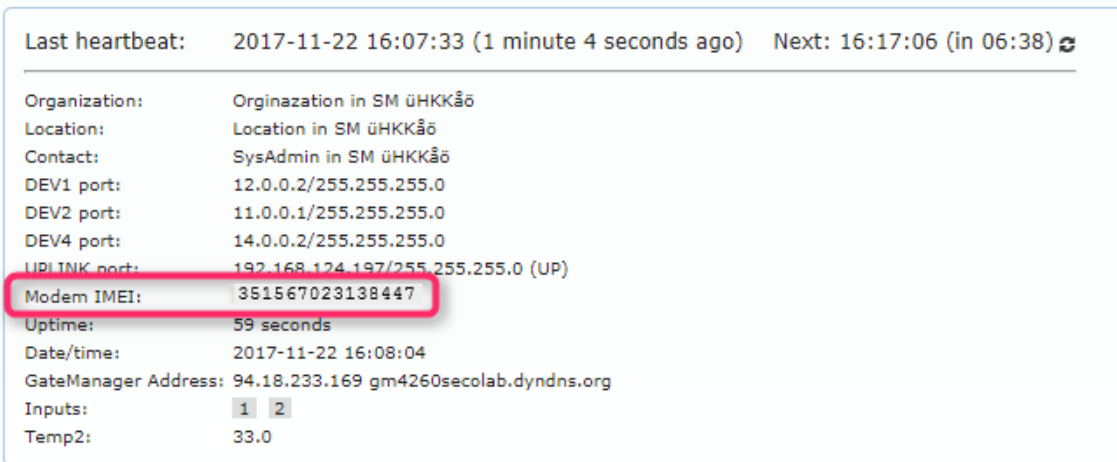
3. SiteManager Hardware

3.1. SiteManager and GateManager shows modem IMEI

With no SIM card, it is now possible to read the IMEI (International Mobile Equipment Identity) number of the installed 3G/LTE modem. In some scenarios, the modem IMEI number is needed for ISP registration. This registration might need to be done before the SIM card is available.

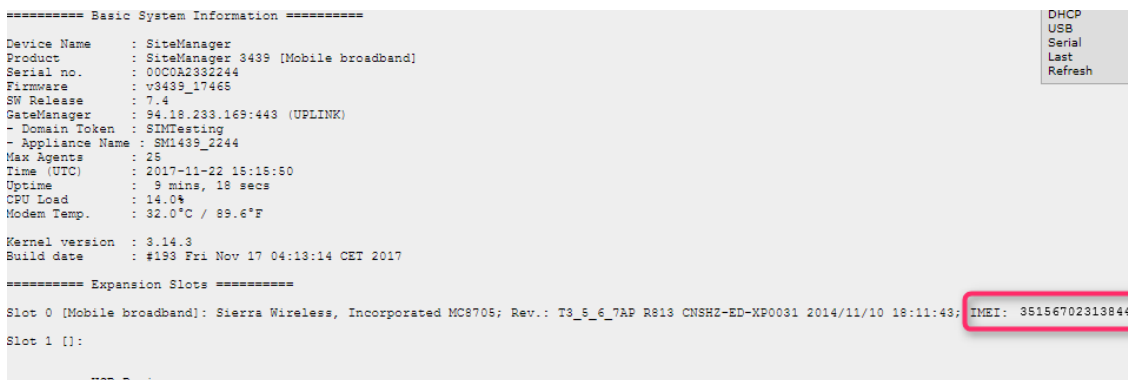
In previous firmware it was only possible to show the IMEI number if a SIM card was inserted.

The GateManager Portal will show the “Modem IMEI” number in the SiteManager Heartbeat section.



The screenshot displays the SiteManager Heartbeat status. At the top, it shows the last heartbeat time as 2017-11-22 16:07:33 (1 minute 4 seconds ago) and the next heartbeat at 16:17:06 (in 06:38). Below this, various system parameters are listed, including Organization, Location, Contact, and network ports. The 'Modem IMEI' is highlighted with a red box and has the value 351567023138447. Other parameters include Uptime (59 seconds), Date/time (2017-11-22 16:08:04), GateManager Address (94.18.233.169 gm4260secolab.dyndns.org), Inputs (1 2), and Temp2 (33.0).

The SiteManager Extended Status will show the IMEI number under the “Expansion Slots” section.



The screenshot shows the SiteManager Extended Status page. It features a 'Basic System Information' section with details like Device Name (SiteManager), Product (SiteManager 3439 [Mobile broadband]), and GateManager address. A 'DHCP USB Serial Last Refresh' button is visible on the right. Below this, the 'Expansion Slots' section is shown, with Slot 0 [Mobile broadband] displaying the IMEI: 351567023138447, which is highlighted with a red box. The page also shows kernel version (3.14.3) and build date (#193 Fri Nov 17 04:13:14 CET 2017).

The SiteManager Troubleshoot page will also show the IMEI number.

UPLINK2	
Linkstate	NOT Connected
Linkinfo	
MAC Address	IMEI:351567023138447 No SIM
Current IP Address	0.0.0.0
Current Netmask	0.0.0.0
IP Address Mode	PPP
Probe Type	None

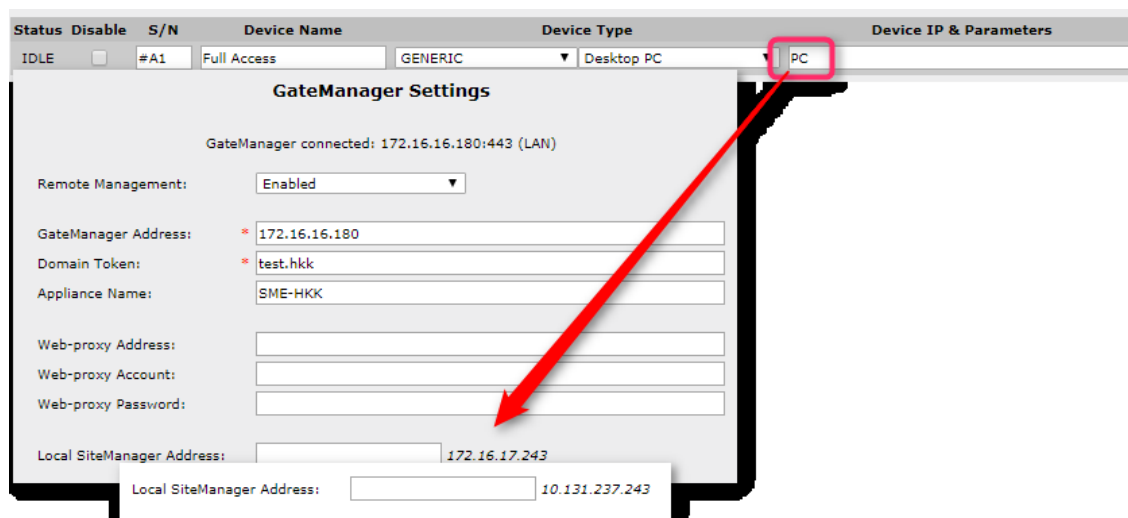
4. SiteManager Embedded

4.1. Support for external USB modem

Inserting a PPP interface, like an external USB modem, in a Windows device did not get identified as a possible DEV interface in 7.3. In 7.4 and later, we now enable PPP interfaces as a DEV/local interface. This means that the PC alias used in the agent below will get set to the PPP interface IP in case no Ethernet interfaces are available.

If there is any Ethernet interface available, this will take precedence over the PPP interface.

As seen in the graphic below, some default agents are using the PC alias.



In 7.4 or later it is now possible for the system (SME) to use a PPP interface as local address. Shown here with the 10.131.237.243, that is the USB Modem IP address.

4.2. Support for WiFi Adapter ONLY setup

The above PPP fix also cover the case if the device where the SME is installed, only have a WiFi adapter and no Ethernet Interface.

4.3. User Mode support (Linux)

It is now possible to run the SiteManager Embedded binary in user mode. If the binary is started in User Mode, it will be written in the log at startup:

```
Jan 30 14:10:13 info: SiteManager Embedded for Linux v. 7.4.18042 - Linux [user-mode]
Jan 30 14:10:13 info: No ping support - assuming devices are always on
```

There are some external limitations to running programs in User Mode on a standard Linux (they may vary with distribution).

First of all, the "/etc/sitemanager" folder will not be available to the SME, so it needs to be moved to the user folder. This can be achieved by starting the SiteManager with the "-C" parameter, which tells it to use its configuration files from a custom folder.

Using "./sitemanager -C. start" will use/create the configuration files ("sme.txt" and ".serial") in the current folder.

Using `./sitemanager -C/home/smeuser/smeconf/ start` will use/create the configuration files from the `/home/smeuser/smeconf/` folder.

The second issue, is that the user in User Mode, will not be able to successfully start the sitemanager binary from its default location (`/usr/local/sitemanager/sitemanager`) as it has the SUID bit set.

Running the SiteManager Embedded in User Mode should be done **without installing** the SiteManager. Just copy the binary to a local folder. If it is “root” that copies the file, make sure that you run `chown xxx.yyy sitemanager` and `chmod 700 sitemanager`, where xxx and yyy are user and group for the user that starts the SiteManager.

A third issue deals with opening RAW sockets and using TCP/UDP ports below 1024, and is mainly up to the Linux distribution. But ping support will not be available (see graphics above), so agents that rely on pinging a device to determine if it is up or not, will be set to “always on”.

The availability of TCP/UDP ports below 1024 can be tested by, ie. creating an active mode FTP agent, and testing its functionality.

4.4. Separate status and log folders

To facilitate the use of the SME in different scenarios (and memory types), the configuration files can now be split from the status files.

Starting the SiteManager Embedded with either “-C” (configuration) and/or “-S” (Status) will split the files into multiple folders.

The “sme.txt” and “.serial” files will be located in the Configuration folder, and the rest of the files (including the system log) will be located in the Status folder.

These options **must** be used every time when using the binary (like starting and stopping the SME).

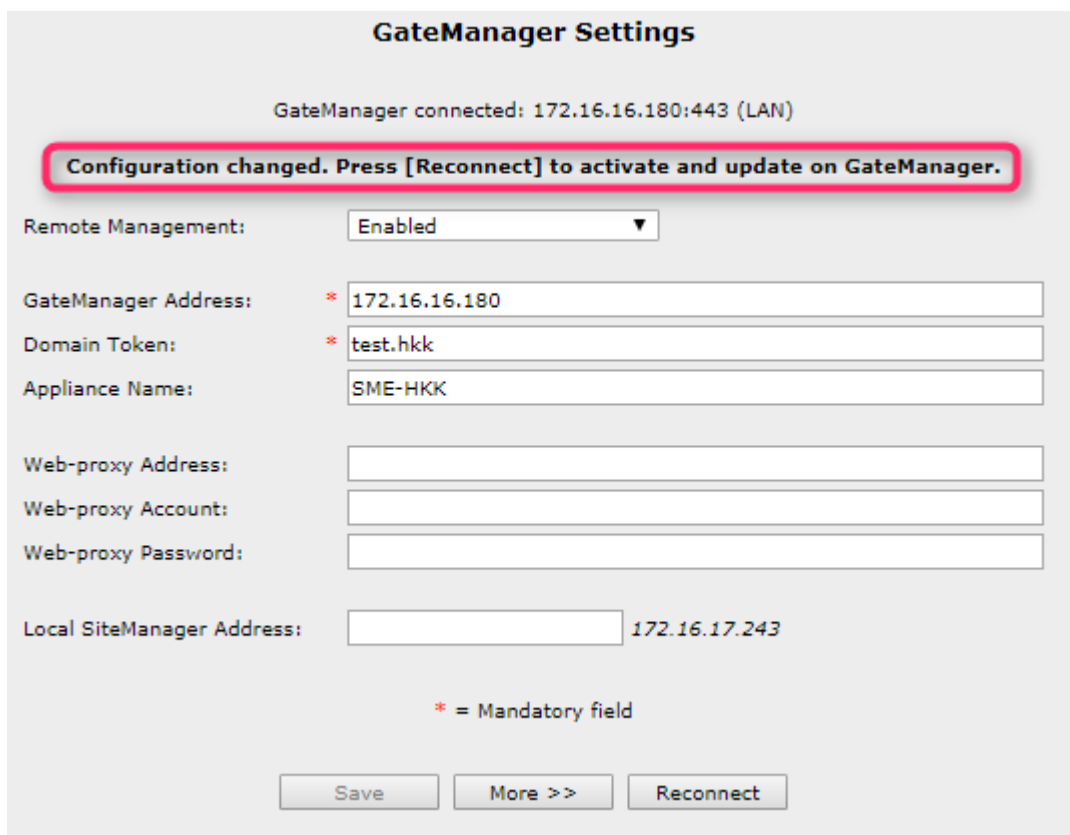
Refer to the “SiteManager Embedded API Function Reference V1.8.1” for more information, or contact Secomea Support.

5. SiteManager General

Relates to: SiteManager Hardware and SiteManager Embedded

5.1. SM GateManager Settings page

A new warning will show in case any of the fields on the GateManager Settings page have been changed.



The screenshot displays the 'GateManager Settings' interface. At the top, it indicates 'GateManager connected: 172.16.16.180:443 (LAN)'. A prominent red-bordered warning box contains the text: 'Configuration changed. Press [Reconnect] to activate and update on GateManager.' Below this, the settings are organized into several sections:

- Remote Management:** A dropdown menu set to 'Enabled'.
- GateManager Address:** A text input field with a red asterisk and the value '172.16.16.180'.
- Domain Token:** A text input field with a red asterisk and the value 'test.hkk'.
- Appliance Name:** A text input field with the value 'SME-HKK'.
- Web-proxy Address:** An empty text input field.
- Web-proxy Account:** An empty text input field.
- Web-proxy Password:** An empty text input field.
- Local SiteManager Address:** A text input field with the value '172.16.17.243'.

A legend below the fields states '* = Mandatory field'. At the bottom, there are three buttons: 'Save', 'More >>', and 'Reconnect'.

Any changes on the GateManager Settings page will now show Configuration changed....

The text will only show until the page has been refreshed. Only changes using the web GUI interface will trigger this warning. Any changes using the JSON API or other interfaces will not trigger the warning.

5.2. Agents updates and additions

The following agents have been either added or updated:

- FANUC Robotics -> Ethernet: Added TCP server port 60005
- ABB -> Robot: Added TCP port 80

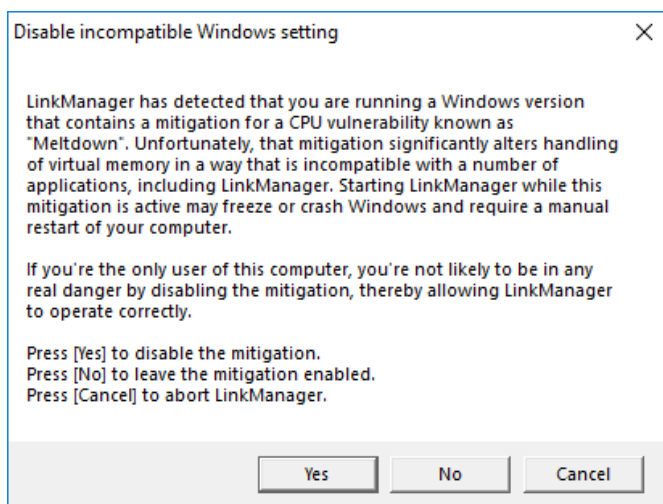
6. LinkManager

6.1. Spectre/Meltdown fix for 64-bit Windows 8 and 10

Starting this year, Microsoft released an early mitigation for the Spectre and Meltdown vulnerabilities. This fix had wide implications on the functionality and speed of Windows 8 and 10, especially on AMD CPU's and unfortunately also on the LinkManager.

When these Microsoft patches are installed, they will freeze the workstation when the LinkManager is started.

We responded with a new version of the LinkManager that would detect and advise what to do depending on your configuration and BIOS settings.



Please refer to our website for current information on this issue:

<https://kb.secomea.com/hc/en-us/articles/115003578669-Downloads-LinkManager-and-Appliance-launcher>

7. **LinkManager Mobile**

Nothing added in this release.

8. **License Portal**

Nothing added in this release.

9. Advanced Tech topics

9.1. LMM API: Incl. IMEI/IMSI in Appliance Details

The response from the Appliance Details query will now include IMEI and IMSI numbers of the appliance, as they are now present in the heartbeat information.

Refer to the “LinkManager Mobile API V3.2” for more information, or contact Secomea Support.

9.2. LMM API: Serial number instead of Appliance ID

Earlier versions used Appliance ID or Agent ID to identify the target device. And the only way to do that, was to traverse the tree.

Now it is possible save some favorite agents, and use the serial number to access the agents.

Refer to the “LinkManager Mobile API V3.2” for more information, or contact Secomea Support.

10. Documentation

The following documentation has been updated in this release.

- SiteManager Embedded API Function Reference V1.8.1
- LinkManager Mobile API V3.2

/end

Secomea A/S

Denmark

CVR No. DK31 36 60 38

Email: support@secomea.com

www.secomea.com