New in Secomea Release 7.1

Nice to know information about the release:

- Secomea Release 7.1 build 16444 public 2016.11.04

Version: 1.0, 2016

secomea

Contents

secomea

secòmea

Change log

Version	Change log
0.9	Initial version
1.0	First release.

1. RELEASE 7.1

Release 7.1 includes several security related changes, details of which are not disclosed here. We strongly recommend that you upgrade all hardware and software devices to this release.

# 2. GateManager

2.1. SMS service activated with Part number

2.1.1. Enabling and disabling SMS Service

SMS service is now controlled for activation similar to EasyLogging/Usage Statistics. If you need the SMS services enabled, you need to order SMS Activation from the License Portal.

Enabling the SMS service will automatically bump the EasyService to a minimum level of BRONZE.

On Own GM, the activation will install a license that allows altering the "SMS Services" setting under server config.It is therefore not the license itself that affects ES level, but whether SMS Services are enabled or not; so in fact if SMS Services were enabled before upgrading to 7.1, you will need the SMS license installed to disable the setting again. If the SMS feature is enabled and desired disabled and no SMS license is installed, you can disable SMS for the root domain of the server, but this will still retain minimum Bronze. Alternatively downgrade, disable and upgrade again.

On Hosting servers ordering SMS will set the SMS setting for the customer domain, and thereby bump the level. This is independent of whether SMS Services are activated on the hosted server or not. So SMS should only be ordered (or made available to order) in LP if the hosted server is configured to support SMS.
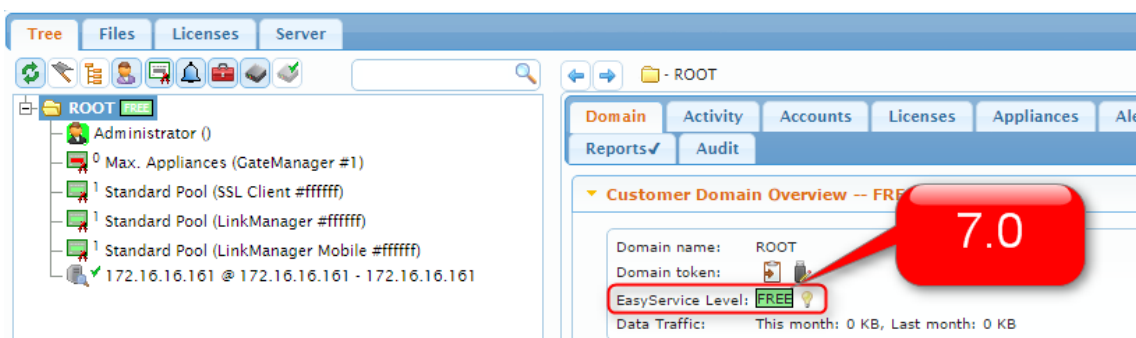
Release 7.0 own GM with SMS Services activated in server config.
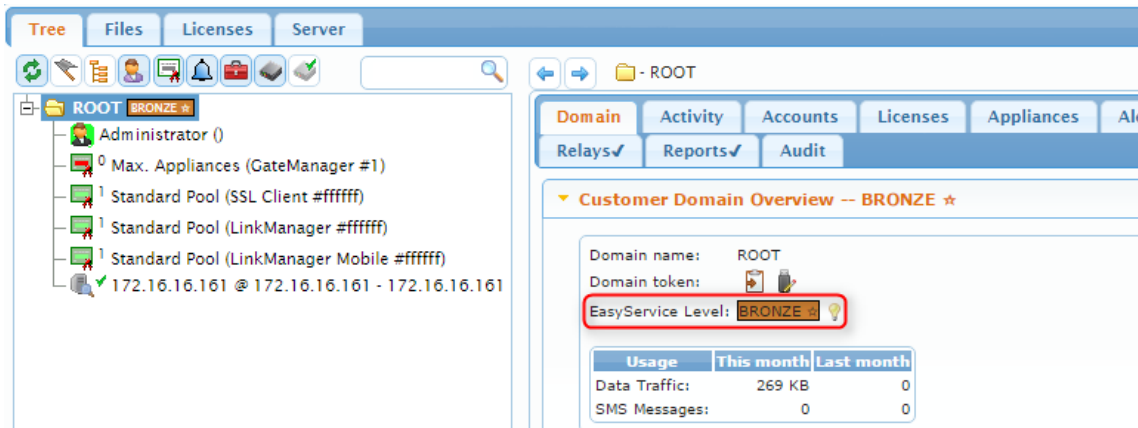
After install of Release 7.1 EasyService level is bumped to BRONZE as a minimum.

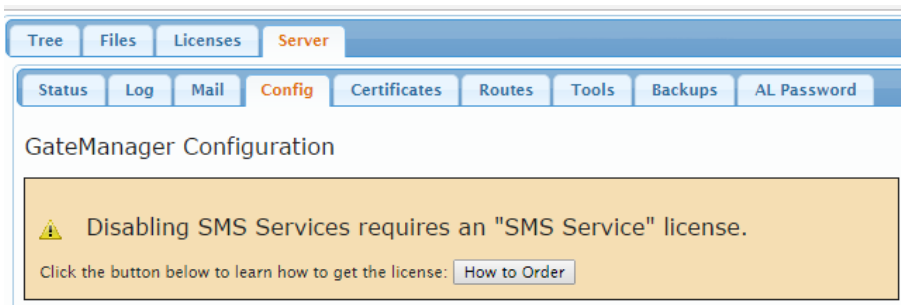Message when attempting to disable SMS services on an own GM where SMS Services were enabled before upgrade, and no SMS activation license is installed

2.2. New GateManager validation

From 7.1 and forward the GateManager DNS name (External Public Hostname) will be validated by resolving the IP address of the DNS name with the public IP address from where the installed GateManager is coming from.

GM syslog could show:

```
Hostname "gm9250dist.dyndns.org" resolves to "1.2.3.4" which differs
from server's current public IP "94.18.233.162"
```

The GateManager will use a subset of known standard DNS servers like google DNS host (8.8.8.8) and OpenDNS. If this fails, the GateManager will try a variety of DNS and HTTP based services, like OpenDNS, ipinfo.io, opendns.com, dyndns.com, and GateManager Discovery Service (GDS / gm00.secomea.com).

Validation failed:

- If the DNS name does not match the public IP address, the GateManager will start up with a failing license and show "Softdongle is missing". The DNS name issue should be fixed and the GateManager should be restarted when done. The GateManager will retry resolving the DNS name every 10 minutes.

- If the GateManager DNS name cannot be resolved due to wrong DNS name or the DNS name is not yet activated, the GateManager will try for another 10 minutes and in that time-period the GateManager will be unreachable.

2.3. Usage Table on ROOT domains

New Usage table has been introduced. In release 7.0 we show usage statistics for the ROOT domain even if there is no EasyLogging/Usage Statistics license.

Previous 7.0 16267:

Release 7.1 16444:

2.4. Domain Contents Summary

A new section is created for the summary part of the Domain Information:

Previously, the contents summary was located under the Customer Domain Overview section. It now it has its own section.

secomea

2.5. Account filter view

The GateManager now allows filtering out joined accounts, which is very useful for installations with a large user base.
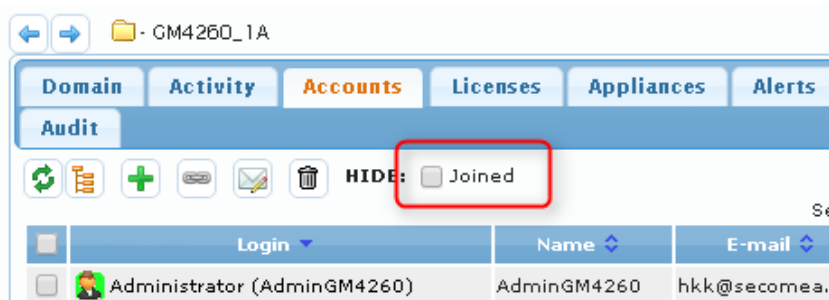
Select the "Joined" option to filter out all instances of joined accounts and leave the view only showing the parent accounts.

2.6. SHA2 Web certificate

Before 7.1, the GateManager was born with a SHA1 web certificate. The web certificate is signed through the GateManager self-signing CA.

The CA in version 7.1 and onwards will be a SHA2 certificate, as many web browsers in the future will prohibit the use of SHA1 certificates.

This can be seen in the GateManager under "Server -> Certificates", the picture below shows the SHA1 certificate:
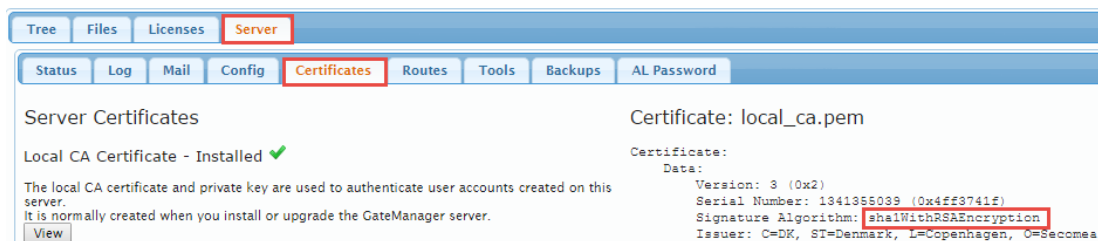
On new 7.1 installations it will change to the picture below:
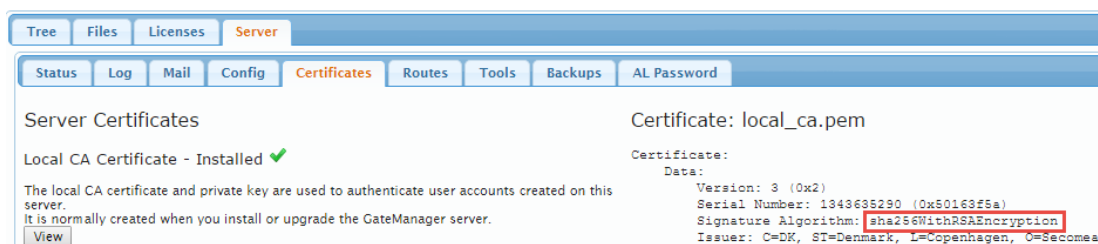
Please note that this change is **only targeted at newly installed 7.1 Gate-Managers**, and not GateManagers upgraded to 7.1, which will retain the original SHA1 certificate

Remember that when you install your own web certificate it will be used instead of the GateManager CA certificate.

Also please note that the GateManager CA signs the GateManager and Link-Manager user certificates.

secomea

2.7. Multiple SMS providers

It is now possible to have multiple SMS providers depending on country/area.

If alerts are send to several different countries, it could be very cost effective to use local SMS providers for specific regions instead of global SMS providers, depending on size and use.

This can now be achieved by creating an SMS script per provider controlled by a central script.

2.7.1. Sample scripts

(The SMS Gateway guide section 3 has been updated with this info http://ftp.gatemanager.dk/DP_GM_SM-0026-Configuring_SMS-Gateways_on_GateManager.pdf)

As an example, let's assume that your local GateManager is placed in Denmark, and your support staff is placed in England.

This means that you would expect two-factor logins and alerts to pass through the SMS provider that is native to the country where the receiving phone is located.You then create three scripts, one for each provider and a control script. This is done on the GateManager under "Files -> Scripts".

For provider 1, create a script by selecting "New script:" and make sure the name starts with "sms-", i.e. "sms-KAP-System-Demo" and click create:

Edit sms-KAP-System-Demo

```
# KAPSYSTEM.COM - SMS gateway setup

user =
pass =

from = GateManager
json = 1
run = wget
host = api.kapsystem.com
auth = inline
protocol = https
url = %p://%H/api/v3/sendsms/json

post = {"authentication": {"username": "%U", "password": "%P"}, "messages": [{"sender":
"%S", "text": "%M", "flash": "0", "datacoding": "8", "recipients": [{"gsm": "%+T"}]}]}
```

Save   Cancel   Delete script

For provider 2, create the script the same way:

Edit sms-cpsms-Demo

```
# CPSMS.DK - SMS gateway setup
# Replace ? below with user name and password

user =
pass =

from = GateManager

run = wget
host = www.cpsms.dk
auth = inline
protocol = http
url = %p://%H/sms/?username=%U&password=%P&recipient=%T&message=%M&from=%S&utf8=%C&flash=%F
```

Save   Cancel   Delete script

Then, following the same procedure, create a script to control your providers, this will be the controlling script used by the SMS service:

secomea

Edit sms-generic

```
[KAP]
include = KAP-System-Demo

[CP]
include = cpsms-Demo

{+45}
gw = KAP

{+44}
gw = CP

{}
drop = 1
```
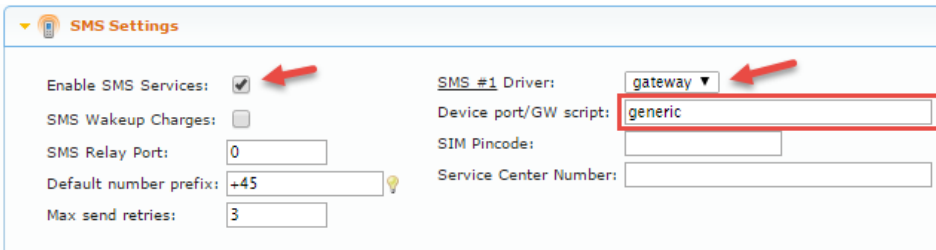
Save | Cancel | Delete script

This matches a part of the telephone number to the desired country/region. For an extensive list of country calling codes, please refer to this page: https://en.wikipedia.org/wiki/List_of_country_calling_codes

When this is set up, go to the SMS service setup and enter your control script. Select "Server -> Config" and put the configuration in to edit mode:

Tree | Files | Licenses | Server

Status | Log | Mail | Config | Cer

GateManager Configuration

Edit ←
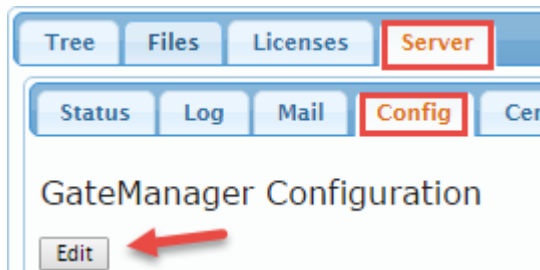
Then go to "SMS settings" and select "gateway" as the driver and "generic" as the gateway script. Remember that the prefix "sms-" is only used when creating the script. Everywhere else the script is referenced without the prefix.

SMS Settings

Enable SMS Services: ☑ ←	SMS #1 Driver: gateway ▼ ←
SMS Wakeup Charges: ☐	Device port/GW script: generic
SMS Relay Port: 0	SIM Pincode:
Default number prefix: +45 💡	Service Center Number:
Max send retries: 3	
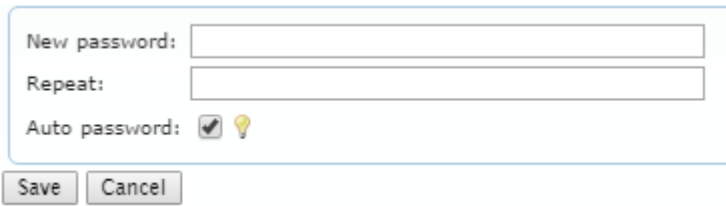
You can then test the scripts by using the "Test SMS" function:

Test SMS

Mobile: +4412345678

Send SMS

Restart SMS Gateway

secomea
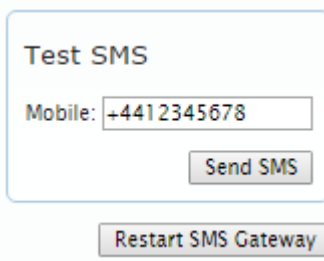
2.8. New "Nice to have" features

2.8.1. Clear fields

Clicking auto password now automatically clears a manually entered password field, and vice versa.

2.8.2. New landing page
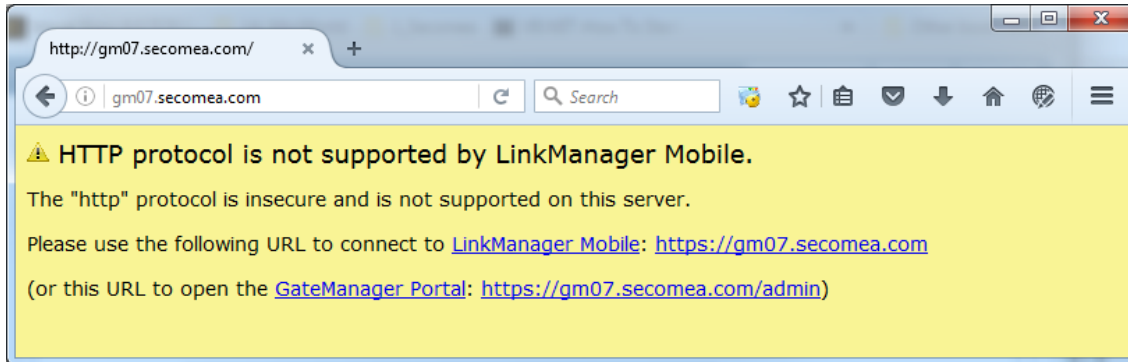
New http redirection page for both LMM and GM Portal link.

2.9. Internal information

GateManager release 7.1 has been prepared for some of the new Cloud-based installation features. More about this in next release.

secomea

3. SiteManager

3.1. Troubleshoot

Starting from Release 7.1 we have implemented a new troubleshooting page. The purpose of this functionality, is to gather information from the SiteManager to help both end user but also the remote support team to get a clear indication of what state the SiteManager is in. This helps making support issues more effective and without guessing the state of the SiteManager.

This first edition has some limitations, that we hope to extend in later releases.

Special high lights

- Troubleshoot can detect if there is an IP address conflict on any of the SiteManager interfaces.

  Troubleshoot will show:

- SiteManager models with 4 port switches can use troubleshoot to identify link state on the 4 switch ports.

- Models like 1029, 1429, 3229 and 3429 do not support the temperature parameter and will show temperature "Unreadable" as expected.

The troubleshoot page can be accessed (and exported) as text, JSON or HTML format output through the following links:

Error! Hyperlink reference not valid.

Error! Hyperlink reference not valid. (experimental only)

Error! Hyperlink reference not valid.

3.1.1. Login to troubleshoot page

Troubleshoot page is read-only and does not need a login authentication. The page is available from devices on both device and uplink network but only if the counter part is on the local broadcast network.

Log in is required if above criteria are not fulfilled.

3.1.2. Nice to know about troubleshoot

Running "troubleshoot" does not intercept any connections

3.2. Diagnostics

The modem diagnostics function, previously available under "Status > Diagnostics", has been moved to the more appropriate location under UPLINK2 (if available).

3.3. Auto-logout

As part of the security update a new auto-logout function is implemented.

Available:

Auto-logout is only active when logged in locally. Using "Go To Appliance" from the GateManager Portal or LinkManager will not activate the "Auto-Log-out" option.
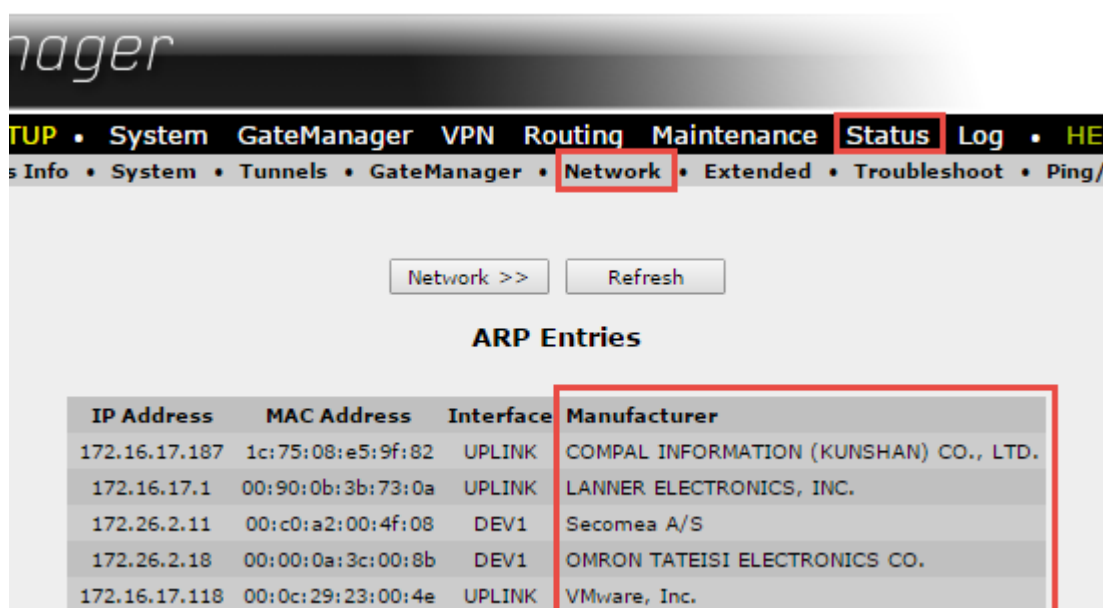
Configure Auto-logout:

The setting is configured under "System -> General -> GUI Timeout":
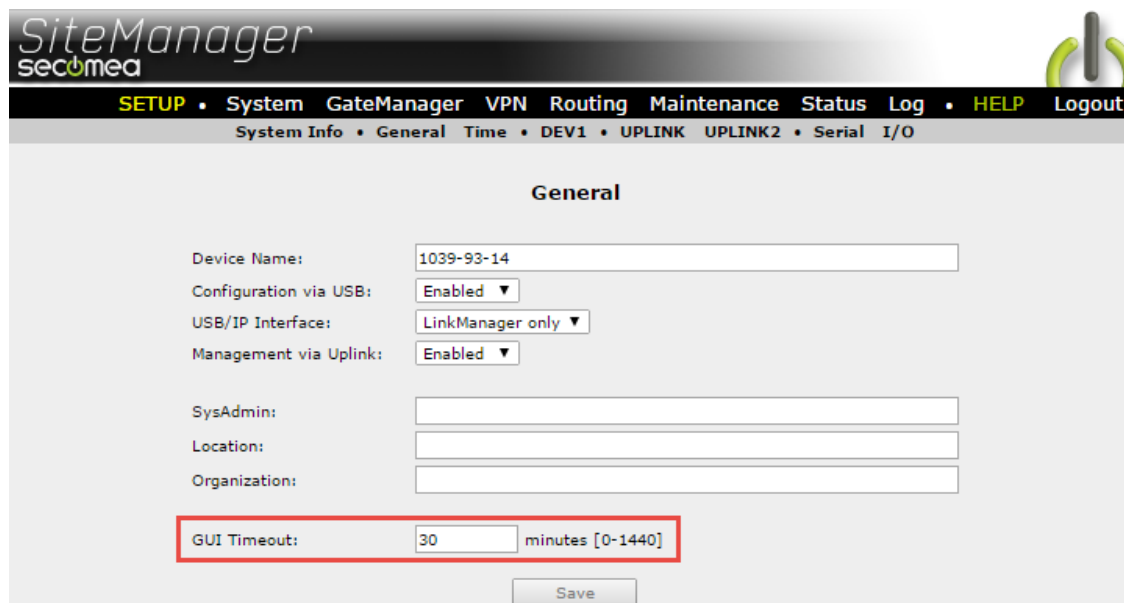
3.4. Vendor information

The ARP table of the SiteManager now has vendor information on MAC addresses. This have been added under "Status -> Network -> ARP".

3.5. New serial port to serial port relaying

It is now possible to relay a serial port on one SiteManager to a serial port on another SiteManager, using relays.

In previous releases it was necessary to initiate a Serial to Serial connection by activating the connection from one end. From 7.1 it is now automatically handled by the SiteManager itself. This means that two serial devices can be remotely connected using two SiteManagers' serial (RS232) interfaces transparently, without additional program development.

Two new "Auto-Relay (DTE/DCE)" serial driver settings have been added and automatically connect to the internal address 127.0.0.1:123. This makes it possible to setup a Server Relay and Device Relay to establish a fully transparent Serial to Serial connection.

(serial device) --- (RS232)(SM) ←→(SM)(RS232) --- (serial device)

-Server relay-   - (device relay)

3.5.1. Example of a usecase:

To visualize this, you may have a network blackout due to a problem with a high end switch in San Francisco that needs urgent maintenance by the IT support in Seattle.

The IT expert can now go to a SiteManager in Seattle and connect a serial cable from the SiteManager to his laptop without using any other software than his terminal program. The switch in San Francisco can be connected directly to a SiteManager with a 3G modem through a Serial console cable.

The IT supporter will now have access to the switch as if it was directly connected to his or her laptop.

Apart from this scenario, most use cases will include direct logging from serial enabled PLC/HMI's to a central log server.

For more information on this, please refer to the appropriate Application Note found on our Support Website (http://support.secomea.com).

4. SiteManager Embedded

4.1. SiteManager Embedded and Multiple NICs

This release includes several optimizations for SiteManager Embedded when installed on a host with multiple Ethernet ports.

4.1.1. Local SiteManager Address

One of the SiteManager interfaces will be identified as the DEV (Device) address by the SiteManager system. This is also assigned to the alias called 'PC'. If the system choses the wrong interface the address can manually be set using the Local SiteManager Address (GateManager -> General) or via the JSON API.

4.1.2. When is Local SiteManager Address important?

As mentioned above the Local SiteManager Address is in use if, or when the SiteManager chooses the wrong network interface as the DEV interface. The right interface is important when using the SiteManager in the following scenarios:

1) When the product where the SiteManager Embedded is installed have more than one interface. If only one interface is present, it will of course be identified as DEV (Device) interface.

2) FTP in ACTIVE mode requires the SME to select the device interface to be able to perform a successful FTP transfer. ACTIVE mode will open the listening port on the device interface and must be rightfully chosen by the SiteManager Embedded.

3) Some PLC software/tools need to use the right IP address in the project to be able to set up the device correct.

4.2. Access to all local IP addresses

Related to SiteManager Embedded Basic. From 7.1 it is now possible to use any local IP alias created on the Windows Host as an agent IP address. The previous release 7.0 did only register the primary local IP address as a valid local IP address.

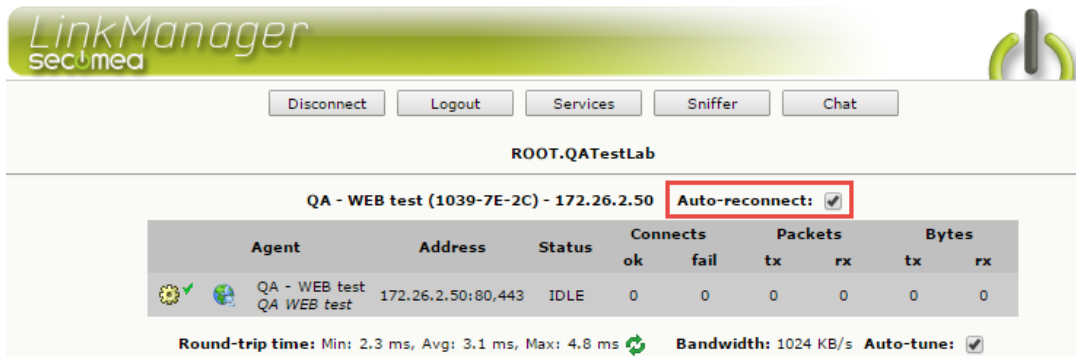This also includes "Server Virtual Addresses" in GateManager Server Relays.

4.3. Faster detection of address change

On SME for Linux and Windows we now detect an address change faster and the GateManager connection is reestablished faster.

Previously, an address change (i.e. DHCP renewal) could take up to 6-20 minutes to reestablish the GateManager connection. Now the time should be limited to a couple of seconds depending on the network.

5. LinkManager

5.1. Auto-reconnect option
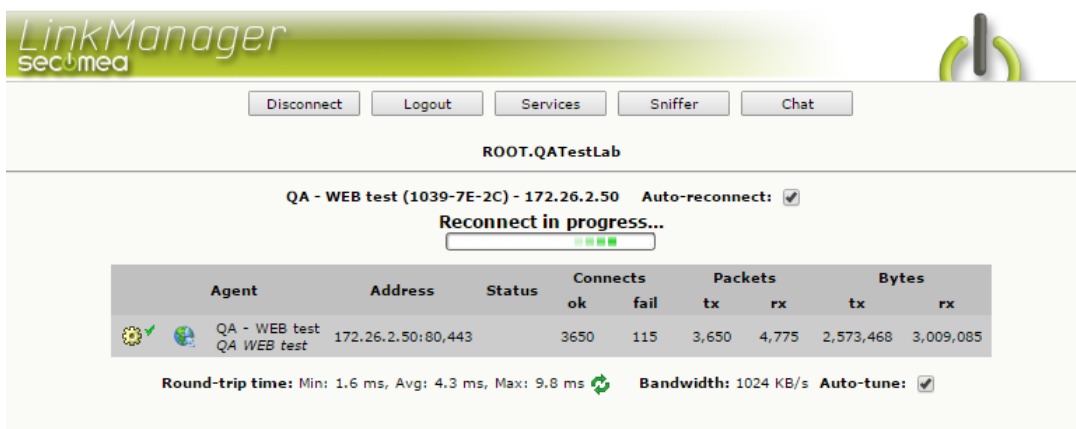
A new feature in LinkManager will try to reestablish the connection to the SiteManager. A counter will increase for every retry (see Chapter 8 for timer defaults).

This is especially useful if you are flashing an HMI panel with a SiteManager Embedded installed. When the flashing has finished, the panel will restart, expecting to reconnect to the software on the PC running LinkManager.

When the SiteManager Embedded appliance goes offline on the GateManager, the LinkManager will try to keep the connection on stand-by until the panel is back from reboot. Then it will resume normal operation.

When the panel goes offline, the LinkManager will display a reconnect warning:

When the panel reconnects, if will display the number of reconnects after the Auto-reconnect option:

If the Auto-reconnect was not activated the LinkManager will disconnect from the panel, and the software on the PC running LinkManager will lose its connection:

secomea

10.127.128.129:3 says:

Connection to remote device lost.

Reason:
SiteManager disconnected

☐ Prevent this page from creating additional dialogs.

OK
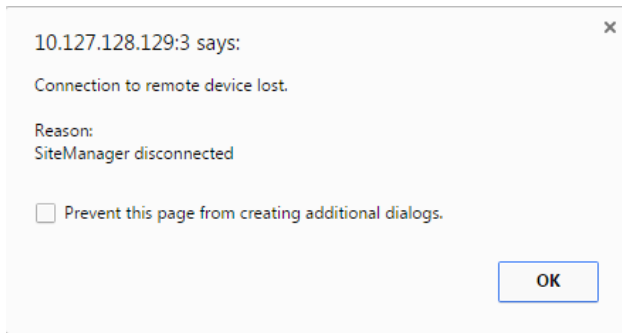
5.1.1. Auto-reconnect in 7.1.16444 last minute update

Observations on re-connect show that some SiteManager hardware models don't fully support or work for re-connect. Investigations still running in R&D.

5.2. Windows 10 Anniversary update

A fix for creating the LinkManager Layer2 adapter has been implemented. This covers a situation where Windows 10 was updated with the Anniversary update.

Open issue: In the writing of this document, we still await Microsoft to make code signing of our drivers available. When this happens we can also install LinkManager on a clean Anniversary installation (Windows build 1607).

5.3. Internal information

The LM-API introduced in release 7.0 has been extended with status request option for connection status only.

sec@mea

6. LinkManager Mobile

6.1. Audit log only shows user activity

Prior to release 7.1, the Audit log in LinkManager Mobile showed all audit log entries for the domain.

Now only the entries relevant for the LinkManager User is shown.

6.2. Extending the Auto-password

From 7.1 and forward the auto-generated password for a LinkManager Mobile account is now 12 characters long.

6.3. New landing page

New HTTP redirection page for both LMM and GM Portal link:
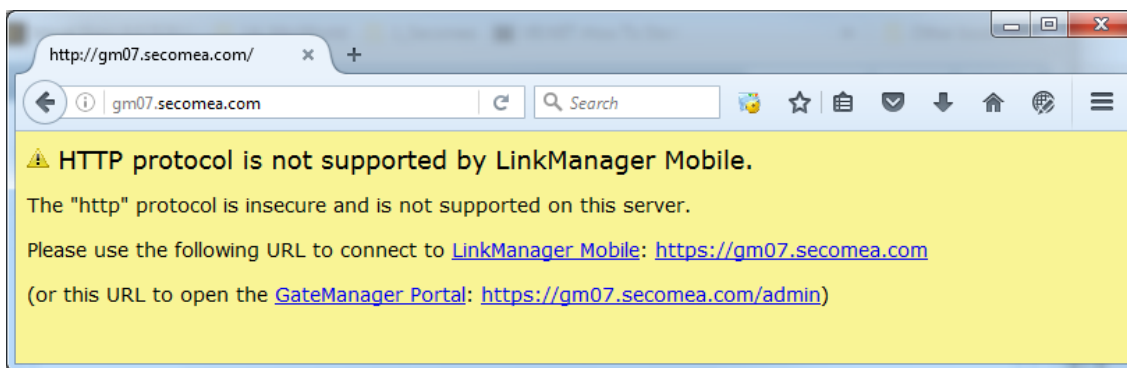
6.4. New naming format on LinkManager Portal

If an Agent (like the WebCam PLC below) is not located in the same domain as its SiteManager Appliance (Host), we will add the SiteManagers name to the agent. I.e.:

WebCam PLC (SM1029_01AC)

secömea

7. License Portal

Update is not available.

secomea

8. Advanced Tech Topics

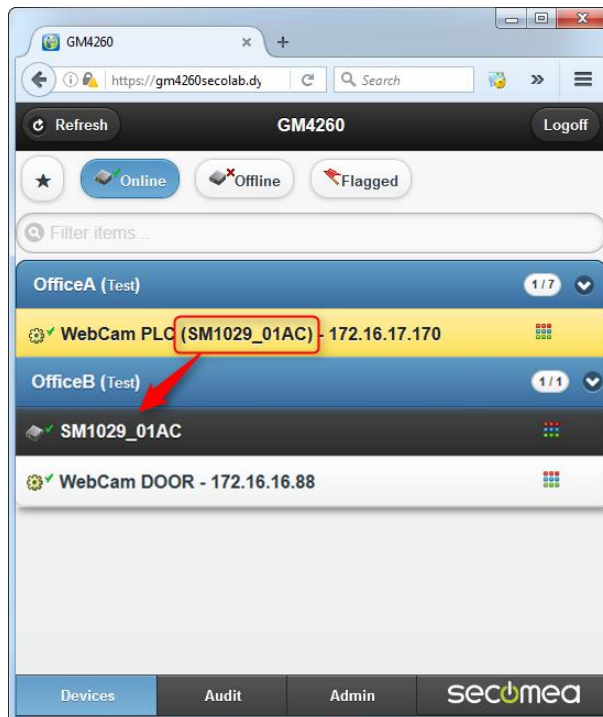In this chapter we will be addressing some of the technological advanced topics that are in this release.

8.1. Forwarding Agent

The forwarding agent has 10 rules in each forwarding agent. The total amount of characters combined in all 10 rules was 247, which was limiting in some situations.

You were allowed to create more than one forwarding agent and the rules that did not fit, would just be moved to another agent, leaving blank fields.

But to counter this, the total character count is now set at 1024, leaving just over 100 characters per rule, which should be enough, even with DNS used on the destination side.

8.2. LinkManager Reconnect

The only user configurable setting within the LinkManager Reconnect functionality is "Reconnect Mode".

The parameters for reconnect are default set as:

- Retry interval: 5 secs

- Number of retries: 180 (results in 15 minutes)

- Poll for connection status interval: 10 secs.

8.3. Inter-device relaying on the SiteManager

A feature used very seldom was removed in release 7.0 due to the new EasyLogging functionality. We now introduce this feature again in release 7.1. Inter-device relaying is when a Device Relay is pointing to a Server Relay on the same SiteManager. If it does not make sense, you probably don't need it and can just note that the feature is available although it likely is not needed in your set up.

8.4. Appliance Launcher field length

The Appliance Launcher has been changed in 7.1. The field length could in some instances be limiting, specifically with regards to Unicode characters.

The Appliance Launcher will now refrain from truncating fields in certain instances.

8.5. No Flash SMS support

Flash SMS will not be allowed on two-factor login. The stability on ISP implementations vary too much to warrant a use for two-factor login.

secомea

8.6. Missing DNS on UPLINK -> UPLINK2 failover

Prior to 7.1 there was an issue where failover from UPLINK to UPLINK2 could result in a situation where the DNS server was not updated.

To trigger the issue:

1) Both UPLINK and UPLINK2 must have the same Priority (First or Second)

2) GateManager must be configured with a DNS name

3) Configured DNS server addresses must fail to resolve DNS if trying on the

other UPLINK interface. Using public DNS server "8.8.8.8" would probably not trigger the issue.

secomea

9. Documentation

The following new documents have been created or updated

➤ Configuring SMS Gateways on GateManager (updated version)
https://support.secomea.com/documentation/configuring-sms-gateways-on-gatemanager/

➤ DX_GM_SM_LM_0118_LM_Access_to_EL_Master_Agent.docx

➤ Direct Serial to Serial doc

10. APPENDIX A

/end

secomea

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com