New in Secomea Release 7.3

Nice to know information about the release:

- Secomea RDM Release 7.3 LM/SME build 17393 public 2017.09.29
- Secomea RDM Release 7.3 SM build 17396 public 2017.09.29
- Secomea GM Release 7.3 build 17395 public 2017.09.29

Version: 1.3, 2017

NewInRelease7.3_1.3.docx

Contents

Change log

Version	Change log
0.1	Initial version
0.2	Edits for public release
1.0	Finalizing public release
1.1	Public release
1.2	Version corrections
1.3	Build number edits

1. RELEASE 7.3

Release 7.3 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. Downgrade from release 7.3

It is important to notice that it is not recommended to downgrade your GateManager to an older release once you have upgraded to 7.3.

If your SiteManagers are still running release 7.2 (build 17145) it is not a problem, but as soon as your SiteManagers have been upgraded to 7.3 or newer, and the GateManager is running 7.3, The SiteManagers will require the highest encryption and will no longer attach to the GateManager if it is downgraded to 7.2.

To make the SiteManager accept a downgraded GateManager again, you must reconfigure the GateManager address.

2.2. In-Browser VNC

2.2.1. Stability

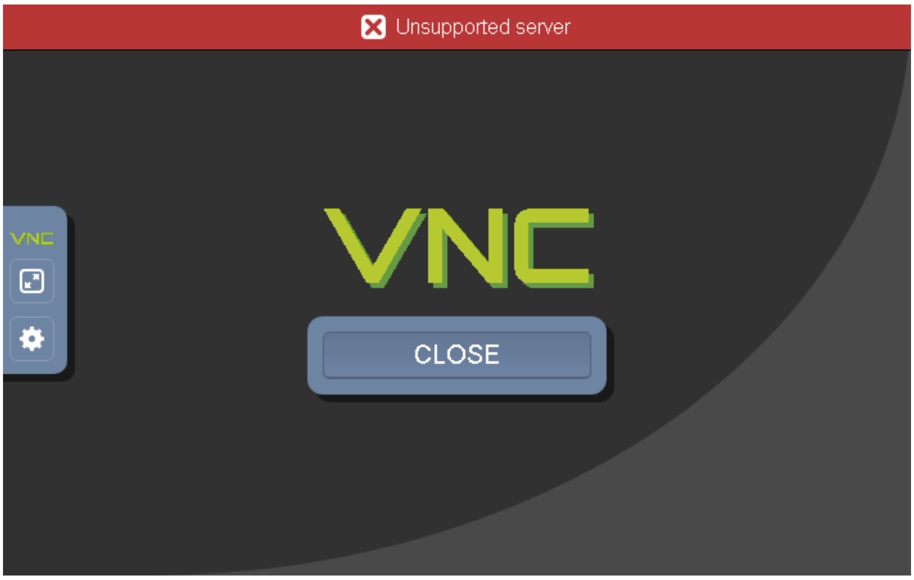
With the new VNC In-Browser feature introduced in 7.2 (the one where you do not need a VNC viewer, but access the server through your browser) you could, in some cases, experience stability issues.
We found and fixed the issues, and the VNC In-Browser is our recommended VNC solution from both computers, tablets and smart phones.

The big advantage of the VNC In-Browser is that it can run on any device with a standard internet browser supporting HTML5.

Performance will depend on the local internet browser.

2.2.2. Update to Server Support

In release 7.3 we added support for more VNC servers. If you have experienced a message like the one shown below, you should upgrade to 7.3 and there is a good chance this will be solved.



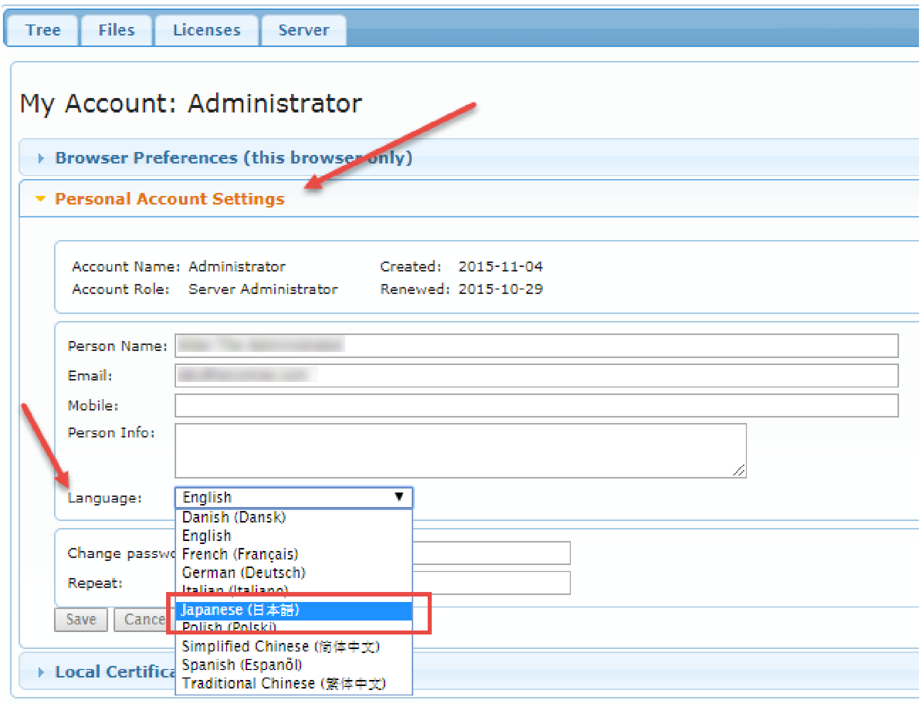
The message “Unsupported server” was observed on units like a Siemens TP277 panel with SmartServer/VNC server installed.

Note: VNC servers can have different security implementations, and not every conceivable combination is supported. If the “Unsupported Server” is encountered, please set the VNC server security to “Standard VNC” or “Legacy”.

2.3. Limited Japanese support in the GateManager GUI

The GateManager has been extended with support for Japanese in selected places in the GUI. This means that all lightbulbs visible to the “Basic Admin” account role are available in Japanese

To see this the translations, change your account language to Japanese:


Tree
Files
Licenses
Server
Browser Preferences (this browser only)
Personal Account Settings
Local Certifica
Save
Cance

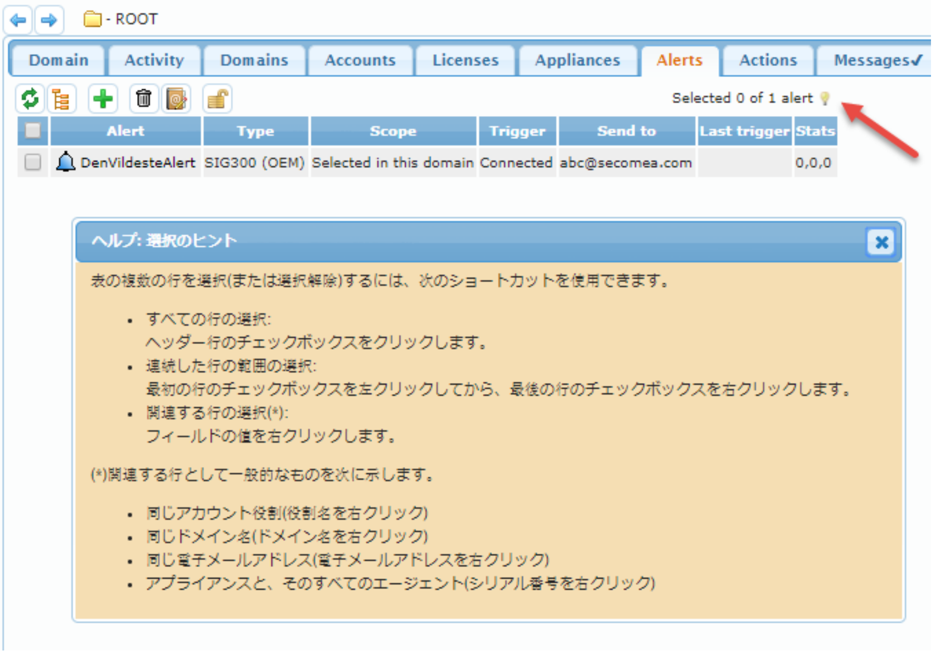
My Account: Administrator

Account Name: Administrator
Account Role: Server Administrator
Created: 2015-11-04
Renewed: 2015-10-29

Person Name: [redacted]
Email: [redacted]
Mobile:
Person Info:
Language: English

Change passwo
Repeat:

Then go to a lightbulb text (i.e. Alerts):



Selected 0 of 1 alert

□	Alert	Type	Scope	Trigger	Send to	Last trigger	Stats
□	DenVildesteAlert	SIG300 (OEM)	Selected in this domain	Connected	abc@secomea.com		0,0,0

ヘルプ: 選択のヒント

表の複数の行を選択(または選択解除)するには、次のショートカットを使用できます。

- すべての行の選択:
  ヘッダー行のチェックボックスをクリックします。
- 連続した行の範囲の選択:
  最初の行のチェックボックスを左クリックしてから、最後の行のチェックボックスを右クリックします。
- 関連する行の選択(*):
  フィールドの値を右クリックします。

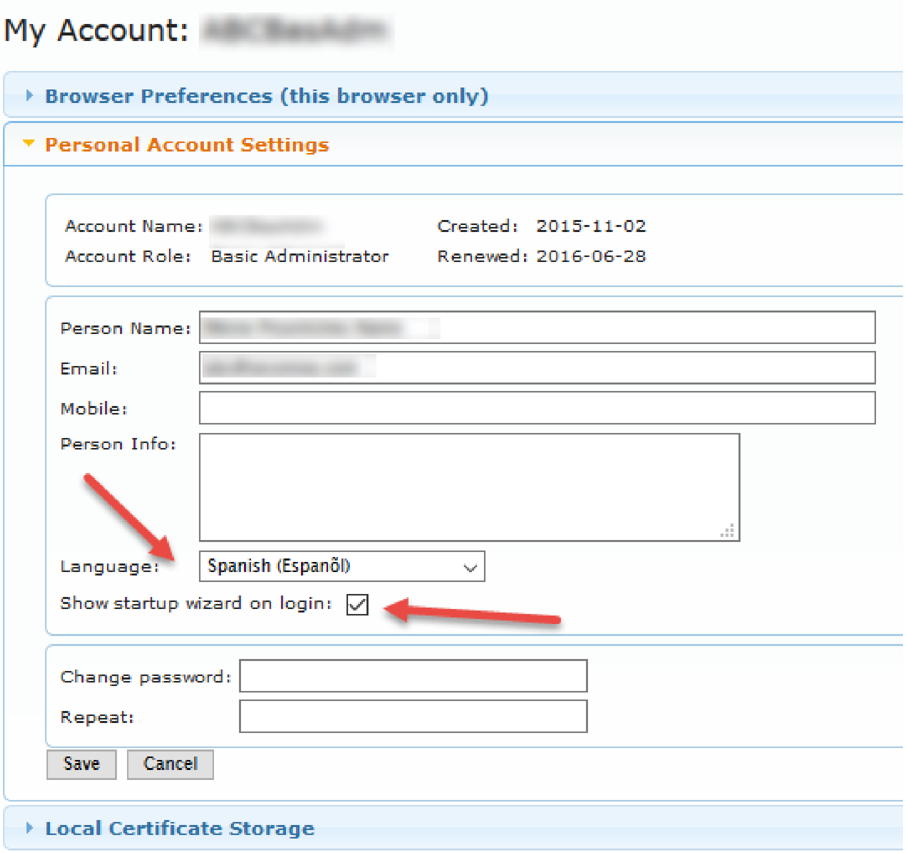
(*)関連する行として一般的なものを次に示します。

- 同じアカウント役割(役割名を右クリック)
- 同じドメイン名(ドメイン名を右クリック)
- 同じ電子メールアドレス(電子メールアドレスを右クリック)
- アプライアンスと、そのすべてのエージェント(シリアル番号を右クリック)

2.4. Startup Wizard extended with Spanish translation

The Startup Wizard now has a Spanish translation.

To see this, go to your personal account settings and set your language to Spanish. Select to “Show startup wizard on login”.



Browser Preferences (this browser only)
Personal Account Settings
Save
Cancel
Local Certificate Storage

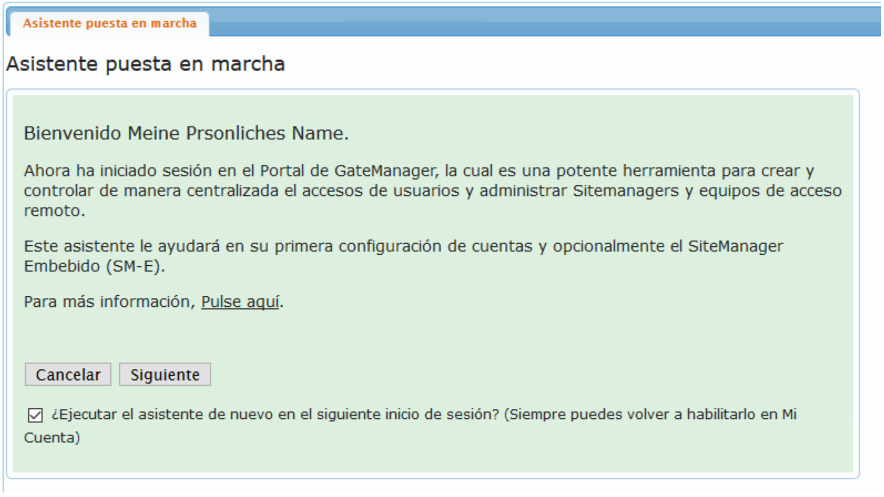
My Account: [redacted]

Account Name: [redacted]
Created: 2015-11-02
Account Role: Basic Administrator
Renewed: 2016-06-28

Person Name: [redacted]
Email: [redacted]
Mobile:
Person Info:
Language: Spanish (Espanõl)
Show startup wizard on login: ☑

Change password:
Repeat:

Then log out and log back in to see the wizard:



Asistente puesta en marcha

Bienvenido Meine Prsonliches Name.

Ahora ha iniciado sesión en el Portal de GateManager, la cual es una potente herramienta para crear y controlar de manera centralizada el accesos de usuarios y administrar Sitemanagers y equipos de acceso remoto.

Este asistente le ayudará en su primera configuración de cuentas y opcionalmente el SiteManager Embebido (SM-E).

Para más información, Pulse aquí.

☑ ¿Ejecutar el asistente de nuevo en el siguiente inicio de sesión? (Siempre puedes volver a habilitarlo en Mi Cuenta)

2.5. Linux interface naming

More Linux distributions are moving away from the “legacy” ethX naming standard.

The new interface naming standard is called “Predictable Network Interface Names” and is introduced in various Linux distributions like Debian 9.

The new names can be “en01”, “ens1”, “enp2s0”, etc.

The GateManager is now compliant with the new naming. In the previous release the GateManager could be confused and prevent it from starting. Syslog would report: “GM: Server Address not specified”.

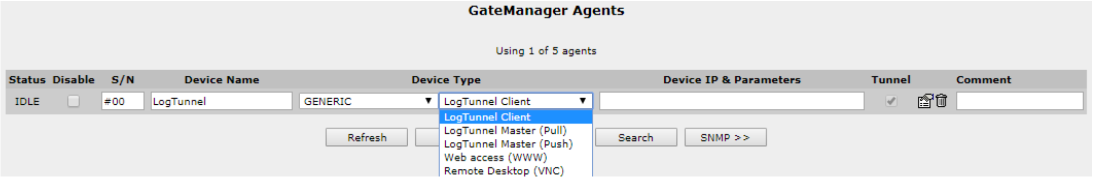
2.6. Static Network Routes

In 7.2 the GateManager Static Network Route option could fail depending on GateManager version and the underlying OS.

In version 7.3 Static Network routes should behave as expected on all platforms and GateManager versions.

2.7. Name change from "EasyLogging" to "LogTunnel"

Starting with Release 7.3 the EasyLogging feature has changed name to “LogTunnel”. This change has been implemented on all products on all platforms and in the documentation and help files.



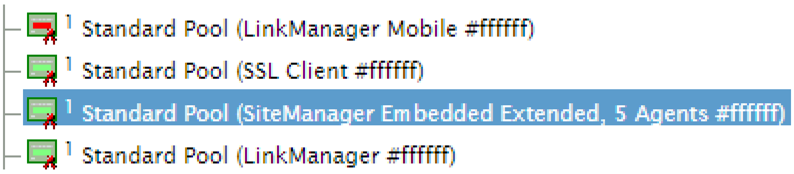
GateManager Agents

Using 1 of 5 agents

Status	Disable	S/N	Device Name	Device Type		Device IP & Parameters	Tunnel	Comment
IDLE	□	#00	LogTunnel	GENERIC	LogTunnel Client		✓	

2.8. Demo SiteManager Embedded License added

With Release 7.3 we have added a “SiteManager Embedded Extended 5 Agents” license to all GateManagers.



1 Standard Pool (LinkManager Mobile #ffffff)
1 Standard Pool (SSL Client #ffffff)
1 Standard Pool (SiteManager Embedded Extended, 5 Agents #ffffff)
1 Standard Pool (LinkManager #ffffff)

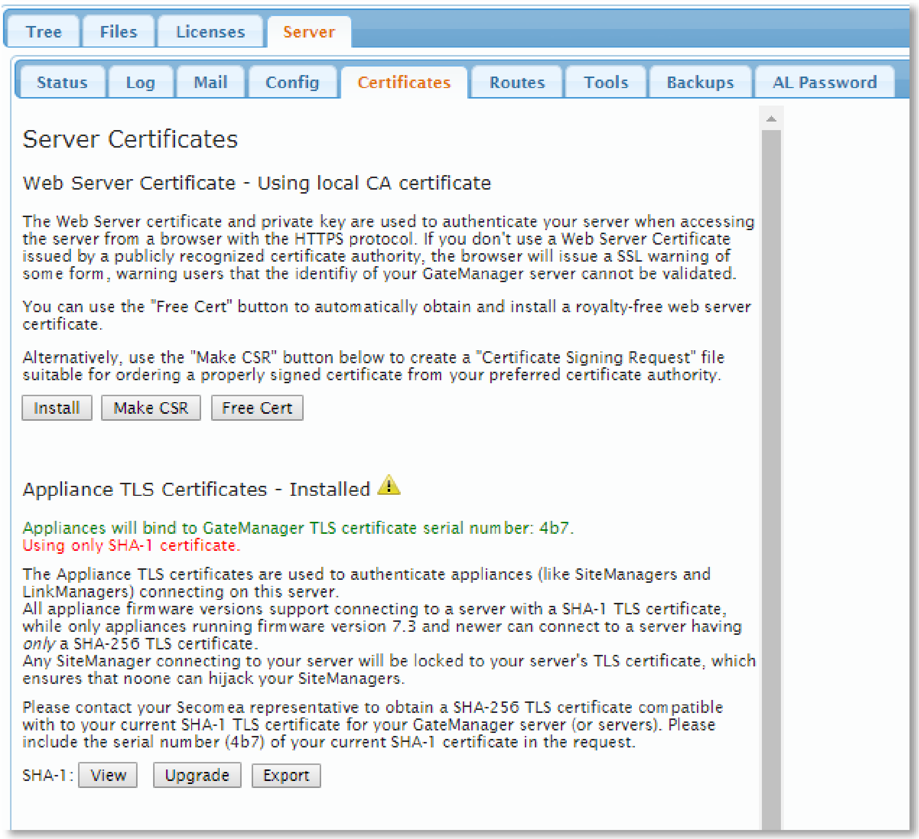
This will allow anyone already owning or installing a GateManager from scratch, to test SiteManager Embedded functionality without having to purchase a license.

Please note that if the GateManager is downgraded to 7.2, the license will be revoked.

2.9. “Appliance” connections upgraded to TLS 1.2/SHA-256

The TLS connections that SiteManagers and LinkManagers are using to connect to the GateManager, can in Release 7.3 be upgraded to a higher encryption level.

In the picture below, this certificate is named “Appliance TLS Certificates”:



Server Certificates

Web Server Certificate - Using local CA certificate

The Web Server certificate and private key are used to authenticate your server when accessing the server from a browser with the HTTPS protocol. If you don't use a Web Server Certificate issued by a publicly recognized certificate authority, the browser will issue a SSL warning of some form, warning users that the identifiy of your GateManager server cannot be validated.

You can use the "Free Cert" button to automatically obtain and install a royalty-free web server certificate.

Alternatively, use the "Make CSR" button below to create a "Certificate Signing Request" file suitable for ordering a properly signed certificate from your preferred certificate authority.

Appliance TLS Certificates - Installed ⚠

Appliances will bind to GateManager TLS certificate serial number: 4b7.
Using only SHA-1 certificate.

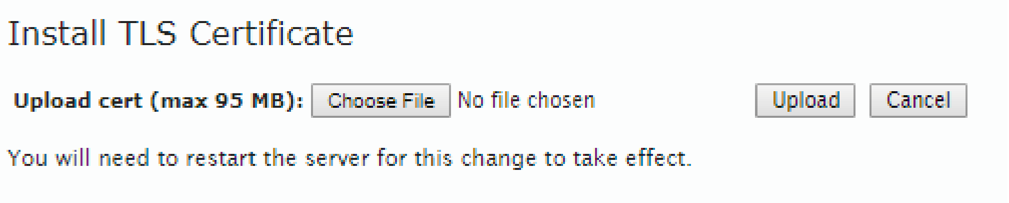
The Appliance TLS certificates are used to authenticate appliances (like SiteManagers and LinkManagers) connecting on this server.
All appliance firmware versions support connecting to a server with a SHA-1 TLS certificate, while only appliances running firmware version 7.3 and newer can connect to a server having *only* a SHA-256 TLS certificate.
Any SiteManager connecting to your server will be locked to your server's TLS certificate, which ensures that noone can hijack your SiteManagers.

Please contact your Secomea representative to obtain a SHA-256 TLS certificate compatible with to your current SHA-1 TLS certificate for your GateManager server (or servers). Please include the serial number (4b7) of your current SHA-1 certificate in the request.

SHA-1:

Please note that the default certificate is a SHA-1 certificate, and to upgrade the certificate to SHA-256, it must be ordered through the **License Portal**.

It is then installed automatically. There could be scenarios where the certificate is delivered manually from Secomea, in this case press the “Upgrade” button and upload it:

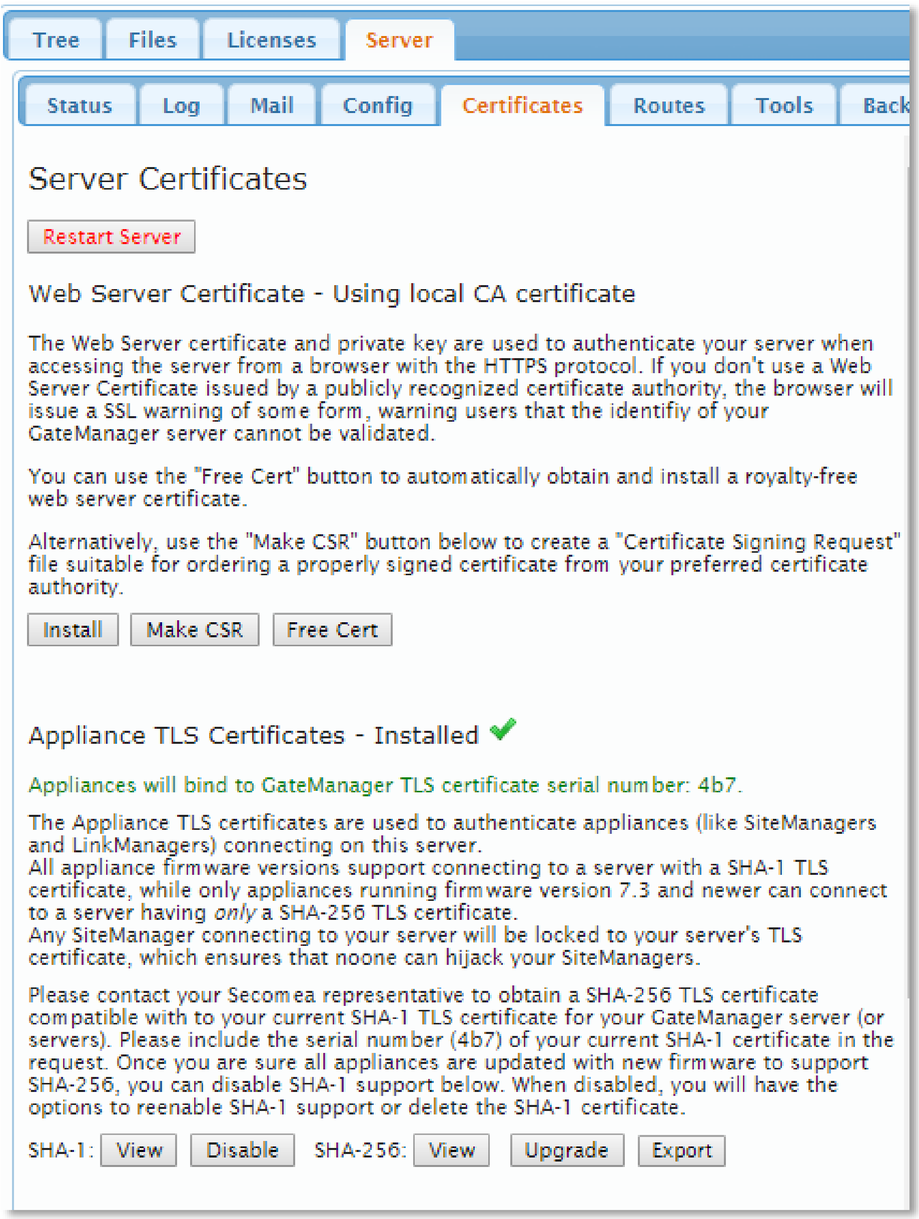


Install TLS Certificate

Upload cert (max 95 MB): No file chosen

You will need to restart the server for this change to take effect.

When the GateManager server is upgraded to SHA-256 the Certificate will be displayed like this:



Server Certificates

Web Server Certificate - Using local CA certificate

The Web Server certificate and private key are used to authenticate your server when accessing the server from a browser with the HTTPS protocol. If you don't use a Web Server Certificate issued by a publicly recognized certificate authority, the browser will issue a SSL warning of some form, warning users that the identifiy of your GateManager server cannot be validated.

You can use the "Free Cert" button to automatically obtain and install a royalty-free web server certificate.

Alternatively, use the "Make CSR" button below to create a "Certificate Signing Request" file suitable for ordering a properly signed certificate from your preferred certificate authority.

Appliance TLS Certificates - Installed ✓

Appliances will bind to GateManager TLS certificate serial number: 4b7.

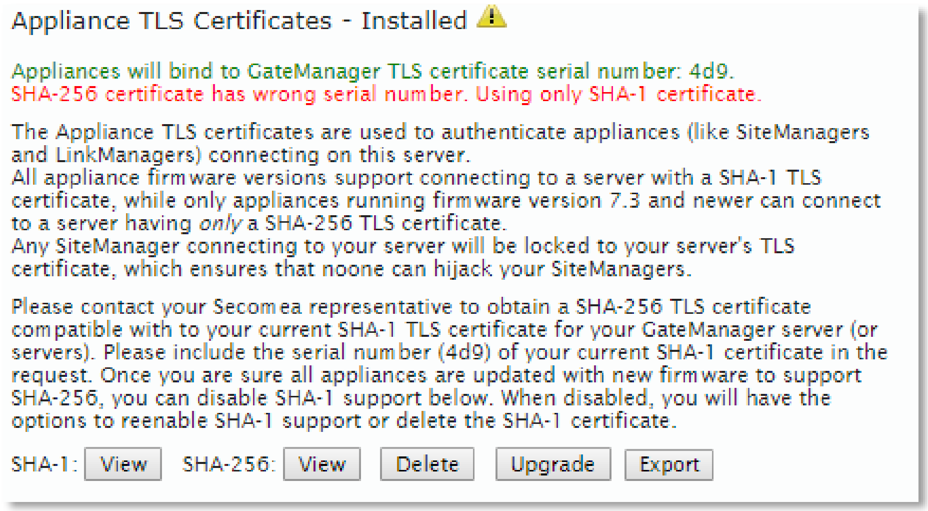
The Appliance TLS certificates are used to authenticate appliances (like SiteManagers and LinkManagers) connecting on this server.
All appliance firmware versions support connecting to a server with a SHA-1 TLS certificate, while only appliances running firmware version 7.3 and newer can connect to a server having *only* a SHA-256 TLS certificate.
Any SiteManager connecting to your server will be locked to your server's TLS certificate, which ensures that noone can hijack your SiteManagers.

Please contact your Secomea representative to obtain a SHA-256 TLS certificate compatible with to your current SHA-1 TLS certificate for your GateManager server (or servers). Please include the serial number (4b7) of your current SHA-1 certificate in the request. Once you are sure all appliances are updated with new firmware to support SHA-256, you can disable SHA-1 support below. When disabled, you will have the options to reenable SHA-1 support or delete the SHA-1 certificate.

A GateManager running with the highest security level using the SHA-256 certificate, will show as above and have the new SHA-256 buttons.

Disabling SHA-1: For security reasons, it is recommended to disable the SHA-1 certificate. Note that SiteManagers that are not upgraded to release 7.3 will be disconnected and LinkManagers with 7.2 or older will not be able to connect. You can always re-enable SHA-1 again and these devices will be able to reconnect.

If trying to install a wrong TLS SHA-256 certificate there is no harm done. It will simply be rejected and show as below:



Appliance TLS Certificates - Installed ⚠

Appliances will bind to GateManager TLS certificate serial number: 4d9.
SHA-256 certificate has wrong serial number. Using only SHA-1 certificate.

The Appliance TLS certificates are used to authenticate appliances (like SiteManagers and LinkManagers) connecting on this server.
All appliance firmware versions support connecting to a server with a SHA-1 TLS certificate, while only appliances running firmware version 7.3 and newer can connect to a server having *only* a SHA-256 TLS certificate.
Any SiteManager connecting to your server will be locked to your server's TLS certificate, which ensures that noone can hijack your SiteManagers.

Please contact your Secomea representative to obtain a SHA-256 TLS certificate compatible with to your current SHA-1 TLS certificate for your GateManager server (or servers). Please include the serial number (4d9) of your current SHA-1 certificate in the request. Once you are sure all appliances are updated with new firmware to support SHA-256, you can disable SHA-1 support below. When disabled, you will have the options to reenable SHA-1 support or delete the SHA-1 certificate.

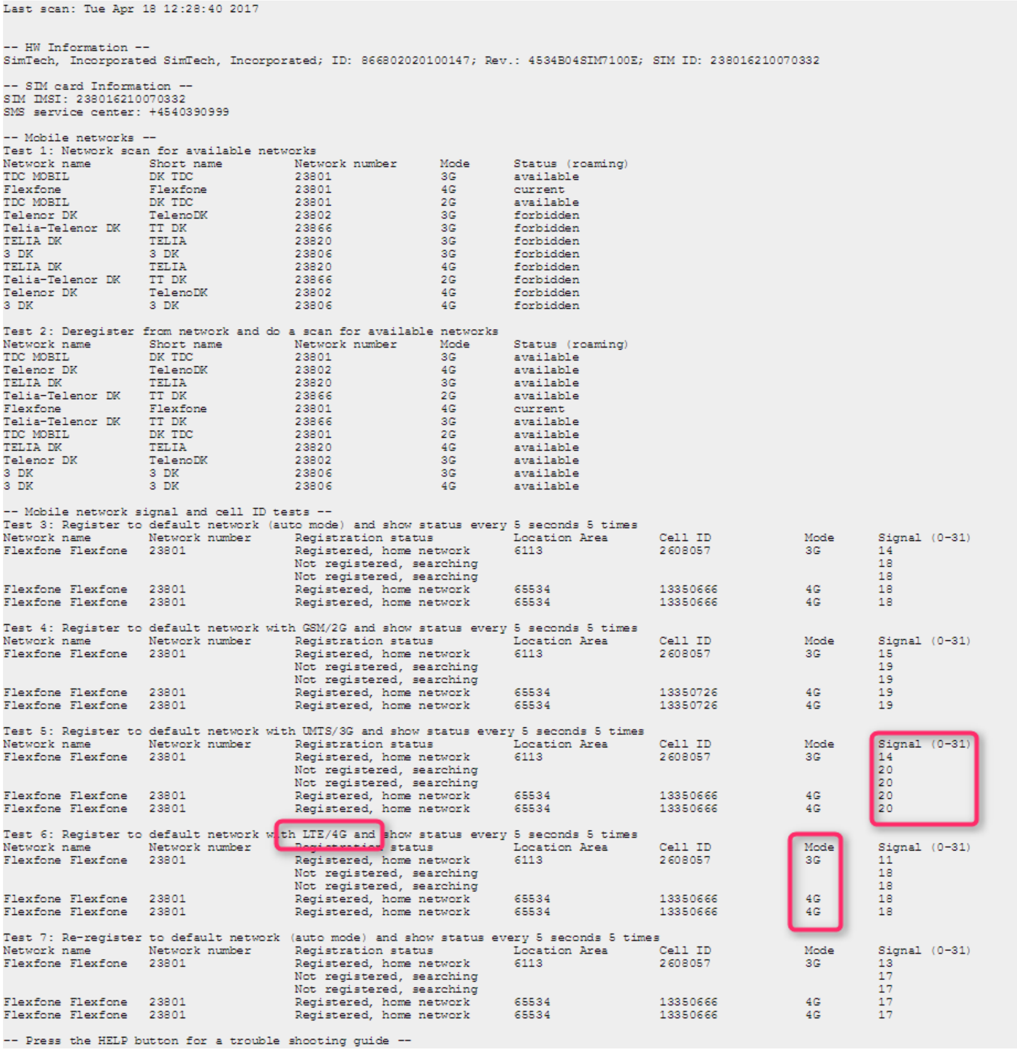
PLEASE NOTE: If the GateManager server AND appliances have been upgraded to 7.3 AND the SHA-256 certificate has been installed, you should NOT downgrade the GateManager to 7.2, as all SiteManagers with 7.3 will be disconnected, and LinkManager users that have connected once with SHA-256 will not be able to connect either.

For more information about Appliance Certificate see APPENDIX A.

3. SiteManager

3.1. Mobile related changes

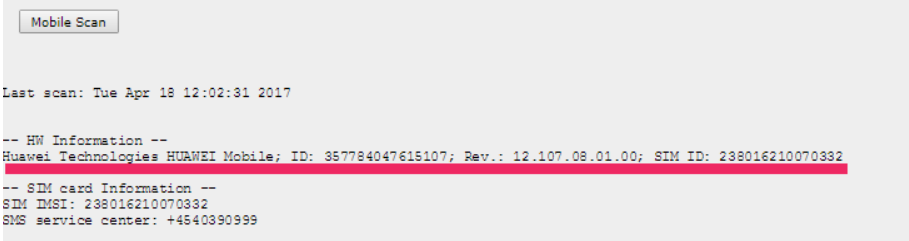
3.1.1. Mobile Scan (UPLINK2 -> Diagnostic) – 4G scanning



```
Last scan: Tue Apr 18 12:28:40 2017


-- HW Information --
SimTech, Incorporated SimTech, Incorporated; ID: 866802020100147; Rev.: 4534B04SIM7100E; SIM ID: 23801621007O332

-- SIM card Information --
SIM IMSI: 238016210070332
SMS service center: +4540390999

-- Mobile networks --
Test 1: Network scan for available networks
Network name        Short name          Network number      Mode      Status (roaming)
TDC MOBIL           DK TDC              23801               3G        available
Flexfone            Flexfone            23801               4G        current
TDC MOBIL           DK TDC              23801               2G        available
Telenor DK          TelenoDK            23802               3G        forbidden
Telia-Telenor DK    TT DK               23866               3G        forbidden
TELIA DK            TELIA               23820               3G        forbidden
3 DK                3 DK                23806               3G        forbidden
TELIA DK            TELIA               23820               4G        forbidden
Telia-Telenor DK    TT DK               23866               2G        forbidden
Telenor DK          TelenoDK            23802               4G        forbidden
3 DK                3 DK                23806               4G        forbidden

Test 2: Deregister from network and do a scan for available networks
Network name        Short name          Network number      Mode      Status (roaming)
TDC MOBIL           DK TDC              23801               3G        available
Telenor DK          TelenoDK            23802               4G        available
TELIA DK            TELIA               23820               3G        available
Telia-Telenor DK    TT DK               23866               2G        available
Flexfone            Flexfone            23801               4G        current
Telia-Telenor DK    TT DK               23866               3G        available
TDC MOBIL           DK TDC              23801               2G        available
TELIA DK            TELIA               23820               4G        available
Telenor DK          TelenoDK            23802               3G        available
3 DK                3 DK                23806               3G        available
3 DK                3 DK                23806               4G        available

-- Mobile network signal and cell ID tests --
Test 3: Register to default network (auto mode) and show status every 5 seconds 5 times
Network name        Network number      Registration status           Location Area       Cell ID             Mode      Signal (0-31)
Flexfone Flexfone   23801               Registered, home network      6113                2608057             3G        14
                                        Not registered, searching                                                       18
                                        Not registered, searching                                                       18
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        18
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        18

Test 4: Register to default network with GSM/2G and show status every 5 seconds 5 times
Network name        Network number      Registration status           Location Area       Cell ID             Mode      Signal (0-31)
Flexfone Flexfone   23801               Registered, home network      6113                2608057             3G        15
                                        Not registered, searching                                                       19
                                        Not registered, searching                                                       19
Flexfone Flexfone   23801               Registered, home network      65534               13350726            4G        19
Flexfone Flexfone   23801               Registered, home network      65534               13350726            4G        19

Test 5: Register to default network with UMTS/3G and show status every 5 seconds 5 times
Network name        Network number      Registration status           Location Area       Cell ID             Mode      Signal (0-31)
Flexfone Flexfone   23801               Registered, home network      6113                2608057             3G        14
                                        Not registered, searching                                                       20
                                        Not registered, searching                                                       20
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        20
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        20

Test 6: Register to default network with LTE/4G and show status every 5 seconds 5 times
Network name        Network number      Registration status           Location Area       Cell ID             Mode      Signal (0-31)
Flexfone Flexfone   23801               Registered, home network      6113                2608057             3G        11
                                        Not registered, searching                                                       18
                                        Not registered, searching                                                       18
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        18
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        18

Test 7: Re-register to default network (auto mode) and show status every 5 seconds 5 times
Network name        Network number      Registration status           Location Area       Cell ID             Mode      Signal (0-31)
Flexfone Flexfone   23801               Registered, home network      6113                2608057             3G        13
                                        Not registered, searching                                                       17
                                        Not registered, searching                                                       17
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        17
Flexfone Flexfone   23801               Registered, home network      65534               13350666            4G        17

-- Press the HELP button for a trouble shooting guide --
```

Several updates have been made for running a Mobile Scan with SiteManager 4G models. In the new 4G scanning, the Mode and Signals are now shown correctly.

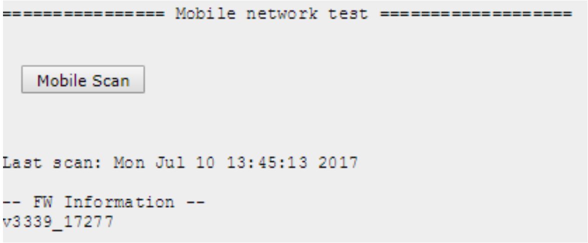
3.1.2. Mobile Scan (UPLINK2 -> Diagnostic) – missing HW info



```
Last scan: Tue Apr 18 12:02:31 2017


-- HW Information --
Huawei Technologies HUAWEI Mobile; ID: 357784047615107; Rev.: 12.107.08.01.00; SIM ID: 238016210070332

-- SIM card Information --
SIM IMSI: 238016210070332
SMS service center: +4540390999
```

The hardware information depicted above was missing on previous firmware. This has been fixed in 7.3.

3.1.3. Mobile Scan (UPLINK2 -> Diagnostic) - extended with FW info



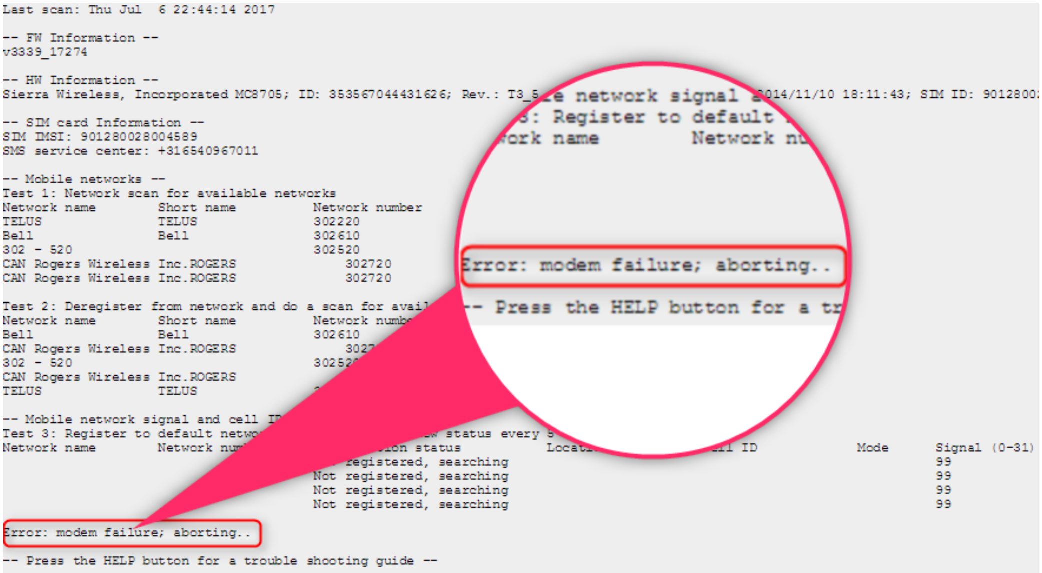
```
================ Mobile network test ===================

Last scan: Mon Jul 10 13:45:13 2017

-- FW Information --
v3339_17277
```

For better troubleshooting, the firmware version is now registered in the result when doing a Mobile Scan,

3.1.4. Mobile Scan (UPLINK2 -> Diagnostic) - now with timeout

In case the SiteManager is located in an area with poor connectivity, it can take up to 30-60 min to complete a full mobile Scan. From 7.3 there will be a limit to the time it will run.

In the example below the system aborts if the modem takes too long to respond, and is reported that the modem has failed:



```
Last scan: Thu Jul  6 22:44:14 2017

-- FW Information --
v3339_17274

-- HW Information --
Sierra Wireless, Incorporated MC8705; ID: 353567044431626; Rev.: T3_5      2014/11/10 18:11:43; SIM ID: 9012800:

-- SIM card Information --
SIM IMSI: 901280028004589
SMS service center: +316540967011

-- Mobile networks --
Test 1: Network scan for available networks
Network name        Short name          Network number
TELUS               TELUS               302220
Bell                Bell                302610
302 - 520                               302520
CAN Rogers Wireless Inc.ROGERS              302720
CAN Rogers Wireless Inc.ROGERS              302720

Test 2: Deregister from network and do a scan for avail
Network name        Short name          Network numb
Bell                Bell                302610
CAN Rogers Wireless Inc.ROGERS              3027
302 - 520                               30252
CAN Rogers Wireless Inc.ROGERS
TELUS               TELUS

-- Mobile network signal and cell ID
Test 3: Register to default netwo                  w status every 5
Network name        Network num                 ion status          Locati           ll ID          Mode      Signal (0-31)
                                            registered, searching                                           99
                                        Not registered, searching                                           99
                                        Not registered, searching                                           99
                                        Not registered, searching                                           99

Error: modem failure; aborting..

-- Press the HELP button for a trouble shooting guide --
```

e network signal a
3: Register to default
ork name Network nu
Error: modem failure; aborting..
-- Press the HELP button for a tr

3.2. SiteManager support for WiFi Access Point (AP)

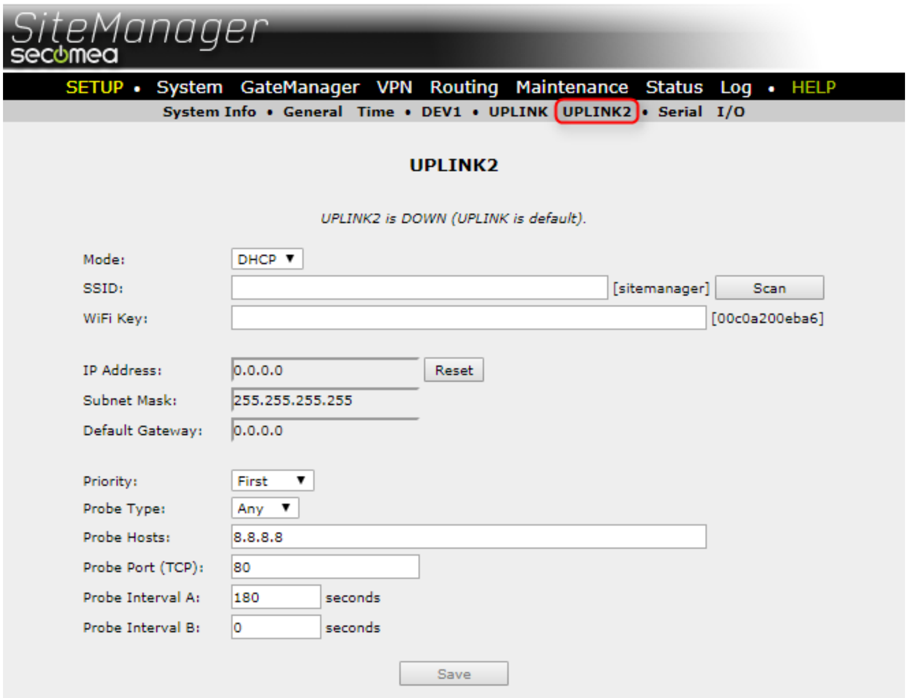
From release 7.3 you can insert a Secomea enabled WiFi USB adapter and enable WiFi AP mode on non xx49 models of SiteManagers.

Please note:

- Only WiFi USB adapters purchased through Secomea will be able to enable this functionality.
- Only the following SiteManager models will support WiFi AP mode:
  1129, 1139, 3329, 3339, 3429 and 1429.
- If the SiteManager was turned on when inserting the WiFi USB adapter, the SiteManager must be rebooted for the functionality to be enabled.

3.2.1. Release 7.2 or earlier

When a USB WiFi adapter was installed, the UPLINK2 interface showed this:


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
System Info • General Time • DEV1 • UPLINK UPLINK2 • Serial I/O

UPLINK2

UPLINK2 is DOWN (UPLINK is default).

Mode: DHCP ▼

SSID: [sitemanager] Scan

WiFi Key: [00c0a200eba6]

IP Address: 0.0.0.0 Reset

Subnet Mask: 255.255.255.255

Default Gateway: 0.0.0.0

Priority: First ▼

Probe Type: Any ▼

Probe Hosts: 8.8.8.8

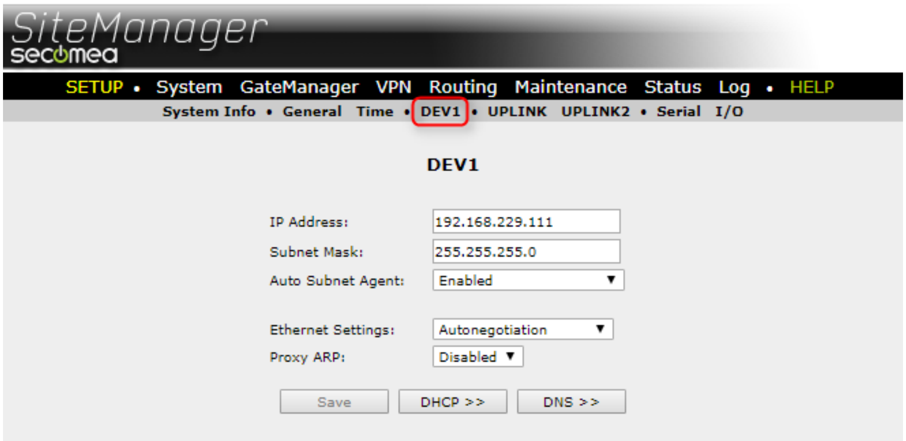
Probe Port (TCP): 80

Probe Interval A: 180 seconds

Probe Interval B: 0 seconds

Save

And the DEV interfaces showed this:


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
System Info • General Time • DEV1 • UPLINK UPLINK2 • Serial I/O

DEV1

IP Address: 192.168.229.111

Subnet Mask: 255.255.255.0

Auto Subnet Agent: Enabled ▼

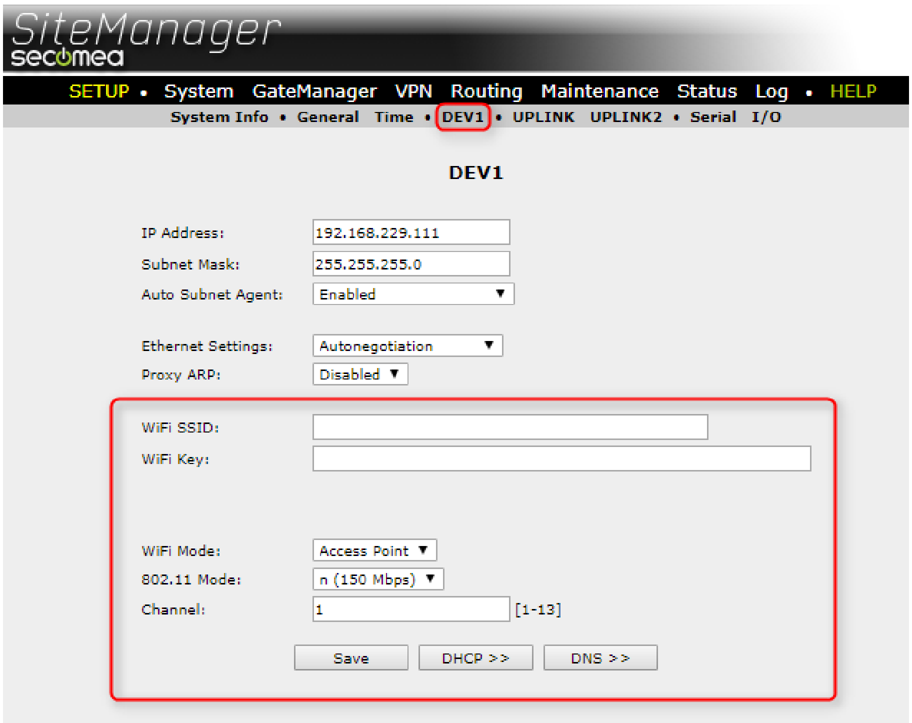
Ethernet Settings: Autonegotiation ▼

Proxy ARP: Disabled ▼

Save DHCP >> DNS >>

3.2.2. Release 7.3

From release 7.3, the following will be displayed on the DEV interface pages:


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
System Info • General Time • DEV1 • UPLINK UPLINK2 • Serial I/O
Save
DHCP >>
DNS >>

DEV1

IP Address: 192.168.229.111

Subnet Mask: 255.255.255.0

Auto Subnet Agent: Enabled

Ethernet Settings: Autonegotiation

Proxy ARP: Disabled

WiFi SSID:

WiFi Key:

WiFi Mode: Access Point

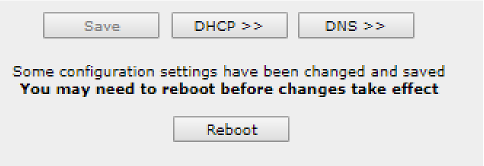
802.11 Mode: n (150 Mbps)

Channel: 1 [1-13]

To configure AP mode for the DEV1 interface, enter SSID and Key (required). Then select the 802.11 mode: “b (11Mbps)”, “g (54 Mbps)“ or “n (150 Mbps)”.

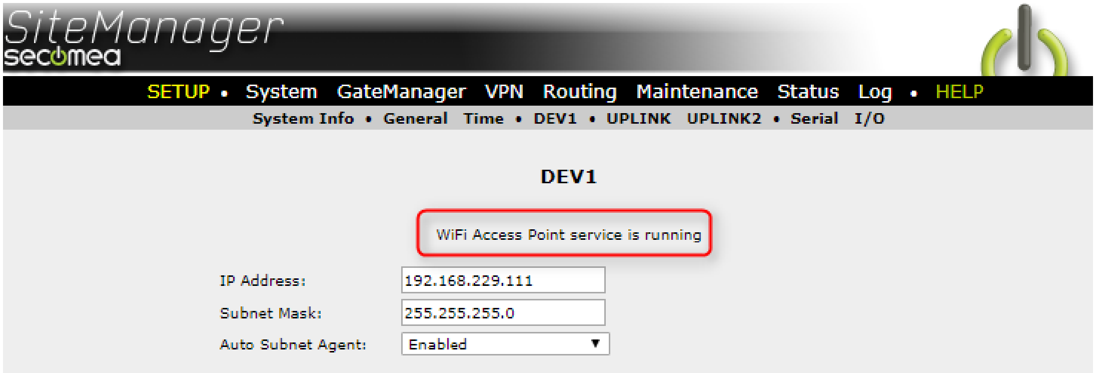
Please note that if the “WiFi SSID:” field is empty, it will default to the Device Name (not the Appliance name), this can be changed at “System -> General -> Device Name”. The default value is “SiteManager”.

When clicking Save, the system will ask you to reboot, to enable the changes.



Some configuration settings have been changed and saved
You may need to reboot before changes take effect

When the device has finished rebooting, it will display a status on the DEV1 page:


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
System Info • General Time • DEV1 • UPLINK UPLINK2 • Serial I/O

DEV1

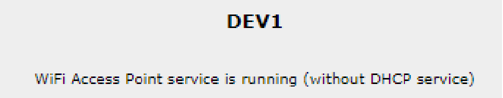
WiFi Access Point service is running

IP Address: 192.168.229.111

Subnet Mask: 255.255.255.0

Auto Subnet Agent: Enabled

If the DEV interface was configured without DHCP, the following message will appear:

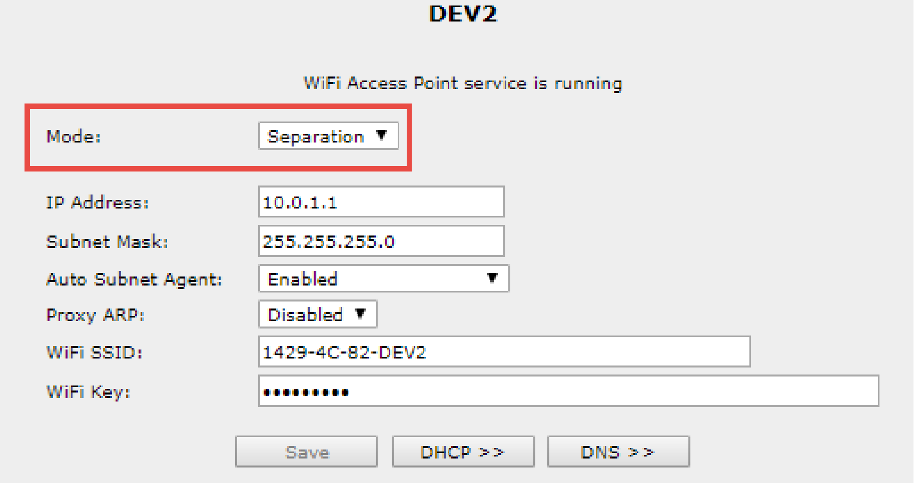


DEV1

WiFi Access Point service is running (without DHCP service)

3.2.3. 4-Port models

On 4-port models, each of the ports can be used as a separate Access Point (AP), provided that the Device interface is in separation mode:

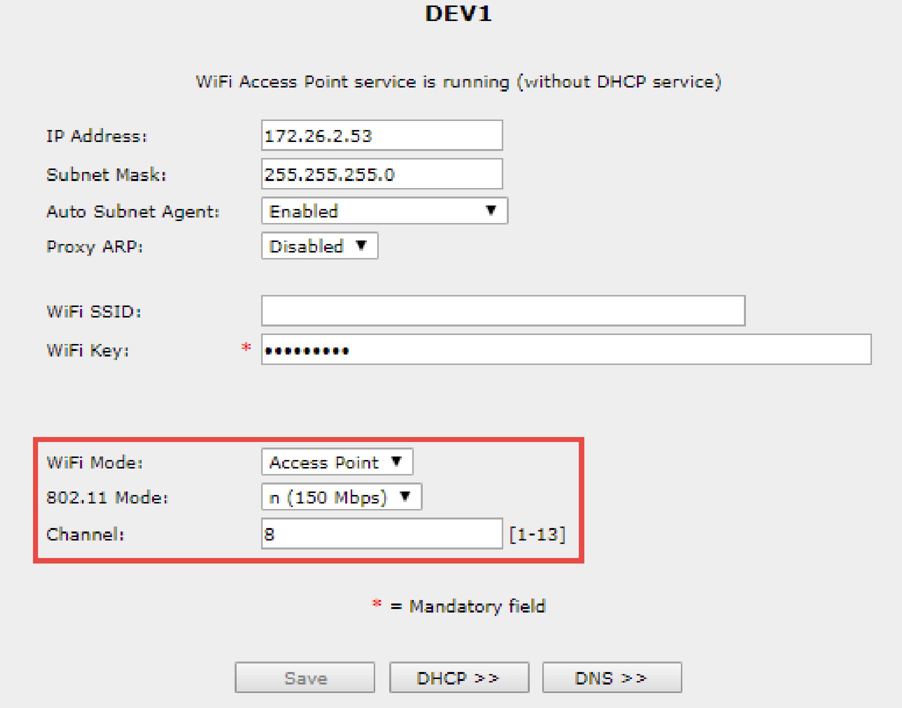


DEV2

WiFi Access Point service is running

Mode:	Separation ▼
IP Address:	10.0.1.1
Subnet Mask:	255.255.255.0
Auto Subnet Agent:	Enabled ▼
Proxy ARP:	Disabled ▼
WiFi SSID:	1429-4C-82-DEV2
WiFi Key:	•••••••••

The basic configuration of the AP mode is done on DEV1, just like the 2-port models:



DEV1

WiFi Access Point service is running (without DHCP service)

IP Address:	172.26.2.53
Subnet Mask:	255.255.255.0
Auto Subnet Agent:	Enabled ▼
Proxy ARP:	Disabled ▼
WiFi SSID:	
WiFi Key: *	•••••••••
WiFi Mode:	Access Point ▼
802.11 Mode:	n (150 Mbps) ▼
Channel:	8 [1-13]

* = Mandatory field

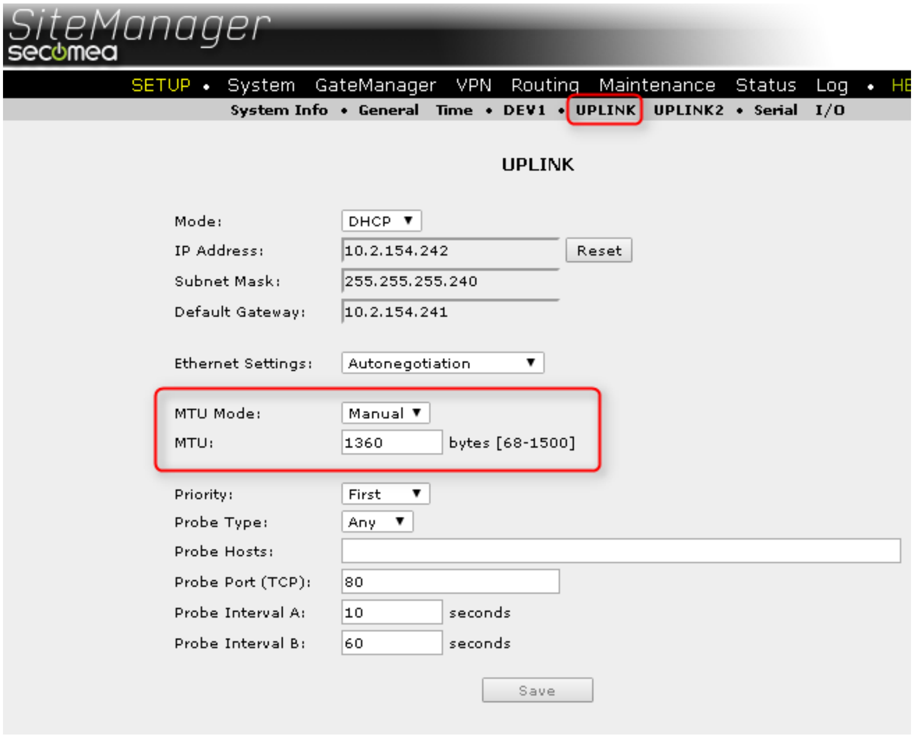
Up to 4 Access Points can be created this way, but the bandwidth will be shared among them, so please be aware of how many clients are connected at any time, and the type of traffic going through the WiFi channel.

Performance in “n” mode is expected to be 1100 kB/s (8,6 Mb/s), and slightly faster from Cable to WiFi.

3.3. MTU option on UPLINK

From 7.3 you have the option to set a max MTU size (Maximum Transmission Unit) on the UPLINK interface. If a situation arises that a component, router and/or firewall discards the necessary MTU path negotiation, it can in most cases be solved by lowering the MTU size.

Try setting the MTU size to 1360, this should help in most cases.


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HE
System Info • General Time • DEV1 • UPLINK UPLINK2 • Serial I/O
Reset
Save

UPLINK

Mode:	DHCP ▼
IP Address:	10.2.154.242
Subnet Mask:	255.255.255.240
Default Gateway:	10.2.154.241
Ethernet Settings:	Autonegotiation ▼
MTU Mode:	Manual ▼
MTU:	1360 bytes [68-1500]
Priority:	First ▼
Probe Type:	Any ▼
Probe Hosts:	
Probe Port (TCP):	80
Probe Interval A:	10 seconds
Probe Interval B:	60 seconds

3.4. Dynamic DNS in the Forwarding Agent

The **Forwarding Agent** in the SiteManager Hardware product line has been extended and enhanced in release 7.3:

These are the major additions to the agent:

- Dynamic hostname resolving within a set number of minutes.
- Support for DNS names on both sides of the “>/>>”: DNS names can now be applied on the source and destination part of the Forwarding Agent.
- Several changes to the GUI, to enhance the user experience and improve troubleshooting and overview.
- Extended logging to let an external syslog server track changes to DNS names.

For more detailed information, please refer to the guide “Forwarding Agent 7.3 - V1.2” in chapter 8.

3.5. Changes to the TroubleShoot functionality

3.5.1. Filter option

The troubleshoot information is also available in JSON, TEXT and HTML formats which can be used as an API for other systems, or requested directly from outside the box without username/password authentication, if it is requested from a device that is directly attached to one of the SiteManager's interfaces (i.e. not via a router).

The troubleshoot URL is:

https://<IPADDR>/tshoot?FORMAT+FILTER...

where IPADDR is an interface address on the SiteManager, and FORMAT is one of html, json, or text.

Without any +FILTER selectors, the entire troubleshoot information is returned for the URL. When you add one or more +FILTER selectors, only the selected sections are returned.

Possible filter selectors are:

Object selectors:

- **gm**: GateManager connection and configuration information
- **agents**: Lists configured agents and their status
- **routes**: SiteManager routing information
- **ifaces** (**dns**, **dhcp**): Network interface status and configuration. Adding “dns” and “dhcp” will show this information also.
- **probe**:
- **io**: Status of the I/O pins on the SiteManager
- **vpn**: The status of EasyTunnel, if configured

Add-on selectors:

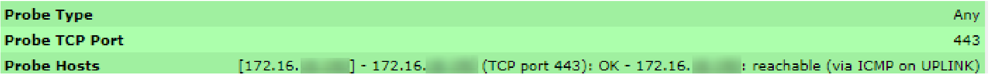
- **legend**: Show the legend list at the start of the output
- **help**: Show help for the different objects returned

The “dns”, “dhcp”, and probe selectors are only used with “ifaces”. When you specify a filter, the legend section and all help-texts are omitted unless you also specify “legend” and/or “help”, respectively.

Example: To get just the GateManager and IO-port status in JSON format, use https://<IPADDR>/tshoot?json+gm+io

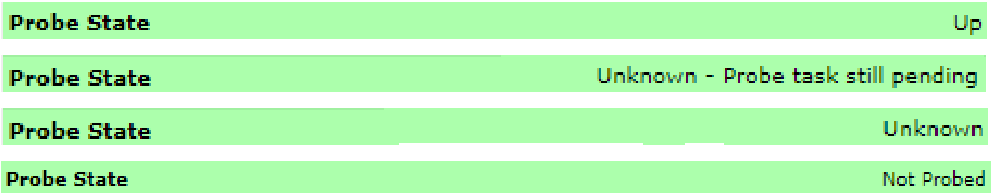
3.5.2. Probe State enhancement

Probe information will be shown for the UPLINK interface like this:



Probe Type	Any
Probe TCP Port	443
Probe Hosts	[172.16.[redacted]] - 172.16.[redacted] (TCP port 443): OK - 172.16.[redacted]: reachable (via ICMP on UPLINK)

If more than one UPLINK interface is preset (i.e. 1039), there will be a Probe State entry as well:



Probe State	Up
Probe State	Unknown - Probe task still pending
Probe State	Unknown
Probe State	Not Probed

3.5.3. Web Proxy format

In some cases, the Web Proxy Address would show as “Wrong format” when a DNS name was entered, this has been reworked in 7.3.

3.6. Proxy password supports Unicode

Unicoded password (UTF-8/16), like Japanese characters, are now supported for WEB Proxy authentication (Username/Password). NTLM, Basic and Digest authentication are also supported.

3.7. Other Agent updates

3.7.1. Hilscher -> USB agent

The Hilscher USB adapter NET100-RE-RS, with Vendor ID: 1939 and Product ID 0001 has been added.

Please note that the design of the unit makes it sensitive to low bandwith. It is expected to work on connection with RTT lower than 40ms.

3.7.2. Inovance -> USB/ETH agent

New vendor Inovance, with support for a PLC (AM600-CPU1608TP) with USB and ETH using InoProShop V1.1.0 and CoDeSys

Note: When using CoDeSys, it must be specifc CoDeSys software, otherwise the USB will fail.

3.7.3. Universal Robots -> VNC service

Added VNC service to the Universal Robots Ethernet agent.

3.7.4. Unitronics -> Remote Operator

Added a new option to the Unitronics Ethernet agent called “Enable Remote Operator access”. This will add an RDP service on port 20256.

3.7.5. BRControls -> Ethernet

Added new “Ethernet” agents, which should be used on all BRControls models except the BRC-45, which has its own agent.

3.7.6. Mitsubishi -> USB HMI (GOT series)

The agent connecting the Mitsubishi USB HMI’s have included the GOT2000 series HMI also.

4. SiteManager Embedded

4.1.1. Raised Interface Count on Linux

The number of supported interfaces enumerated by the SiteManager Embedded has been raised to 16.

This means that interfaces used by the SiteManager Embedded must be in the first 16 interfaces.

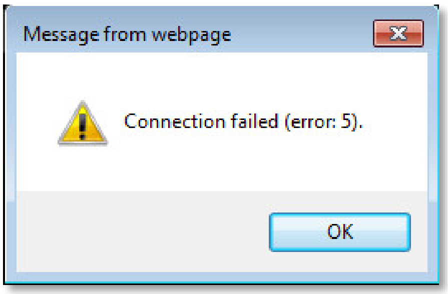
5. LinkManager

5.1. Updated feedback messages

A regression in 7.2 reintroduced non-humanized error messages.

Release 7.3 is now updated with the correct messages:

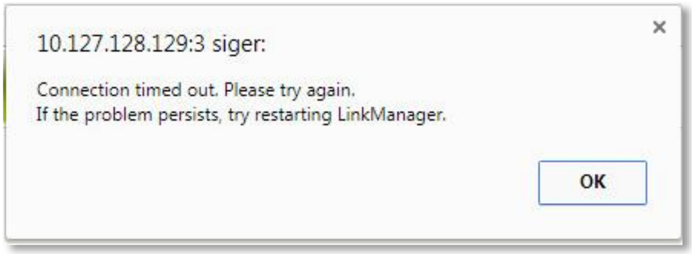
Old 7.2:



Message from webpage

Connection failed (error: 5).

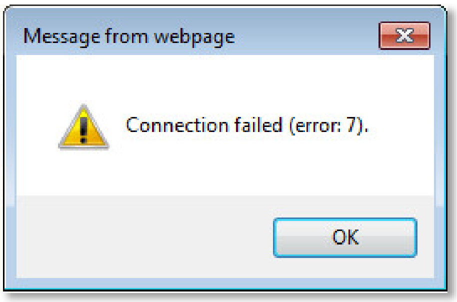
New 7.3:



10.127.128.129:3 siger:

Connection timed out. Please try again.
If the problem persists, try restarting LinkManager.

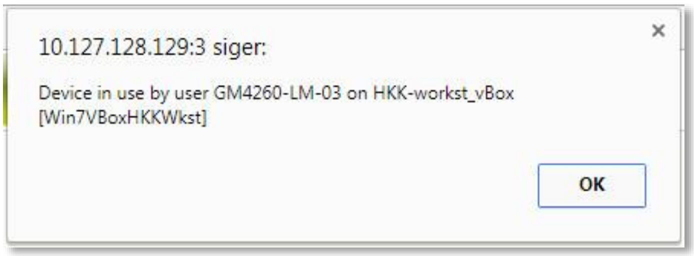
Old 7.2:



Message from webpage

Connection failed (error: 7).

New 7.3:



10.127.128.129:3 siger:

Device in use by user GM4260-LM-03 on HKK-workst_vBox
[Win7VBoxHKKWkst]

6. LinkManager Mobile

6.1. Updates to LinkManager Mobile

There have been no major updates to LinkManager mobile in this release.

7. Advanced Tech Topics

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

7.1. API changes

7.1.1. Reset and Factory Reset

It is now possible to make two types of reset from the API:

Reset: This deletes only the configuration.

Factory Reset: This will delete all configuration and all logs.

See chapter 3 in the SiteManager Embedded API documentation for 7.3 for detailed information.

8. Documentation

The following new documents have been created or updated:

SiteManager Embedded Function Reference - V1.7

Forwarding Agent 73 - V1.2

Appendix A

1. Troubleshooting Appliance TLS certificate

GateManager/SiteManager release 7.3 support upgraded Appliance TLS Certificate (SHA-256).

This Appendix should be referred to in case you decide to downgrade your GateManager or change the default settings. Otherwise, you will not be affected by any of the following scenarios.

Please notice: The new TLS certificate will automatically be installed from the License Portal if possible, if not, it can be installed manually as shown in chapter: “Appliance” connections upgraded to TLS 1.2/SHA-256.

1.1. Scenario 1: GateManager is downgraded

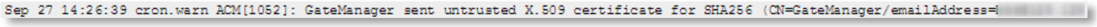
When the GateManager is upgraded to 7.3 and a SHA-256 TLS certificate is installed, all SiteManagers will upgrade the connection to SHA-256 + TLS 1.2 and reject any other SHA-1 or TLS 1.0 connections. This is only in case the SiteManager is also upgraded to 7.3 or later.

If you decide to downgrade your GateManager to 7.2 or older all your Appliances mentioned before will reject the GateManager because 7.2 only support TLS 1.0.

To recover the Appliance connection, you must reconfigure the GateManager address on the appliance. This will be a new situation and the Appliance will accept the GateManager again.

SiteManager with 7.3 will accept any old or new GateManager version. But as soon as the SiteManager has connected to a GateManager it will remember its GateManager security level and not accept a lower level.

SiteManager system log will show:



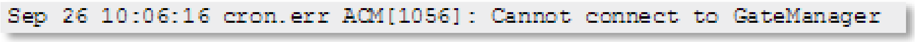
```
Sep 27 14:26:39 cron.warn ACM[1052]: GateManager sent untrusted X.509 certificate for SHA256 (CN=GateManager/emailAddress=[redacted]
```

1.2. Scenario 2: SHA-1 is disabled

GateManager is upgraded to 7.3 and a SHA-256 Appliance TLS certificate has been installed. Additional the old SHA-1 Appliance TLS has been disabled.

Result is that all SiteManagers with an old 7.2 firmware will not be able to connect to the GateManager.

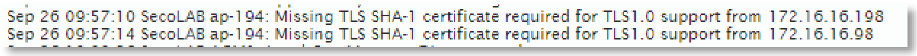
SiteManager system log will show:



```
Sep 26 10:06:16 cron.err ACM[1056]: Cannot connect to GateManager
```

GateManager system log will show:

Search for the public IP address of the SiteManager and the GateManager system log must show:



```
Sep 26 09:57:10 SecoLAB ap-194: Missing TLS SHA-1 certificate required for TLS1.0 support from 172.16.16.198
Sep 26 09:57:14 SecoLAB ap-194: Missing TLS SHA-1 certificate required for TLS1.0 support from 172.16.16.98
```

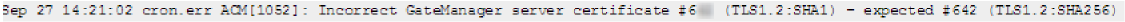
Note: reenabling a disabled SHA-1 TLS certificate requires a reboot of the GateManager.

The SiteManager will keep trying to reconnect to the GateManager so the SiteManagers with the old 7.2 firmware will connect as soon as the GateManager is online again.

1.3. Scenario 2: SHA-256 is disabled

If for some reason the SHA-256 TLS certificate is disabled, this could be in relation to restoring an old backup, all SiteManagers supporting SHA-256 TLS will start rejecting the GateManager.

SiteManager system log will show:



```
Sep 27 14:21:02 cron.err ACM[1052]: Incorrect GateManager server certificate #6[redacted] (TLS1.2:SHA1) - expected #642 (TLS1.2:SHA256)
```

As soon as you install the correct SHA-256 TLS certificate again, all SiteManagers will re-connect immediately.

/end

Secomea A/S

Denmark

CVR No. DK31 36 60 38

Email: info@secomea.com

www.secomea.com