New in Secomea Release 7.2

Nice to know information about the release:

- Secomea Release 7.2 build 17145 public 2017.04.07

Version: 1.2, 2017

Contents

Change log

Version	Change log
0.1	Initial version
0.2	Reformatting
0.4	Additional chapters added
0.5	Update .PACKAGE chapter 2.6
1.1	Final version
1.2	Added Extra Padlock case in Appendix A

1. RELEASE 7.2

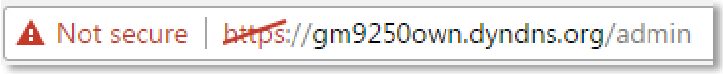
Release 7.2 includes several security related changes, details of which are not disclosed here. We strongly recommend that you upgrade all hardware and software devices to this release.

2. GateManager

2.1. Free Web-Server Certificate (Lets Encrypt)

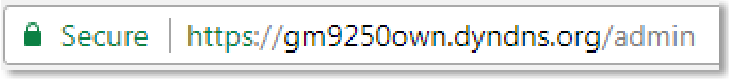
From GateManager release 7.2 it is now possible to install a royalty-free Web-server Certificate. If your server already has a trusted Web certificate there is no reason to use this option.

Before:



Not secure | ~~https~~://gm9250own.dyndns.org/admin

After:



Secure | https://gm9250own.dyndns.org/admin

We have implemented the Let's Encrypt service, and an install wizard that should be self-explained as far as possible.

Requirements:

- Full Qualified Domain Name - the GateManager will need a public DNS name
- There must be access from the internet to port 80 on the GateManager
- GateManager must have full DNS service access to the internet (outbound UDP port 53)
- The DNS name and the public IP address of the GateManager must be the same

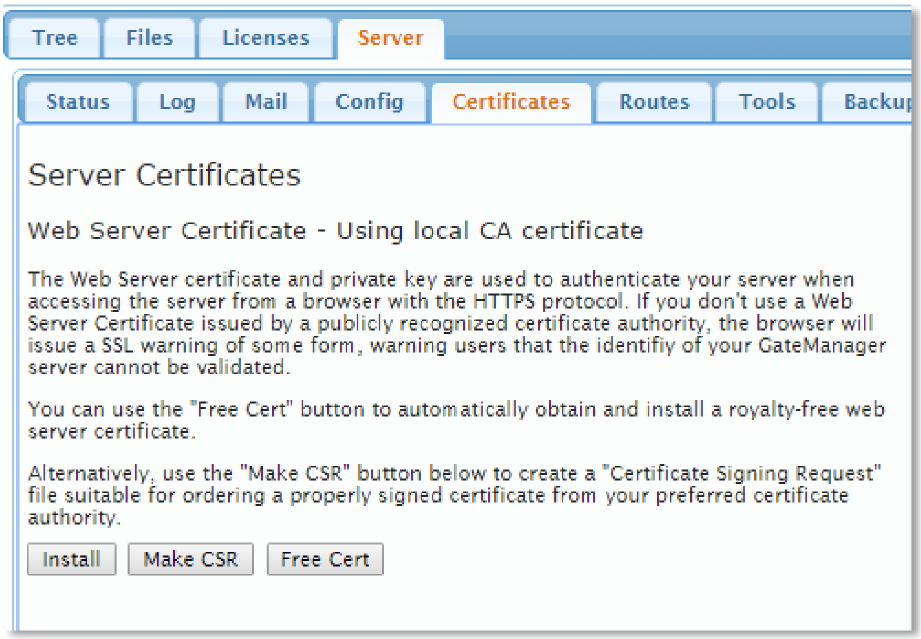
Some of the requirements are not mandatory and if the requirements are not fulfilled the installation wizard will prompt and guide with instructions.

Nice to know:

- The Web Certificate will automatically be renewed every 30 days.
- Do not manually try to renew the certificate too many times. There are a limit and exceeding this limit the GateManager will be rejected. Release time will be 7 days (see appendix).
- For testing it is recommended to use a staging server. (see appendix "Staging server for experimental tests")
- There is no guarantee that various web browser providers will NOT reject the Let's Encrypt CA in the future, but when writing this, the certificate has full support with all major browser providers.

2.1.1. Successful installation

Log in as Server Administrator and select Server -> Certificates.



Server Certificates

Web Server Certificate - Using local CA certificate

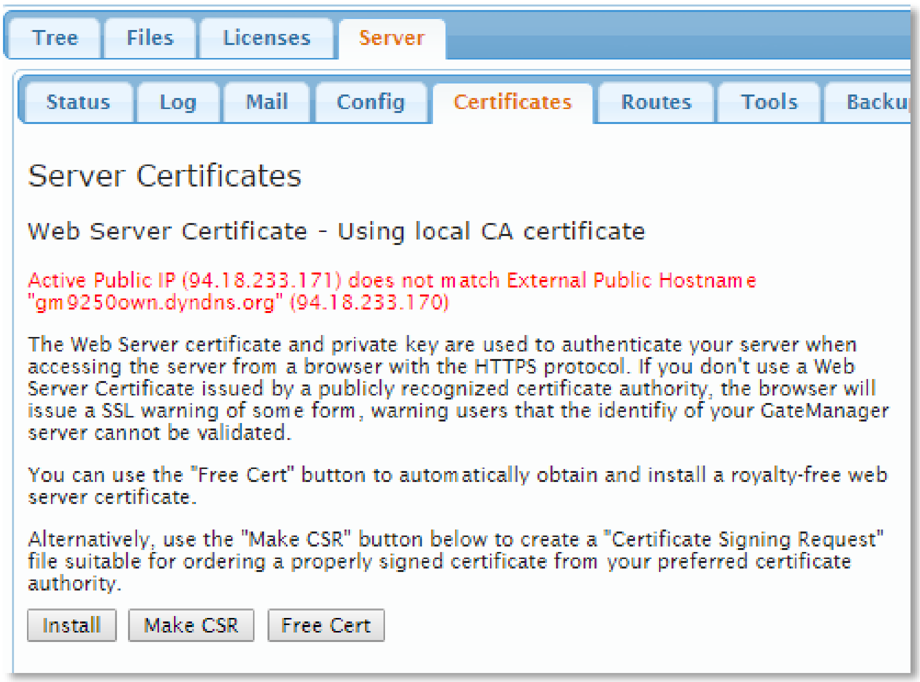
The Web Server certificate and private key are used to authenticate your server when accessing the server from a browser with the HTTPS protocol. If you don't use a Web Server Certificate issued by a publicly recognized certificate authority, the browser will issue a SSL warning of some form, warning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

This server is configured correct and you can press [Free Cert] to start the Let's Encrypt process.

If in case, there should be a configuration issue, it will be shown in red as shown in the figure below:



Server Certificates

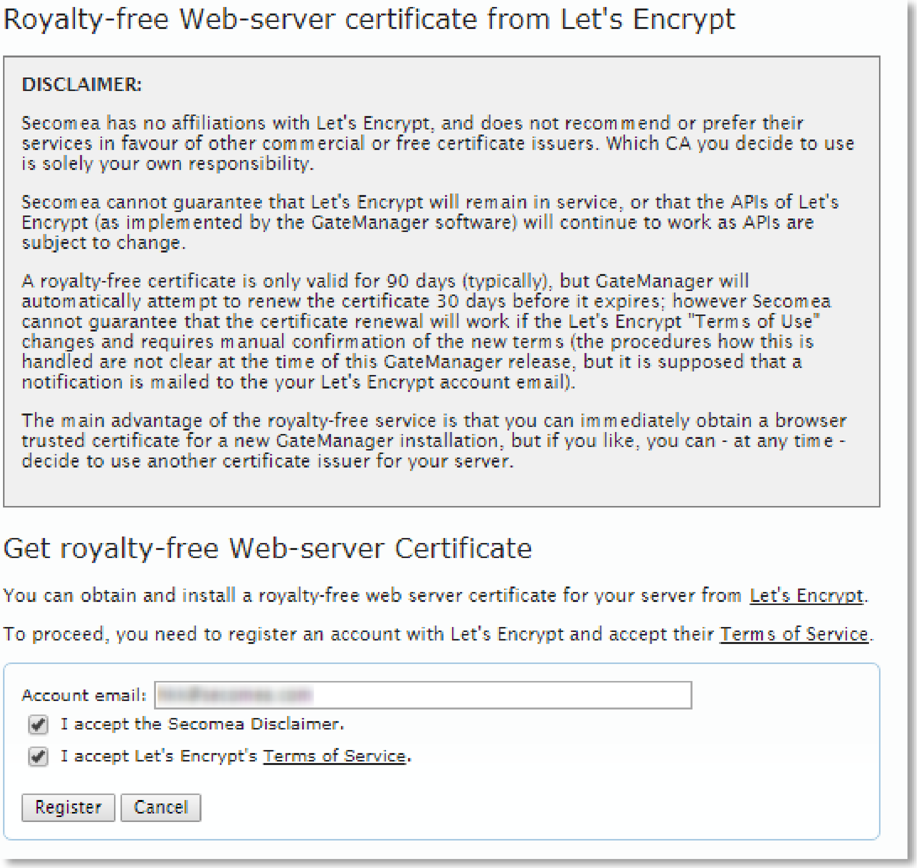
Web Server Certificate - Using local CA certificate

Active Public IP (94.18.233.171) does not match External Public Hostname "gm9250own.dyndns.org" (94.18.233.170)

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.



Royalty-free Web-server certificate from Let's Encrypt

DISCLAIMER:

Secomea has no affiliations with Let's Encrypt, and does not recommend or prefer their services in favour of other commercial or free certificate issuers. Which CA you decide to use is solely your own responsibility.

Secomea cannot guarantee that Let's Encrypt will remain in service, or that the APIs of Let's Encrypt (as implemented by the GateManager software) will continue to work as APIs are subject to change.

A royalty-free certificate is only valid for 90 days (typically), but GateManager will automatically attempt to renew the certificate 30 days before it expires; however Secomea cannot guarantee that the certificate renewal will work if the Let's Encrypt "Terms of Use" changes and requires manual confirmation of the new terms (the procedures how this is handled are not clear at the time of this GateManager release, but it is supposed that a notification is mailed to the your Let's Encrypt account email).

The main advantage of the royalty-free service is that you can immediately obtain a browser trusted certificate for a new GateManager installation, but if you like, you can - at any time - decide to use another certificate issuer for your server.

Get royalty-free Web-server Certificate

You can obtain and install a royalty-free web server certificate for your server from Let's Encrypt.

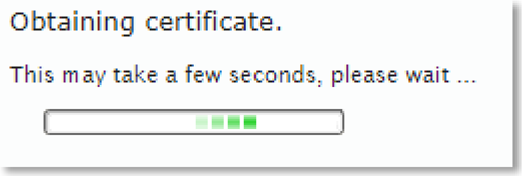
To proceed, you need to register an account with Let's Encrypt and accept their Terms of Service.

Account email: [redacted]

☑ I accept the Secomea Disclaimer.

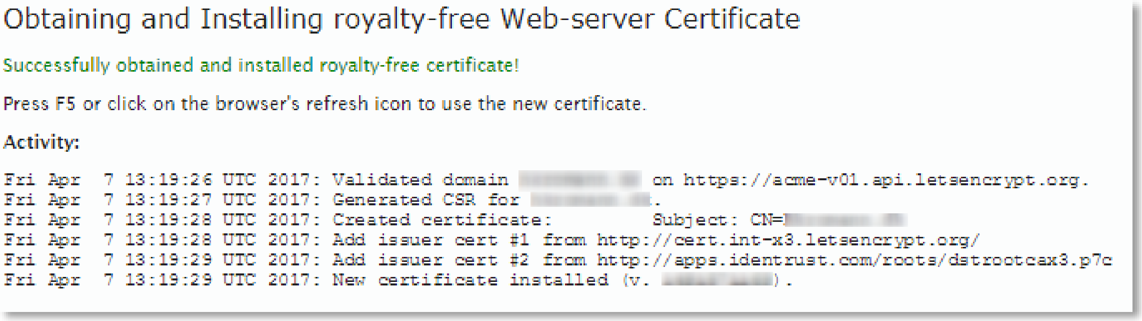
☑ I accept Let's Encrypt's Terms of Service.

Pressing the [Register] button will start the Web-server Certificate process and the certificate will automatically be installed.



Obtaining certificate.

This may take a few seconds, please wait ...



Obtaining and Installing royalty-free Web-server Certificate

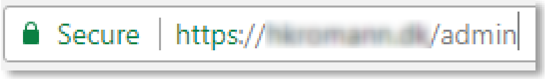
Successfully obtained and installed royalty-free certificate!

Press F5 or click on the browser's refresh icon to use the new certificate.

Activity:

```
Fri Apr  7 13:19:26 UTC 2017: Validated domain [redacted] on https://acme-v01.api.letsencrypt.org.
Fri Apr  7 13:19:27 UTC 2017: Generated CSR for [redacted].
Fri Apr  7 13:19:28 UTC 2017: Created certificate:        Subject: CN=[redacted]
Fri Apr  7 13:19:28 UTC 2017: Add issuer cert #1 from http://cert.int-x3.letsencrypt.org/
Fri Apr  7 13:19:29 UTC 2017: Add issuer cert #2 from http://apps.identrust.com/roots/dstrootcax3.p7c
Fri Apr  7 13:19:29 UTC 2017: New certificate installed (v. [redacted]).
```

The browser address bar should now show:

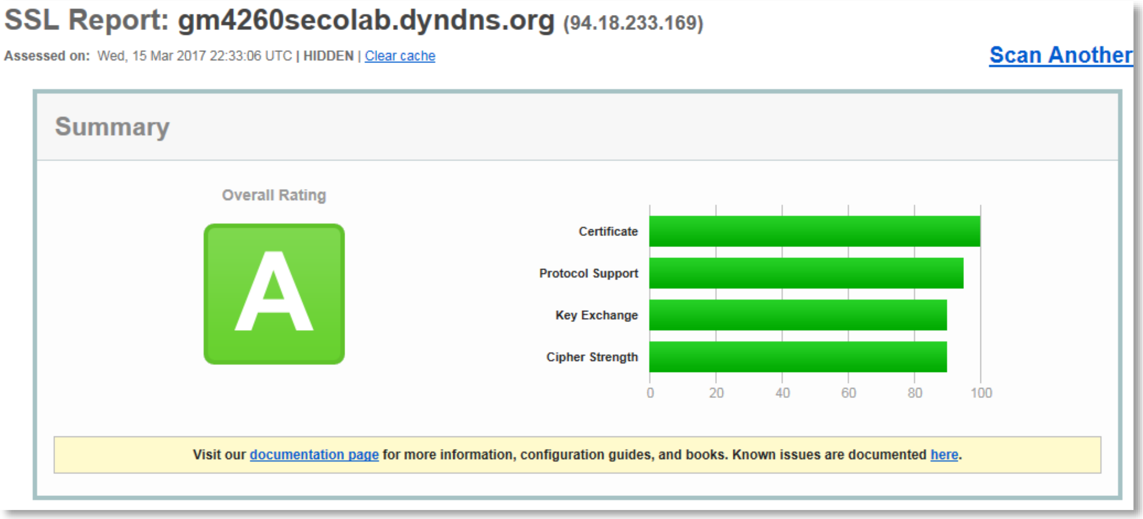


Secure | https://[redacted]/admin

You might need to close the browser to make a fresh update.

For troubleshooting and more information see APPENDIX – Let’s Encrypt

2.1.2. SSL test using Free Web-certificate - Top Rating



SSL Report: gm4260secolab.dyndns.org (94.18.233.169)

Assessed on: Wed, 15 Mar 2017 22:33:06 UTC | HIDDEN | Clear cache

Scan Another

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

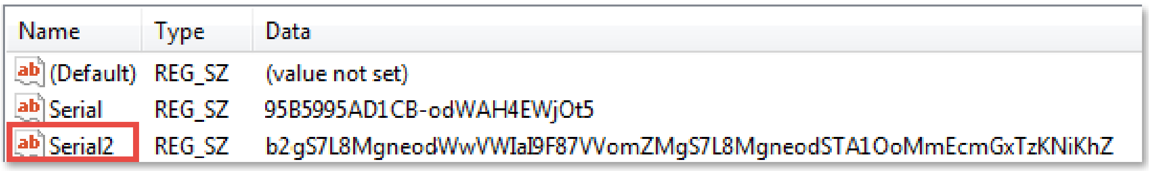
On this GateManager we installed a free Let's Encrypt Web-server Certificate and ran an online SSL scan from "ssllabs.com".

2.2. Secondary ID (Serial 2)

Requirements:

- Both SiteManager and GateManager must run 7.2 to activate Secondary ID.

From release 7.2, all appliances have been issued a Secondary ID.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Serial	REG_SZ	95B5995AD1CB-odWAH4EWjOt5
Serial2	REG_SZ	b2gS7L8MgneodWwVWIaI9F87VVomZMgS7L8MgneodSTA1OoMmEcmGxTzKNiKhZ

In addition to the normal serial number generated by the appliance, we have added a Secondary ID (also named "Serial2") to enhance security.

2.2.1. Secondary ID secure your SiteManager

The first time a SiteManager connect to a GateManager version 7.2 it will exchange the Secondary ID and only GateManager and this SiteManager will know this number. If another SiteManager try to reuse a previous SiteManager's connection it will be rejected because it doesn't know the Secondary ID.

This is especially important for SiteManager Embedded that in some cases can be hard copied and thereby use the same Serial number, but Serial2 (Secondary ID) will be unique.

2.2.2. Known issues implementing Secondary ID

In general, there will be no issue when starting using the Secondary ID implemented in 7.2. It is only in case a SiteManager is downgraded to pre-7.2 releases or for some reason has been flashed and the Secondary ID has been removed. For more details about issues see APPENDIX – Troubleshooting Secondary ID

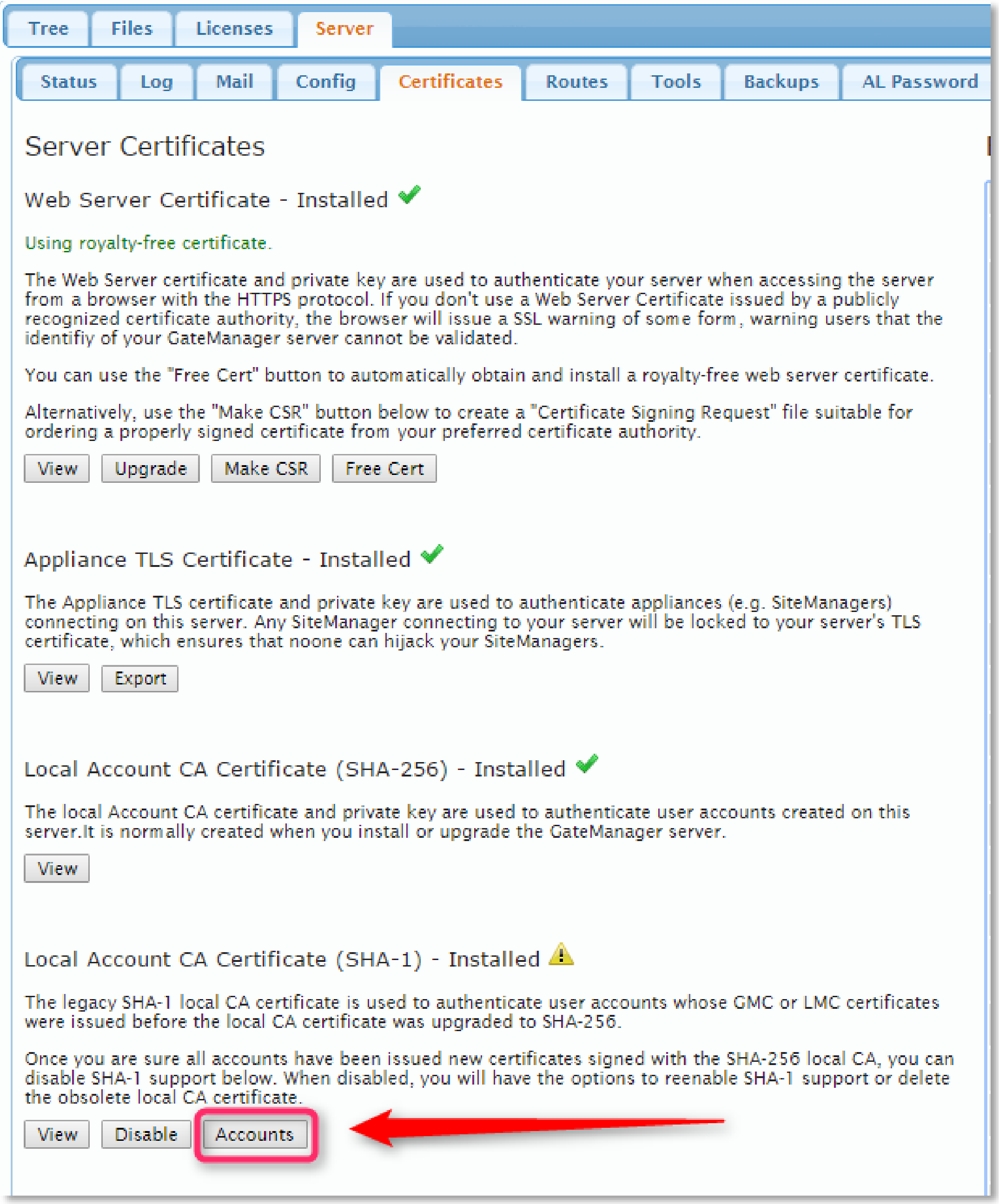
2.3. Account Certificates changed to SHA-256

From release 7.2, the GateManager will start using SHA-256 certificates for all accounts created after the upgrade.

Old and existing accounts will continue to use the previous SHA-1 certificate until it is renewed.

Renewing account certificates can be performed on each account or using the global renew feature.

This requires a Server Administrator account.



Server Certificates

Web Server Certificate - Installed ✓

Using royalty-free 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 Certificate - Installed ✓

The Appliance TLS certificate and private key are used to authenticate appliances (e.g. SiteManagers) connecting on this server. Any SiteManager connecting to your server will be locked to your server's TLS certificate, which ensures that noone can hijack your SiteManagers.

Local Account CA Certificate (SHA-256) - Installed ✓

The local Account CA certificate and private key are used to authenticate user accounts created on this server.It is normally created when you install or upgrade the GateManager server.

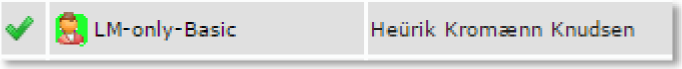
Local Account CA Certificate (SHA-1) - Installed ⚠

The legacy SHA-1 local CA certificate is used to authenticate user accounts whose GMC or LMC certificates were issued before the local CA certificate was upgraded to SHA-256.

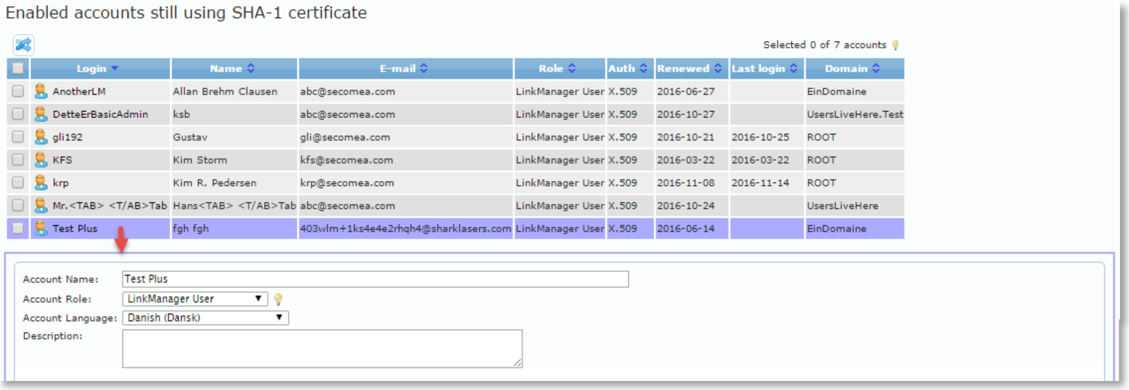
Once you are sure all accounts have been issued new certificates signed with the SHA-256 local CA, you can disable SHA-1 support below. When disabled, you will have the options to reenable SHA-1 support or delete the obsolete local CA certificate.

When pressing the “Accounts” button a list of all accounts that are using the old SHA-1 certificate will be shown. From this menu, it is possible to renew all or selected accounts in one go.

When an account is renewed, it will be marked as shown below:



✓	LM-only-Basic	Heürik Kromænn Knudsen



Enabled accounts still using SHA-1 certificate

Selected 0 of 7 accounts

☐	Login	Name	E-mail	Role	Auth	Renewed	Last login	Domain
☐	AnotherLM	Allan Brehm Clausen	abc@secomea.com	LinkManager User	X.509	2016-06-27		EinDomaine
☐	DetteErBasicAdmin	ksb	abc@secomea.com	LinkManager User	X.509	2016-10-27		UsersLiveHere.Test
☐	gli192	Gustav	gli@secomea.com	LinkManager User	X.509	2016-10-21	2016-10-25	ROOT
☐	KFS	Kim Storm	kfs@secomea.com	LinkManager User	X.509	2016-03-22	2016-03-22	ROOT
☐	krp	Kim R. Pedersen	krp@secomea.com	LinkManager User	X.509	2016-11-08	2016-11-14	ROOT
☐	Mr.<TAB> <T/AB>Tab	Hans<TAB> <T/AB>Tab	abc@secomea.com	LinkManager User	X.509	2016-10-24		UsersLiveHere
☐	Test Plus	fgh fgh	403wlm+1ks4e4e2rhqh4@sharklasers.com	LinkManager User	X.509	2016-06-14		EinDomaine

Account Name: Test Plus

Account Role: LinkManager User

Account Language: Danish (Dansk)

Description:

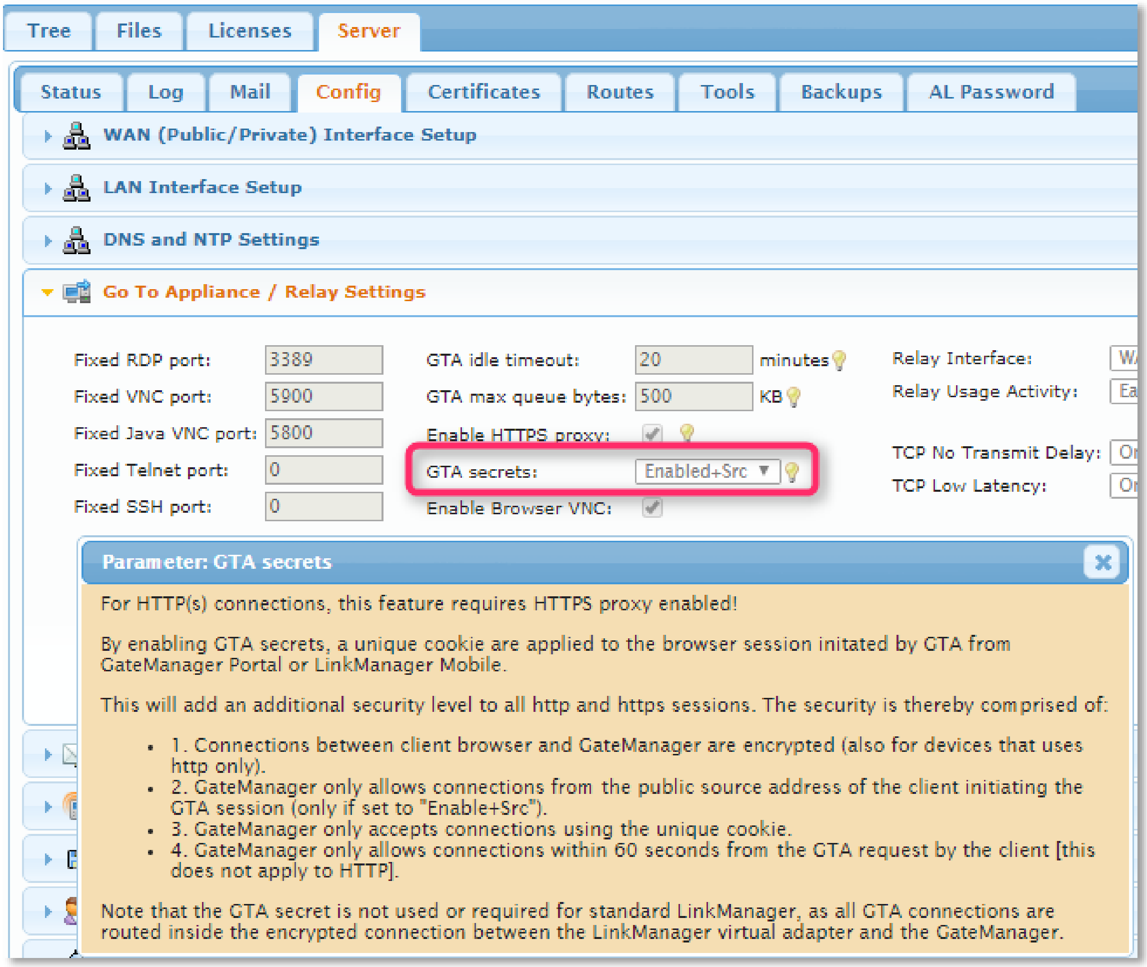
IMPORTANT! – renewing an account will send a new account certificate to the user and the old certificate can no longer be used.

2.4. GateManager support dual source IP

From release 7.2 it is now possible to disable the source IP restrictions on the GateManager. Previous GateManager versions would have a restriction on the source IP of the client this is no longer necessary due to the encryption implemented. This also solves the cases where a company is using dual internet connections for load balancing or as many mobile internet providers are using multiple gateways to the internet.

GateManager Server Administrators only:

Server > Config > Go To Appliance / Relay Settings:



Fixed RDP port: 3389

Fixed VNC port: 5900

Fixed Java VNC port: 5800

Fixed Telnet port: 0

Fixed SSH port: 0

GTA idle timeout: 20 minutes

GTA max queue bytes: 500 KB

Enable HTTPS proxy: ☑

GTA secrets: Enabled+Src

Enable Browser VNC: ☑

Relay Interface: W

Relay Usage Activity: Ea

TCP No Transmit Delay: O

TCP Low Latency: O

Parameter: GTA secrets

For HTTP(s) connections, this feature requires HTTPS proxy enabled!

By enabling GTA secrets, a unique cookie are applied to the browser session initated by GTA from GateManager Portal or LinkManager Mobile.

This will add an additional security level to all http and https sessions. The security is thereby comprised of:

- 1. Connections between client browser and GateManager are encrypted (also for devices that uses http only).
- 2. GateManager only allows connections from the public source address of the client initiating the GTA session (only if set to "Enable+Src").
- 3. GateManager only accepts connections using the unique cookie.
- 4. GateManager only allows connections within 60 seconds from the GTA request by the client [this does not apply to HTTP].

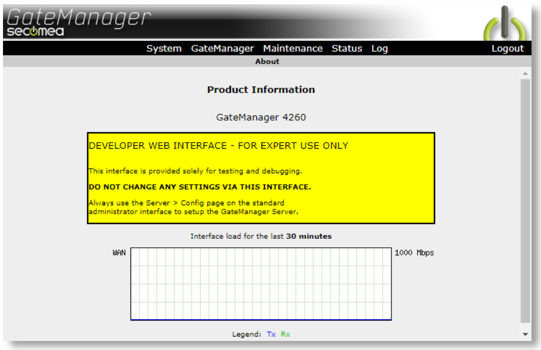
Note that the GTA secret is not used or required for standard LinkManager, as all GTA connections are routed inside the encrypted connection between the LinkManager virtual adapter and the GateManager.

Note: This don not relate to LinkManager GTA (Go To Appliance) because it always use a tunnelled connection.

2.5. Internal DEBUG GUI

By default, the Debug GUI has been disabled.

Debug GUI on https://<SERVERIP>:444 enables access to the GateManager backend OS and is only useful for debugging and troubleshooting.



Product Information

GateManager 4260

DEVELOPER WEB INTERFACE - FOR EXPERT USE ONLY

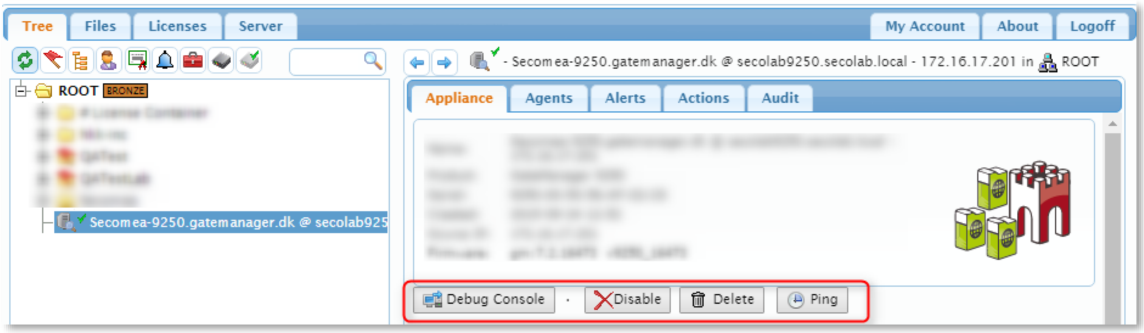
This interface is provided solely for testing and debugging.

DO NOT CHANGE ANY SETTINGS VIA THIS INTERFACE.

Always use the Server > Config page on the standard administrator interface to setup the GateManager Server.

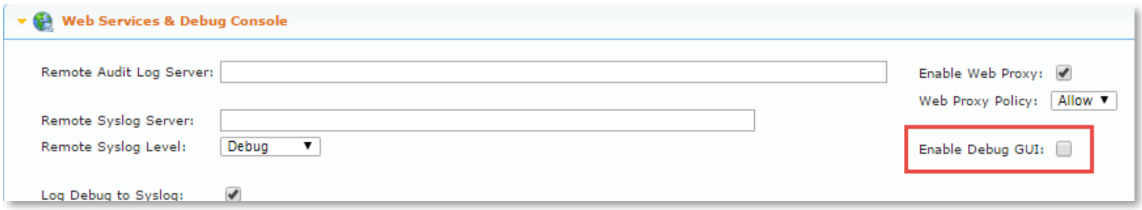
Interface load for the last 30 minutes

The “Debug GUI” button has been removed from the GateManager Appliance view:



- Secomea-9250.gatemanager.dk @ secolab9250.secolab.local - 172.16.17.201 in ROOT

To enable the Debug GUI again, go to Server -> Config -> Web Services & Debug Console:



Remote Audit Log Server:

Remote Syslog Server:

Remote Syslog Level: Debug

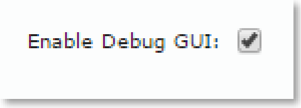
Log Debug to Syslog: ☑

Enable Web Proxy: ☑

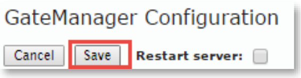
Web Proxy Policy: Allow

Enable Debug GUI: □

Place a checkmark and click “Save”:

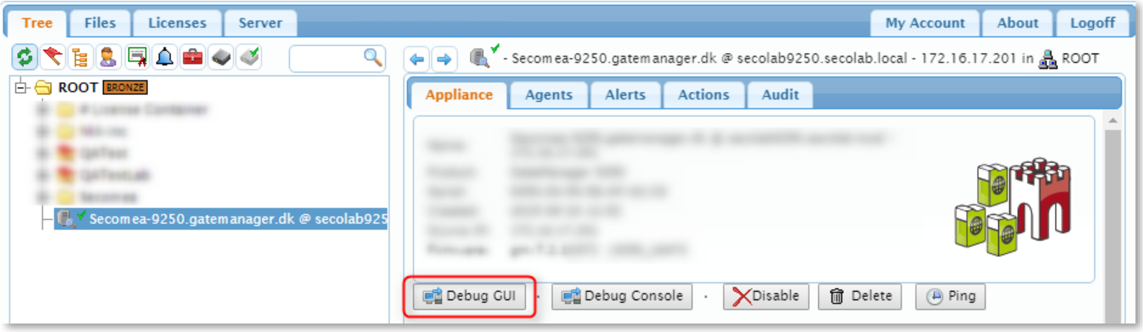


Enable Debug GUI: ☑



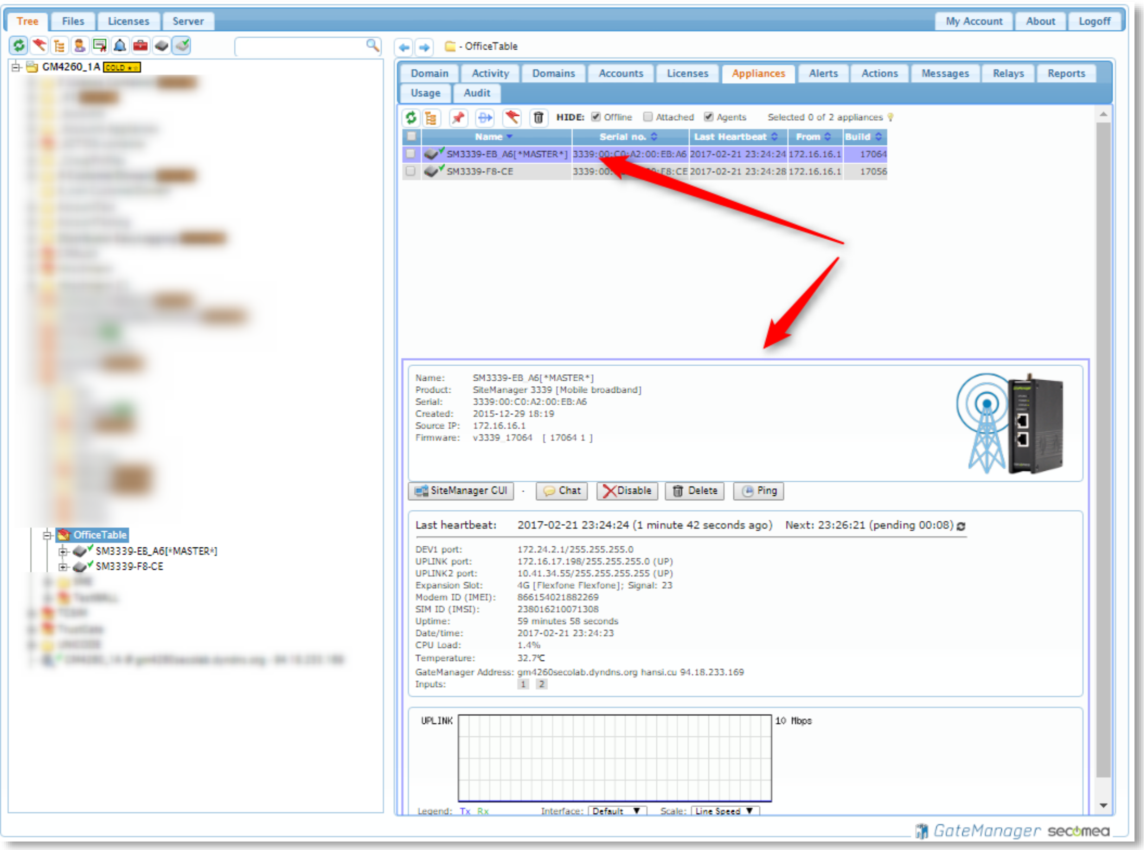
Restart server: □

After a refresh of the GateManager view, the “Debug GUI” button will have returned:



- Secomea-9250.gatemanager.dk @ secolab9250.secolab.local - 172.16.17.201 in ROOT

2.6. Show selected item details in the right-side panel



HIDE: ☑ Offline □ Attached ☑ Agents Selected 0 of 2 appliances

□	Name	Serial no.	Last Heartbeat	From	Build
□	SM3339-EB_A6[*MASTER*]	3339:00:C0:A2:00:EB:A6	2017-02-21 23:24:24	172.16.16.1	17064
□	SM3339-F8-CE	3339:00:[illegible]:F8:CE	2017-02-21 23:24:28	172.16.16.1	17056

Name:	SM3339-EB_A6[*MASTER*]
Product:	SiteManager 3339 [Mobile broadband]
Serial:	3339:00:C0:A2:00:EB:A6
Created:	2015-12-29 18:19
Source IP:	172.16.16.1
Firmware:	v3339_17064 [17064 1]

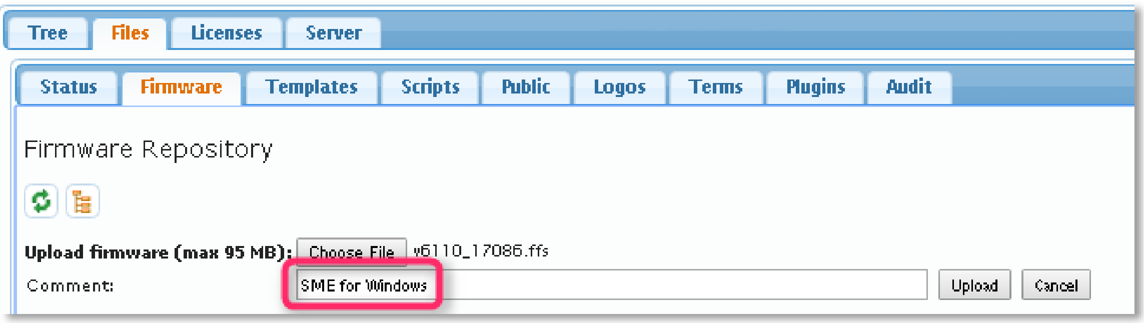
Last heartbeat: 2017-02-21 23:24:24 (1 minute 42 seconds ago) Next: 23:26:21 (pending 00:08)

DEV1 port:	172.24.2.1/255.255.255.0
UPLINK port:	172.16.17.198/255.255.255.0 (UP)
UPLINK2 port:	10.41.34.55/255.255.255.255 (UP)
Expansion Slot:	4G [Flexfone Flexfone]; Signal: 23
Modem ID (IMEI):	866154021882269
SIM ID (IMSI):	238016210071308
Uptime:	59 minutes 58 seconds
Date/time:	2017-02-21 23:24:23
CPU Load:	1.4%
Temperature:	32.7℃
GateManager Address:	gm4260secolab.dyndns.org hansi.cu 94.18.233.169
Inputs:	1 2

From any list in the right-side window you can now click an item to show the appliance/object details below.

2.7. Comment on Firmware

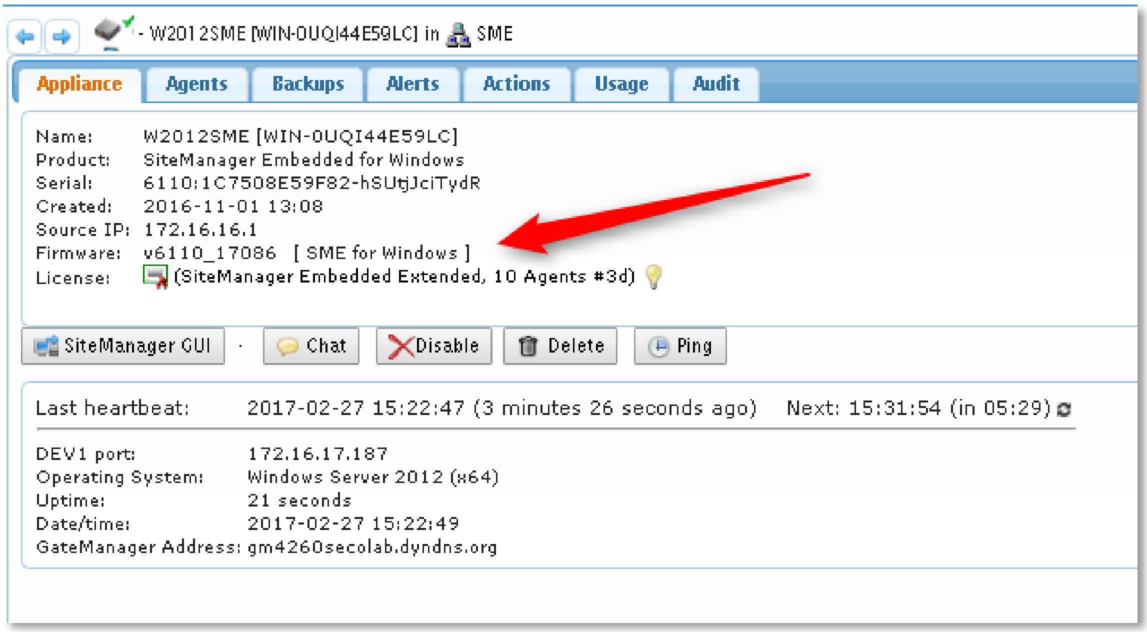
As always you can add a comment to the uploaded firmware on the GateManager Server. From 7.2 this comment will also be shown in the appliance detail window.



Upload firmware (max 95 MB): v6110_17086.ffs

Comment: SME for Windows

Add a Comment when uploading a new firmware, i.e. “SME for Windows”.



Name: W2012SME [WIN-0UQI44E59LC]
Product: SiteManager Embedded for Windows
Serial: 6110:1C7508E59F82-hSUtjJciTydR
Created: 2016-11-01 13:08
Source IP: 172.16.16.1
Firmware: v6110_17086 [SME for Windows]
License: (SiteManager Embedded Extended, 10 Agents #3d)

Last heartbeat: 2017-02-27 15:22:47 (3 minutes 26 seconds ago) Next: 15:31:54 (in 05:29)

DEV1 port: 172.16.17.187
Operating System: Windows Server 2012 (x64)
Uptime: 21 seconds
Date/time: 2017-02-27 15:22:49
GateManager Address: gm4260secolab.dyndns.org

The Comment is then shown after the firmware build number. This is intended to link a product number, like v6110, to a description.

The fact that this SiteManager Embedded (SME) is for a Windows operation system will now be explained by the text “[SME for Windows]”.

If you need to change the comment, just upload the firmware one more time.

2.8. Firmware comment autogenerated from firmware pack

From release 7.2 you can make your own ZIP archive of firmware bundles that each contain a comment as described in the “Comment on Firmware” chapter. In this way, you do not have to enter a comment when you upload the ZIP archive to the GateManager.

This is only relevant if you have your own GateManager. These comments can only be changed or created by the Server Administrator.

2.8.1. Example of firmware comments

Create a folder on your local PC called “Release 7.2”.

In this folder, create a text file called “.PACKAGE.TXT” (including the leading . (dot)).

Edit the “.PACKAGE.TXT” file so that it contains one line:

```
PACKAGE=Public_Release_7.2
```

Paste in all the firmware files (*.ffs) in to this folder and ZIP it in to the file:

Public_Release_7.2.zip

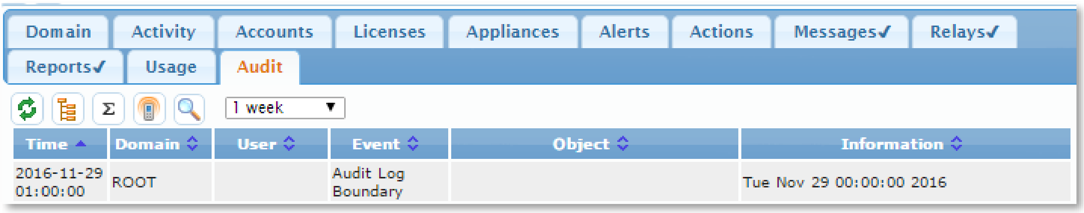
Uploading the zip file to GateManager will automatically create the comment “Public Release 7.2” for all firmware files.

2.8.2. Individual comments

If you need to have a different comment for one or more firmware files you just to create a sub-folder (any name will do) and place a “.PACKAGE.TXT” file in this folder together with the .ffs file.

2.9. “Audit Log Boundary” once every day (log heartbeat)

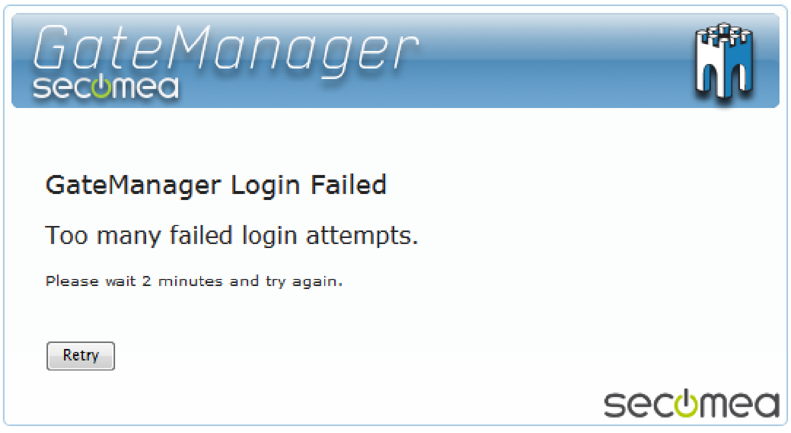
A customer request to monitor if the system is still alive has been implemented. In case the GateManager has not reported anything to the event log or to the remote syslog we now send a boundary log every day at 00:00 o’clock that serves as a heartbeat.



Time	Domain	User	Event	Object	Information
2016-11-29 01:00:00	ROOT		Audit Log Boundary		Tue Nov 29 00:00:00 2016

2.10. Failed Login Limits with certificate

Just as “Username/Password” accounts on the GateManager, certificate logins are now a part of the Failed Login limits. More than 3 failed logins will result in the following:



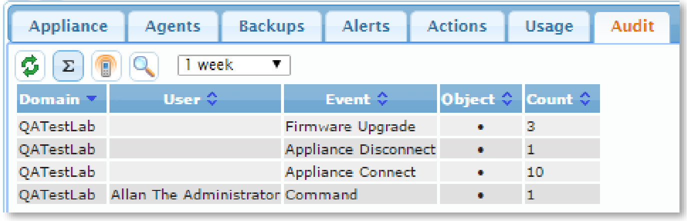
GateManager Login Failed

Too many failed login attempts.

Please wait 2 minutes and try again.

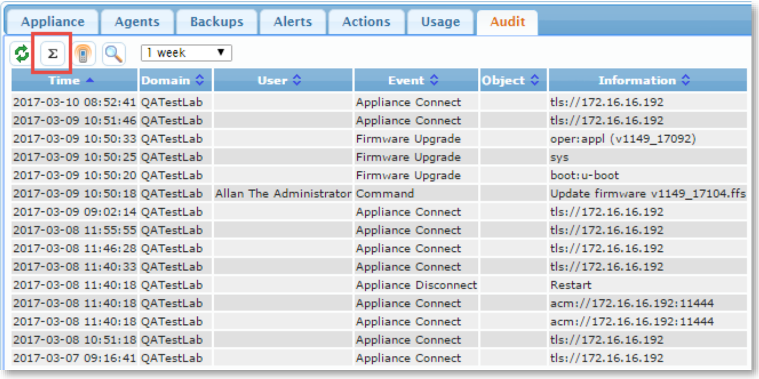
2.11. Audit log Summary View not default

Beginning from 7.2, the Summary View in the Audit tab is no longer the default view. Before 7.2 it would look like this:



Domain	User	Event	Object	Count
QATestLab		Firmware Upgrade	•	3
QATestLab		Appliance Disconnect	•	1
QATestLab		Appliance Connect	•	10
QATestLab	Allan The Administrator	Command	•	1

After 7.2, the default setting the same data will now look like this:

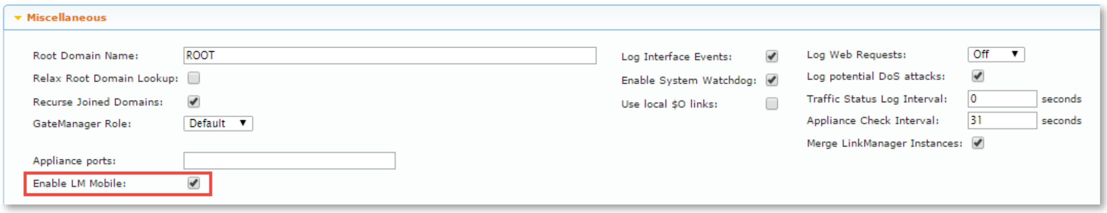


Time	Domain	User	Event	Object	Information
2017-03-10 08:52:41	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-09 10:51:46	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-09 10:50:33	QATestLab		Firmware Upgrade		oper:appl (v1149_17092)
2017-03-09 10:50:25	QATestLab		Firmware Upgrade		sys
2017-03-09 10:50:20	QATestLab		Firmware Upgrade		boot:u-boot
2017-03-09 10:50:18	QATestLab	Allan The Administrator	Command		Update firmware v1149_17104.ffs
2017-03-09 09:02:14	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-08 11:55:55	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-08 11:46:28	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-08 11:40:33	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-08 11:40:18	QATestLab		Appliance Disconnect		Restart
2017-03-08 11:40:18	QATestLab		Appliance Connect		acm://172.16.16.192:11444
2017-03-08 11:40:18	QATestLab		Appliance Connect		acm://172.16.16.192:11444
2017-03-08 10:51:18	QATestLab		Appliance Connect		tls://172.16.16.192
2017-03-07 09:16:41	QATestLab		Appliance Connect		tls://172.16.16.192

2.12. Disabling LinkManager Mobile

It is now possible to disable LinkManager Mobile globally on the server.

This can only be done in “Expert Mode” under “Server -> Config -> Miscellaneous”:



Miscellaneous

Root Domain Name: ROOT
Relax Root Domain Lookup: ☐
Recurse Joined Domains: ☑
GateManager Role: Default ▼
Appliance ports:
Enable LM Mobile: ☑

Log Interface Events: ☑
Enable System Watchdog: ☑
Use local $0 links: ☐

Log Web Requests: Off ▼
Log potential DoS attacks: ☑
Traffic Status Log Interval: 0 seconds
Appliance Check Interval: 31 seconds
Merge LinkManager Instances: ☑

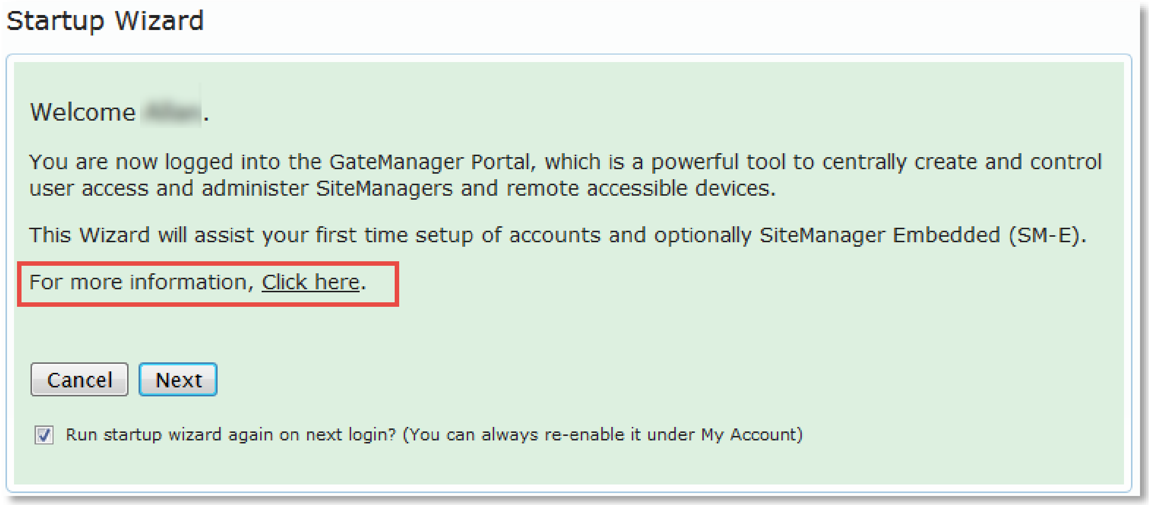
Turning this option off will not block the LinkManager Mobile login screen. When the user is authenticated, the server will display the following message:

```
GateManager Login Failed
LinkManager Mobile service is disabled.
```

This option will not require a reboot of the server.

2.13. New Startup Wizard welcome screen

The Startup Wizard now contains a link to the Getting Started guide:



Startup Wizard

Welcome [redacted].

You are now logged into the GateManager Portal, which is a powerful tool to centrally create and control user access and administer SiteManagers and remote accessible devices.

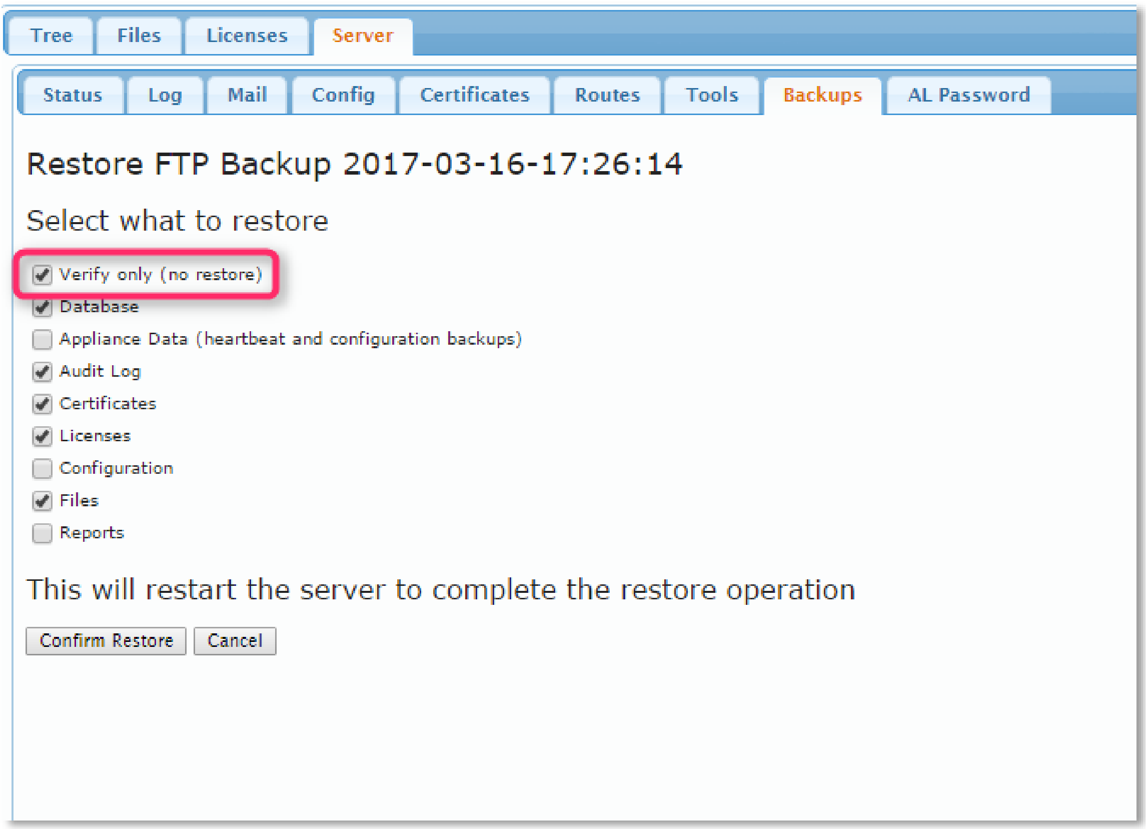
This Wizard will assist your first time setup of accounts and optionally SiteManager Embedded (SM-E).

For more information, Click here.

☑ Run startup wizard again on next login? (You can always re-enable it under My Account)

2.14. New Backup verification option

It is now possible to verify an existing GateManager backup before restoring the complete GateManager.



Restore FTP Backup 2017-03-16-17:26:14

Select what to restore

☑ Verify only (no restore)
☑ Database
☐ Appliance Data (heartbeat and configuration backups)
☑ Audit Log
☑ Certificates
☑ Licenses
☐ Configuration
☑ Files
☐ Reports

This will restart the server to complete the restore operation

When this option is selected, the server will perform a restart.

2.14.1. Result

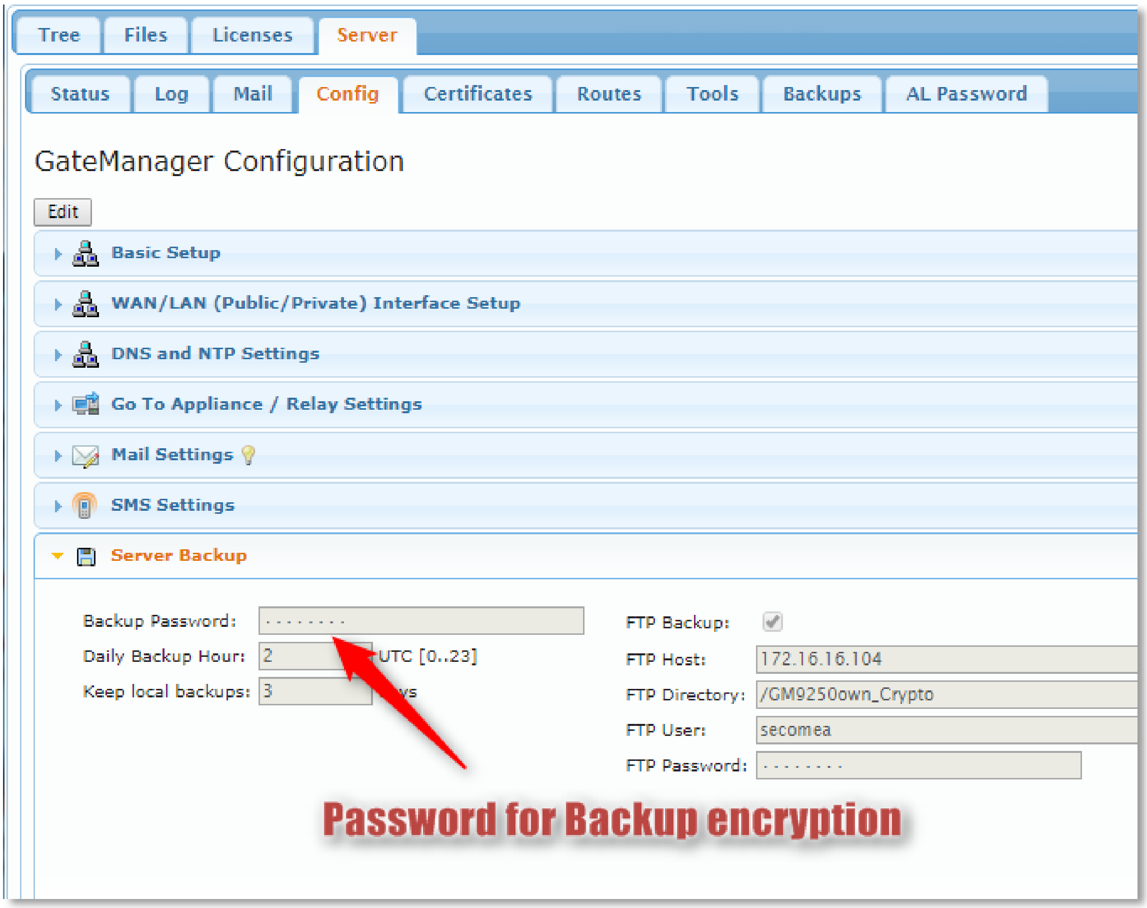
When the verify process is initiated it will provide the following output:

```
Verifying FTP Backup 2017-03-16-17:26:14

Restore log

Retrieve Backup File Started ...
Retrieve Backup File Done: Thu Mar 16 17:30:09 UTC 2017
Restore: Checking backup file
Restore: Backup file ok
Restore: Unpacking backup file
Restore: unpacking zipped files
Restore: CHECK COMPLETED
```

2.15. Encrypted Backup and Exports



GateManager Configuration

Backup Password: ········

Daily Backup Hour: 2 UTC [0..23]

Keep local backups: 3

FTP Backup: ☑

FTP Host: 172.16.16.104

FTP Directory: /GM9250own_Crypto

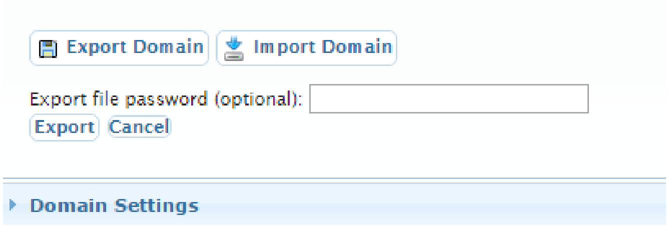
FTP User: secomea

FTP Password: ········

Password for Backup encryption

Entering a password will enable AES256 encrypted backup.

This is also possible when exporting a domain from the GateManager Portal:



Export file password (optional):

2.16. Two-factor Authentication

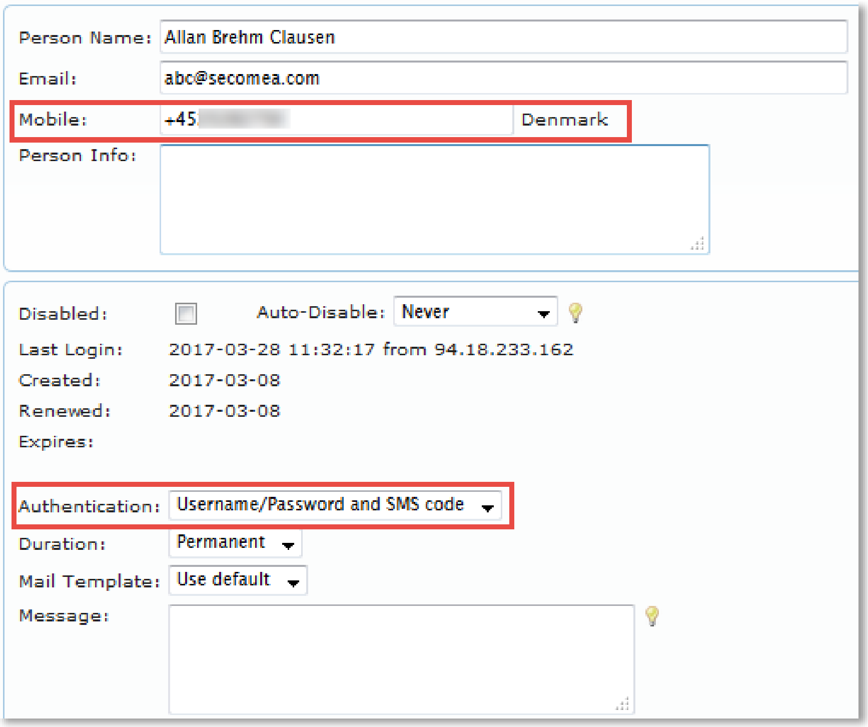
The new two-factor authentication is available for both LinkManager and LinkManager Mobile accounts.

2.16.1. Prerequisites

1. The GateManager must have SMS service enabled.
2. The account using two-factor authentication must have a mobile phone number registered under “Mobile:”.
3. The Domain where the accounts are placed must have SMS service enabled.

2.16.2. LinkManager Mobile

When using LinkManager mobile, create the account with the following parameters:



Person Name: Allan Brehm Clausen

Email: abc@secomea.com

Mobile: +45[redacted] Denmark

Person Info:

Disabled: □ Auto-Disable: Never

Last Login: 2017-03-28 11:32:17 from 94.18.233.162

Created: 2017-03-08

Renewed: 2017-03-08

Expires:

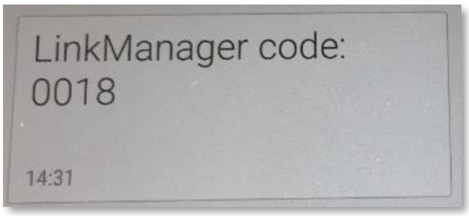
Authentication: Username/Password and SMS code

Duration: Permanent

Mail Template: Use default

Message:

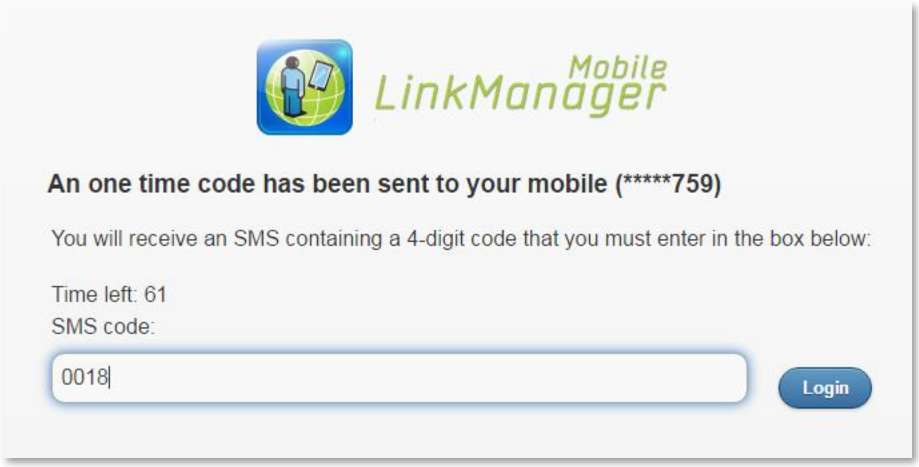
Then login to the GateManager through the normal LinkManager Mobile username/password page. After successful login, an SMS text will be send to your mobile:



LinkManager code:
0018

14:31

And the following will be displayed:



An one time code has been sent to your mobile (***759)**

You will receive an SMS containing a 4-digit code that you must enter in the box below:

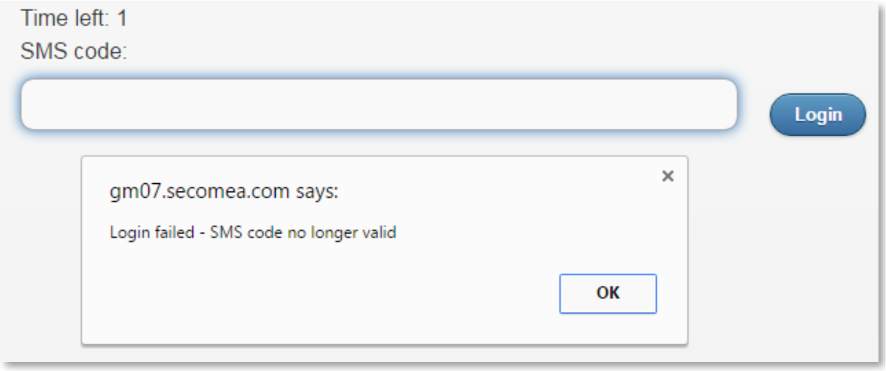
Time left: 61

SMS code:

0018

Enter the code and click "Login".

If the code is not entered within 100 seconds, the page will time-out:



Time left: 1

SMS code:

gm07.secomea.com says:

Login failed - SMS code no longer valid

2.16.3. LinkManager

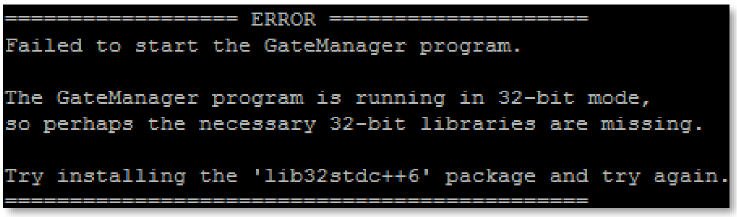
See the chapter on ”Two-factor Authentication” for LinkManager.

2.17. Starter package mails

The starter package mails, in all languages, now generically points to http://info.secomea.com/basic, referencing the existence of a “Getting Started Guide”.

2.18. 8250 Installation on 64-bit OS

When the GateManager 8250 is installed on a 64-bit operating system, it will now warn about missing 32 bit libraries:



```
================== ERROR ====================
Failed to start the GateManager program.

The GateManager program is running in 32-bit mode,
so perhaps the necessary 32-bit libraries are missing.

Try installing the 'lib32stdc++6' package and try again.
=============================================
```

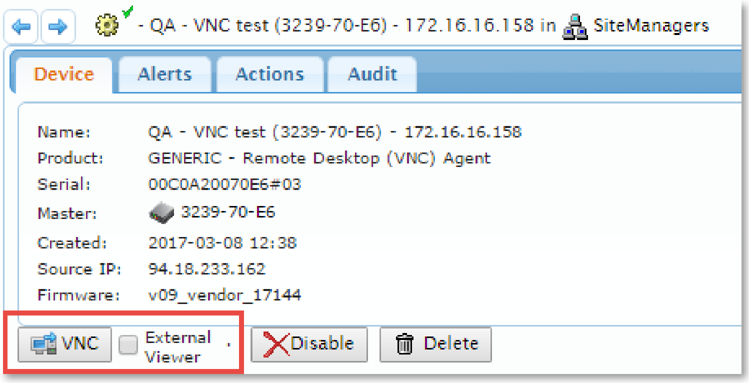
Then just install the libraries a restart the installation (i.e. on Debian use “apt-get install libstdc++6”).

The installer will then identify the aborted installation and note that it as “Incomplete GateManager installation found” and then continue with the installation.

2.19. In-Browser VNC viewer

For information about the functionality and prerequisites of the In-Browser VNC viewer, please see the section "In-Browser VNC Viewer".

For selecting a GTA to a VNC service, go to the Agent (see agent "Configuring the agent" in the LinkManager mobile section) and observe the details frame on the right:

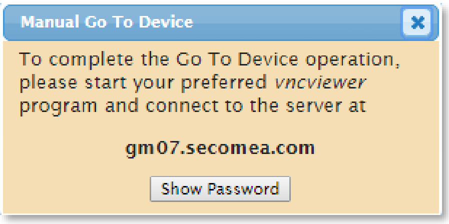

- QA - VNC test (3239-70-E6) - 172.16.16.158 in SiteManagers
Device
Alerts
Actions
Audit
VNC
Disable
Delete

Name: QA - VNC test (3239-70-E6) - 172.16.16.158
Product: GENERIC - Remote Desktop (VNC) Agent
Serial: 00C0A20070E6#03
Master: 3239-70-E6
Created: 2017-03-08 12:38
Source IP: 94.18.233.162
Firmware: v09_vendor_17144

□ External Viewer

If no checkmark is placed in "External Viewer", the In-Browser VNC viewer is chosen.

If a checkmark is present, the normal 7.1 functionality is selected:



Manual Go To Device

To complete the Go To Device operation, please start your preferred *vncviewer* program and connect to the server at

gm07.secomea.com

Please note the 30 second time-out for the above box. If no connection attempt has been made within 30 seconds, the connection will be closed.

2.20. Miscellaneous

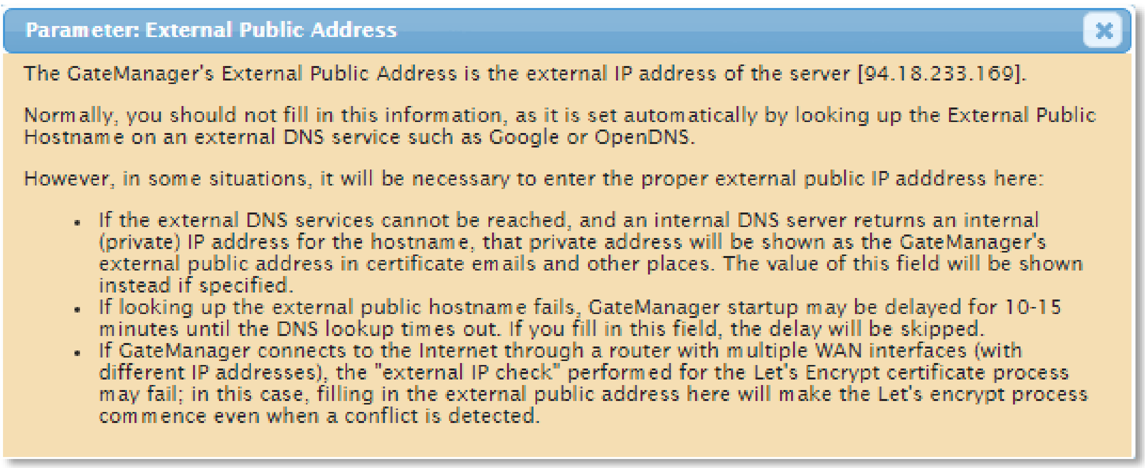
The GateManager will not be tracked by web crawlers like Google and Bing anymore. "noindex" and "nofollow" have been added to the GateManager and LinkManager Mobile.

2.21. New help bulb's

As always, we add new help information on the GateManager Portal.

Available for GateManager server administrators only:

Server > Config:



Parameter: External Public Address

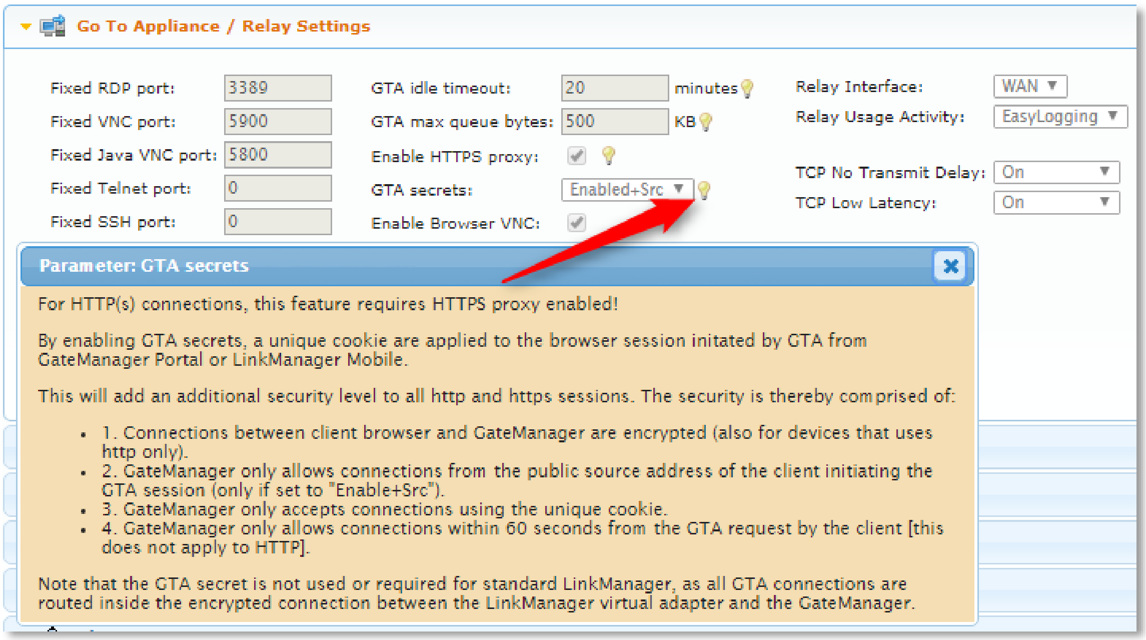
The GateManager's External Public Address is the external IP address of the server [94.18.233.169].

Normally, you should not fill in this information, as it is set automatically by looking up the External Public Hostname on an external DNS service such as Google or OpenDNS.

However, in some situations, it will be necessary to enter the proper external public IP adddress here:

- If the external DNS services cannot be reached, and an internal DNS server returns an internal (private) IP address for the hostname, that private address will be shown as the GateManager's external public address in certificate emails and other places. The value of this field will be shown instead if specified.
- If looking up the external public hostname fails, GateManager startup may be delayed for 10-15 minutes until the DNS lookup times out. If you fill in this field, the delay will be skipped.
- If GateManager connects to the Internet through a router with multiple WAN interfaces (with different IP addresses), the "external IP check" performed for the Let's Encrypt certificate process may fail; in this case, filling in the external public address here will make the Let's encrypt process commence even when a conflict is detected.

Server > Config > Go To Appliance / Relay Settings:



Go To Appliance / Relay Settings

Fixed RDP port: 3389
Fixed VNC port: 5900
Fixed Java VNC port: 5800
Fixed Telnet port: 0
Fixed SSH port: 0

GTA idle timeout: 20 minutes
GTA max queue bytes: 500 KB
Enable HTTPS proxy: ☑
GTA secrets: Enabled+Src
Enable Browser VNC: ☑

Relay Interface: WAN
Relay Usage Activity: EasyLogging
TCP No Transmit Delay: On
TCP Low Latency: On

Parameter: GTA secrets

For HTTP(s) connections, this feature requires HTTPS proxy enabled!

By enabling GTA secrets, a unique cookie are applied to the browser session initated by GTA from GateManager Portal or LinkManager Mobile.

This will add an additional security level to all http and https sessions. The security is thereby comprised of:

- 1. Connections between client browser and GateManager are encrypted (also for devices that uses http only).
- 2. GateManager only allows connections from the public source address of the client initiating the GTA session (only if set to "Enable+Src").
- 3. GateManager only accepts connections using the unique cookie.
- 4. GateManager only allows connections within 60 seconds from the GTA request by the client [this does not apply to HTTP].

Note that the GTA secret is not used or required for standard LinkManager, as all GTA connections are routed inside the encrypted connection between the LinkManager virtual adapter and the GateManager.

3. EasyLogging/Relaying

3.1. Inter-device relaying

It is now possible to setup a static Device Relay to access an existing Server Relay on the same SiteManager.

It is also possible to create a device agent and using a LinkManager connection to access the Static Server Relay.

This was possible in 6.2 but has been unavailable since introduction of EasyLogging in 7.0.

3.2. Failure to reenable relay after device down

If the EasyLogging client became unavailable to ICMP ping and then comes back up again, it would not reenable the EasyLog Client relay.

This has been fixed in 7.2.

3.3. Support for EasyLog Master Push agent on SM-E

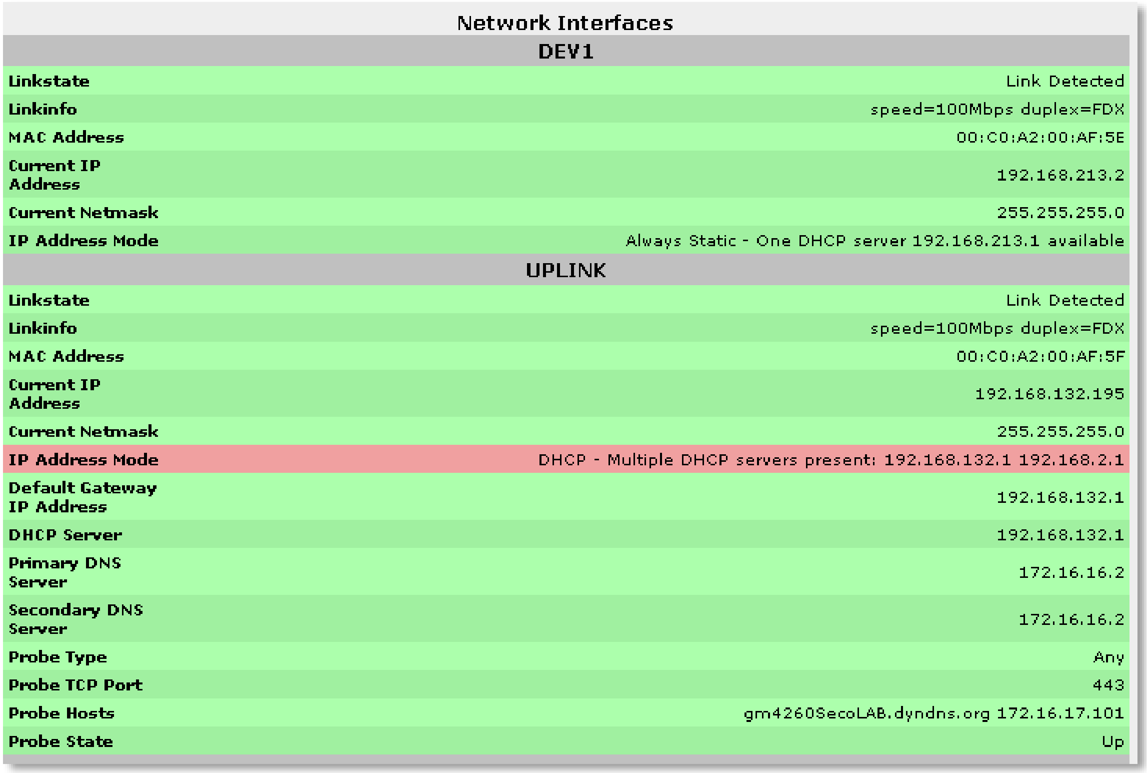
SiteManager Embedded has been extended to be able to run a Push Master Agent.

This enables the SiteManager Embedded to act as “Log-Master Pull” on cloud based SCADA systems that are based on devices pushing data to them.

4. SiteManager

4.1. Troubleshoot extended

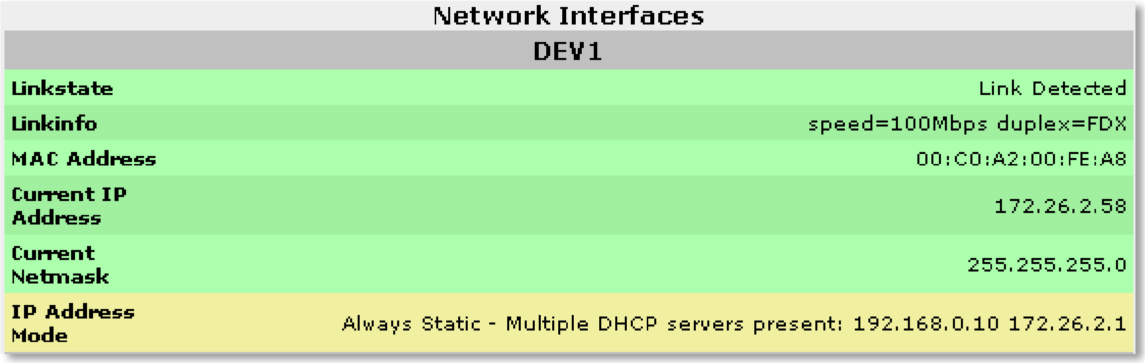
The troubleshoot function has been extended with new test on multiple DHCP servers, UPLINK probe feedback, proxy settings test on UPLINK and a few graphical updates.



Network Interfaces

DEV1	
Linkstate	Link Detected
Linkinfo	speed=100Mbps duplex=FDX
MAC Address	00:C0:A2:00:AF:5E
Current IP Address	192.168.213.2
Current Netmask	255.255.255.0
IP Address Mode	Always Static - One DHCP server 192.168.213.1 available
UPLINK	
Linkstate	Link Detected
Linkinfo	speed=100Mbps duplex=FDX
MAC Address	00:C0:A2:00:AF:5F
Current IP Address	192.168.132.195
Current Netmask	255.255.255.0
IP Address Mode	DHCP - Multiple DHCP servers present: 192.168.132.1 192.168.2.1
Default Gateway IP Address	192.168.132.1
DHCP Server	192.168.132.1
Primary DNS Server	172.16.16.2
Secondary DNS Server	172.16.16.2
Probe Type	Any
Probe TCP Port	443
Probe Hosts	gm4260SecoLAB.dyndns.org 172.16.17.101
Probe State	Up

The SiteManager will now detect multiple DHCP servers on the UPLINK or the DEV network.

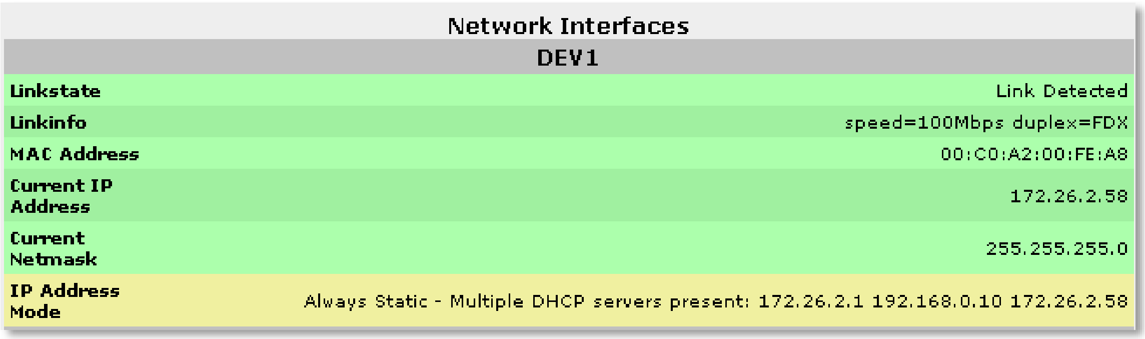


Network Interfaces

DEV1	
Linkstate	Link Detected
Linkinfo	speed=100Mbps duplex=FDX
MAC Address	00:C0:A2:00:FE:A8
Current IP Address	172.26.2.58
Current Netmask	255.255.255.0
IP Address Mode	Always Static - Multiple DHCP servers present: 192.168.0.10 172.26.2.1

In this case two DHCP servers are recorded on the DEV1 network.

Indication is Yellow because it can in some installations be wanted to have multiple DHCP servers.



Network Interfaces

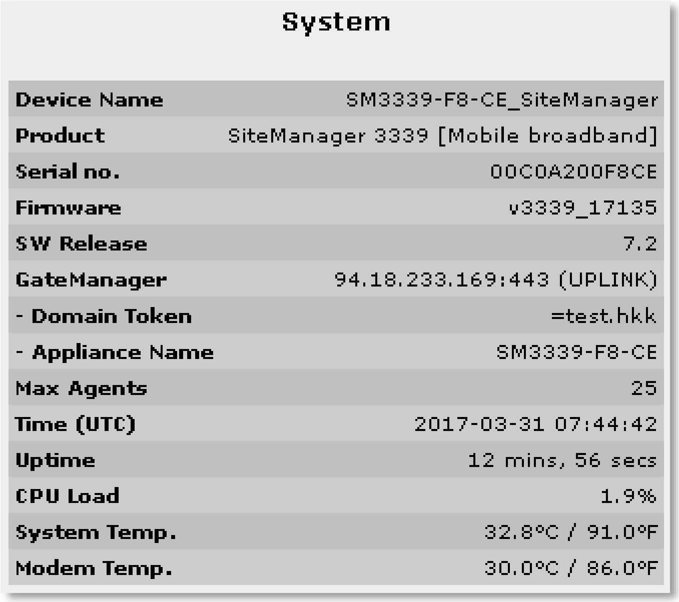
DEV1	
Linkstate	Link Detected
Linkinfo	speed=100Mbps duplex=FDX
MAC Address	00:C0:A2:00:FE:A8
Current IP Address	172.26.2.58
Current Netmask	255.255.255.0
IP Address Mode	Always Static - Multiple DHCP servers present: 172.26.2.1 192.168.0.10 172.26.2.58

In this case the SiteManagers own DHCP server on DEV1 is also enabled and is likely not wanted.

4.2. System and modem temperature

Appliances with build in modem now show both system temperature and modem temperature.

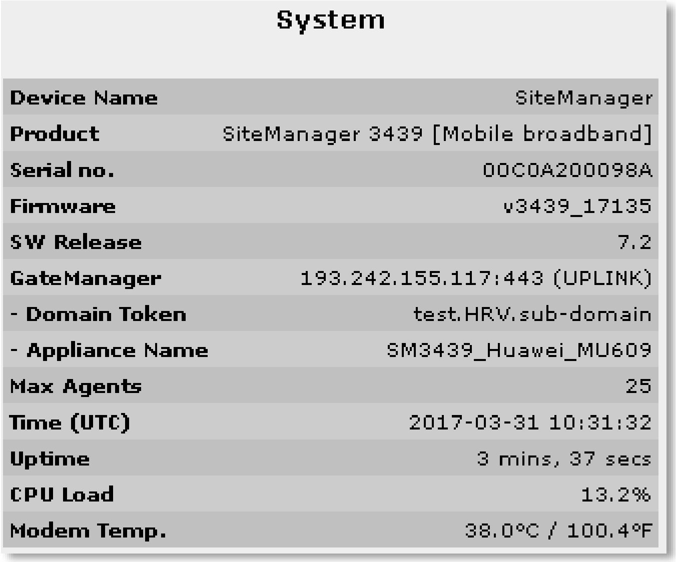
This is only available in models like 1139 and 3339.



System

Device Name	SM3339-F8-CE_SiteManager
Product	SiteManager 3339 [Mobile broadband]
Serial no.	00C0A200F8CE
Firmware	v3339_17135
SW Release	7.2
GateManager	94.18.233.169:443 (UPLINK)
- Domain Token	=test.hkk
- Appliance Name	SM3339-F8-CE
Max Agents	25
Time (UTC)	2017-03-31 07:44:42
Uptime	12 mins, 56 secs
CPU Load	1.9%
System Temp.	32.8°C / 91.0°F
Modem Temp.	30.0°C / 86.0°F

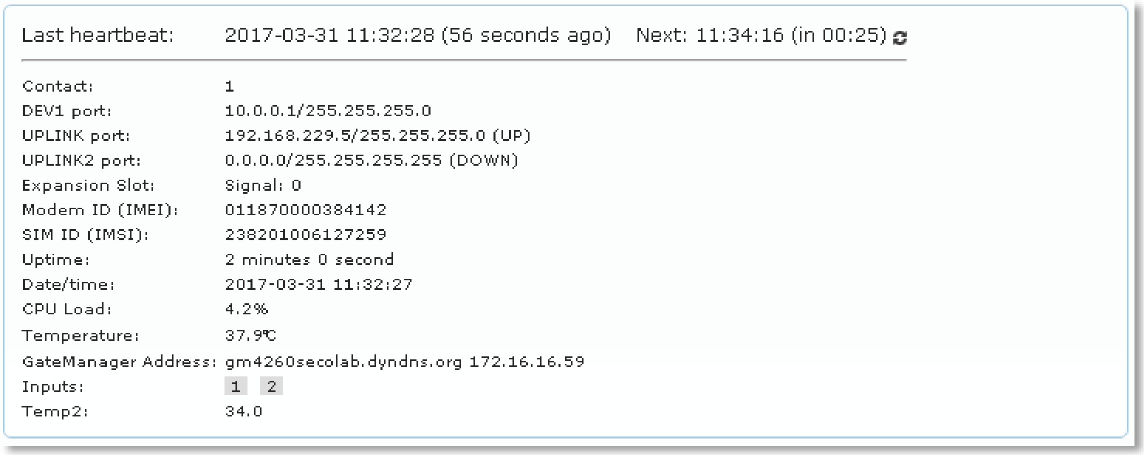
SiteManager 3439 will show only modem temperature:



System

Device Name	SiteManager
Product	SiteManager 3439 [Mobile broadband]
Serial no.	00C0A200098A
Firmware	v3439_17135
SW Release	7.2
GateManager	193.242.155.117:443 (UPLINK)
- Domain Token	test.HRV.sub-domain
- Appliance Name	SM3439_Huawei_MU609
Max Agents	25
Time (UTC)	2017-03-31 10:31:32
Uptime	3 mins, 37 secs
CPU Load	13.2%
Modem Temp.	38.0°C / 100.4°F

In GateManager you will see the modem temperature as TEMP2 if available:

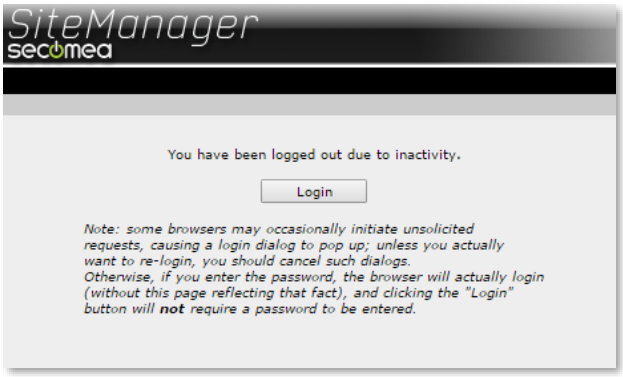


Last heartbeat: 2017-03-31 11:32:28 (56 seconds ago) Next: 11:34:16 (in 00:25)

Contact:	1
DEV1 port:	10.0.0.1/255.255.255.0
UPLINK port:	192.168.229.5/255.255.255.0 (UP)
UPLINK2 port:	0.0.0.0/255.255.255.255 (DOWN)
Expansion Slot:	Signal: 0
Modem ID (IMEI):	011870000384142
SIM ID (IMSI):	238201006127259
Uptime:	2 minutes 0 second
Date/time:	2017-03-31 11:32:27
CPU Load:	4.2%
Temperature:	37.9℃
GateManager Address:	gm4260secolab.dyndns.org 172.16.16.59
Inputs:	1 2
Temp2:	34.0

4.3. Default GUI time-out

When logging directly in to the SiteManager GUI (not through the GateManager) the default timeout for the session have been set to 10 minutes (down from 30).



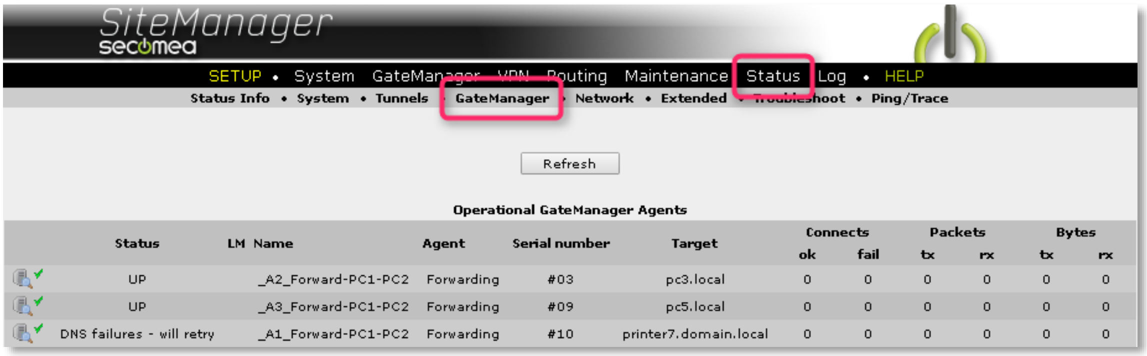
You have been logged out due to inactivity.

Note: some browsers may occasionally initiate unsolicited requests, causing a login dialog to pop up; unless you actually want to re-login, you should cancel such dialogs. Otherwise, if you enter the password, the browser will actually login (without this page reflecting that fact), and clicking the "Login" button will ***not*** *require a password to be entered.*

4.4. Forwarding Agent update

Various updates and fixes are scheduled for the Forwarding Agent in the upcoming release 7.3.

4.4.1. Forwarding Agent with support for dynamic hostname update


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
Status Info • System • Tunnels • GateManager • Network • Extended • Troubleshoot • Ping/Trace
Refresh

Operational GateManager Agents

	Status	LM	Name	Agent	Serial number	Target	Connects		Packets		Bytes	
							ok	fail	tx	rx	tx	rx
✓	UP		_A2_Forward-PC1-PC2	Forwarding	#03	pc3.local	0	0	0	0	0	0
✓	UP		_A3_Forward-PC1-PC2	Forwarding	#09	pc5.local	0	0	0	0	0	0
✓	DNS failures - will retry		_A1_Forward-PC1-PC2	Forwarding	#10	printer7.domain.local	0	0	0	0	0	0

You can now use hostnames in the Forwarding Agent. The agent will periodically be scanned in case the hostname has changed over time. A DNSPOLL interval can be set on each Forwarding Agent.

The Status > GateManager page will show as in the figure above where some of the hostnames has timed out and will again be reactivated when the hostname again can be resolved.

4.4.2. Error messages:

Because Forwarding Agent is a script language you must expect to see various mysterious messages in case the hostnames cannot be resolved.

Here are a few examples when the hostnames cannot be resolved, note that when the hostnames again can be resolved the error will disappear:

```
-   iptables v1.4.6: can't initialize iptables table `nat': No chain/target/match by
    that name Perhaps iptables or your kernel needs to be upgraded.
-
-   iptables: Invalid argument. Run `dmesg' for more information.
```

In most cases where will be a hint about the course of the problem like below hint that show that the hostname pc3.local fail to resolve in to an IP address:

```
-   Unknown target host:: pc3.local
```

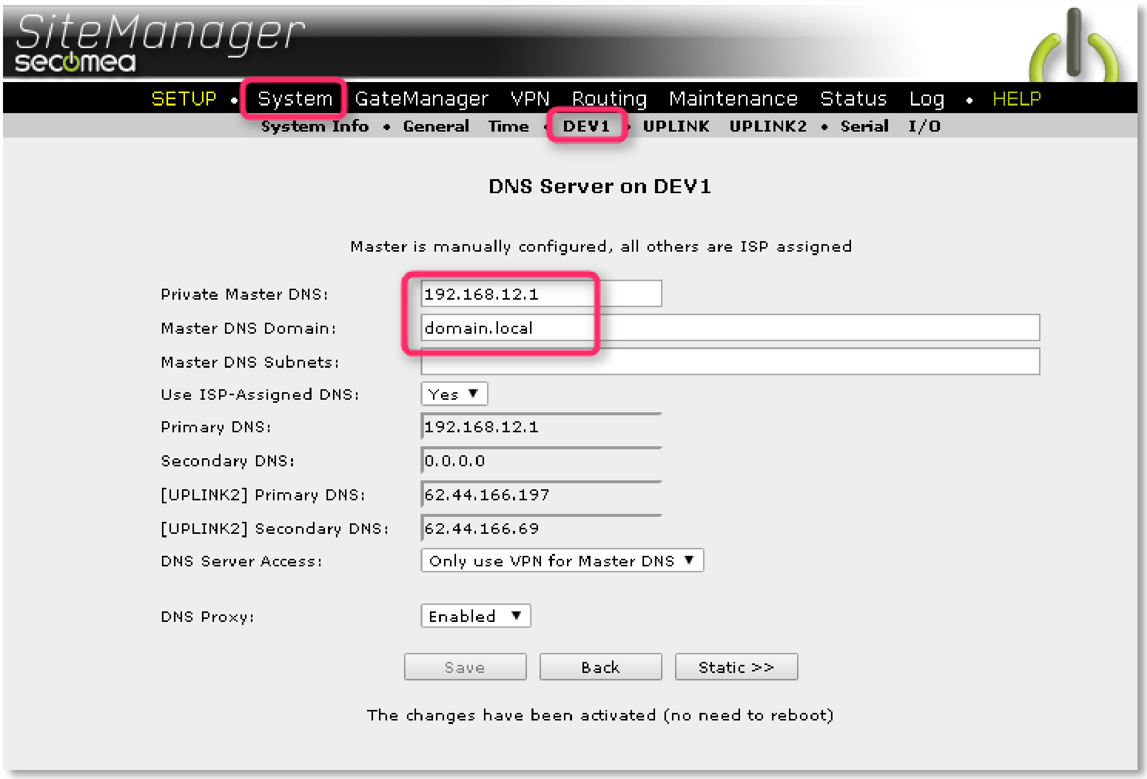
4.4.3. Forwarding Agent and dual UPLINK

If you are setting up Forwarding Agent using local hostnames like *myPC.domain.local* or *printer7.domain.local* you can only use the local DNS server to resolve these hostnames. This require that your SiteManager will keep using the local DNS server even when SiteManager shift to UPLINK2(4G) as default uplink interface.

This is how you do it.

Lets say the local domain is domain.local so the printer on 7th floor is called printer7.domain.local.

1) Setup the local DNS settings on your SiteManager:


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

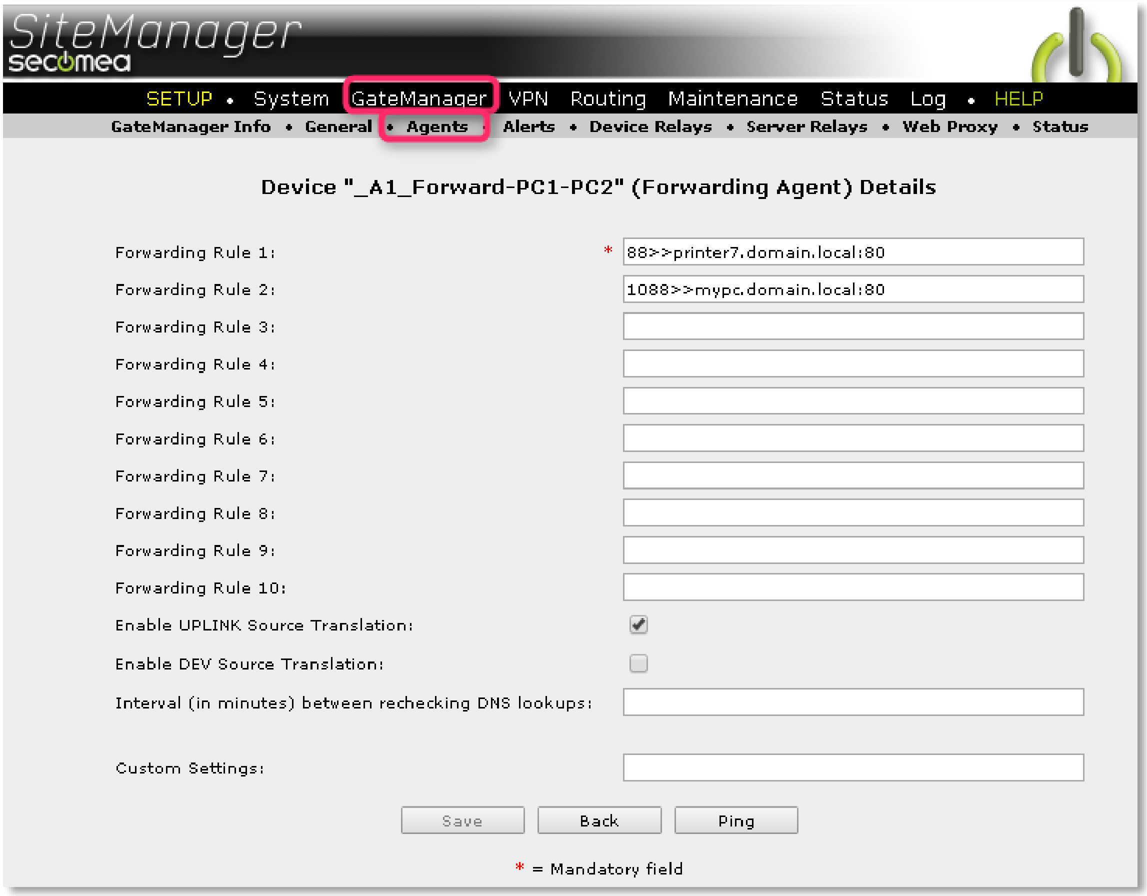
DNS Server on DEV1

Master is manually configured, all others are ISP assigned

Private Master DNS:	192.168.12.1
Master DNS Domain:	domain.local
Master DNS Subnets:	
Use ISP-Assigned DNS:	Yes ▼
Primary DNS:	192.168.12.1
Secondary DNS:	0.0.0.0
[UPLINK2] Primary DNS:	62.44.166.197
[UPLINK2] Secondary DNS:	62.44.166.69
DNS Server Access:	Only use VPN for Master DNS ▼
DNS Proxy:	Enabled ▼

The changes have been activated (no need to reboot)

2) Setting up the Forwarding Agent with the know two hostnames:


SiteManager
secomea
SETUP • System GateManager VPN Routing Maintenance Status Log • HELP
GateManager Info • General • Agents • Alerts • Device Relays • Server Relays • Web Proxy • Status
Save
Back
Ping

Device "_A1_Forward-PC1-PC2" (Forwarding Agent) Details

Forwarding Rule 1: *	88>>printer7.domain.local:80
Forwarding Rule 2:	1088>>mypc.domain.local:80
Forwarding Rule 3:	
Forwarding Rule 4:	
Forwarding Rule 5:	
Forwarding Rule 6:	
Forwarding Rule 7:	
Forwarding Rule 8:	
Forwarding Rule 9:	
Forwarding Rule 10:	
Enable UPLINK Source Translation:	☑
Enable DEV Source Translation:	☐
Interval (in minutes) between rechecking DNS lookups:	
Custom Settings:	

* = Mandatory field

Primary DNS is 192.168.12.1, but this is only when UPLINK is default interface. When UPLINK2 takes over, SiteManager will also set 62.44.166.197 as primary DNS. Because Master Domain is set to domain.local all hostnames/dns names using that hostdomain it will continue using 192.168.12.1 as DNS server for these hostnames.

Note that “pc” in myPC.domain.local must be in lower case.

4.5. Other Agent updates

4.5.1. Schneider -> Ethernet agent

Add Schneider Vijeo Extended Designer (VXD) support (tcp port 3300-3350 and 8000-8050).

4.5.2. Schneider -> USB HMI agent

Add Schneider STO 715 HMI with vendor ID: 114E:000D

4.5.3. Beckhoff -> Ethernet Agent

The existing “Ethernet” agent was renamed to “Legacy (Ethernet)”.

A new Ethernet agent has been created. This agent does not utilize the path “upnpdevice/index.htm” when accessing the WWW service.

Also, HTTP timers and connection limits have been reverted to default settings.

4.5.4. Desktop PC Agent

Failed services are now pinged every 30 seconds (up from 10).

4.5.5. Mitsubishi Agent

The Mitsubishi agent have been renamed to “Mitsubishi Electric”.

4.5.6. Hilscher USB

New Hilscher > Gateway (USB) supporting a number of netX Gateway solution devices. Note that this is limited to a RTT of 40 msec.

4.6. APN updates

3 Japanese APN's have been added to the SiteManager:

```
Carrier: NTT Docomo(iij), MCC: 440, MNC: 10,
APN: sd.iijmobile.jp, User: mobile@iij, Password: iij
```

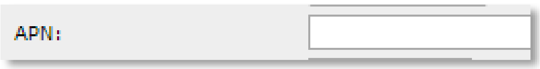
```
Carrier: NTT Docomo(nifty), MCC: 440, MNC: 10,
APN: mda.nifty.com, User: mda@nifty, Password: nifty
```

```
Carrier: NTT Docomo(ocn), MCC: 440, MNC: 10,
APN: lte-d.ocn.ne.jp, User: mobileid@ocn, Password: mobile
```

4.7. Force the APN option

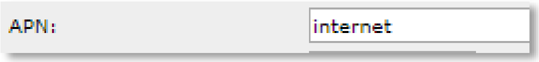
If in case, you don't want the SiteManager to automatically select between the known APN's you can force the SiteManager to only try the configured APN.

If the APN field is blank the SiteManager will try all know APN's for this SIM card:



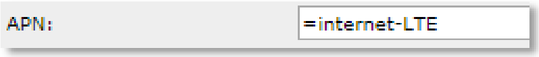
APN:

If the APN is specified it will try 10 times the configured APN and then try to list of known APN's for this SIM card:



APN: internet

Leading = sign will force SiteManager to keep using the specified APN:

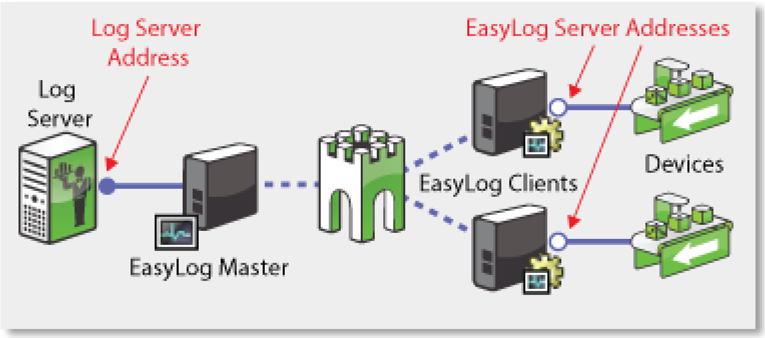


APN: =internet-LTE

5. SiteManager Embedded

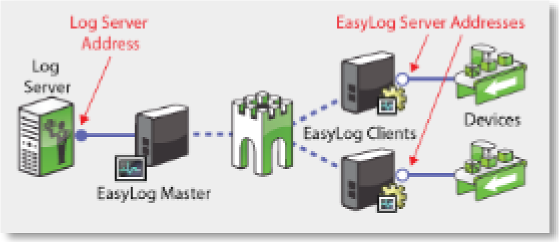
5.1. EasyLog Master (PUSH) agent

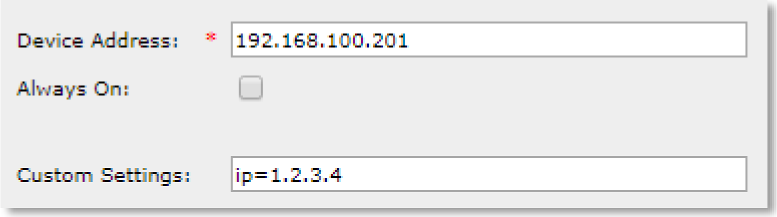
From Release 7.2 we now include one EasyLog Master Agent. The PUSH agent is supported for all SiteManager Embedded models.



5.2. EasyLog Client update

A fix for SiteManager Embedded and its EasyLog(PUSH) Client now allow any IP aliases created on the host to be used as EasyLog Server Addresses. Previous version did not notice any aliases on the host to be valid.





Device Address: * 192.168.100.201

Always On: □

Custom Settings: ip=1.2.3.4

The address 1.2.3.4 must manually be created on the host and SiteManager Embedded will accept this as the Easylog Server Address and the Device "pushing" data is 192.168.100.201

5.3. Enhanced Write Filter (EWF) support

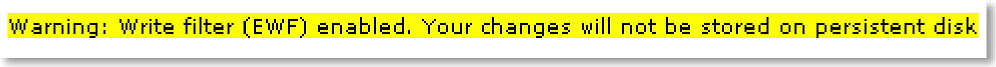
Special attention to EWF and the new Secondary ID add on in this release 7.2. See chapter Secondary ID (Serial 2) for related information.

In some SiteManager Embedded (SME) installations, the host will have "Enhanced Write Filter" (EWF) installed and activated. To make any changes to the SME configuration you need to disable EWF or the changes will be rolled back after a reboot of the host.

When the SiteManager Embedded detects the presence of an EWF system, the [Upgrade] button will disappear. As the panel/HMI will not receive the upgrade properly when EWF is enabled, the option has been disabled.

EWF will prevent any systems on the host to make changes to the storage. If the SME has been reconfigured or in this case create a Secondary ID stored in Windows Registry, it will all be erased on the next report of the host/panel.

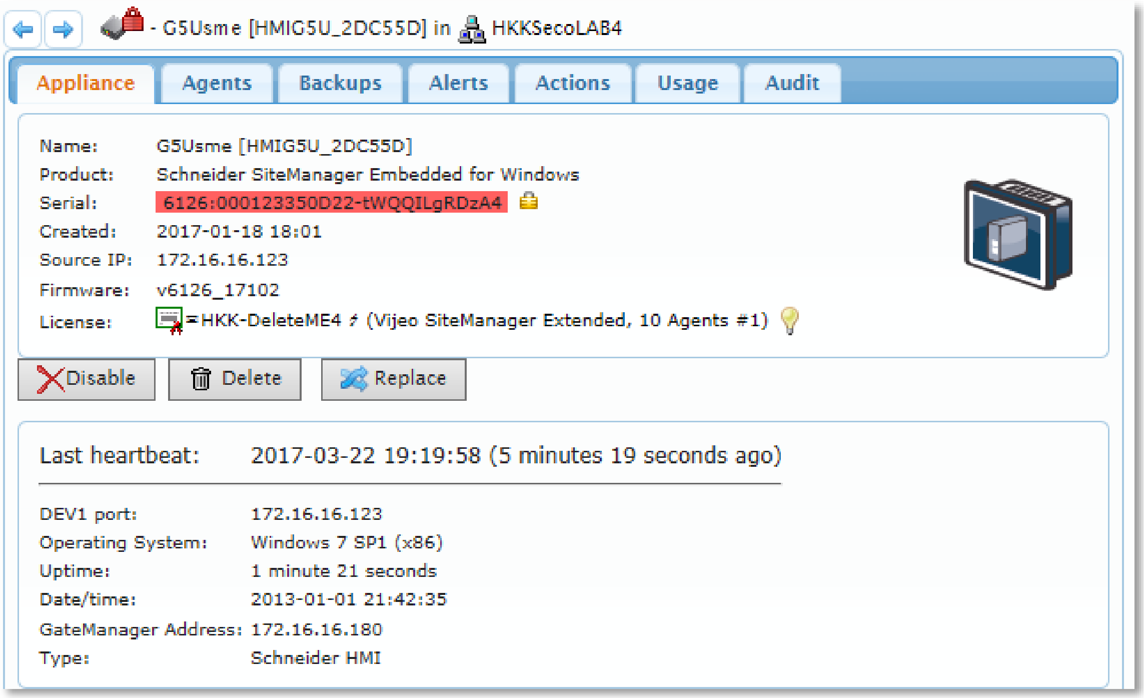
The SiteManager Embedded WEB GUI will show a Warning if EWF is enabled:



Warning: Write filter (EWF) enabled. Your changes will not be stored on persistent disk

If the SME is upgraded and the host/HMI has at some time been repowered, then the Secondary ID has not been stored due to EWF and therefor no longer included in the SME configuration.

This will result in the scenario described here "Secondary ID (Serial 2)":



- G5Usme [HMIG5U_2DC55D] in HKKSecoLAB4

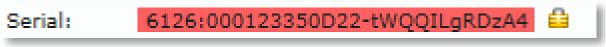
Name: G5Usme [HMIG5U_2DC55D]
Product: Schneider SiteManager Embedded for Windows
Serial: 6126:000123350D22-tWQQILgRDzA4
Created: 2017-01-18 18:01
Source IP: 172.16.16.123
Firmware: v6126_17102
License: =HKK-DeleteME4 (Vijeo SiteManager Extended, 10 Agents #1)

Last heartbeat: 2017-03-22 19:19:58 (5 minutes 19 seconds ago)

DEV1 port: 172.16.16.123
Operating System: Windows 7 SP1 (x86)
Uptime: 1 minute 21 seconds
Date/time: 2013-01-01 21:42:35
GateManager Address: 172.16.16.180
Type: Schneider HMI

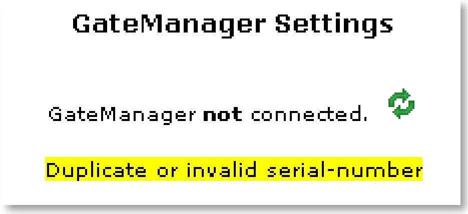
Note: The GateManager Portal will show the build: 17102 but SME is now back to previous build: 17033 (see "Secondary ID (Serial 2)")

The result is that the SME will be rejected and locked-out by the GateManager and shown as:



Serial: 6126:000123350D22-tWQQILgRDzA4

The SiteManager Embedded GUI will show:



GateManager Settings

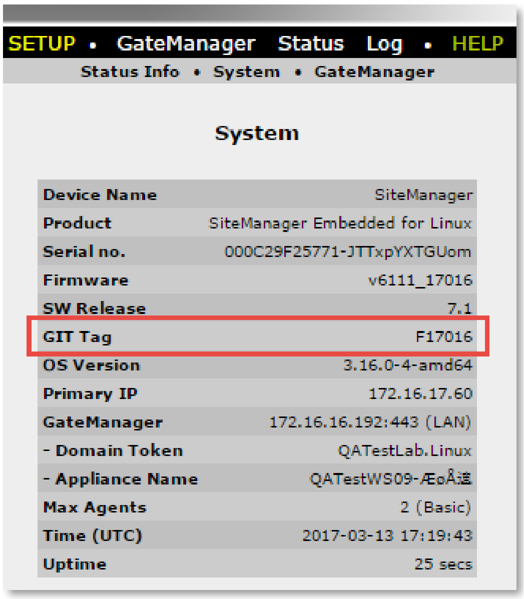
GateManager **not** connected.

Duplicate or invalid serial-number

For how directions on reconnecting, see "Reconnect periods" in APPENDIX – Troubleshooting Secondary ID.

5.4. Extended version information

If a special firmware version is released, it will be parallel to the master branch. When this happens, a new version information field will be added to the “Status -> System” menu of the SiteManager Embedded GUI:


SETUP • GateManager Status Log • HELP
Status Info • System • GateManager

System

Device Name	SiteManager
Product	SiteManager Embedded for Linux
Serial no.	000C29F25771-JTTxpYXTGUom
Firmware	v6111_17016
SW Release	7.1
GIT Tag	F17016
OS Version	3.16.0-4-amd64
Primary IP	172.16.17.60
GateManager	172.16.16.192:443 (LAN)
- Domain Token	QATestLab.Linux
- Appliance Name	QATestWS09-ÆøÅ這
Max Agents	2 (Basic)
Time (UTC)	2017-03-13 17:19:43
Uptime	25 secs

5.5. Agent updates

5.5.1. Desktop PC Agent

The Desktop PC agent will now TCP ping failed services every 30 seconds (up from 10).

The services are now only checked at agent start up, as to not overload sensitive services.

5.5.2. Subnet Agent

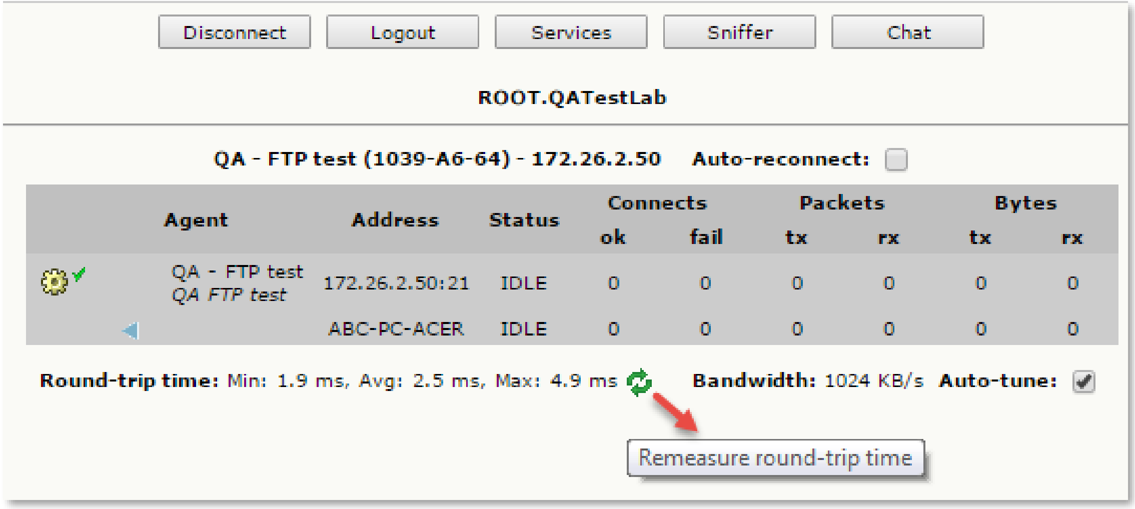
Starting the SiteManager Embedded on Windows CE could in some cases end up in a state where the Subnet Agent was down.

It will now allow for interface changes to occur after it has been started.

6. LinkManager

6.1. Round-trip Time

Due to some confusion, the “Refresh” icon has a mouse-over explaining the functionality of the icon. It will not reset the connection, but remeasure the total round-trip time from the the PC running the LinkManager to the SiteManager and back.



ROOT.QATestLab

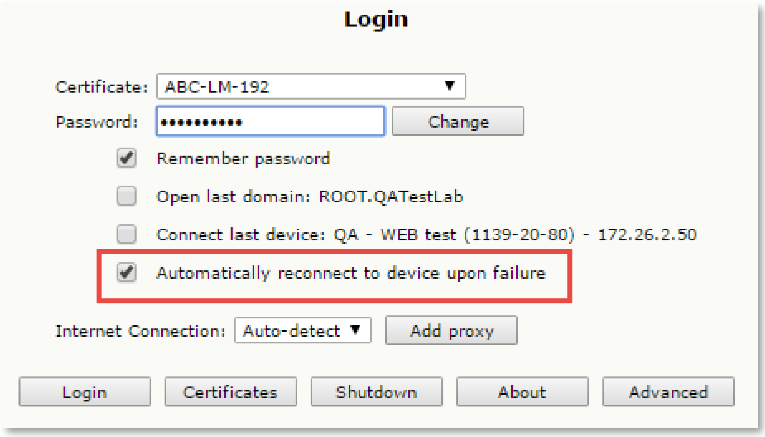
QA - FTP test (1039-A6-64) - 172.26.2.50 Auto-reconnect: □

Agent	Address	Status	Connects		Packets		Bytes	
			ok	fail	tx	rx	tx	rx
QA - FTP test *QA FTP test*	172.26.2.50:21	IDLE	0	0	0	0	0	0
	ABC-PC-ACER	IDLE	0	0	0	0	0	0

Round-trip time: Min: 1.9 ms, Avg: 2.5 ms, Max: 4.9 ms **Bandwidth:** 1024 KB/s **Auto-tune:** ☑

6.2. Auto-connect as default

Auto-connect is now enabled as the default setting for LinkManager connections.


Login

Certificate: ABC-LM-192

Password: ••••••••••

☑ Remember password

□ Open last domain: ROOT.QATestLab

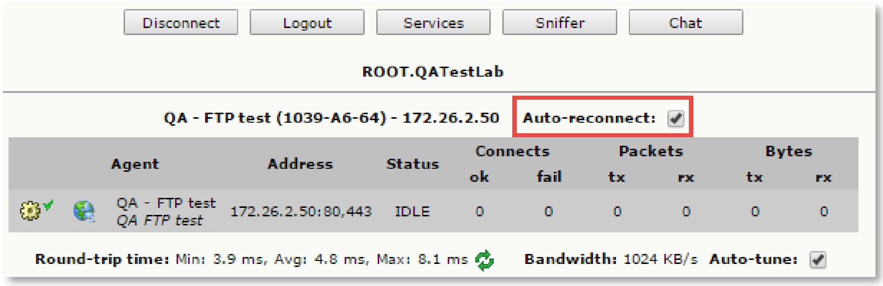
□ Connect last device: QA - WEB test (1139-20-80) - 172.26.2.50

☑ Automatically reconnect to device upon failure

Internet Connection: Auto-detect

It can be changed by unticking the box, and will be remembered through different browsers.

When a connection is established the chosen setting can be seen here:



ROOT.QATestLab

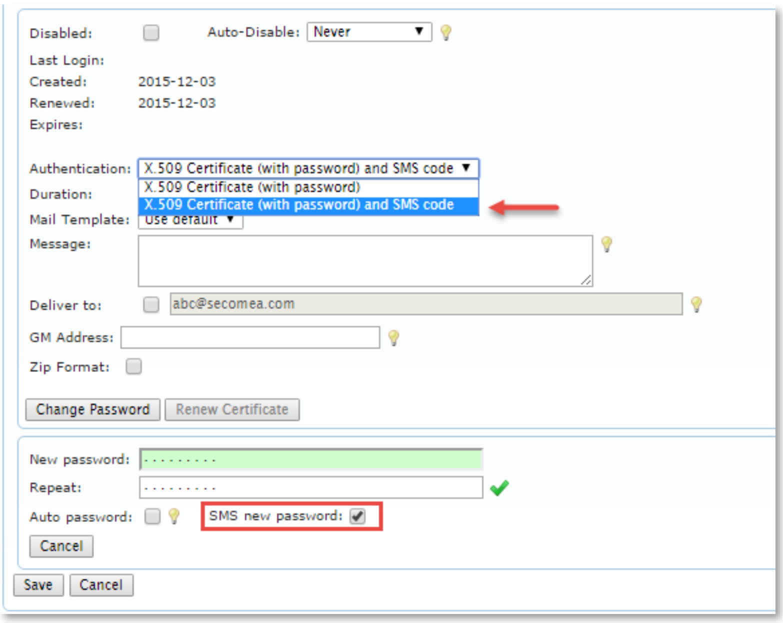
QA - FTP test (1039-A6-64) - 172.26.2.50 Auto-reconnect: ☑

Agent	Address	Status	Connects		Packets		Bytes	
			ok	fail	tx	rx	tx	rx
QA - FTP test *QA FTP test*	172.26.2.50:80,443	IDLE	0	0	0	0	0	0

Round-trip time: Min: 3.9 ms, Avg: 4.8 ms, Max: 8.1 ms **Bandwidth:** 1024 KB/s **Auto-tune:** ☑

6.3. LinkManager login with password & SMS code

The new SMS passcode system can be used with LinkManager Accounts, both to send the initial password, and to use a mobile phone for 2-factor authentication.



Disabled: □ Auto-Disable: Never ▼

Last Login:

Created: 2015-12-03

Renewed: 2015-12-03

Expires:

Authentication: X.509 Certificate (with password) and SMS code ▼

X.509 Certificate (with password)
X.509 Certificate (with password) and SMS code

Duration:

Mail Template: Use default ▼

Message:

Deliver to: □ abc@secomea.com

GM Address:

Zip Format: □

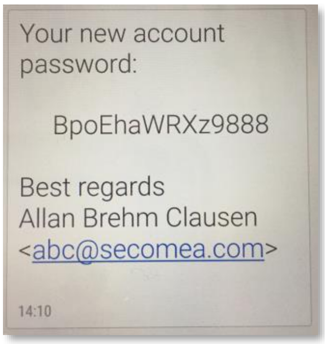
Change Password
Renew Certificate

New password: ....

Repeat: .... ✓

Auto password: □ SMS new password: ☑

When it is selected to SMS the new password, the following text will appear.



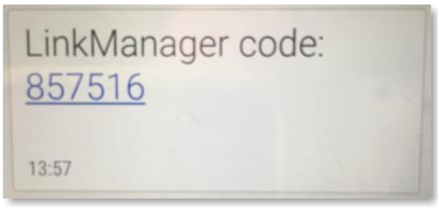
Your new account password:

BpoEhaWRXz9888

Best regards
Allan Brehm Clausen
<abc@secomea.com>

14:10

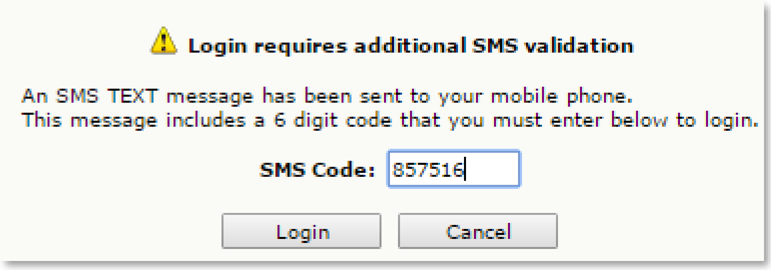
When logging in to the LinkManager with the new certificate, an SMS will be send with the SMS passcode:



LinkManager code: 857516

13:57

Then enter the passcode and log in to the GateManager:



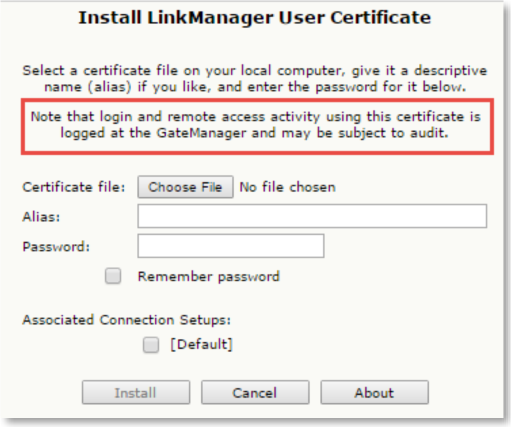
⚠ Login requires additional SMS validation

An SMS TEXT message has been sent to your mobile phone.
This message includes a 6 digit code that you must enter below to login.

SMS Code: 857516

6.4. New LinkManager disclaimer

The LinkManager console now displays a disclaimer when installing and renewing the certificate.



Install LinkManager User Certificate

Select a certificate file on your local computer, give it a descriptive name (alias) if you like, and enter the password for it below.

Note that login and remote access activity using this certificate is logged at the GateManager and may be subject to audit.

Certificate file: Choose File No file chosen

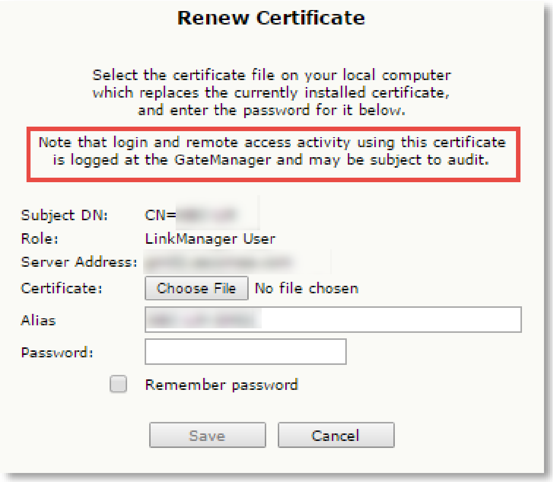
Alias:

Password:

□ Remember password

Associated Connection Setups:

□ [Default]



Renew Certificate

Select the certificate file on your local computer which replaces the currently installed certificate, and enter the password for it below.

Note that login and remote access activity using this certificate is logged at the GateManager and may be subject to audit.

Subject DN: CN=[redacted]

Role: LinkManager User

Server Address: [redacted]

Certificate: Choose File No file chosen

Alias [redacted]

Password:

□ Remember password

6.5. Two-factor Authentication

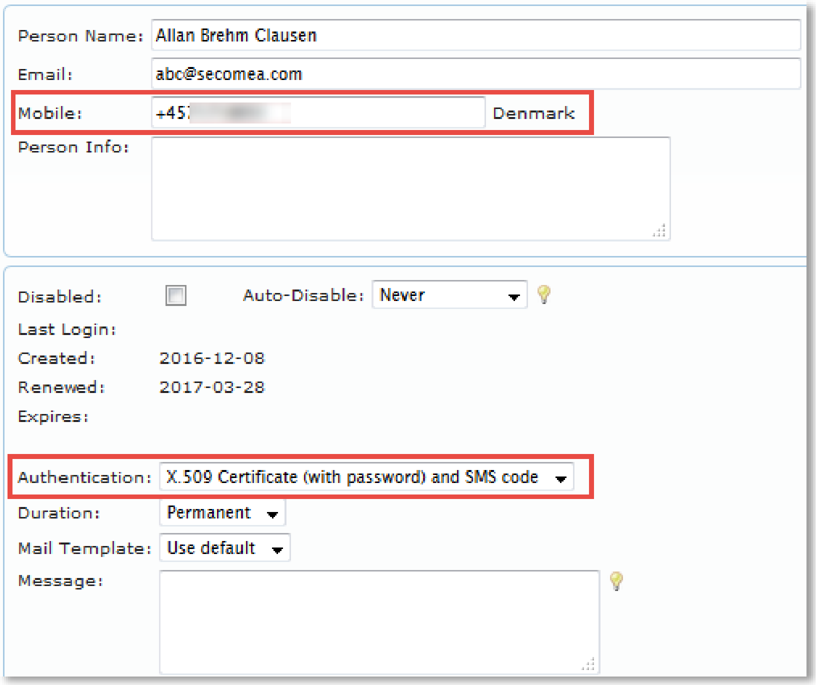
The new two-factor authentication are available for both LinkManager and LinkManager Mobile accounts.

6.5.1. Prerequisites

1. The GateManager must have SMS service enabled.
2. The account using two-factor authentication must have a mobile phone number registered under “Mobile:”.
3. The Domain where the accounts are placed must have SMS service enabled.
4. The LinkManager version must be 7.2 or above.

6.5.2. LinkManager Login

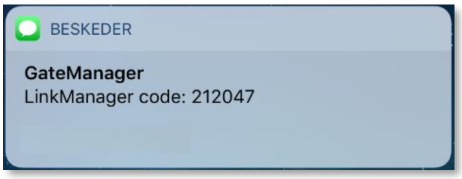
Create the LinkManager account with the following parameters:



Person Name:	Allan Brehm Clausen
Email:	abc@secomea.com
Mobile:	+45[redacted] Denmark
Person Info:	
Disabled:	□ Auto-Disable: Never
Last Login:	
Created:	2016-12-08
Renewed:	2017-03-28
Expires:	
Authentication:	X.509 Certificate (with password) and SMS code
Duration:	Permanent
Mail Template:	Use default
Message:	

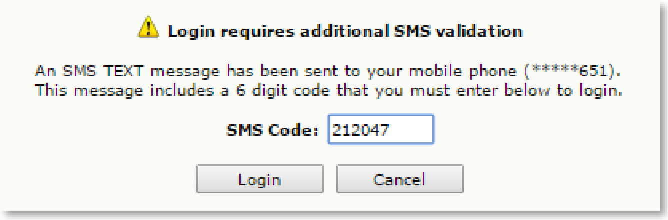
The information about the SMS code is not embedded in the certificate. If the Authentication SMS setting is toggled the certificate will not be renewed, as the SMS code information is stored on the GateManager account.

Then login to the GateManager through the normal LinkManager program. After successful login, an SMS text will be send to your mobile:



GateManager
LinkManager code: 212047

And the following will be displayed in your LinkManager:



Login requires additional SMS validation

An SMS TEXT message has been sent to your mobile phone (*****651).
This message includes a 6 digit code that you must enter below to login.

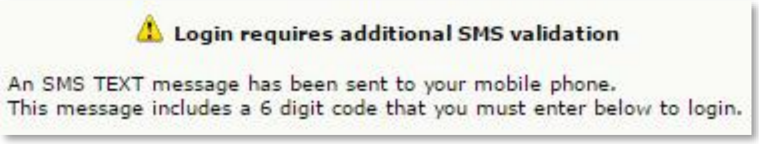
SMS Code: 212047

Click “Login” to use the passcode.

6.5.3. Pre 7.2 LinkManagers (IMPORTANT!)

IMPORTANT: When using a LinkManager version before 7.2, it will not have the two-factor authentication feature implemented.

This will leave the user without the code input box. See screenshot:



Login requires additional SMS validation

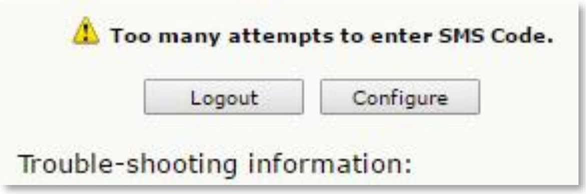
An SMS TEXT message has been sent to your mobile phone.
This message includes a 6 digit code that you must enter below to login.

It will not be possible for the user to login with this version of the LinkManager.

6.5.4. Other information

When the passcode has been used, it will stay valid for 12 hours for the local LinkManager in this period you can login without using the SMS code.

There are 3 attempts to enter the SMS code. Then this will be displayed:



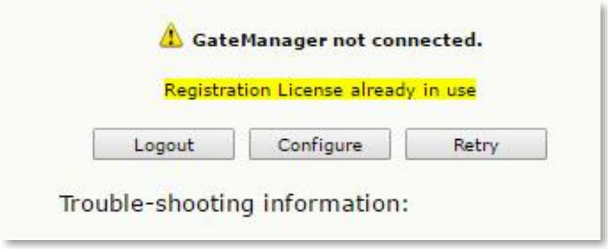
Too many attempts to enter SMS Code.

Trouble-shooting information:

6.6. Downgrading LinkManager and SecondaryID

Please note that if you downgrade the LinkManager to a pre 7.2 version, the LinkManager Appliance Object will not have a valid registration code.

This will result in the following warning when logging in through the LinkManager:

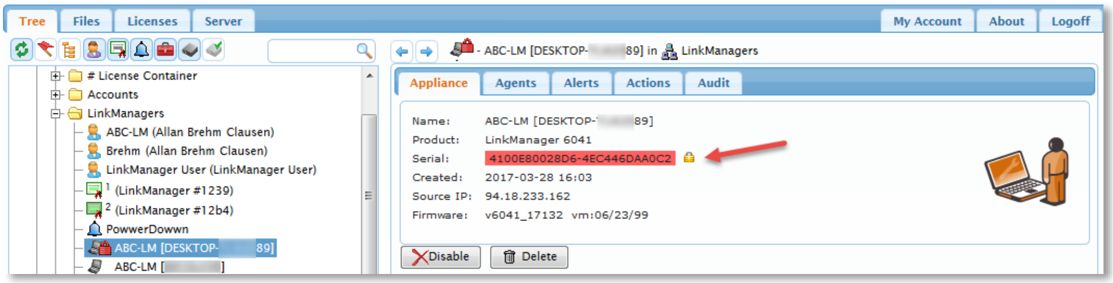


GateManager not connected.

Registration License already in use

Trouble-shooting information:

You will then have to manually accept it through the padlock icon on the GateManager:



- ABC-LM [DESKTOP-[redacted]89] in LinkManagers

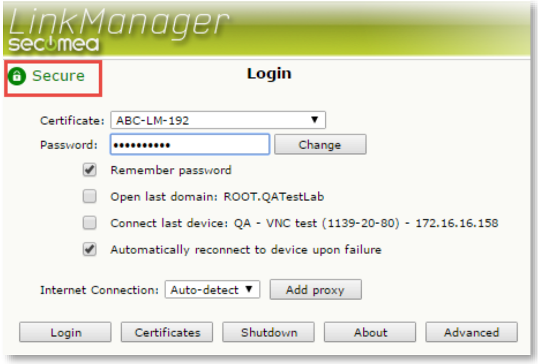
License Container
Accounts
LinkManagers
ABC-LM (Allan Brehm Clausen)
Brehm (Allan Brehm Clausen)
LinkManager User (LinkManager User)
1 (LinkManager #1239)
2 (LinkManager #12b4)
PowwerDowwn
ABC-LM [DESKTOP-[redacted]89]
ABC-LM [[redacted]]

Name: ABC-LM [DESKTOP-[redacted]89]
Product: LinkManager 6041
Serial: 4100E80028D6-4EC446DAA0C2
Created: 2017-03-28 16:03
Source IP: 94.18.233.162
Firmware: v6041_17132 vm:06/23/99

Then you can login again.

6.7. LinkManager Security Advisory Statement

A new Security information has been added to the LinkManager:



Certificate: ABC-LM-192

Password: ••••••••••

☑ Remember password

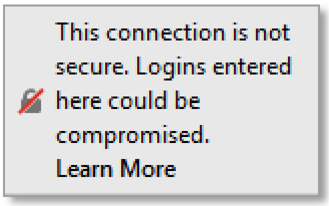
□ Open last domain: ROOT.QATestLab

□ Connect last device: QA - VNC test (1139-20-80) - 172.16.16.158

☑ Automatically reconnect to device upon failure

Internet Connection: Auto-detect

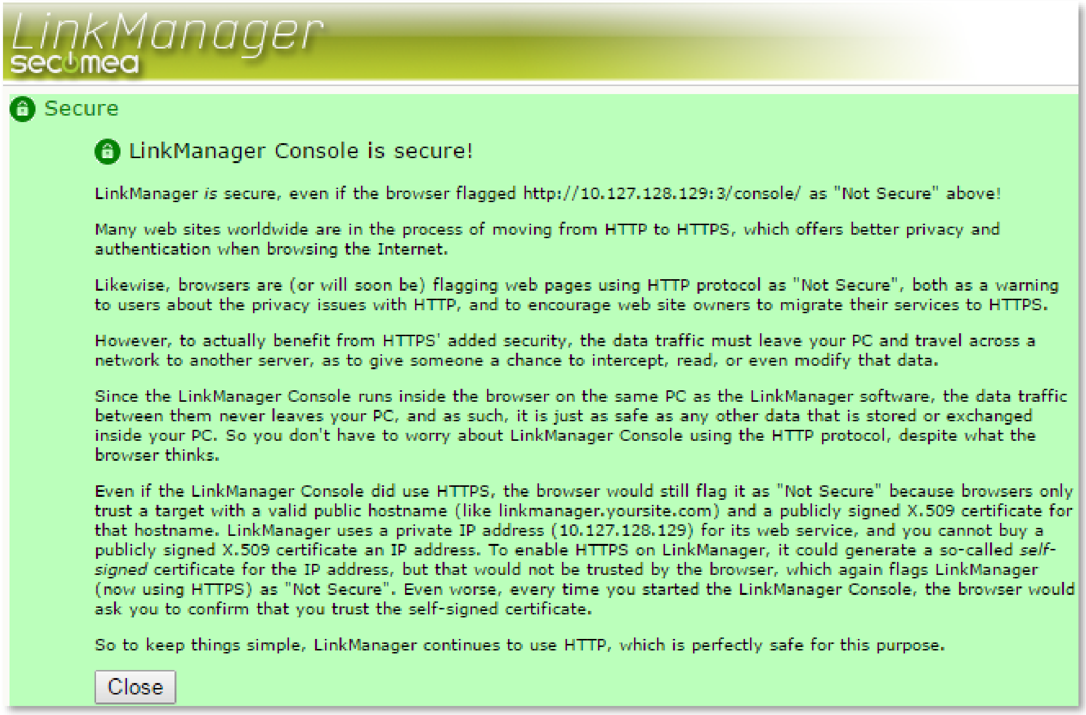
New browsers unconditionally labels non TLS/SSL sessions as “unsafe” if a password field or other input field is present:



This connection is not secure. Logins entered here could be compromised. Learn More

The LinkManager does not need to make a secure connection as no data on the specific connection ever leaves the local PC unencrypted.

An explanation for this scenario has been provided when clicking the padlock:



LinkManager Console is secure!

LinkManager *is* secure, even if the browser flagged http://10.127.128.129:3/console/ as "Not Secure" above!

Many web sites worldwide are in the process of moving from HTTP to HTTPS, which offers better privacy and authentication when browsing the Internet.

Likewise, browsers are (or will soon be) flagging web pages using HTTP protocol as "Not Secure", both as a warning to users about the privacy issues with HTTP, and to encourage web site owners to migrate their services to HTTPS.

However, to actually benefit from HTTPS' added security, the data traffic must leave your PC and travel across a network to another server, as to give someone a chance to intercept, read, or even modify that data.

Since the LinkManager Console runs inside the browser on the same PC as the LinkManager software, the data traffic between them never leaves your PC, and as such, it is just as safe as any other data that is stored or exchanged inside your PC. So you don't have to worry about LinkManager Console using the HTTP protocol, despite what the browser thinks.

Even if the LinkManager Console did use HTTPS, the browser would still flag it as "Not Secure" because browsers only trust a target with a valid public hostname (like linkmanager.yoursite.com) and a publicly signed X.509 certificate for that hostname. LinkManager uses a private IP address (10.127.128.129) for its web service, and you cannot buy a publicly signed X.509 certificate an IP address. To enable HTTPS on LinkManager, it could generate a so-called *self-signed* certificate for the IP address, but that would not be trusted by the browser, which again flags LinkManager (now using HTTPS) as "Not Secure". Even worse, every time you started the LinkManager Console, the browser would ask you to confirm that you trust the self-signed certificate.

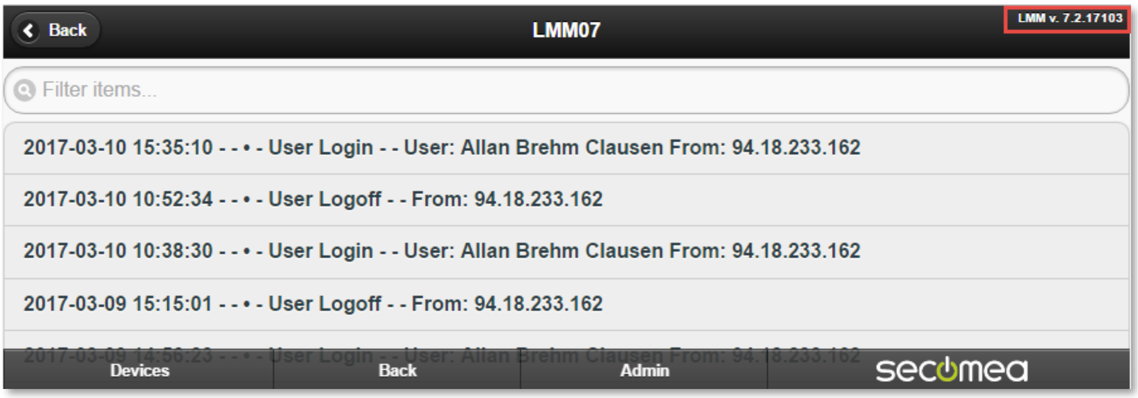
So to keep things simple, LinkManager continues to use HTTP, which is perfectly safe for this purpose.

7. LinkManager Mobile

7.1. Version information

It is now possible to see the version number in LinkManager Mobile

Click “Audit” and the information are located in the upper right hand corner.



```
2017-03-10 15:35:10 - - • - User Login - - User: Allan Brehm Clausen From: 94.18.233.162
2017-03-10 10:52:34 - - • - User Logoff - - From: 94.18.233.162
2017-03-10 10:38:30 - - • - User Login - - User: Allan Brehm Clausen From: 94.18.233.162
2017-03-09 15:15:01 - - • - User Logoff - - From: 94.18.233.162
2017-03-09 14:56:23 - - • - User Login - - User: Allan Brehm Clausen From: 94.18.233.162
```

7.2. Login screen functionality

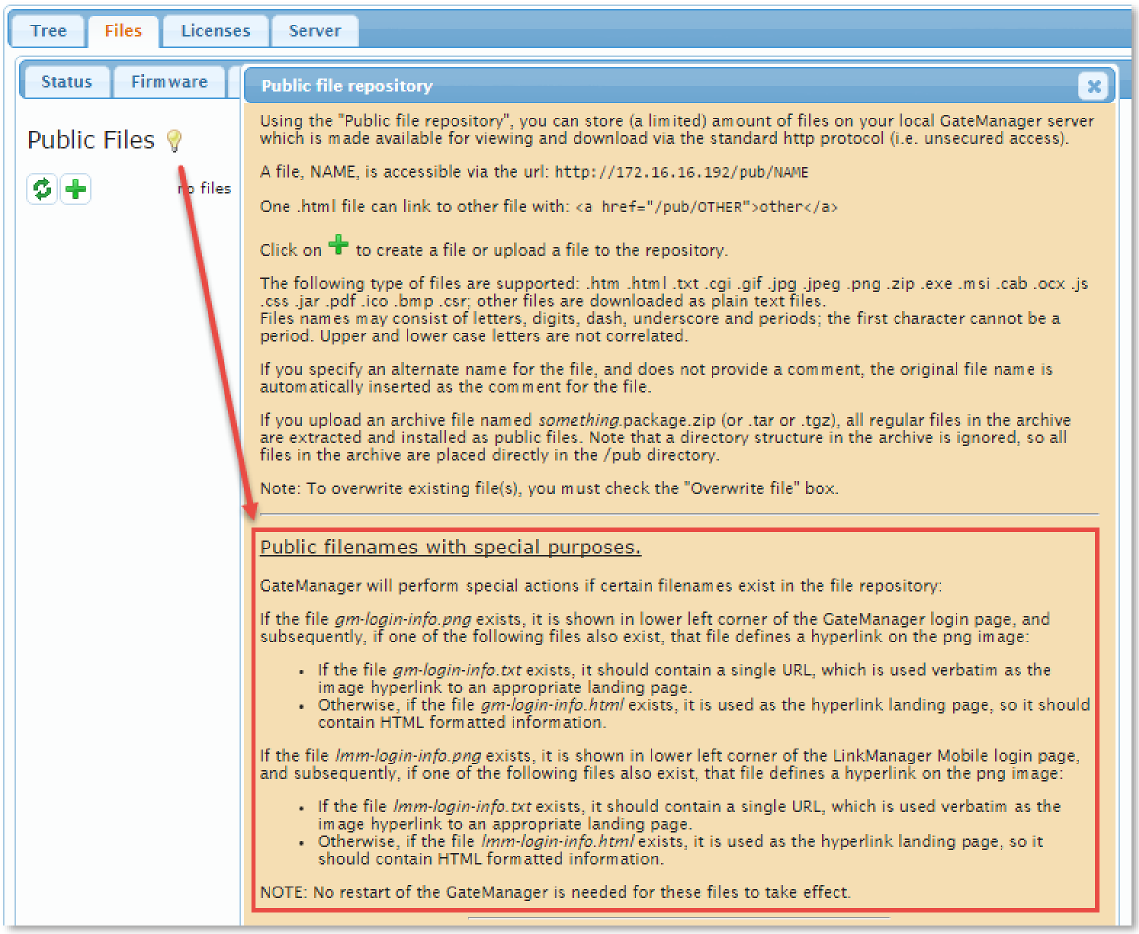
It is now possible to add a logo to the LinkManager Mobile login screen, to either display a legal message (or any other HTML formatted page) or link to an existing page.

The logo should be created as a PNG file named “lmm-login-info.png” and uploaded to the server under “Files -> Public”.

Then there is a choice between an HTML file (named “lmm-lgin-info.html”) that contains the whole page or a text file (called “lmm-lgin-info.txt”) that contains a link to another page.

If both files are present, the text file will take precedence.

There is a new lightbulb text explaining the process:



Public file repository

Using the "Public file repository", you can store (a limited) amount of files on your local GateManager server which is made available for viewing and download via the standard http protocol (i.e. unsecured access).

A file, NAME, is accessible via the url: `http://172.16.16.192/pub/NAME`

One .html file can link to other file with: `<a href="/pub/OTHER">other</a>`

Click on ✚ to create a file or upload a file to the repository.

The following type of files are supported: .htm .html .txt .cgi .gif .jpg .jpeg .png .zip .exe .msi .cab .ocx .js .css .jar .pdf .ico .bmp .csr; other files are downloaded as plain text files.
Files names may consist of letters, digits, dash, underscore and periods; the first character cannot be a period. Upper and lower case letters are not correlated.

If you specify an alternate name for the file, and does not provide a comment, the original file name is automatically inserted as the comment for the file.

If you upload an archive file named *something*.package.zip (or .tar or .tgz), all regular files in the archive are extracted and installed as public files. Note that a directory structure in the archive is ignored, so all files in the archive are placed directly in the /pub directory.

Note: To overwrite existing file(s), you must check the "Overwrite file" box.

Public filenames with special purposes.

GateManager will perform special actions if certain filenames exist in the file repository:

If the file *gm-login-info.png* exists, it is shown in lower left corner of the GateManager login page, and subsequently, if one of the following files also exist, that file defines a hyperlink on the png image:

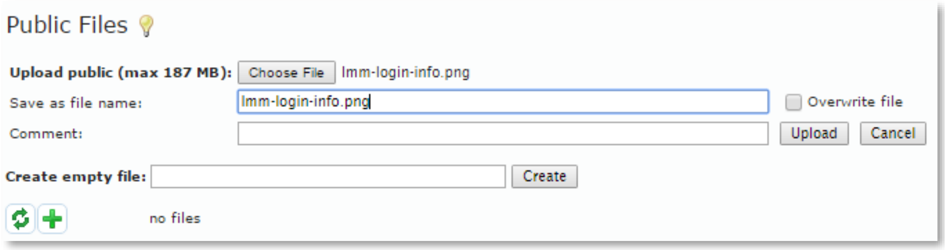
- If the file *gm-login-info.txt* exists, it should contain a single URL, which is used verbatim as the image hyperlink to an appropriate landing page.
- Otherwise, if the file *gm-login-info.html* exists, it is used as the hyperlink landing page, so it should contain HTML formatted information.

If the file *lmm-login-info.png* exists, it is shown in lower left corner of the LinkManager Mobile login page, and subsequently, if one of the following files also exist, that file defines a hyperlink on the png image:

- If the file *lmm-login-info.txt* exists, it should contain a single URL, which is used verbatim as the image hyperlink to an appropriate landing page.
- Otherwise, if the file *lmm-login-info.html* exists, it is used as the hyperlink landing page, so it should contain HTML formatted information.

NOTE: No restart of the GateManager is needed for these files to take effect.

The files are uploaded through the "plus" icon and must have the exact file-name:



Public Files

Upload public (max 187 MB): Choose File lmm-login-info.png

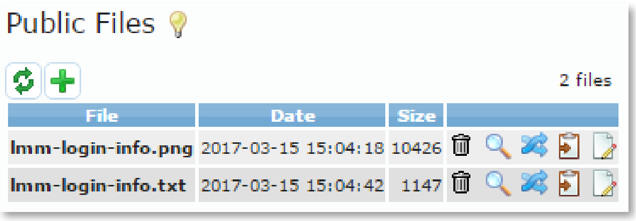
Save as file name: lmm-login-info.png ☐ Overwrite file

Comment:

Create empty file:

no files

When both files are present, like this:

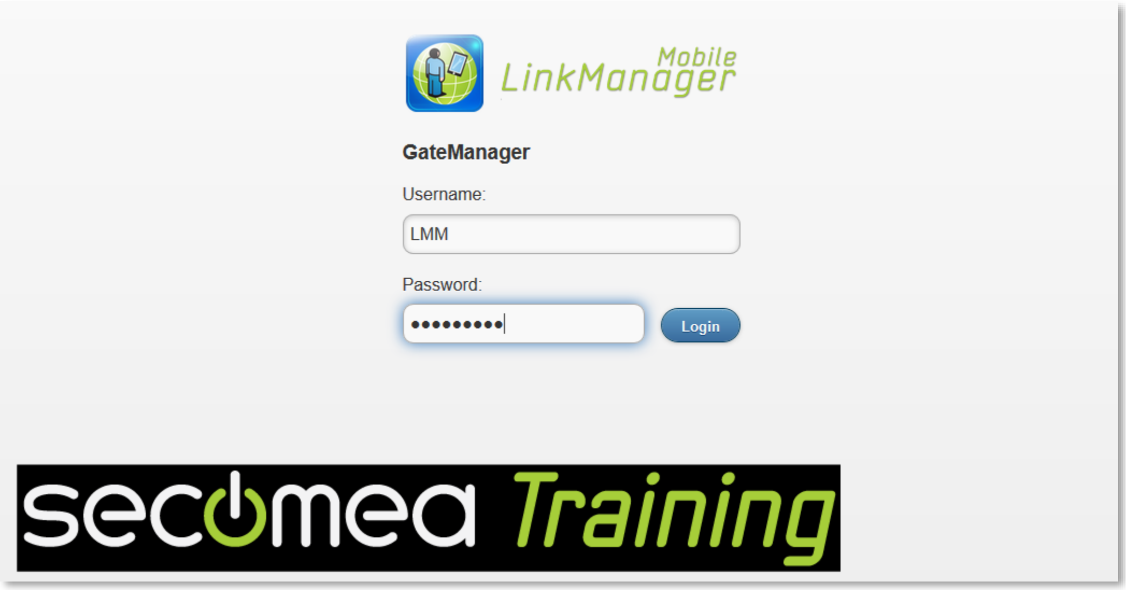


Public Files

2 files

File	Date	Size	
lmm-login-info.png	2017-03-15 15:04:18	10426	
lmm-login-info.txt	2017-03-15 15:04:42	1147	

The result will appear when logging in to LinkManager Mobile:



7.3. In-Browser VNC Viewer

This release contains a new build-in VNC viewer to be used from any device using a major Web Browser.

7.3.1. Prerequisites

The connection will take place through an encrypted session and there are no external dependencies.

Supported browsers:

- Google Chrome
- Internet Explorer
- Microsoft Edge
- Mozilla FireFox
- Opera*
- Safari*

(* see below for limitations)

The VNC server type should not make a big difference, testing was done on major VNC servers (UltraVNC, TightVNC, etc.) including native versions for panels with Windows CE - like the EfonVNC, which is widely used on brand name panels.

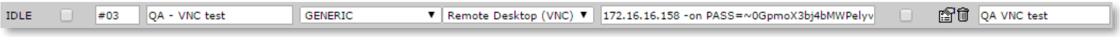
7.3.2. Known issues

Please note the following:

1. A self-signed web certificate is not allowed. If detected, the In-Browser VNC option will be either be disabled or not selectable.
2. Opera will not have full functionality on iOS, Android and Linux
3. Konqueror is not supported
4. Safari will not function in private mode, as the LocalStorage is then set to 0 (this might hold true for other browsers).
5. Mozilla FireFox on Android could in some instances display a hand icon instead of the configuration icon, but the placement and functionality is working.
6. Please not that In-Browser VNC will not connect if the “User name:” field is used.
7. Locking the mobile device will disable the connection to the target.

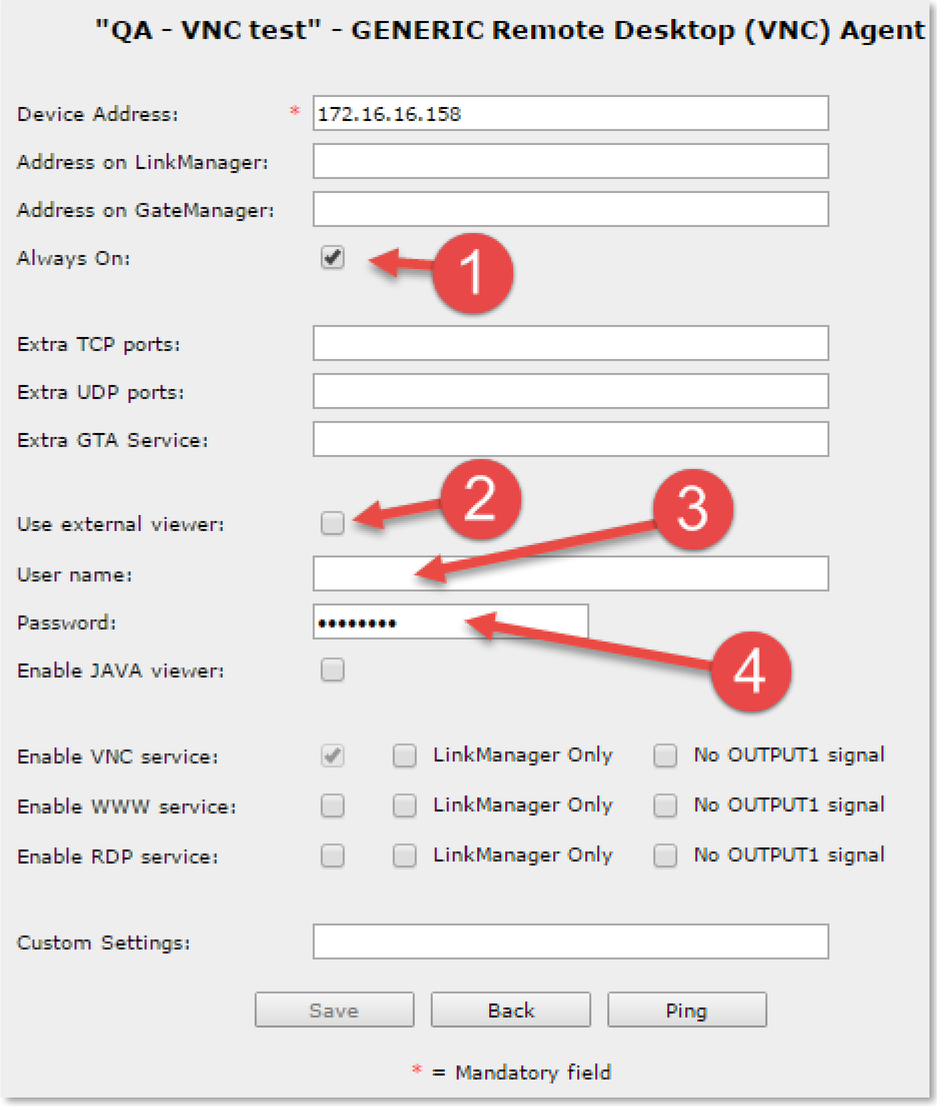
7.3.3. Configuring the agent

Setting up an In-Browser VNC agent is no different from an external agent. Just create any VNC capable agent, like the “Remote Destop (VNC)” agent:



IDLE	□	#03	QA - VNC test	GENERIC ▼	Remote Desktop (VNC) ▼	172.16.16.158 -on PASS=~0GpmoX3bj4bMWPelyv	□	QA VNC test

Clicking properties will give you additional options:



"QA - VNC test" - GENERIC Remote Desktop (VNC) Agent

Device Address: * 172.16.16.158

Address on LinkManager:

Address on GateManager:

Always On: ☑

Extra TCP ports:

Extra UDP ports:

Extra GTA Service:

Use external viewer: □

User name:

Password: ••••••••

Enable JAVA viewer: □

Enable VNC service: ☑ □ LinkManager Only □ No OUTPUT1 signal

Enable WWW service: □ □ LinkManager Only □ No OUTPUT1 signal

Enable RDP service: □ □ LinkManager Only □ No OUTPUT1 signal

Custom Settings:

* = Mandatory field

1 Selecting “Always On:” is necessary on most Windows 7 and 10 installations when using the VNC viewer to access a workstation screen. This is due to the internal firewall, that prohibits IMCP pings from coming through. The Agent uses ICMP ping to check if the agent target is up. Either configure the firewall to let the ICMP ping though, or just assume the unit is up by selecting “Always On:”.

2 In-Browser VNC viewer already enabled when upgrading to 7.2. An external VNC viewer can always be selected over the internal viewer when using either GTA from GateManager or LinkManager mobile. This can be set globally from the agent directly by selecting “Use external viewer:”.

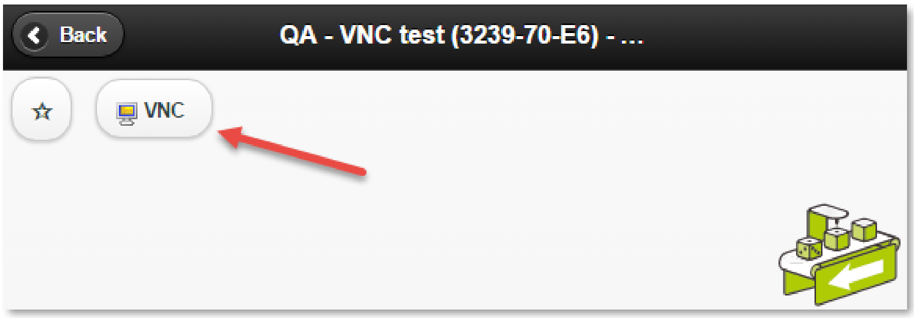
Use cases for this option, could be special native VNC servers that require tailored clients or APPs that was created to handle the VNC client.

3 As stated above, please do not use the “User name:” with the In-Browser VNC viewer. This option was meant to pass information to the LinkManager service. Not to LinkManager Mobile.

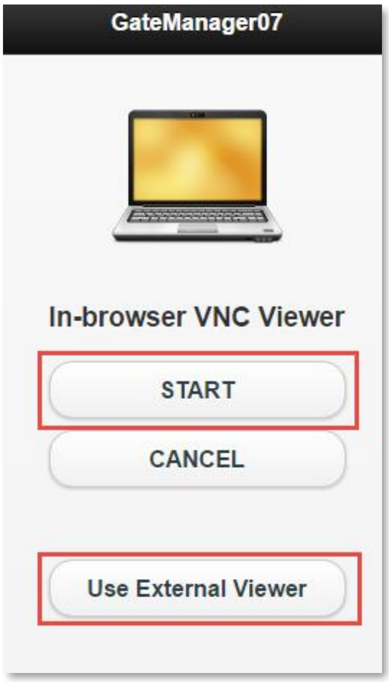
4 Setting a password will enable the In-Browser VNC viewer to pass it to the server and do a login without credentials.

7.3.4. Selecting internal or external viewer

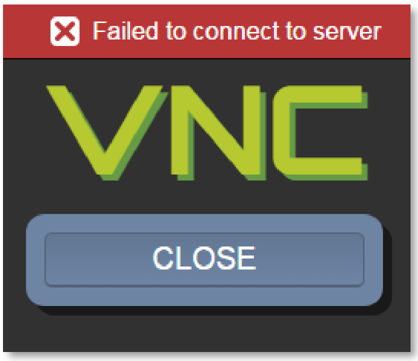
When using LinkManager mobile, just select the VNC service like in 7.1:



Then click “START” to get access to the VNC server through the In-Browser VNC viewer.



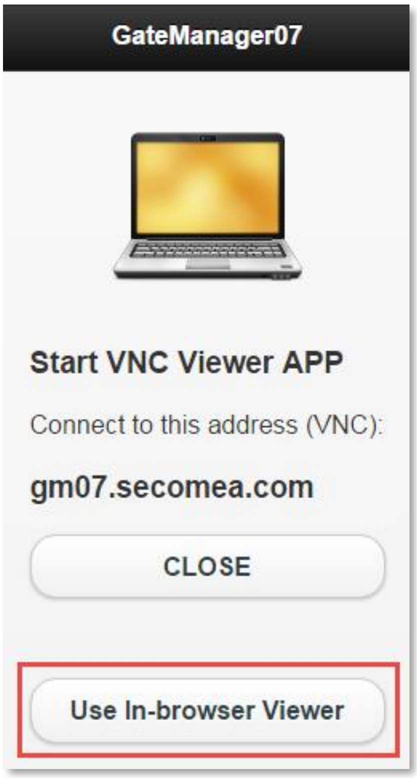
Note that this screen has a 30 second time-out, and “START” should be selected within the 30 second timeframe. Otherwise the VNC client cannot connect:



Failed to connect to server

The same is true for selecting “Use External Viewer” and starting the external program.

If the External viewer is selected, it can be changed back to the Internal Viewer here:



GateManager07

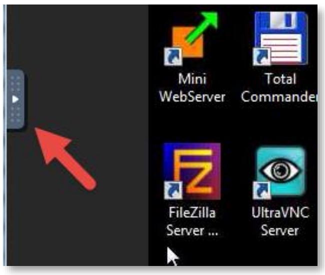
Start VNC Viewer APP

Connect to this address (VNC):

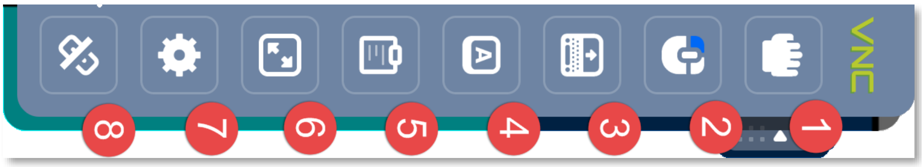
gm07.secomea.com

7.3.5. Using the In-Browser viewer

When connected to the VNC server using the In-Browser VNC viewer, there will be an option tab to the left of the screen:



Clicking this tab will roll out the options menu:



The options menu (rotated for readability) can have a different number of icons depending on platform and use. The one depicted here is from FireFox on iOS.

1 Hand Icon: This icon appears when the VNC target screen is larger than the host screen, typically on mobile devices.

Clicking this icon will turn the pointer into a hand icon and let you move the target screen around.

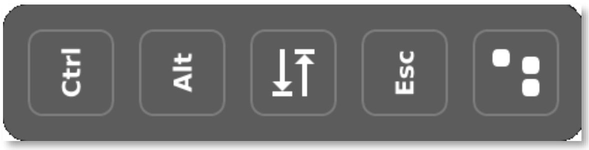
2 Mouse Icon: Clicking icon this will toggle between left, right and middle mouse button. The icons start with the left button (marked blue).

This icon appears on mobile devices and is used to emulate a mouse click from the desired mouse button.

3 Keyboard icon: When the host system does not have a keyboard (Normally on mobile devices), pressing this button will bring up the virtual keyboard on the device.

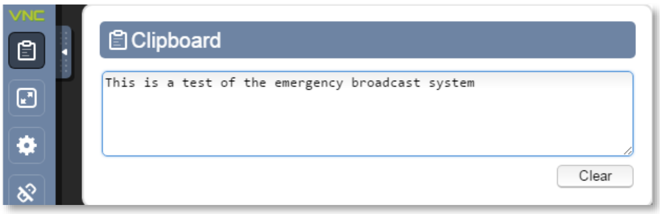
4 Key icon: To send special keyboard combinations, this icon can be used. The picture below (rotated for readability) lets the user select between (from left to right):

- **Ctrl** key (Control)
- **Alt** key (Alternate)
- **Tab** key (Tabulator)
- **Esc** Key (Escape)
- **Ctrl-Alt-Del** key sequence



5 Clipboard icon: With this icon, text can be pasted from the host to the target system. See example below

When text is entered, it will be available for the local OS on system that supports it. Clicking “Clear” will erase the clipboard data.

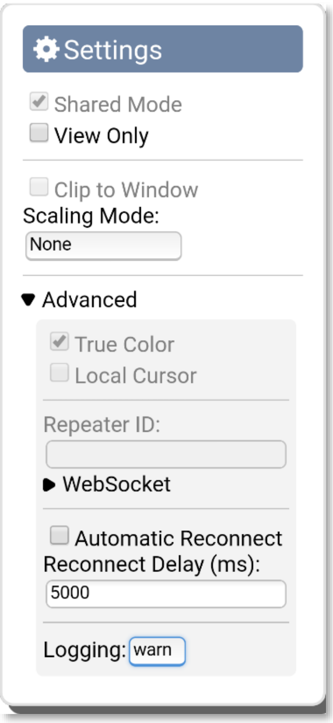


This is a test of the emergency broadcast system

6 Fullscreen icon: Pressing this button will display the VNC target screen without borders or other headers. This icon is present on Android but not all operating systems, iOS will not have this ability. Please note that this button has nothing to do with image scaling.

7 Settings icon: Pressing this button will bring up the settings menu (see picture below).

Some of these settings are selected by default and cannot be changed. This includes the “WebSocket” and the “Shared Mode” settings. Other settings might be unavailable depending on context and host platform.



Settings

☑ Shared Mode
□ View Only

□ Clip to Window
Scaling Mode: None

▼ Advanced

☑ True Color
□ Local Cursor

Repeater ID:

▶ WebSocket

□ Automatic Reconnect
Reconnect Delay (ms): 5000

Logging: warn

View Only: This setting is self-explanatory; it locks the target so no changes can be made. This option persists through browser sessions and devices on the same GateManager.

Scaling Mode: There are 4 options, “None”, “Local Scaling”, “Local Downscaling” and “Remote Resizing”.

“None” will display the target precisely the size as the original, leaving the image either too big or too small, the hand icon can be used to mode the image around.

“Local Scaling” will do both upscaling and down-scaling, while “Local Downscaling” only allows downscaling.

“Remote Resizing” will request the target to resize the target screen to match that of the VNC viewers host screen.

Logging: can be switched between “Error”, “Warn”, “Info” and “Debug”. This setting will control the logging to the Java Script Console.

Automatic reconnect should not be configured as it has no effect in this scenario.

8 Exit icon: Pressing this icon will terminate the current selection and return to the Appliance view.

8. Advanced Tech Topics

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

8.1. API changes

8.1.1. Extended Status Information

The HTML “Tray Icon Status” (/icon) contained information not found in the JSON Connection Status (/api/status). Section 3.3 has been updated with new “attach” and “license” labels. See the API documentation for 7.2 for detailed information.

8.1.2. Hostname changes

A new configuration parameter has been added to the JSON API, called “Hostname”, available for Windows and Linux.

The hostname forwarded to GateManager in the heartbeat as part of the appliance name <Name>["hostname"] See chapter 9 in the API documentation.

If Hostname is not specified (<blank>), SME will read the hostname from the host system.

8.1.3. Windows 10 Anniversary update (1607)

As a result of the changes to device driver security in the Windows 10 Anniversary Update (1607), all driver certificates have been resigned by Microsoft.

The new driver signing is important as it allows them to be used when secure boot is enabled on Windows 10.

9. Documentation

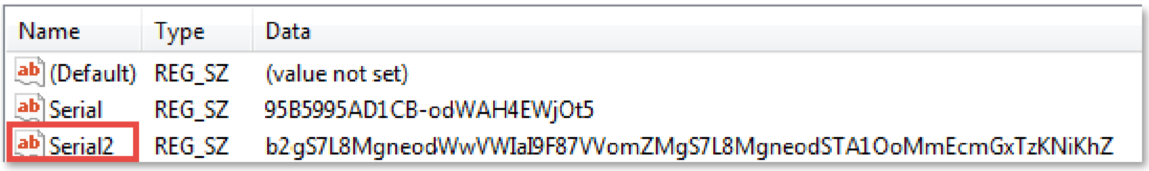
The following new documents have been created or updated

- API Documentation V1.6

10. APPENDIX – Troubleshooting Secondary ID

Continue from Chapter 2.2 above Secondary ID (Serial 2)

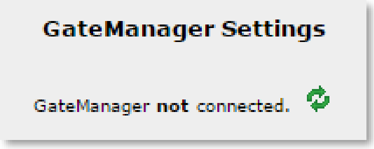
From release 7.2, all appliances have been issued a Secondary ID.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Serial	REG_SZ	95B5995AD1CB-odWAH4EWjOt5
Serial2	REG_SZ	b2gS7L8MgneodWwVWIal9F87VVomZMgS7L8MgneodSTA1OoMmEcmGxTzKNiKhZ

In addition to the normal serial number generated by the appliance, we have added a Secondary ID (also named “Serial2”) to enhance security.

If this number changes from the one stored on the GateManager, it will be rejected by the GateManager with an error message on the appliance:

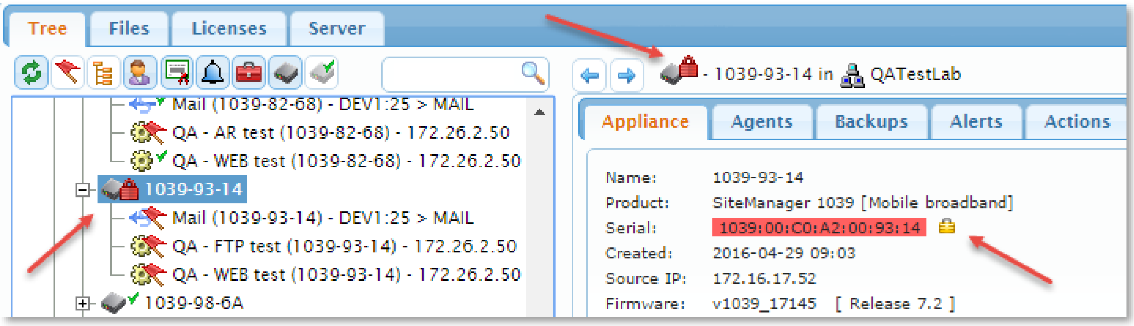


GateManager Settings

GateManager **not** connected.

A padlock icon will appear on the GateManager, both on the Appliance icon at the left, and at the top (red).

There will also be a yellow padlock icon on the far right of the screen:



Mail (1039-82-68) - DEV1:25 > MAIL
QA - AR test (1039-82-68) - 172.26.2.50
QA - WEB test (1039-82-68) - 172.26.2.50
1039-93-14
Mail (1039-93-14) - DEV1:25 > MAIL
QA - FTP test (1039-93-14) - 172.26.2.50
QA - WEB test (1039-93-14) - 172.26.2.50
1039-98-6A

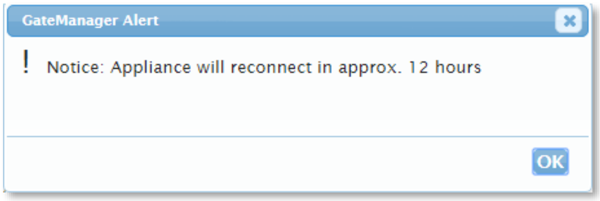
- 1039-93-14 in QATestLab

Name: 1039-93-14
Product: SiteManager 1039 [Mobile broadband]
Serial: 1039:00:C0:A2:00:93:14
Created: 2016-04-29 09:03
Source IP: 172.16.17.52
Firmware: v1039_17145 [Release 7.2]

Selecting this padlock icon will manually allow the appliance to be accepted by the GateManager and connect.

Note that the GateManager has not yet exchanged status information, and the SiteManager is listed as 7.2 (17145) until it can connect again to the GateManager. Although it’s currently on 7.1 (16444).

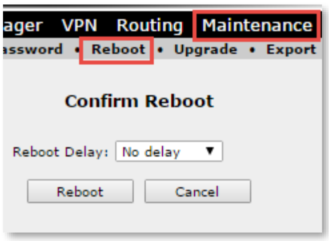
When the padlock icon has been selected, the appliance will be in a suspended state before reconnecting.



GateManager Alert

! Notice: Appliance will reconnect in approx. 12 hours

To shorten wait time, the appliance will reconnect immediately after a reboot:



Confirm Reboot

Reboot Delay: No delay

10.1.1. Reconnect periods

When the appliance reconnects, its reconnect period will depend upon the firmware version. If the appliance is on a 7.1 firmware version (and below) the appliance will take 12 hours to reconnect. On 7.2 and above it will take a maximum of 15 minutes. This can be overridden on both versions by restarting the appliance (i.e. starting and stopping the SiteManager Embedded service or rebooting the SiteManager Hardware).

10.1.2. Padlocked scenarios

Under normal operation a padlock will not occur, but it could appear in special scenarios.

A special scenario (as stated below) could be that a SiteManager was manually downgraded through the SiteManager GUI from 7.2 to 7.1 using an ".ffs" file, thus having its Secondary ID deleted as the 7.1 version has no knowledge of it. When reconnecting after the upgrade, a mismatch between the GateManager and the SiteManager will occur.

Example of scenarios that produce a padlock icon:

- Downgrading any SiteManager using the internal upgrade function in the SiteManager GUI (Maintenance -> Upgrade), from 7.2 and above to 7.1 and below.
- On SiteManager Embedded, deleting the Secondary ID (i.e. due to factory reset, registry changes or file deletion)
- Downgrading a LinkManager to a pre 7.2 version (see "Pre 7.2 LinkManagers (IMPORTANT!)")

10.1.3. Technical details

The Secondary ID is a string of 1-127 characters (range from 0x21 to 0x7e).

When auto generated by the system it will default to a 64-character random string value (a-z, A-Z, 0-9).

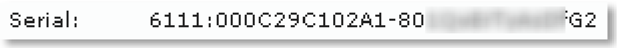
It identifies the Appliance (SiteManagers, LinkManager Appliances, etc.) towards the GateManager along with the normal serial number.

10.1.4. Padlock will show in two variations

If you have the Padlock showing you have two appliances using the same serial number. One SiteManager is the intended SiteManager and the other must be a hijacked SiteManager. The Secondary ID prevent the hijacked SiteManager to be active so everything is OK.

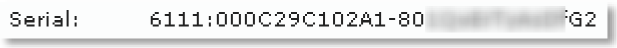
Let's see an example.

1) *Intended SiteManager* connect



Serial: 6111:000C29C102A1-80[redacted]G2

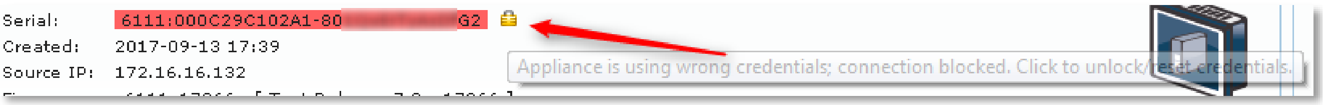
2) *Hijacked SiteManager* connect at the same time



Serial: 6111:000C29C102A1-80[redacted]G2

You will not see any issue because the correct SiteManager is still connected and the Hijacked SiteManager will in silence be rejected.

3) *Intended SiteManager* goes offline while *Hijacked SiteManager* try to connect:



Serial: 6111:000C29C102A1-80[redacted]G2

Created: 2017-09-13 17:39

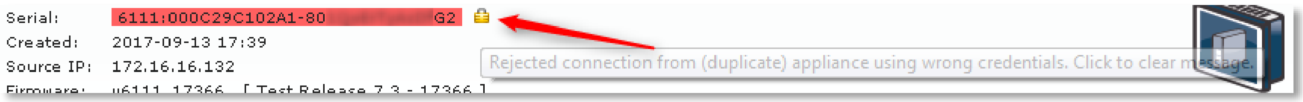
Source IP: 172.16.16.132

Appliance is using wrong credentials; connection blocked. Click to unlock/reset credentials.

Hijacked SiteManager will be rejected.

Mouse over will show: "Appliance is using wrong credentials; connection blocked. Click to unlick/reset credentials."

4) *Intended SiteManager* connect again:



```
Serial:      6111:000C29C102A1-80 [redacted] G2
Created:     2017-09-13 17:39
Source IP:   172.16.16.132
Firmware:    u6111 17366   [ Test Release 7.3 - 17366 ]
```

Rejected connection from (duplicate) appliance using wrong credentials. Click to clear message.

When the *Intended SiteManager* reconnect (powered on) it will again take over the connection.

Mouse over will show: “Rejected connection from (duplicate) appliance using wrong credentials. Click to clear message.”

Pressing the padlock icon will just remove the RED background. *Hijacked SiteManager* will still be rejected in the background, like in first (1) case.

Note: The SiteManager GUI button will only show when it is *Intended SiteManager* that is connected.

11. APPENDIX – Let's Encrypt

The following chapter will show a few hints when trying to install the Royalty-free Web-server Certificate.

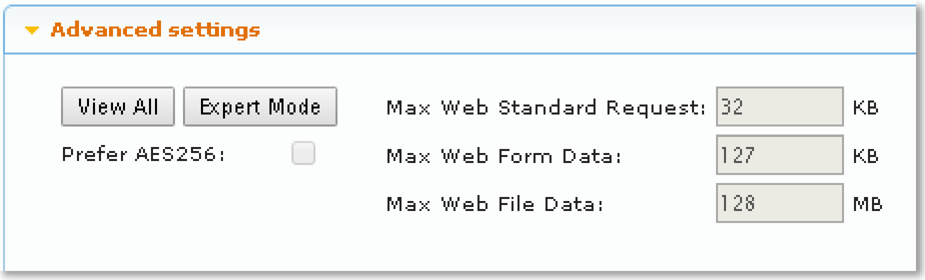
11.1. Staging server for experimental tests

Use the Staging environment if you need to make experiments before your installation is ready for a real Web-Certificate

https://letsencrypt.org/docs/staging-environment/

https://letsencrypt.org/docs/rate-limits/

11.1.1. To switch to staging server:



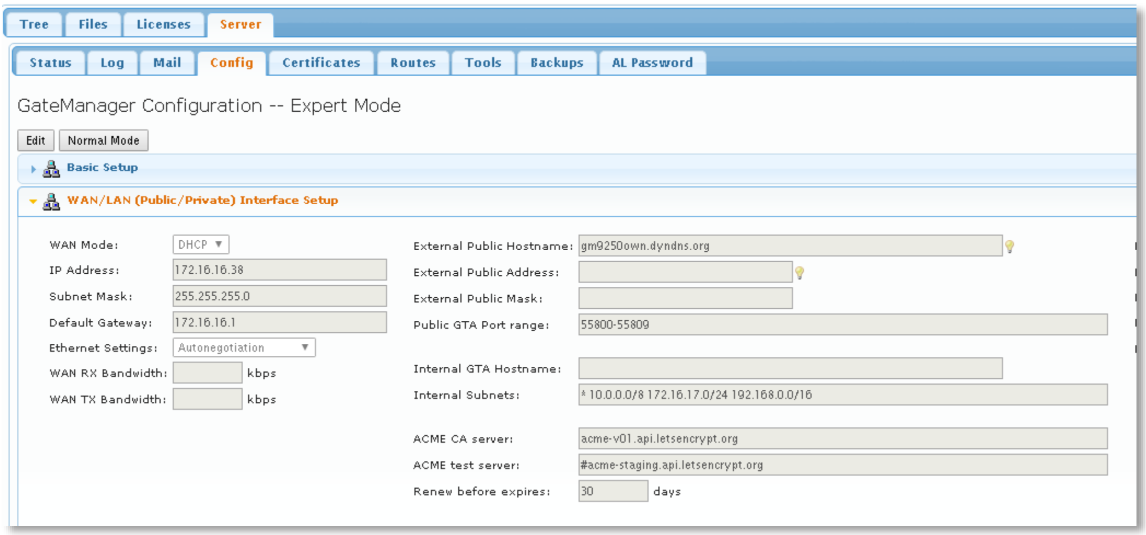
Prefer AES256: □

Max Web Standard Request: 32 KB

Max Web Form Data: 127 KB

Max Web File Data: 128 MB

Enable Expert Mode



GateManager Configuration -- Expert Mode

WAN/LAN (Public/Private) Interface Setup

WAN Mode: DHCP

IP Address: 172.16.16.38

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.16.1

Ethernet Settings: Autonegotiation

WAN RX Bandwidth: kbps

WAN TX Bandwidth: kbps

External Public Hostname: gm9250own.dyndns.org

External Public Address:

External Public Mask:

Public GTA Port range: 55800-55809

Internal GTA Hostname:

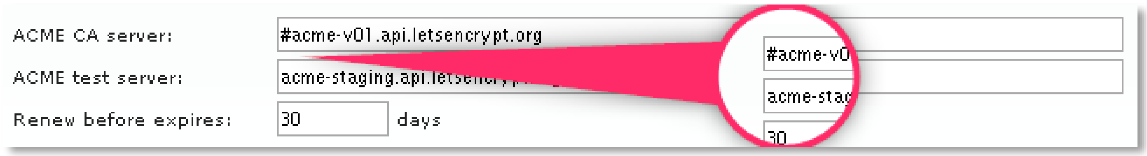
Internal Subnets: * 10.0.0.0/8 172.16.17.0/24 192.168.0.0/16

ACME CA server: acme-v01.api.letsencrypt.org

ACME test server: #acme-staging.api.letsencrypt.org

Renew before expires: 30 days

Enter Edit mode and change the ACME fields like:



ACME CA server: #acme-v01.api.letsencrypt.org

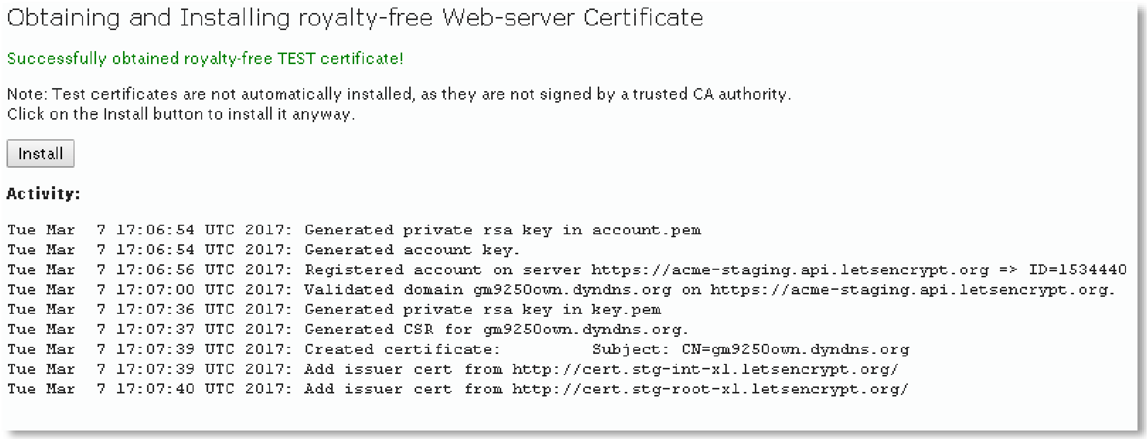
ACME test server: acme-staging.api.letsen

Renew before expires: 30 days

Staging mode for testing and unlimited **Duplicate Certificates**.

The server will need a reboot.

Result of a Staging certificate request:



Obtaining and Installing royalty-free Web-server Certificate

Successfully obtained royalty-free TEST certificate!

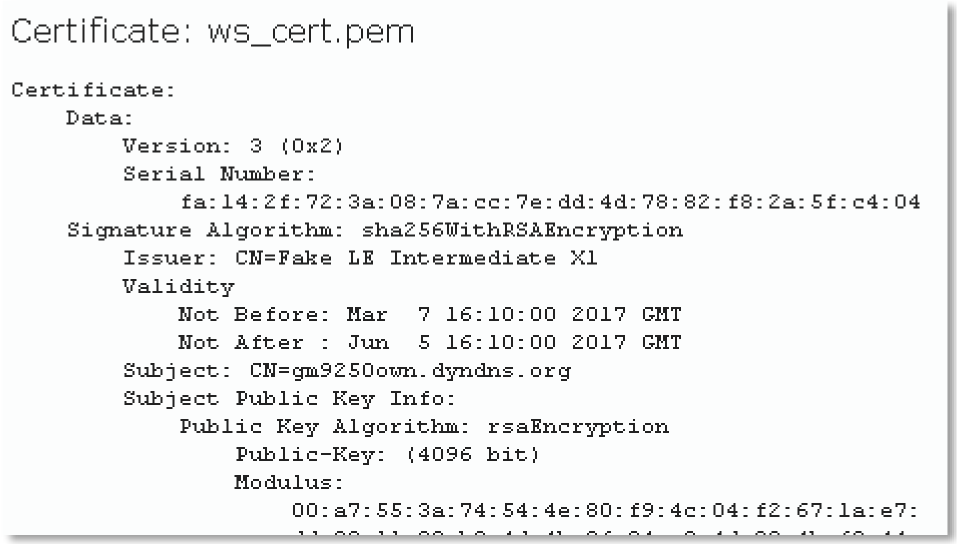
Note: Test certificates are not automatically installed, as they are not signed by a trusted CA authority.
Click on the Install button to install it anyway.

Activity:

```
Tue Mar  7 17:06:54 UTC 2017: Generated private rsa key in account.pem
Tue Mar  7 17:06:54 UTC 2017: Generated account key.
Tue Mar  7 17:06:56 UTC 2017: Registered account on server https://acme-staging.api.letsencrypt.org => ID=1534440
Tue Mar  7 17:07:00 UTC 2017: Validated domain gm9250own.dyndns.org on https://acme-staging.api.letsencrypt.org.
Tue Mar  7 17:07:36 UTC 2017: Generated private rsa key in key.pem
Tue Mar  7 17:07:37 UTC 2017: Generated CSR for gm9250own.dyndns.org.
Tue Mar  7 17:07:39 UTC 2017: Created certificate:         Subject: CN=gm9250own.dyndns.org
Tue Mar  7 17:07:39 UTC 2017: Add issuer cert from http://cert.stg-int-x1.letsencrypt.org/
Tue Mar  7 17:07:40 UTC 2017: Add issuer cert from http://cert.stg-root-x1.letsencrypt.org/
```

11.1.2. Result:

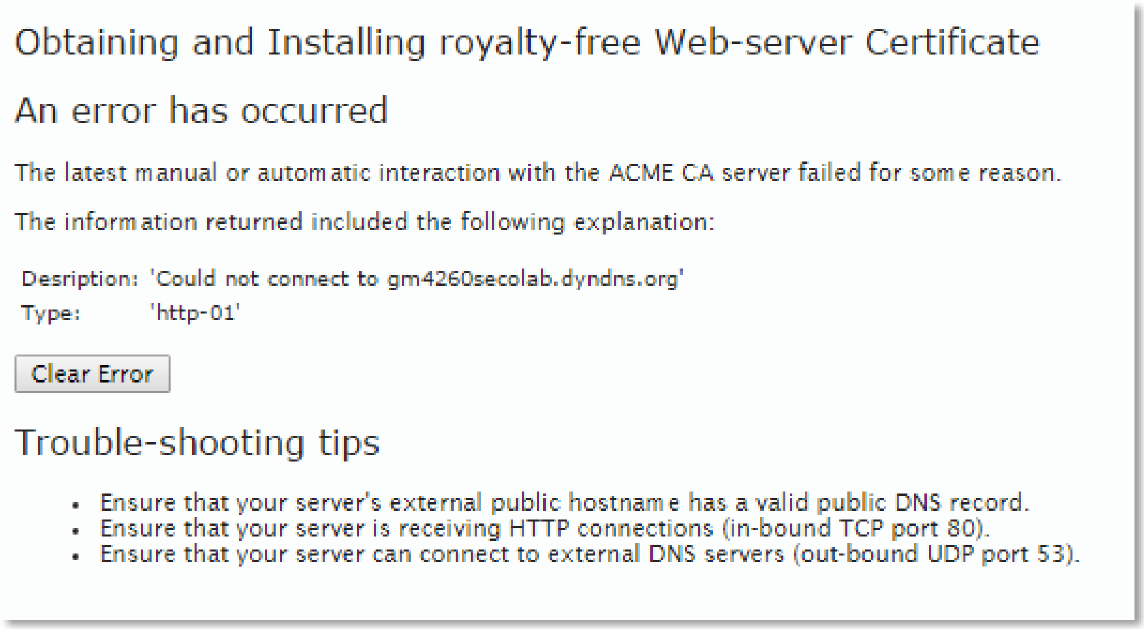
The certificate will NOT be a trusted Cert. for various browsers as expected



Certificate: ws_cert.pem

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fa:14:2f:72:3a:08:7a:cc:7e:dd:4d:78:82:f8:2a:5f:c4:04
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Fake LE Intermediate X1
        Validity
            Not Before: Mar  7 16:10:00 2017 GMT
            Not After : Jun  5 16:10:00 2017 GMT
        Subject: CN=gm9250own.dyndns.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:a7:55:3a:74:54:4e:80:f9:4c:04:f2:67:1a:e7:
```

11.2. Failed request will prompt a trouble-shooting tips



Obtaining and Installing royalty-free Web-server Certificate

An error has occurred

The latest manual or automatic interaction with the ACME CA server failed for some reason.

The information returned included the following explanation:

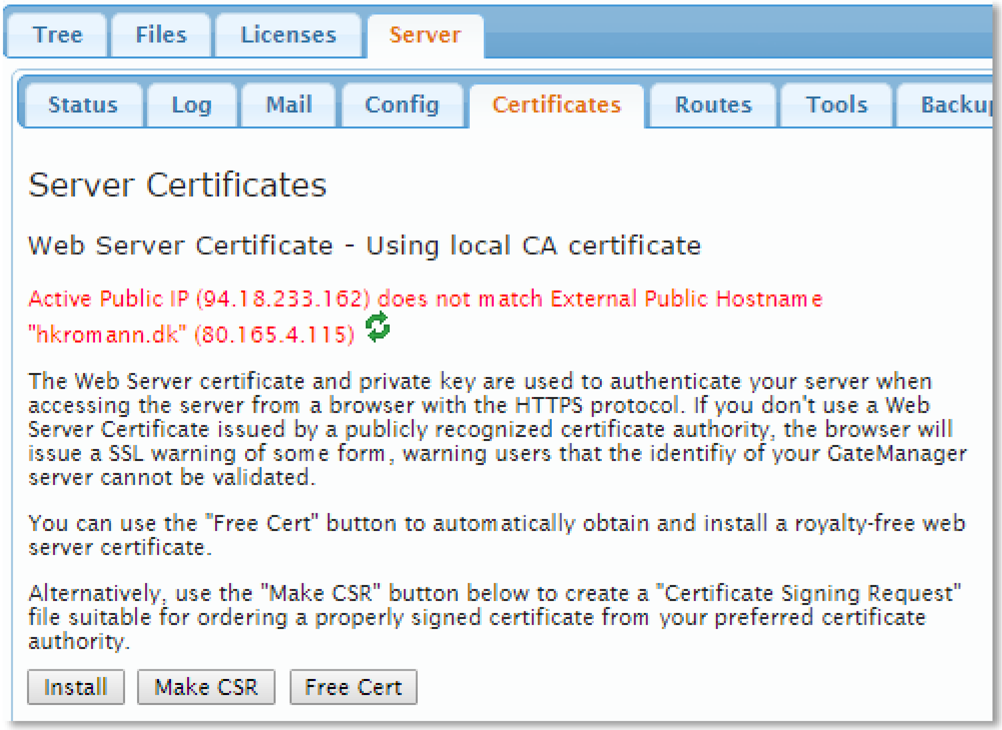
```
Desription: 'Could not connect to gm4260secolab.dyndns.org'
Type:       'http-01'
```

Trouble-shooting tips

- Ensure that your server's external public hostname has a valid public DNS record.
- Ensure that your server is receiving HTTP connections (in-bound TCP port 80).
- Ensure that your server can connect to external DNS servers (out-bound UDP port 53).

In this case, it is likely that there is not port 80 access from the internet to the local GateManager address (http-01).

11.3. CASE: Public IP and public hostname don’t match



Server Certificates

Web Server Certificate - Using local CA certificate

Active Public IP (94.18.233.162) does not match External Public Hostname "hkromann.dk" (80.165.4.115)

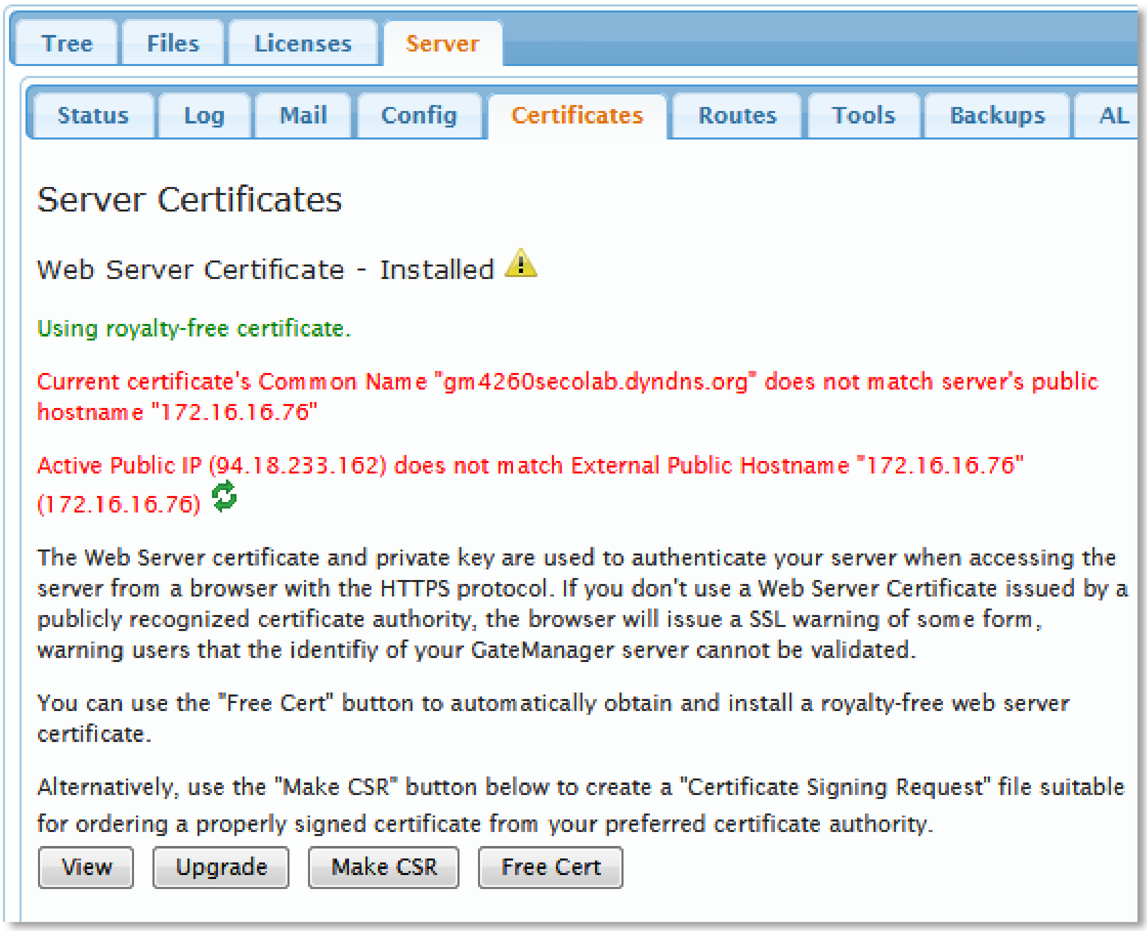
The Web Server certificate and private key are used to authenticate your server when accessing the server from a browser with the HTTPS protocol. If you don't use a Web Server Certificate issued by a publicly recognized certificate authority, the browser will issue a SSL warning of some form, warning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

In this case the Server source IP don’t match the hostname’s assigned IP like: hkromann.dk.

11.4. Valid Web-Certificate but server lost it’s hostname



Server Certificates

Web Server Certificate - Installed ⚠

Using royalty-free certificate.

Current certificate's Common Name "gm4260secolab.dyndns.org" does not match server's public hostname "172.16.16.76"

Active Public IP (94.18.233.162) does not match External Public Hostname "172.16.16.76" (172.16.16.76)

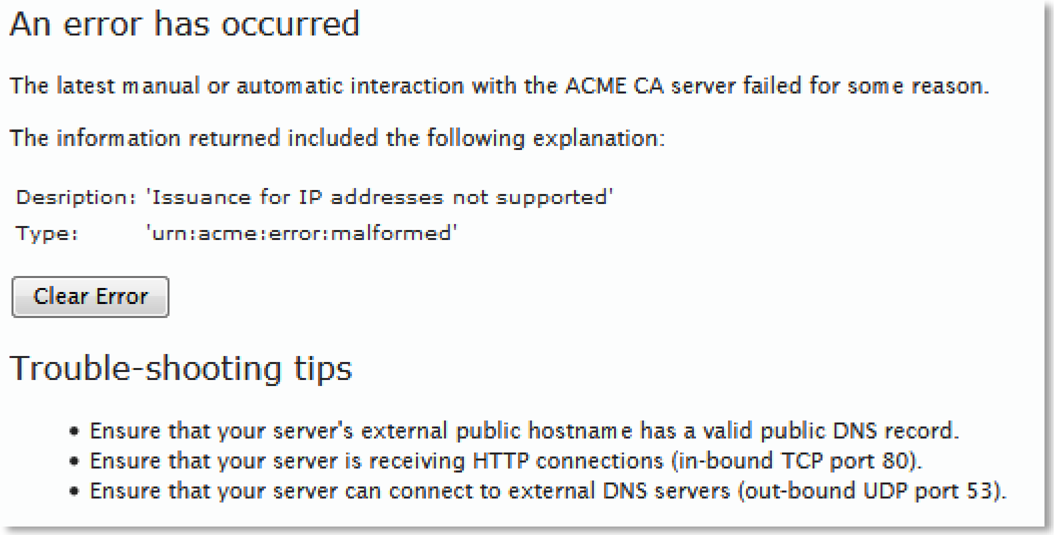
The Web Server certificate and private key are used to authenticate your server when accessing the server from a browser with the HTTPS protocol. If you don't use a Web Server Certificate issued by a publicly recognized certificate authority, the browser will issue a SSL warning of some form, warning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

In this case the server don’t even have a hostname. And the current Web-Certificate don’t match the hostname (172.16.16.76).

11.5. GateManager with no hostname is not supported



An error has occurred

The latest manual or automatic interaction with the ACME CA server failed for some reason.

The information returned included the following explanation:

```
Desription: 'Issuance for IP addresses not supported'
Type:       'urn:acme:error:malformed'
```

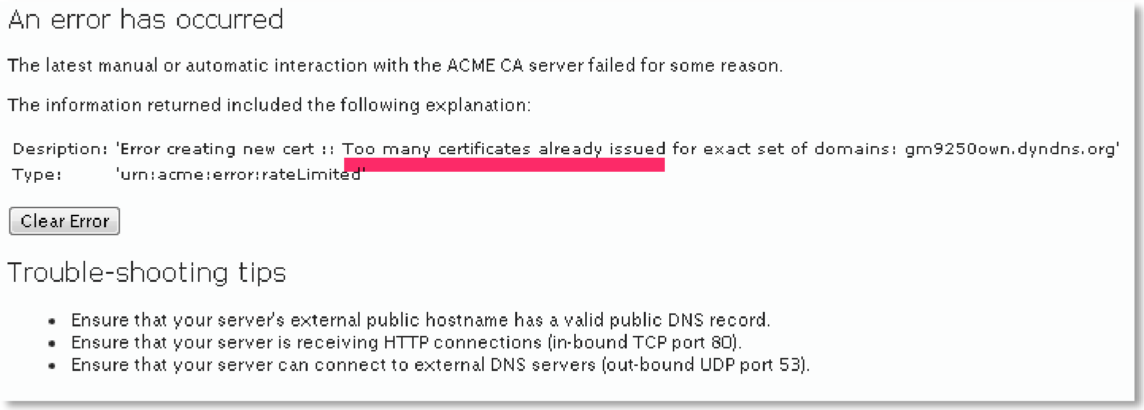
Trouble-shooting tips

- Ensure that your server's external public hostname has a valid public DNS record.
- Ensure that your server is receiving HTTP connections (in-bound TCP port 80).
- Ensure that your server can connect to external DNS servers (out-bound UDP port 53).

It is not possible to request a certificate for an IP address.

11.6. Too many renewals

In case the certificate has been renewed too frequently it will be rejected. In writing the limit is set to 5 certificates pr. 7 days. See chapter above for “Staging environment” in case certificate testing is necessary.



An error has occurred

The latest manual or automatic interaction with the ACME CA server failed for some reason.

The information returned included the following explanation:

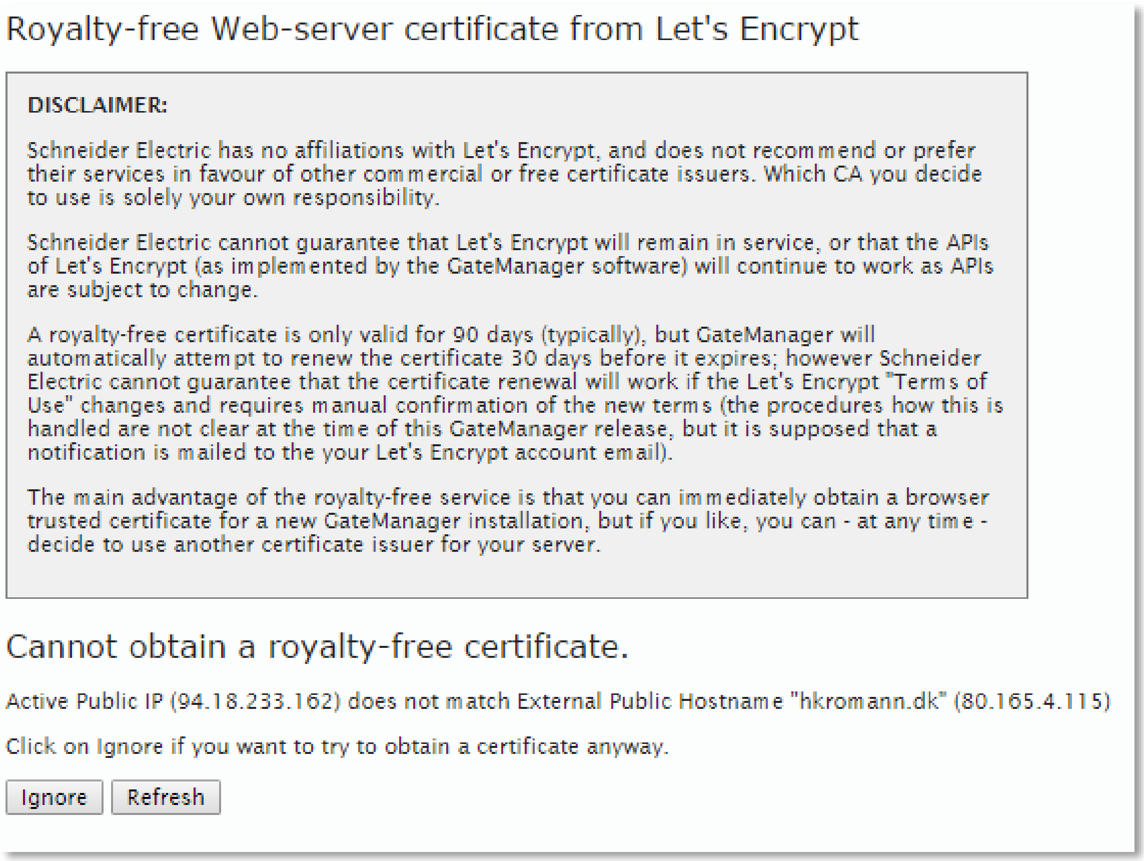
```
Desription: 'Error creating new cert :: Too many certificates already issued for exact set of domains: gm9250own.dyndns.org'
Type:       'urn:acme:error:rateLimited'
```

Trouble-shooting tips

- Ensure that your server's external public hostname has a valid public DNS record.
- Ensure that your server is receiving HTTP connections (in-bound TCP port 80).
- Ensure that your server can connect to external DNS servers (out-bound UDP port 53).

```
Error: Rejected - Error creating new cert :: Too many certificates
already issued for exact set of domains: gm9250own.dyndns.org
```

11.7. Install Certificate anyway



Royalty-free Web-server certificate from Let's Encrypt

DISCLAIMER:

Schneider Electric has no affiliations with Let's Encrypt, and does not recommend or prefer their services in favour of other commercial or free certificate issuers. Which CA you decide to use is solely your own responsibility.

Schneider Electric cannot guarantee that Let's Encrypt will remain in service, or that the APIs of Let's Encrypt (as implemented by the GateManager software) will continue to work as APIs are subject to change.

A royalty-free certificate is only valid for 90 days (typically), but GateManager will automatically attempt to renew the certificate 30 days before it expires; however Schneider Electric cannot guarantee that the certificate renewal will work if the Let's Encrypt "Terms of Use" changes and requires manual confirmation of the new terms (the procedures how this is handled are not clear at the time of this GateManager release, but it is supposed that a notification is mailed to the your Let's Encrypt account email).

The main advantage of the royalty-free service is that you can immediately obtain a browser trusted certificate for a new GateManager installation, but if you like, you can - at any time - decide to use another certificate issuer for your server.

Cannot obtain a royalty-free certificate.

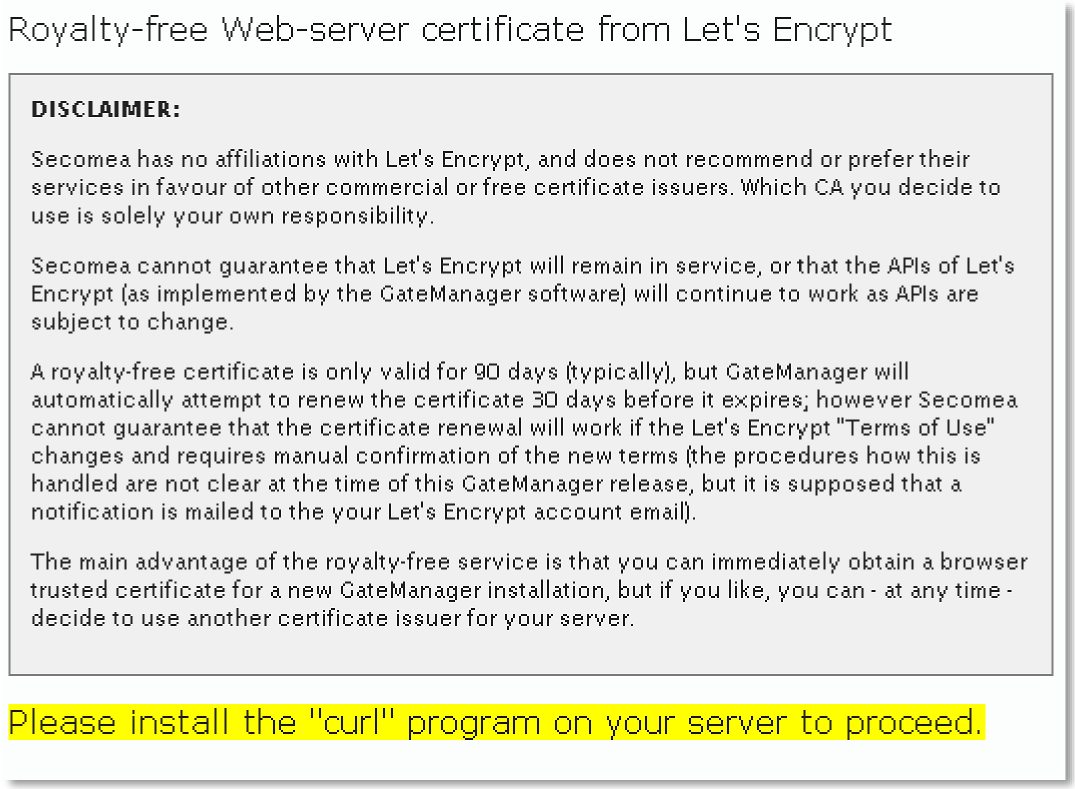
Active Public IP (94.18.233.162) does not match External Public Hostname "hkromann.dk" (80.165.4.115)

Click on Ignore if you want to try to obtain a certificate anyway.

It is possible to install the Web-certificate even if the hostname and public IP don’t match. This can be in case the GateManager has dual WAN connections and therefor might use the failover address when it try to request the Lets Encrypt Certificate.

Important! There must still be TCP:80 access on the right IP address to the Server for the Lets Encrypt to validate the server. In this case it is 80.165.4.115 need to be the one connecting to GateManager on port 80.

11.8. Missing CURL on GM 8250



Royalty-free Web-server certificate from Let's Encrypt

DISCLAIMER:

Secomea has no affiliations with Let's Encrypt, and does not recommend or prefer their services in favour of other commercial or free certificate issuers. Which CA you decide to use is solely your own responsibility.

Secomea cannot guarantee that Let's Encrypt will remain in service, or that the APIs of Let's Encrypt (as implemented by the GateManager software) will continue to work as APIs are subject to change.

A royalty-free certificate is only valid for 90 days (typically), but GateManager will automatically attempt to renew the certificate 30 days before it expires; however Secomea cannot guarantee that the certificate renewal will work if the Let's Encrypt "Terms of Use" changes and requires manual confirmation of the new terms (the procedures how this is handled are not clear at the time of this GateManager release, but it is supposed that a notification is mailed to the your Let's Encrypt account email).

The main advantage of the royalty-free service is that you can immediately obtain a browser trusted certificate for a new GateManager installation, but if you like, you can - at any time - decide to use another certificate issuer for your server.

Please install the "curl" program on your server to proceed.

In case the Linux installation did not include the curl program. Go to the Linux console and install curl.

Redhat/CentOS distributions:

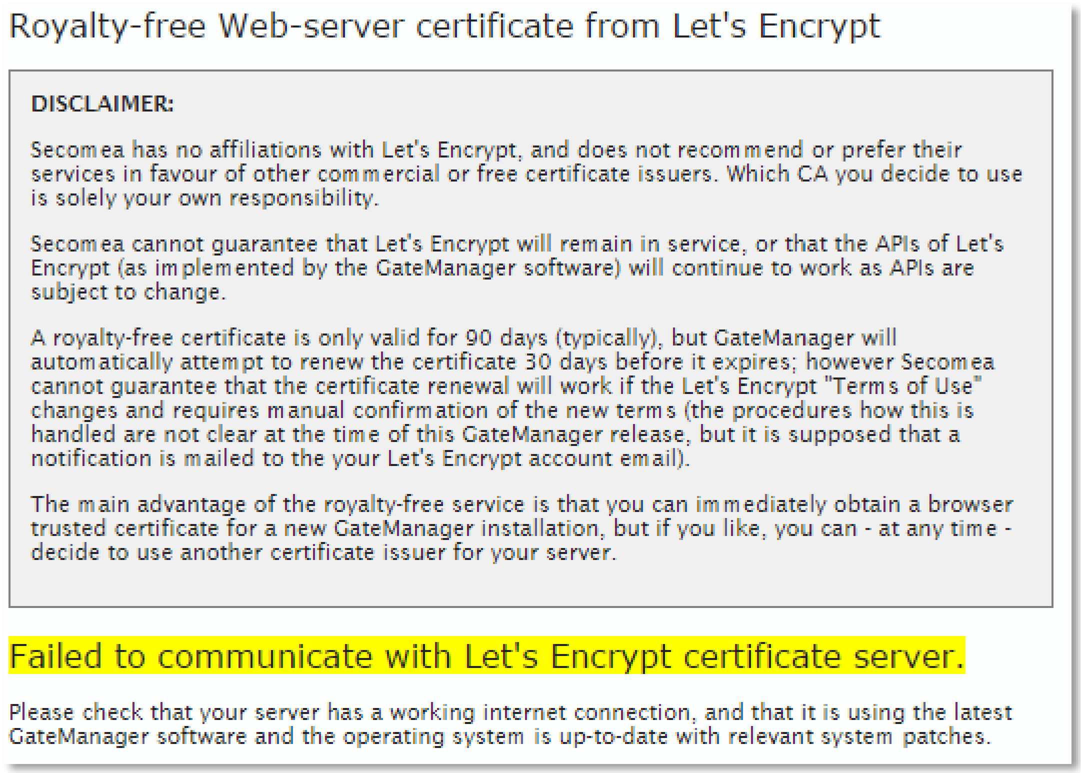
```
# yum install curl
```

Debian/ubunto disatributions:

```
# apt-get install curl
```

11.9. Running on outdated Linux system

If for some reason the Linux system is not up to date you might have trouble completing the Let’s Encrypt process. The GateManager will raise the Yellow message below:



Royalty-free Web-server certificate from Let's Encrypt

DISCLAIMER:

Secomea has no affiliations with Let's Encrypt, and does not recommend or prefer their services in favour of other commercial or free certificate issuers. Which CA you decide to use is solely your own responsibility.

Secomea cannot guarantee that Let's Encrypt will remain in service, or that the APIs of Let's Encrypt (as implemented by the GateManager software) will continue to work as APIs are subject to change.

A royalty-free certificate is only valid for 90 days (typically), but GateManager will automatically attempt to renew the certificate 30 days before it expires; however Secomea cannot guarantee that the certificate renewal will work if the Let's Encrypt "Terms of Use" changes and requires manual confirmation of the new terms (the procedures how this is handled are not clear at the time of this GateManager release, but it is supposed that a notification is mailed to the your Let's Encrypt account email).

The main advantage of the royalty-free service is that you can immediately obtain a browser trusted certificate for a new GateManager installation, but if you like, you can - at any time - decide to use another certificate issuer for your server.

Failed to communicate with Let's Encrypt certificate server.

Please check that your server has a working internet connection, and that it is using the latest GateManager software and the operating system is up-to-date with relevant system patches.

In most cases a standard update of the linux OS is enough like:

Redhat/CentOS distribution:

```
# yum update
```

Debian/Ubunto distribution:

```
# apt-get update
```

/end

Secomea A/S
Denmark
CVR No. DK31 36 60 38
Email: info@secomea.com
www.secomea.com