GateManager™ Server model 8250 / 9250
Installation STEP 2

This document describes how to configure the Secomea GateManager server with the minimum of configuration.

The intended audience for this document is the GateManager Server Administrator.

Version: 4.0, May 2018
Applicable to GateManager version 7.0 or later

secomea

Table of Contents

secomea

Document Version history

- 3.5 - Initial version

- 3.6 - Clarified difference between 8250 and 9250 in Section 4 (Customer ID). Introducing this version history.

- 3.7 - Section 3.6 was corrected to clarify the "Account mail from" syntax.

- 4.0 - Various changes subsequent to R7.0 and introduction of License Portal for license distribution

- 4.1 – Clarify usage of Server Administrator account, 3.7

secυmea

1. Introduction

1.1. Prerequisites for configuring according to this Guide

This guide will assist you to configure the GateManager with the minimum of settings, and which typically will be sufficient for running in production.

Prerequisites:

- The GateManager has been installed according to the document: **Installation STEP 1** guide by the IT department or a person with IT authorities. This document exists in a version specific to GateManager model **8250** or **9250**

- Make sure that the following information is at hand before configuration can be started. This information should be provided by the person that installed the server according to the STEP 1 guide:

Required information about the GateManager installation	
<GM Address>: The public identification that the GateManager can be reached on from the Internet and which Secomea uses to create the Software License Dongle. It is either a static IP address or a **Fully Qualified Domain Name** (FQDN).	_____
FTP Backup Share Credentials This is optional, but highly recommended!	IP: _____ FTP dir.: _____ Name: _____ Password: _____
SMB Backup share credentials Available for model 8250 only	IP Address: _____ SMB share: _____ SMB Workgroup:_____ SMB Directory:_____ SMB User: _____ SMB Passwd: _____

sec*mea

1.2. Related Documents

The following guides are available from the Secomea partner website – www.secomea.com

- **GateManager Server 8250 Installation STEP 0**

  This guide describes preparation of the Linux platform before GateManager installation. If installing at a hosting center, the VM image with a Linux installation with preinstalled hosting center tools may be provided. This guide uses CentOS as example.

- **GateManager Server 8250 Installation STEP 1**

  This guide describes the installation of the GateManager server on a Linux platform. This step is typically done by the IT department.

- **GateManager Server 9250 Installation STEP 1**

  This guide describes how to deploy the GateManager 9250 virtual image on a virtual hosting server.

- **GateManager Server 8250 / 9250 Installation STEP 2 (THIS GUIDE)**

  This guide describes the necessary steps to configure the GateManager to become operational and to setup backup. The guide is intended for the appointed GateManager Server administrator.

- **GateManager PREMIUM Domain Administration**

  This gives an overview of the daily administration tasks, such as organizing accounts and devices in Domains, provide specific access to specific equipment, create Alerts etc.

secomea

2. Login and perform basic configuration

This section will focus on configuring the minimum settings required to make the GateManager server fully operational.

In the following, we will refer to settings like *<GM Address>* or FTP server credentials from the table in section 1.

2.1. Login to GateManager for the first time

To complete the next section, we assume that you can connect to the GateManager Public IP address (private/local IP address can also be used).

We recommend the web browser Chrome for best user experience, or alternatively Firefox or Safari. Microsoft Internet Explorer (minimum version 9) can be used, but Microsoft web browsers are generally inefficient for interpreting java scripts.
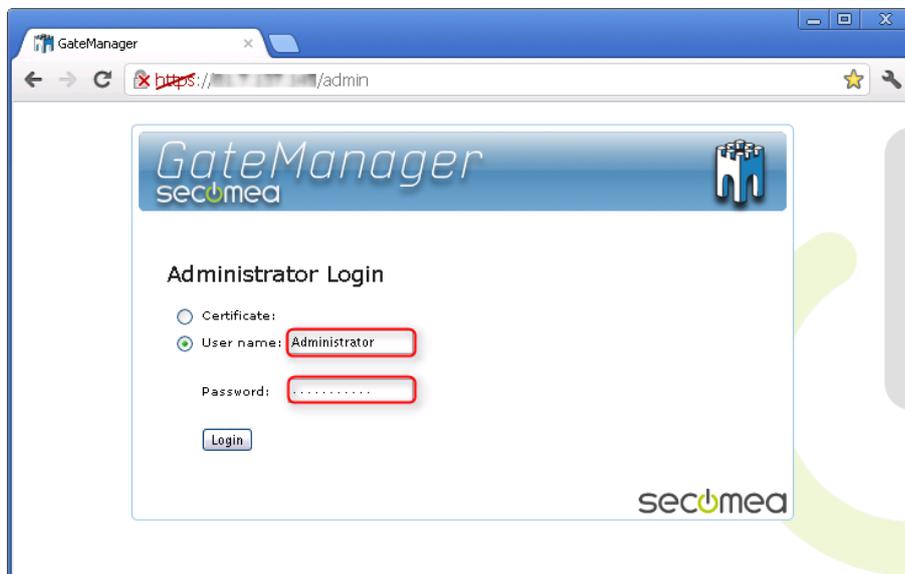
1. Launch the GateManager with the following url:
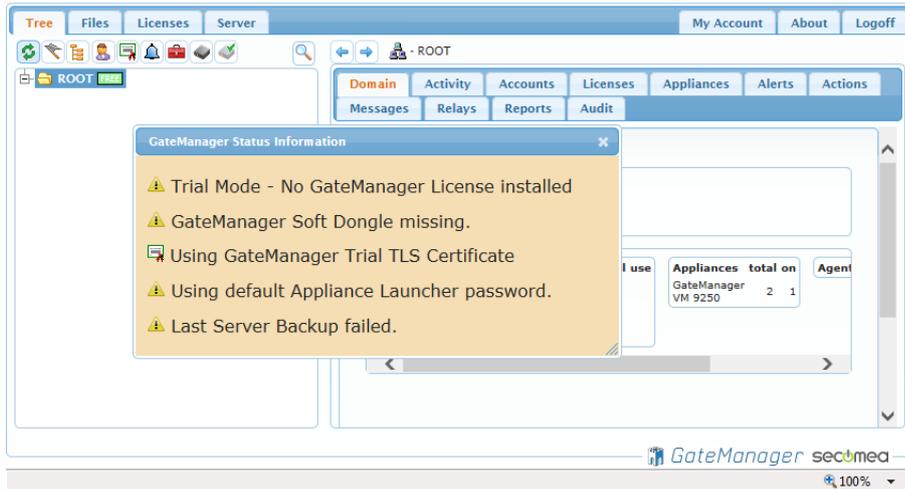
        https://<GM Address>/admin

Default credentials are:

      User name: **Administrator**   (capital A)

      Password: **gatemanager**

secomea

2. When logging in, a splash screen will inform about the general server's current status:

- **Trial Mode.** This indicates that the GateManager does not have a unique TLS certificate installed. The GateManager will be fully functional.
  Installing a TLS certificate will give your GateManager a unique identity, which increases the security, as your SiteManager will then be bound to this server and fully prevent man-in-the-middle attacks through identity spoofing.

- **GateManager Soft Dongle missing**. This means that the GateManager is running in DEMO mode. In DEMO mode, the GateManager supports one LinkManager one LinkManager Mobile and two connected Appliances (SiteManager or TrustGate). It is not allowed to use GateManager for production purposes in DEMO mode.

  Installing a Soft Dongle will remove the LinkManager limit, and increase the max number of appliances limit (see **Section** 4 on page **20** for more info on ordering licenses).

- **Using default Appliance Launcher password.** The backend system also called GateManager OS is still using default password. This password is only used by the Appliance Launcher and which can only access the GateManager OS by broadcast from the local network. Still it should be changed to prevent unintended access. (Menu: Server > AL Password).

- **Last Server Backup failed.** The backup has not been configured yet. See **APPENDIX A, Setting up Backup**.

2.2. Optionally upgrade GateManager to the latest version

It is a good idea at this time to check if there is a newer GateManager firmware version available (check the current version in the About section, and check the Secomea website for a newer version).

A new GateManager version may include the latest bug fixes, support for new appliance types etc.

Refer to **APPENDIX B, Upgrading GateManager firmware** for details.

3. Configuring GateManager environment settings

To make the GateManager fully operational, you must configure the following minimum settings on the GateManager:

- Define a Server Name and web browser title

- Enter/verify the primary DNS

- Public DNS name or IP address that is port-forwarded to the GateManager.

- Setup and verify email relay settings.

- Create a new Server Administrator account and/or change the administrator account (new password and enable certificate). Also consider making a new server administrator account for access by your Service Provider.

3.1. Define a Server Name and Browser Title

1. Login with the default administrator account

2. Select **Server > Config**, and select **Edit** for the **Basic Setup** section.
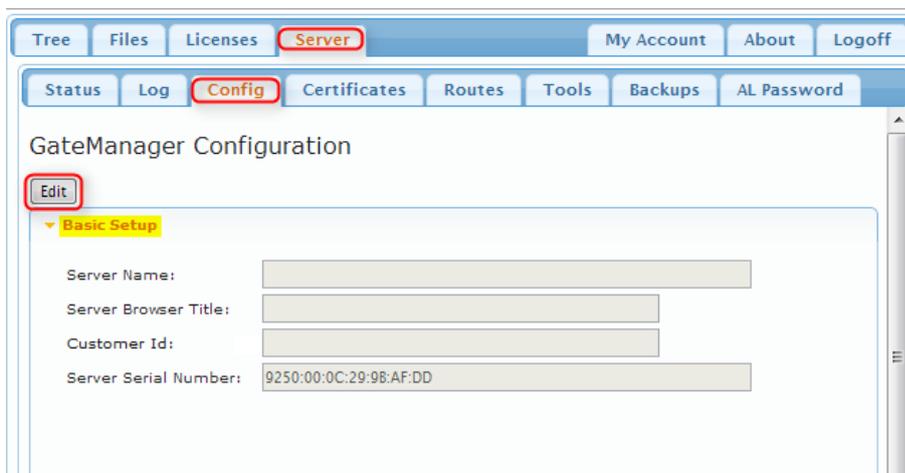
1. Enter a unique name for the server, and the information that should be displayed as browser name when accessing the server using the GateManager Administrator web portal and LinkManager Mobile. Select **Save**.

secomea
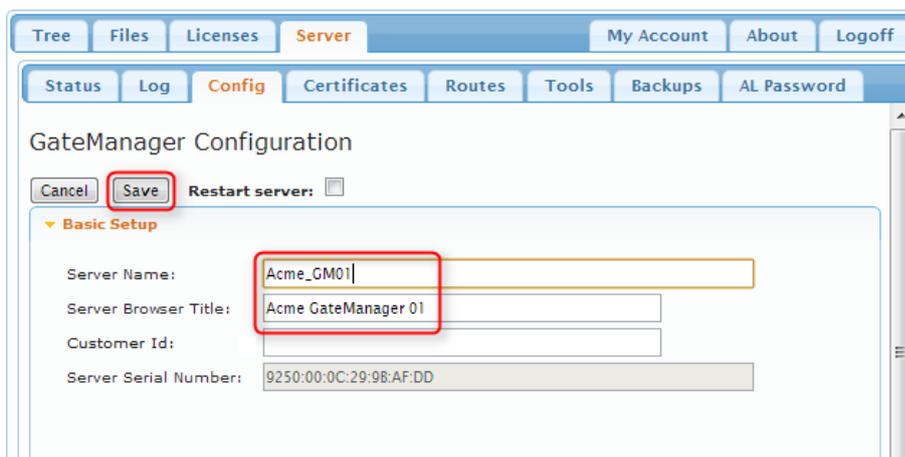
3.2. Enter/verify the Primary DNS server

The GateManager will need access to a DNS server, in order to resolve the external hostname of itself (if used), and for resolving the mail relay server and NTP server.

1. **For model 8250** – DNS and NTP settings are configured as part of the STEP0 guide (settings are entered from the Linux command line).

   For model 9250 - Under **DNS and NTP Settings**, ensure that there is a valid DNS server entered. If the GateManager is receiving its WAN address by DHCP, this setting will be automatically populated with the DNS received from the DHCP server.
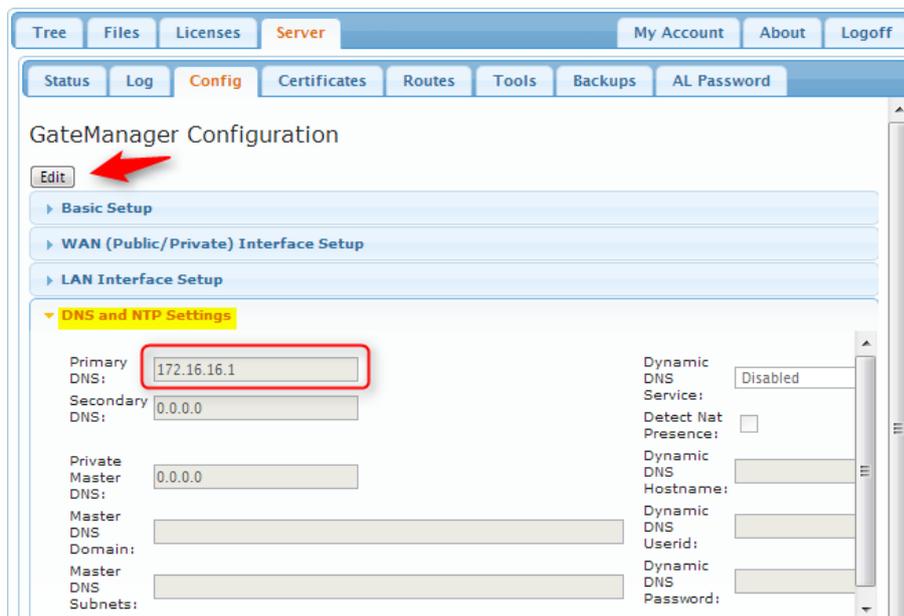
3.3. Enter the Public Hostname

⚠ *Be aware that the Public Hostname is encoded into the activation license (Soft Dongle) and changes to these settings may invalidate the license.*

NOTE if no Public Hostname (FQDN) has been assigned to the server, then you must enter the Public IP address in the External Public Hostname field.

1. Under **WAN/LAN/Primary (Public/Private) Interface Setup** enter the FQDN (Fully Qualified Domain Name) or the Public IP address for this server and press **Save.**

   ⚠ *Do NOT select Restart server yet!*

secomea
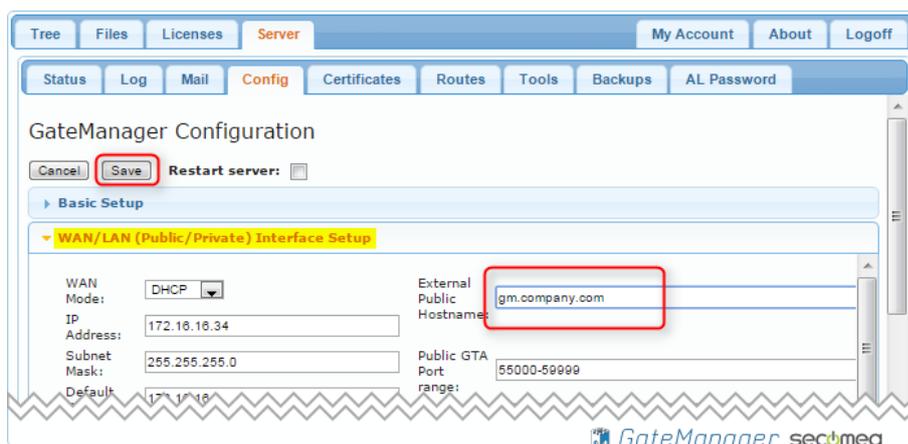
**Note:** The layout and title of this page varies slightly between GateManager models 8250 and 9250.

3.3.1. Possible error messages when saving:

If the system reports Unknown **hostname** it can be related to the fact that no DNS server has been configured, or the DNS server is not working.

In this case, you will have to contact the IT administrator responsible for the GateManager installation and/or see the menu **DNS and NTP Settings** (for GateManager 8250 see the STEP0 guide, as the settings are controlled by the Linux OS).
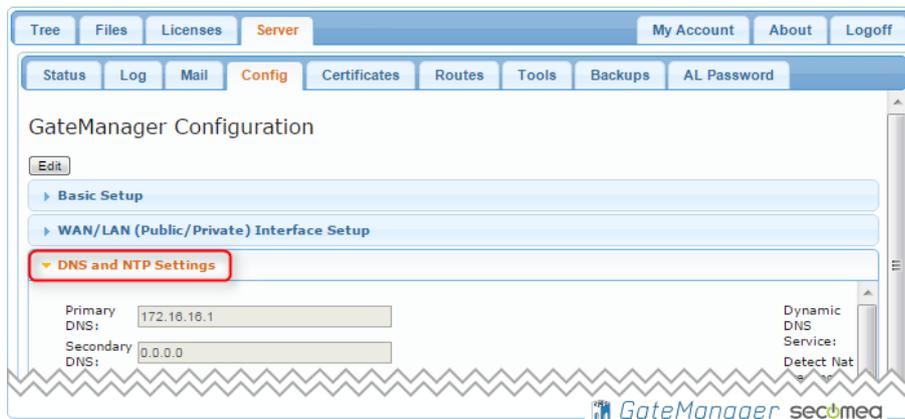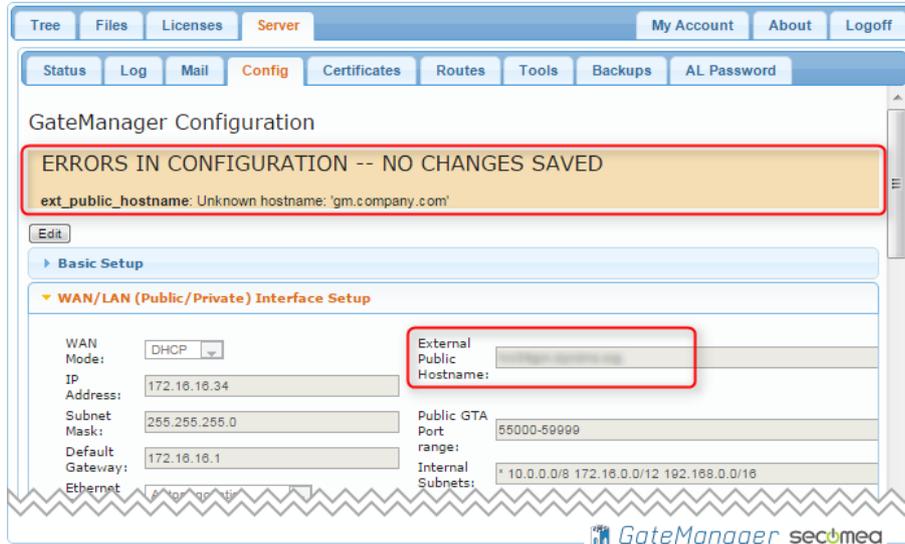
You can use the Tools menu to speed up the troubleshooting process

secomea
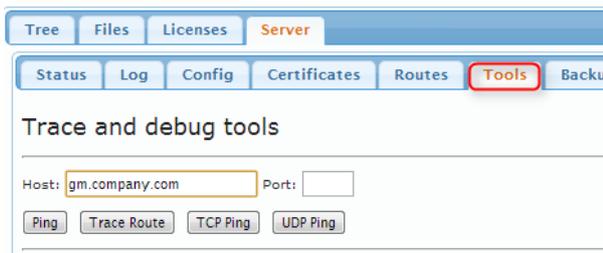
2. When the settings have been configured and saved correctly, select the "Restart now" button.

3. The GateManager server will restart and will become online in less than a minute.
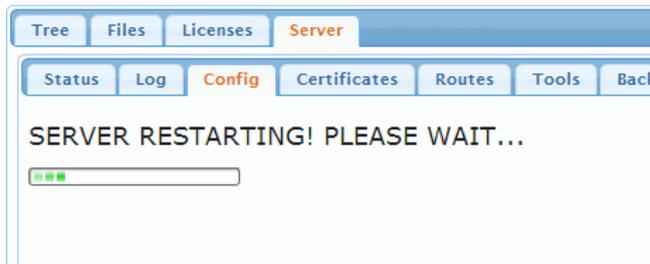
3.4. Configure mail settings

The ability to send email is absolutely essential to the GateManager!

3.4.1. Mail configuration on GateManager 8250

Model 8250 always uses the Linux systems mail client to either send or relay mails. It is not configured in the GateManager menus. Refer to the STEP0 guide for details.

The only, but important, setting to configure in the GateManager menu is the "Default Mail From" address. This consist of three parts that constitute the full sender address format **name <mailbox@domain>** that recipients will see in all mails sent from this GateManager.
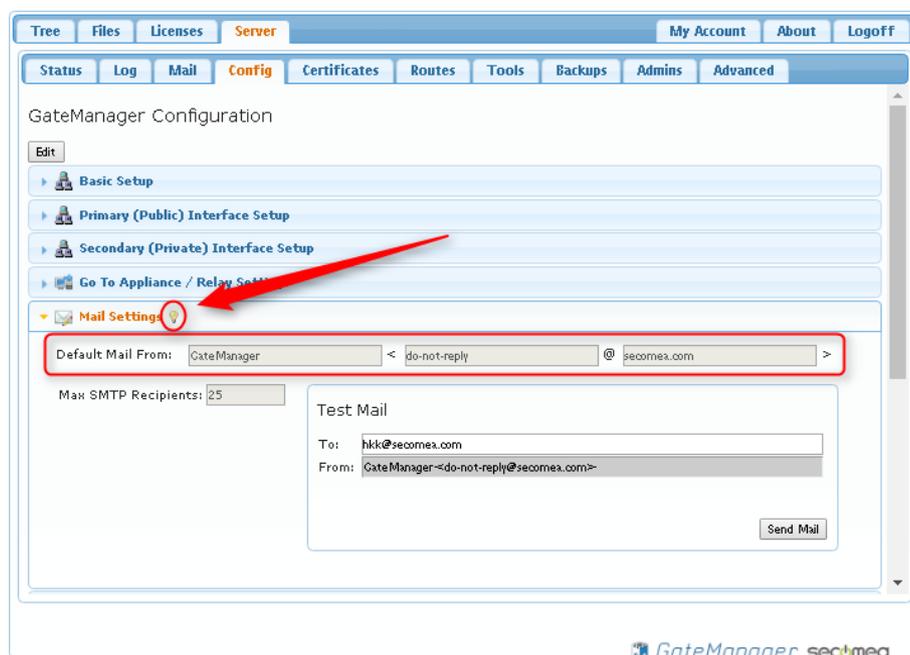
Refer to the light-bulb for further explanation.

3.4.2. Mail configuration on GateManager 9250

The GateManager 9250 has an integrated mail server, but can also be configured to relay mail via an external SMTP server.

In the GateManager configuration click **Edit** and enter the **Mail Settings** section.

Here you should consider as a minimum the "Default Mail From" and the Local SMTP Domain.

Contact your IT administrator or you ISP for necessary information.
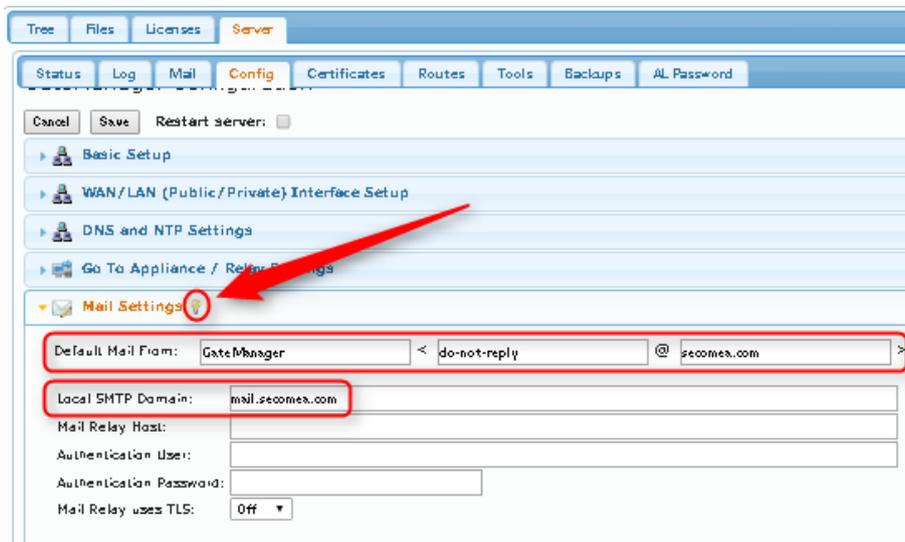
Refer to the light-bulb help for further explanation.

HINT: If you cannot get access to your corporate SMTP server, you can use web mail services such as Gmail or Hotmail/Live-mail as relay. The following example uses Gmail (you will need to have a mail account on the mail server, and the relay port 587 must be open outgoing in the corporate firewall)
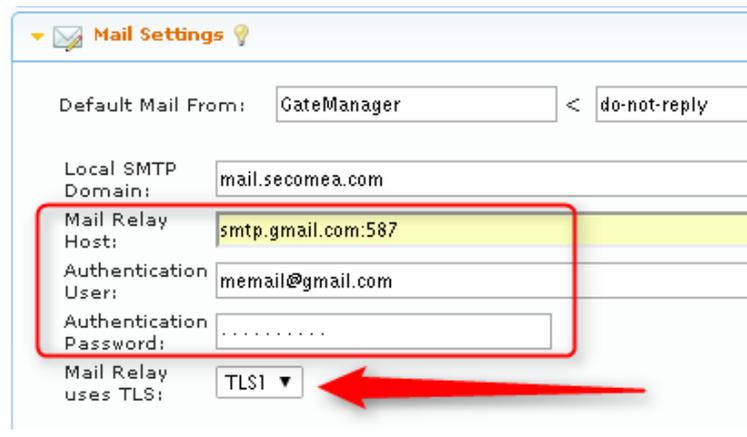

NOTE: It has not been verified if using e.g. Gmail for large volumes of emails would cause problems. So using such public mail services should only be used for demonstration purposes or as an interim solution.

3.5. Check sending of mails

You should check with the Test Mail option that your settings are correct and are accepted by recipient mail servers.

1. Enter the Mail Settings section and type your email and click Send Mail
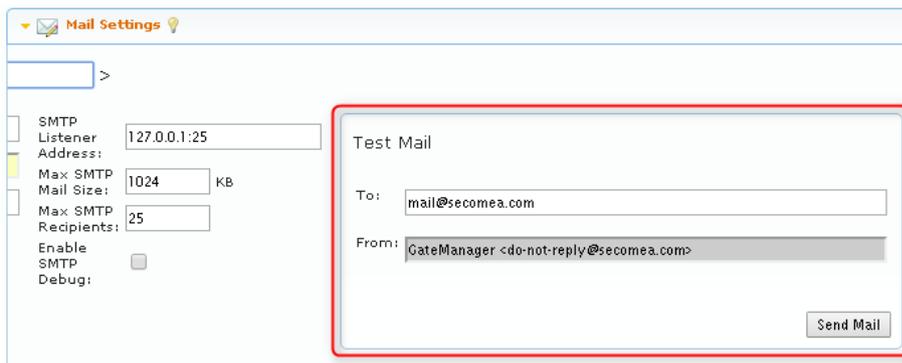
2. The resulting email would look like this:
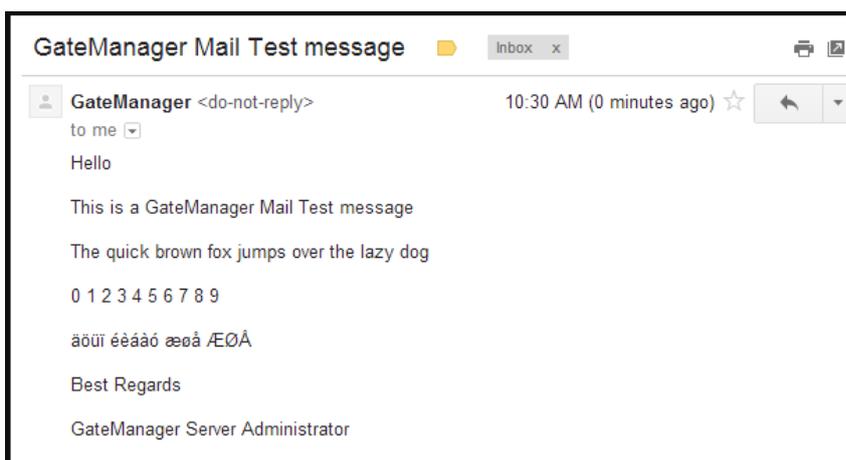
HINT: If you are establishing a dedicated relay server for the GateManager instead of using your existing corporate relay server, your emails could be rejected. Try sending to a Gmail or Hotmail/Live-mail account as described above, and always check your Spam filter.

3.6. Specify the mail sender for Accounts and Alerts

Starting from GateManager Release 7.0 there will no longer be any mail sender options to specify from the Accounts or Alerts Settings. All "Mail From" settings are handled from "Mail Settings".

If you have changed the default setting for "Account Mail From" or Alert "From Address" you will still see the fields being available.

It is recommended that you clear the contents of these fields, which will automatically let the "Mail Settings" take effect for all mail.

If you have a very special need for differentiating on the mails triggered by alerts and account mails, you can leave the fields as is, but you should still very strongly consider deleting the contents of the fields as shown below:

Delete "Account Mail From" if exists:

Delete Alert "From Address" if exists:
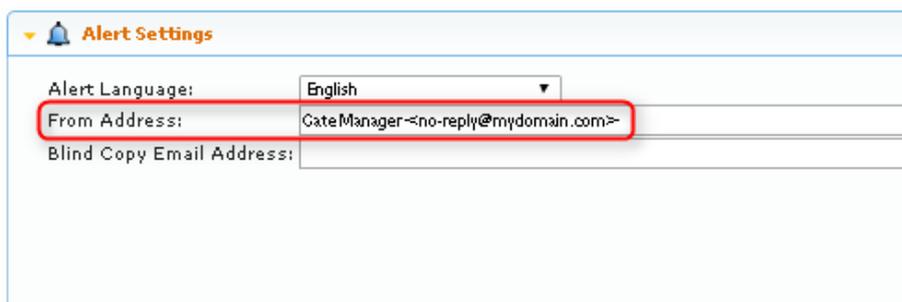
By deleting the contents of these fields you are assured that all "Mail From" settings are handled by the Mail Settings described in the previous section.

.

secωmea

3.7. Setup Server Administrator account(s)

It is highly recommended to change the default Server Administrator account password (gatemanager), to something stronger. It is also advisable to enable two factor login for the account by changing Authentication from "User name and Password" to "X.509 Certificate..".

However, if the account is changed to use X.509 certificate, and the certificate is lost (e.g. it could be discarded by the email server that receives the email with the certificate attachment), you would lock yourself out of the server completely. Therefore, it is highly recommended to create a new Server Administrator account, before changing or disabling the default account.

The following explains the necessary steps:

1. Select the Tree tab, and enable viewing of user accounts, by clicking the account icon so its background turns light blue. You will now see the account that you are currently logged in with displayed with a green background.
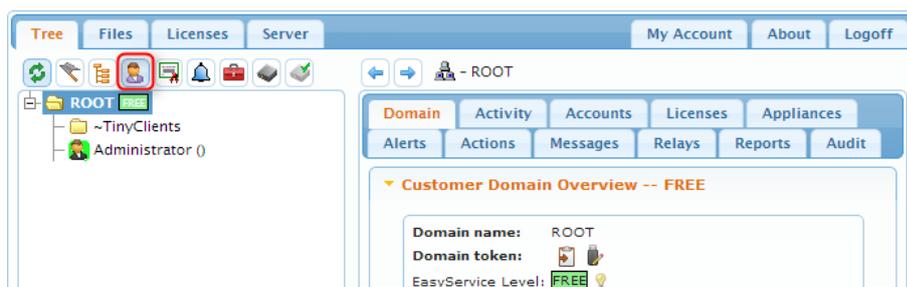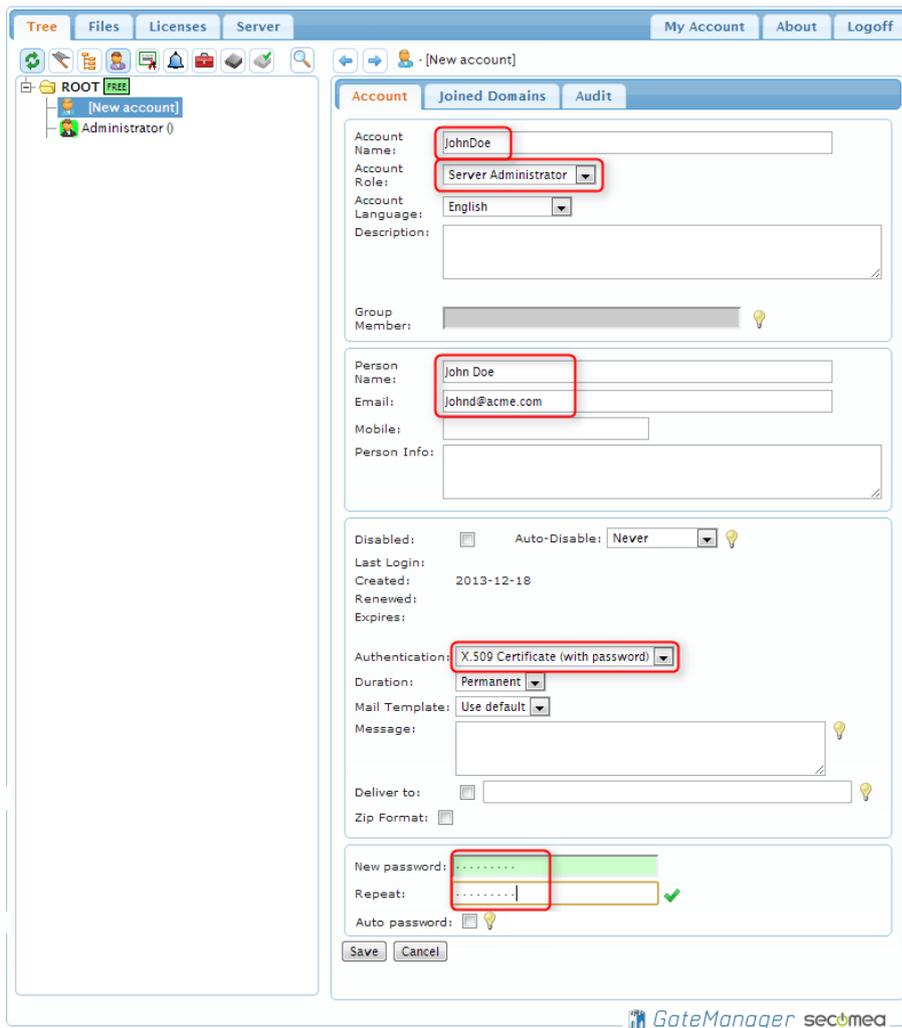

2. Click on the Administrator account, and insert your own name and email for the account. Select **Save.**
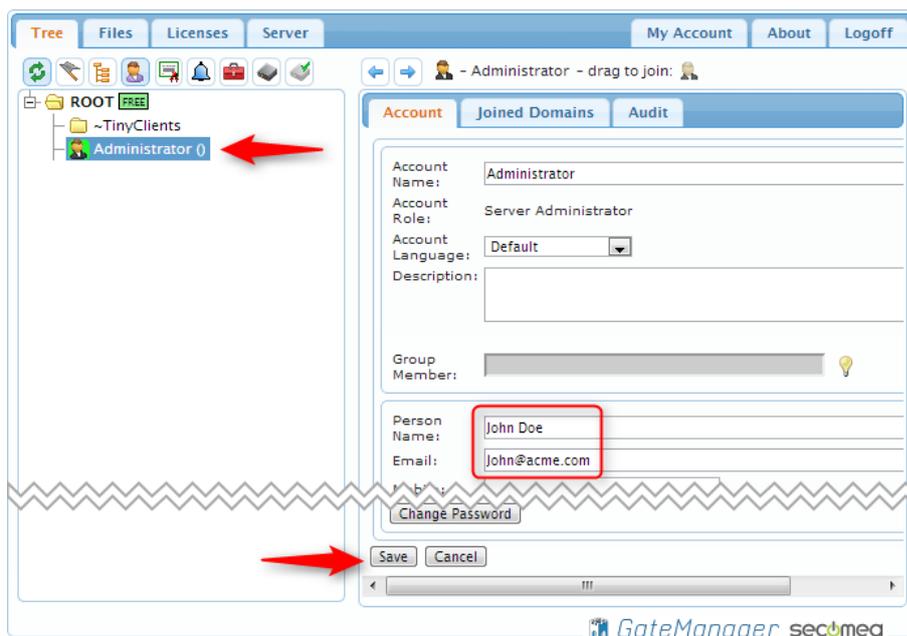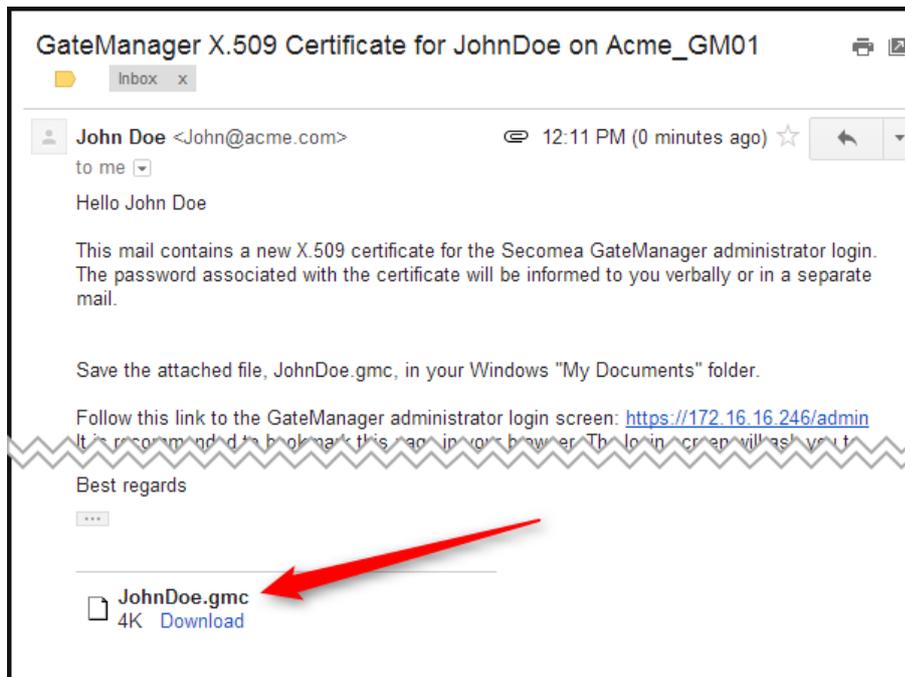
3. Standing in the Root domain, select **Accounts** and click the plus sign to create a new account:
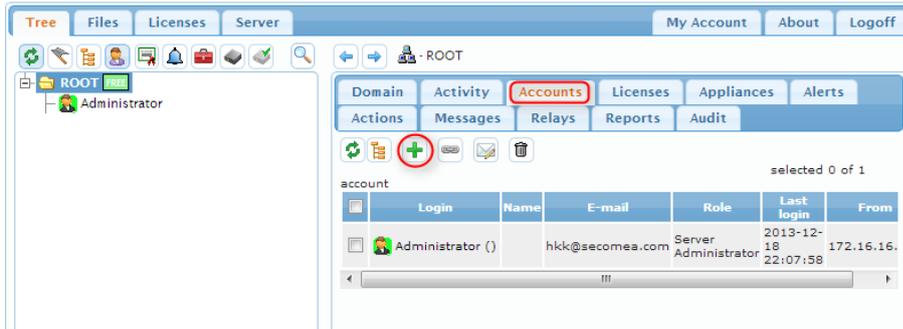
4. Fill in the following minimum settings:

secomea

5. In the mailbox of the email you entered, you should now receive an email with the certificate attached

6. You now have a backup Server Administrator account, and you can safely change the password of the default Server Administrator account, and also enable X.509 authentication for it, or you could even disable it.

⚠ *DO NOT LEAVE THE DEFAULT ADMINISTRATOR ACCOUNT WITH THE DEFAULT PASSWORD, AS THE ACCOUNT IS EXPOSED ON THE INTERNET.*

Also consider creating a new Server Administrator for your GateManager Service Provider, in case you want remote support for additional set-up of the server.

3.8. Change password for Appliance Launcher (AL) access (Model 9250 only)

Note: *Model 8250 cannot be configured using the Appliance Launcher. Low level network settings are configured directly in the Linux OS. See the STEP0 guide for details.*

Select **Server > AL Password**, and define a new password.
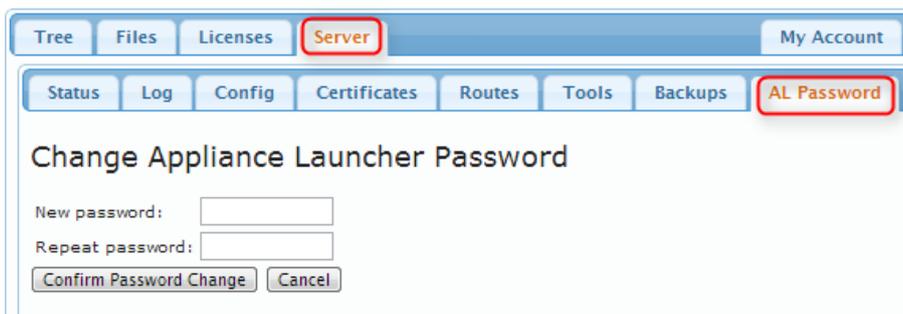
Note that this is only for preventing unauthorized access to the GateManager network settings from the local network of the GateManager.

The password is not used for accessing the GateManager Administrator web portal, but used only for accessing a limited web GUI for the embedded OS

secⓘmea

on which the GateManager runs. All settings configurable by the Appliance Launcher can also be configured from within the GateManager Administrator web portal.

> *CONGRATULATIONS*
>
> *If you have setup the GateManager according to the previous sections, the GateManager will be fully operational - but for demo or trial purposes only.*
>
> *For operating the GateManager in production mode, you should install license certificates as explained in the following section.*
>
> *For an introduction to the basic operation of the GateManager Administrator interface, refer to this guide:*
>
> ***http://info.secomea.com/premium***

4. Ordering licenses and setup order information

By default, the GateManager is running in Trial mode, which means it supports only one LinkManager, one LinkManager Mobile and two connected Appliances (Appliances being SiteManagers and/or TrustGates).

You will need to install an activation license (aka Soft Dongle) to unlock the LinkManager and Appliance limits, and allow the GateManager to be used for production purposes; you will also need a TLS certificate to prevent potential man-in-the-middle attacks.

If you are ordering for a GateManager model 8250 skip to **step 3**. *For a model 9250, proceed with the following steps to set Customer ID.*

1. Enter the **Licenses** menu

2. The First time you enter the menu you will be prompted to enter a Customer ID that will give your GateManager a unique identification

   Press **Save** and the GateManager will automatically reboot.

3. Enter the menu **Licenses → Order.** You now have two options:
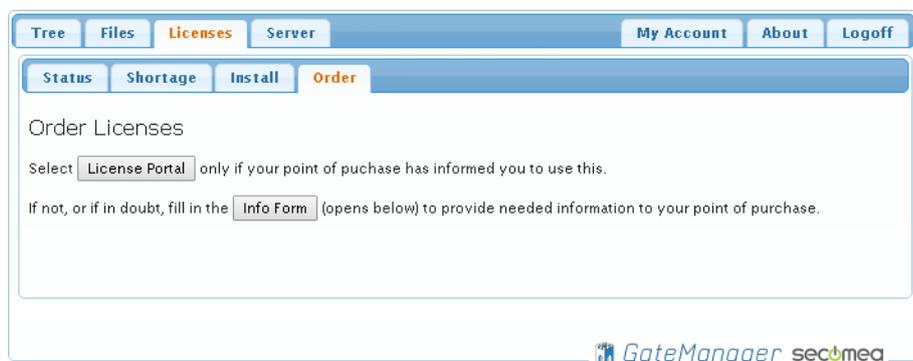
You will be using the License Portal if you have been provided with a login for the portal.

Otherwise press the [Info Form] button and fill in the form. The form will be mailed to your point of purchase including the necessary information about you GateManager, in order to create your license keys.

secômea

4.1. Example of an Info Form:

5. Installing licenses

5.1. Activation License(s)

If the GateManager is online (connected to the Internet), Activation Licenses will automatically be installed on the GateManager by the License Portal (The order in the License Portal may have been entered by you or your point of purchase)

5.1.1. Verifying if GateManager is Online

If Online the GateManager is capable of being automatically activated and/or having additional licenses automatically installed by the License Portal.

Check if the GateManager is Online Under Server → Status:

If your GateManager is not online, the email from the License Portal confirming the order will have the licenses attached for manual installation.

The same email will contain instructions for installations. If in doubt, refer to **APPENDIX E. Manual installation of licenses**

secomea

5.1.2. Verifying that activation was successful

Before Activation the "Max. Appliances license" in the tree view will be red and show "0".
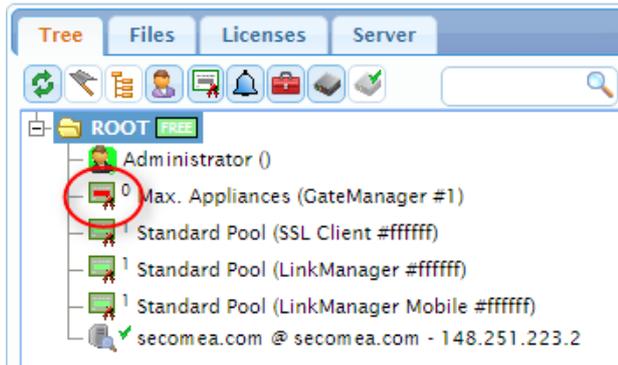

After activation this value will be 25-5000 according to the ordered GateManager license agreement.

In ordering the GateManager with **EasyService** the value will show 5000. If you have ordered **Limited Service** agreement, you would have started out with an Appliance license of 25 and the screen will show:
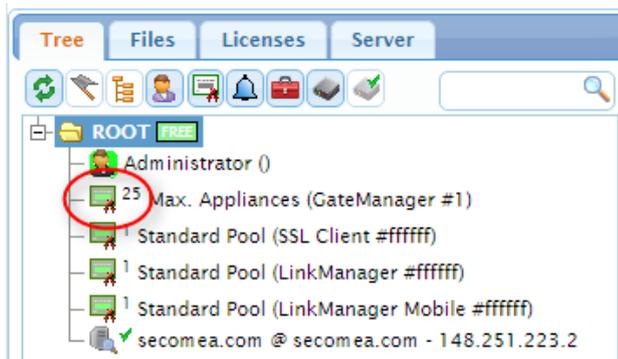
Max Appliance Upgrades under the Limited Service agreement can be purchased separately, and are installed the same way.
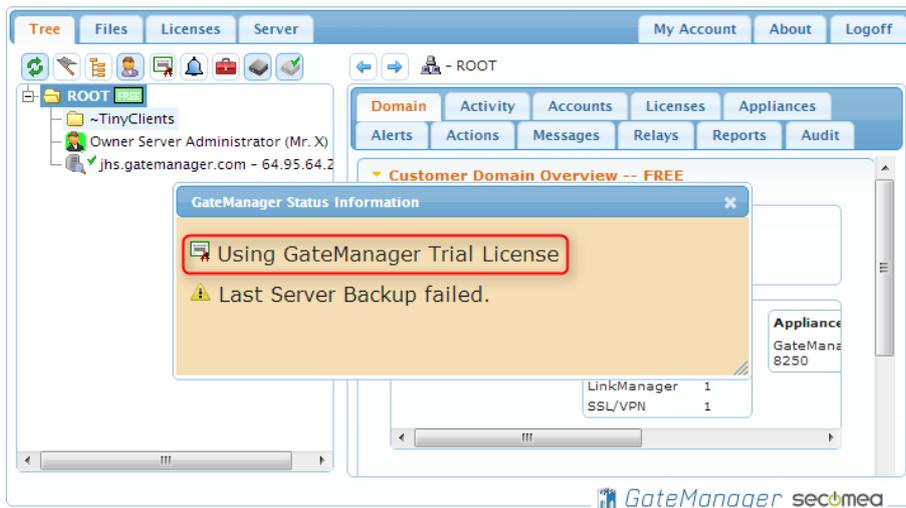
If additional licenses were ordered, they will be show with the order number as description:
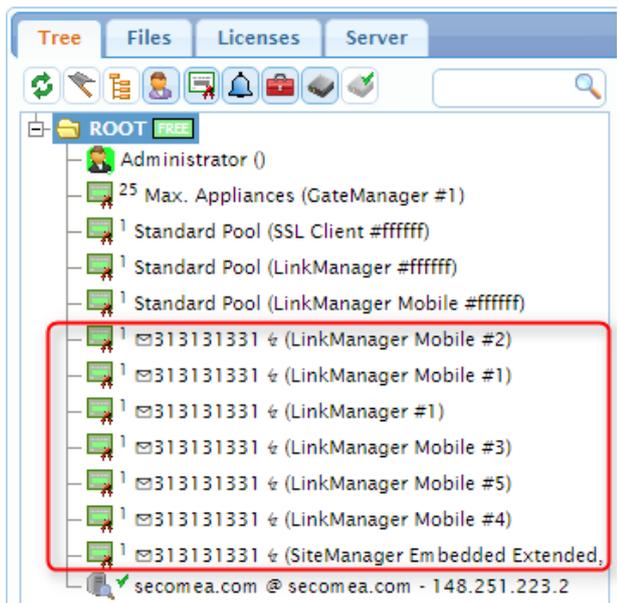
5.2. TLS certificate.

Even if your GateManager is online and the activation license(s) were installed correctly, you will have to install the TLS certificate manually.

When logging into the GateManager, you will see the following information:

The GateManager is fully functional, but "Trial License" indicates that it is not advised to run the GateManager in production mode, as it may be prone to man-in-the-middle attacks.
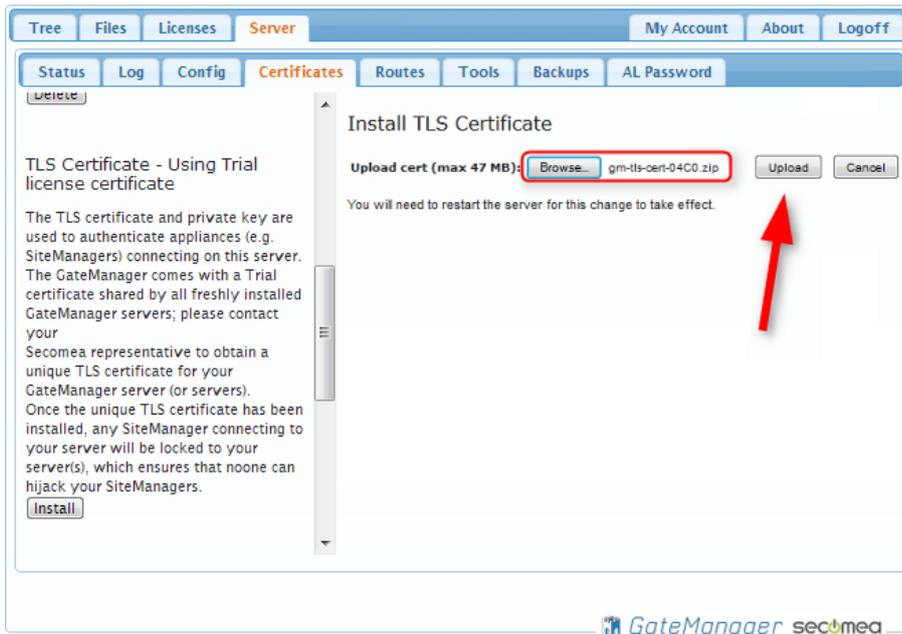
You will receive the TLS certificate file as attachment to an email from the License Portal. The same email will include the following instructions.

1. Save the ZIP file attachment from the email to your computer

   (If you cannot locate the email, and you have an account on the License Portal, you can login and download the file from the Order History)
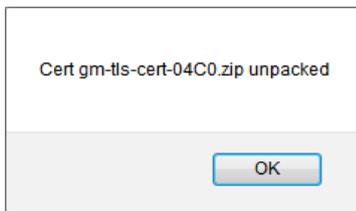
2. In the GateManager Portal enter the menu Server --> Certificates and scroll to section **TLS Certificate**.
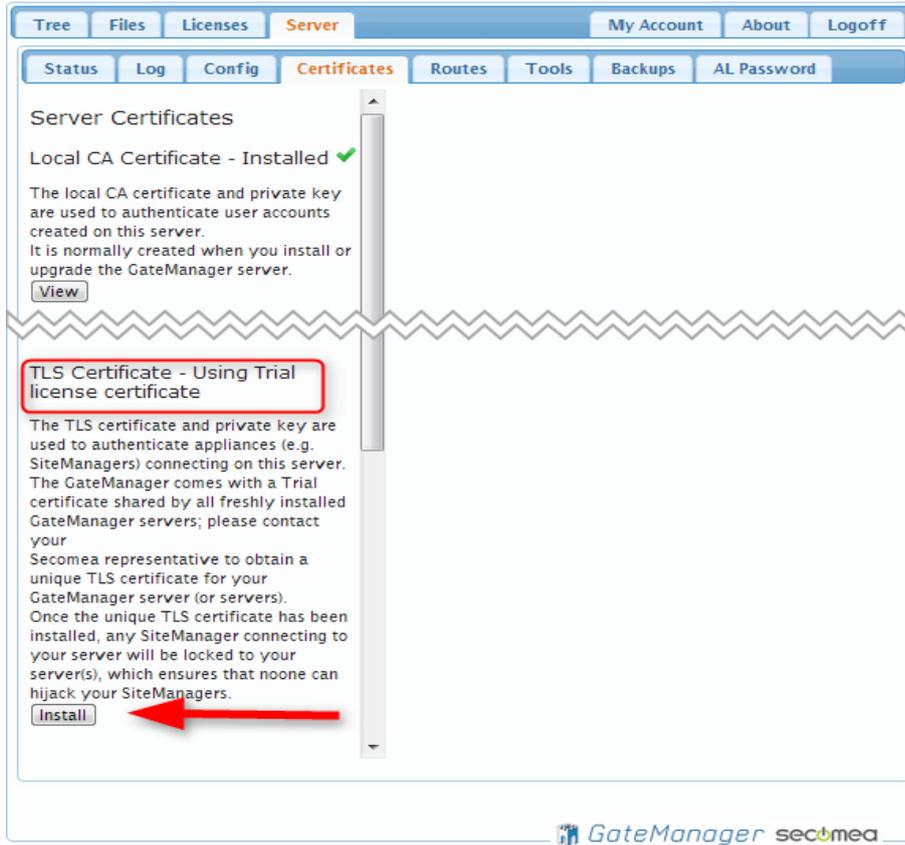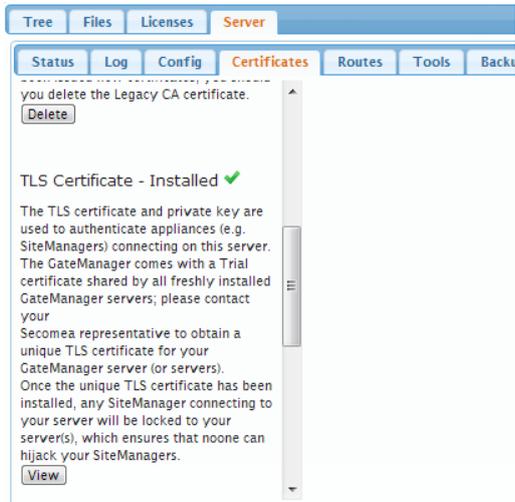

3. Select Install and upload the zip file (you should NOT unzip the file prior to the upload).

secomea

If successful, you will receive this message:

Cert gm-tls-cert-04C0.zip unpacked

OK

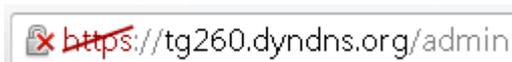The TLS certificate is now installed:

secomea

6. Web Server Certificate (Optional)

The GateManager is now fully functional, but you will notice a https security warning in your browser address bar when logging in (✗ https://). This is because the local CA certificate that is auto-generated for this GateManager installation is used as Web server certificate, and is not signed by a publicly recognized certificate authority.

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 do not 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 identity of your GateManager server cannot be validated. You can use the "Make CSR" button below to create a "Certificate Signing Request" file suitable for ordering a properly signed certificate.
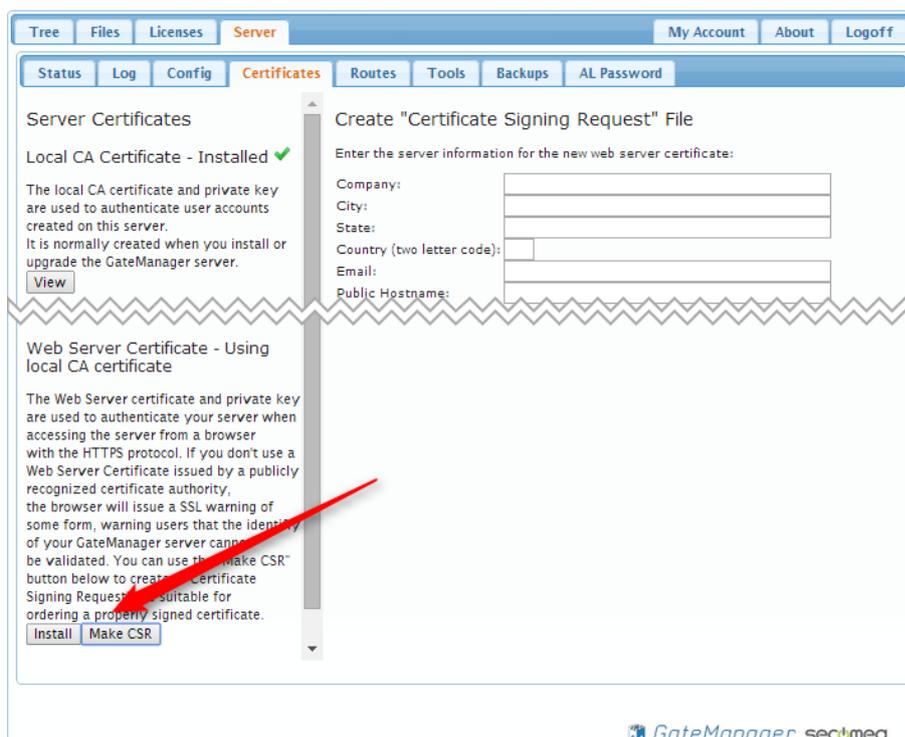
- No WEB Server Certificate:

    ✗ https://tg260.dyndns.org/admin

- Using standard SSL Certificate:

    🔒 https://gm21.secomea.com/admin
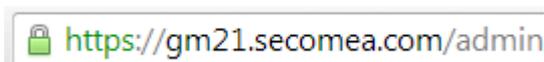
- Using SSL Certificate with EV (Extended Validation)

    🔒 Secomea A/S [DK] https://gm07.secomea.com/admin

6.1. How to create and install a WEB Certificate (SSL Certificate):

1. Make a CSR file on your GateManager (requires GateManager v.5.4 or later) – The CSR file is a 2048 bit format.

secomea

2. Find a certificate provider of your choice such as GeoTrust, GlobalSign, Thawte, AlphaSSL etc. You will use the CSR file just generated in this process. Look for SSL Certificate or a WEB Server Certificate. If a Server platform is needed in the selection process you can specify e.g. Apache.

Note: When you apply for a certificate by the authorization service, the FQDN you provide as the GateManager's FQDN must match exactly the entire FQDN configured in the GateManager. Also the format of the certificate must be SHA-1 or SHA-2, and it should be a .PEM format (or alternatively PKCS #8).

This is an example of requesting the certificate:
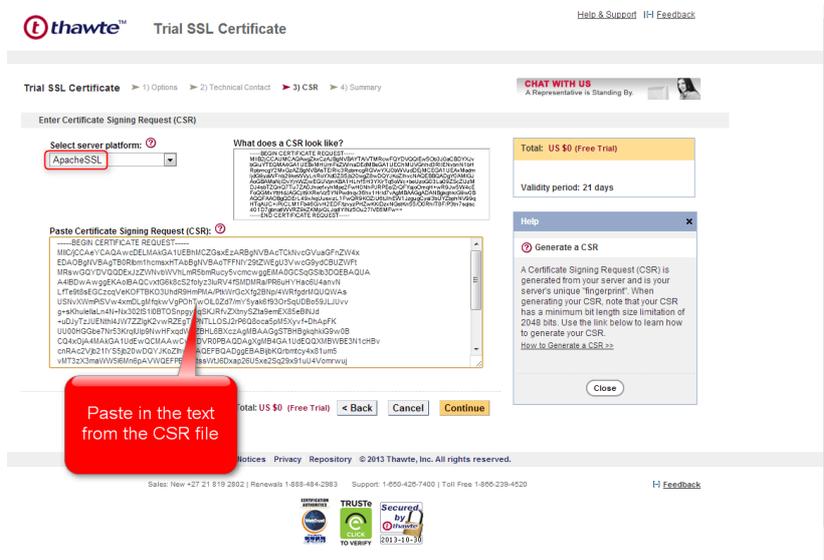
3. You will most likely receive emails with instructions on how to proceed. Important is that you receive an SSL certificate that you can install as follows:
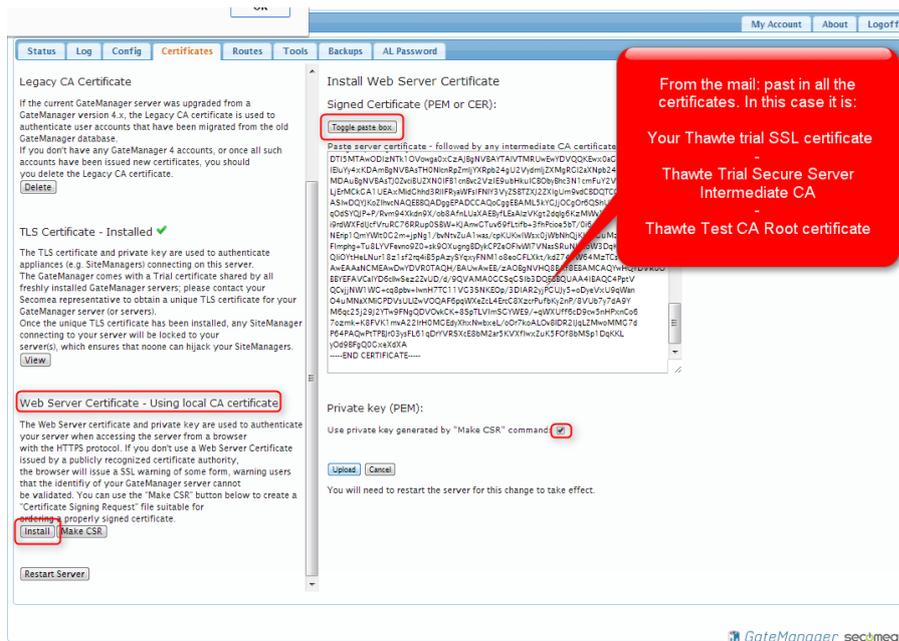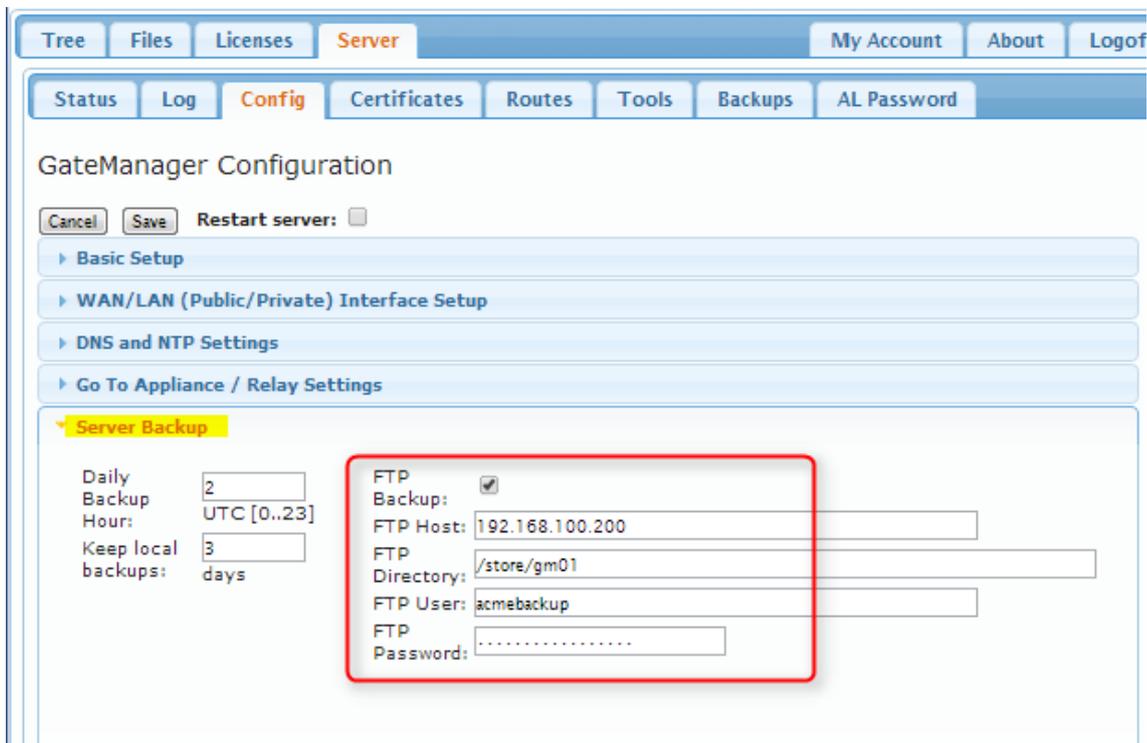
APPENDIX A, Setting up Backup

Backup will ensure that you can recover GateManager data including the database and the GateManager settings/licenses. This does not include a backup of the appliance firmware in the Files section.

Note: If running GateManager virtualized it is advised to take a backup of the server host once and for all. Stop the GateManager virtual machine and take a copy of the images (a so called "year-0" copy). In case the entire GateManager server need to be restored you just have to restore the "Year-0" copy and restore the data-backup (More details on restoring a "year-0" backup can be found in the STEP 1 guide).

FTP Backup

A clear advantage of FTP backup is that the FTP server does not have to be in the same location as the GateManager server and thus subsequently represents an additional security measure in the event the server physically disappears.

Select **Server → Config** and expand the **Server Backup** section. Fill in the FTP settings according to the information. Press the **[Save]** button. It is not necessary to restart the server.
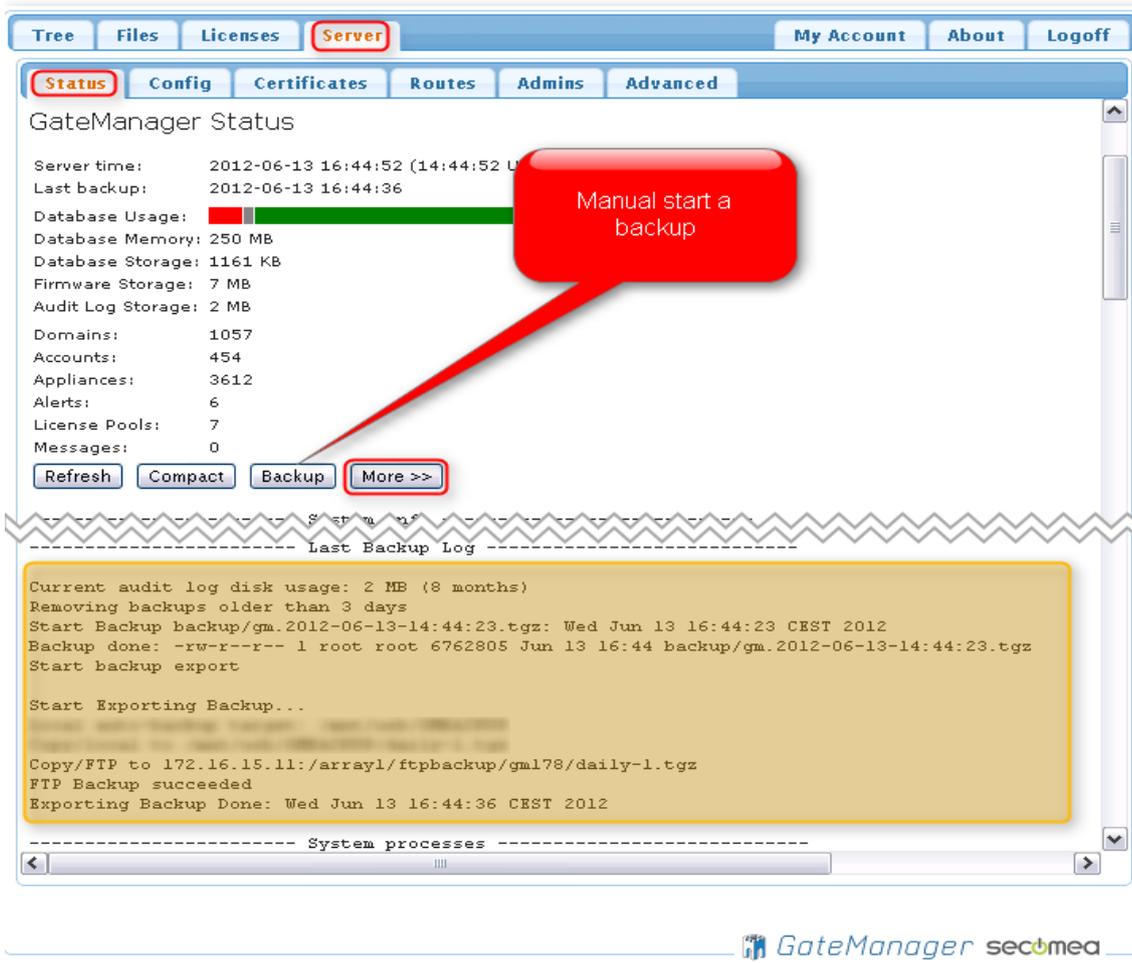

Troubleshooting FTP backup

When an FTP backup is configured, a backup to the FTP server will be scheduled to run at 04:00 every night. For testing you can perform a manual backup as shown below.

Select **Server → Status** and press the **[More]** button to see the latest backup log. Press the **[Backup]** button to manually start a backup process.

The **Last Backup Log** will potentially show an error, originating from before the FTP backup was configured.

When the backup has finished it must show "FTP Backup succeeded" followed by "Exported Backup Done".

SMB Backup (Model 8250 only)

Note: Support for SMB backup is possible, but generally not recommended. Use FTP if possible.

Since the SMB backup feature is not fully supported, it is recommended that the share is made to match the settings of the share shown in example below.

Select **Server → Config** and expand the **Server Backup** section. Fill in the SMB settings according to the information in the table from the Introduction section.

secomea
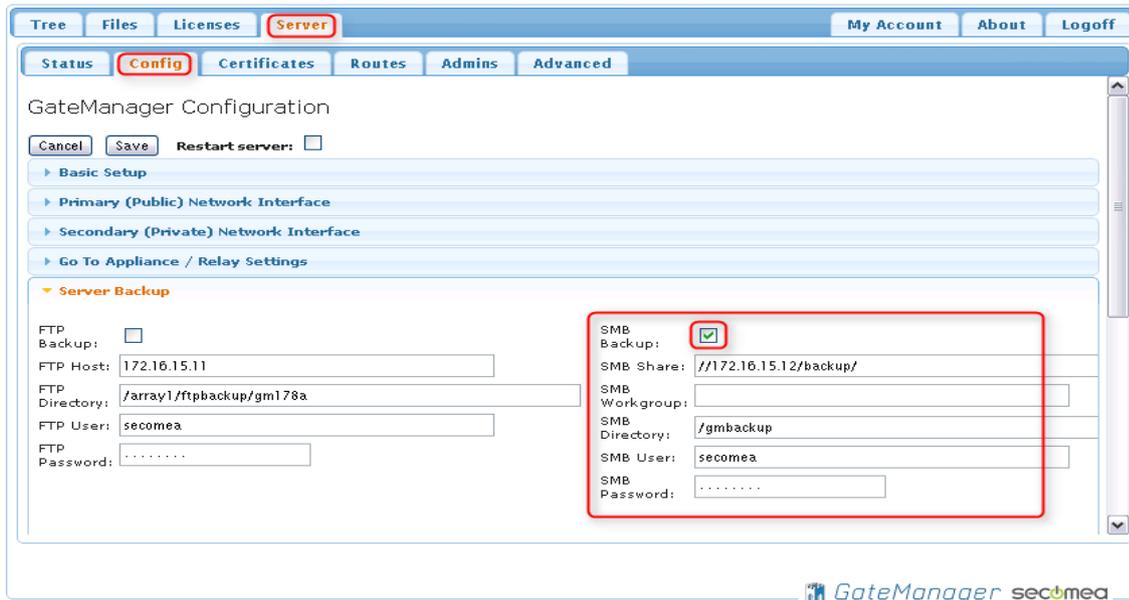
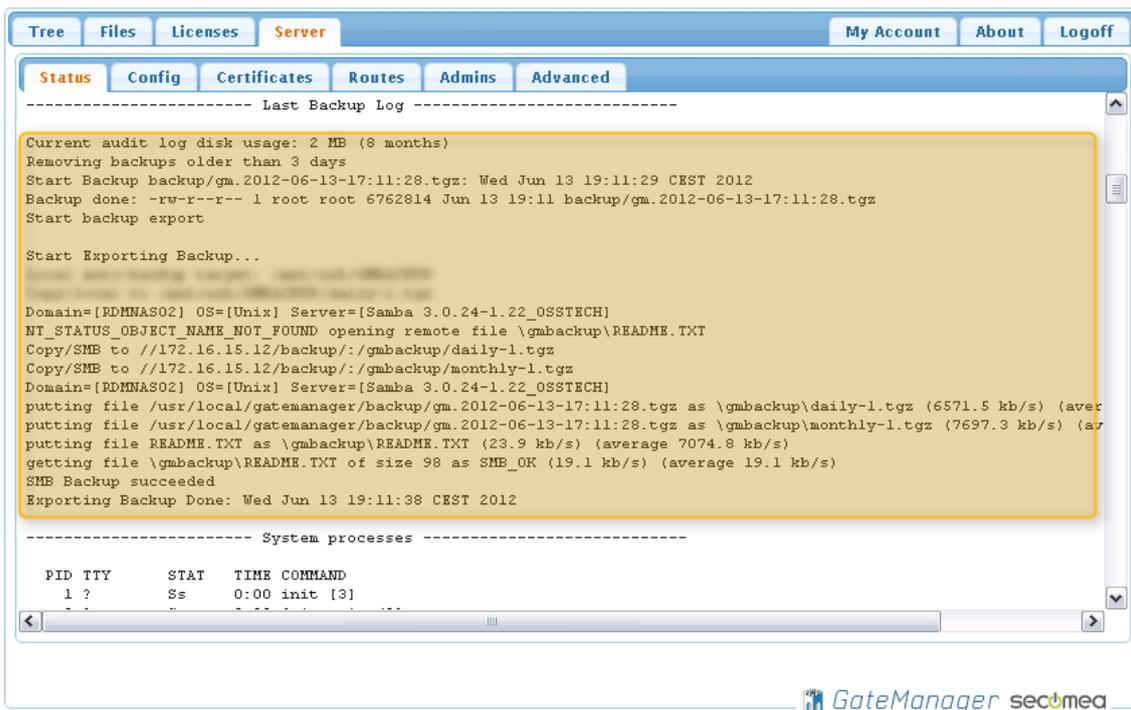## Trouble shooting SMB backup (Model 8250 only)

When an SMB backup is configured a backup will be scheduled to run at 04:00 every night. For testing you can perform a manual backup as shown below.

Select Server → **Status** and press the **[More]** button to see the latest back-up log. Press the **[Backup]** button to manually start a backup process.

secomea
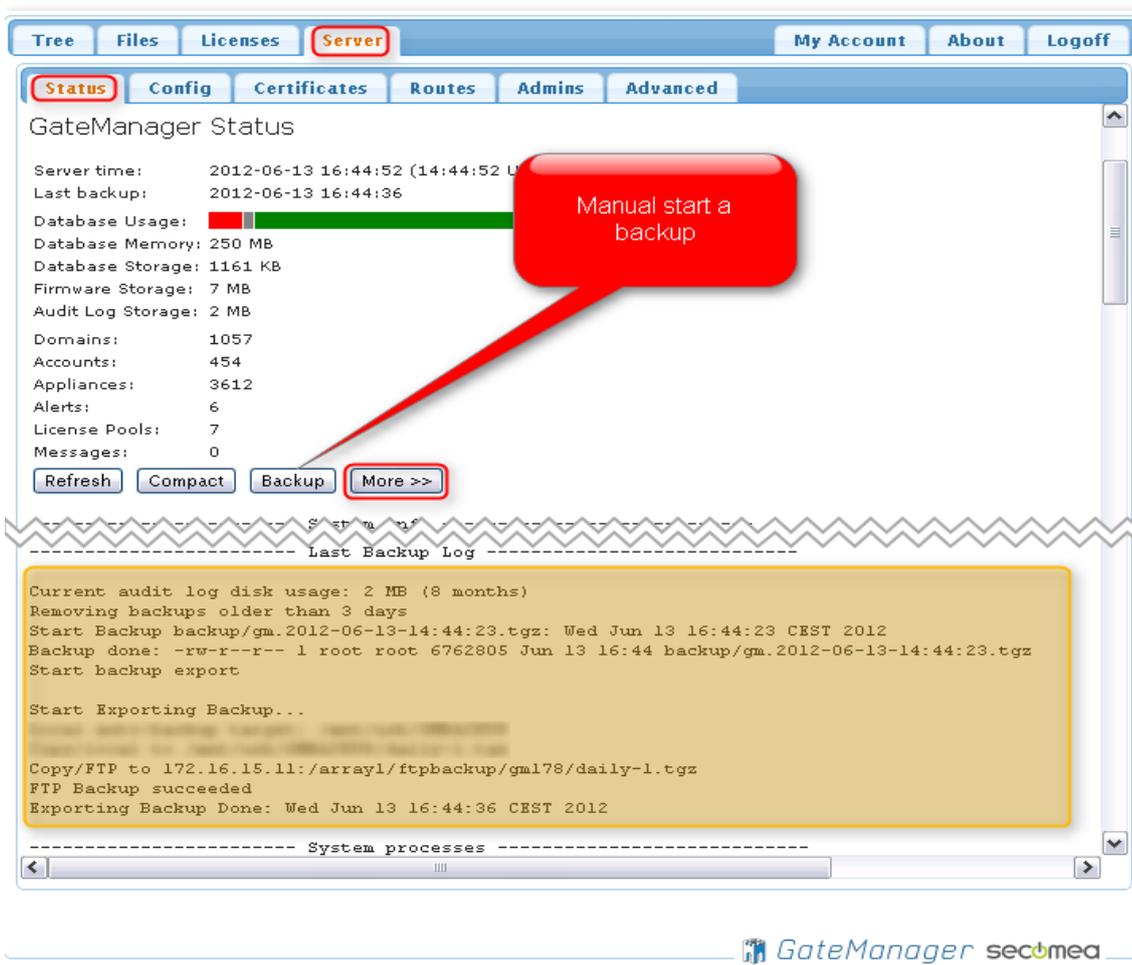
When the backup has finished it must show "SMB Backup succeeded" followed by "Exported Backup Done".

- Example of a successful SMB backup:

- Example of a failed SMB backup:

  The SMB Backup failed with the text *smbclient: command not found* – this indicates that the Samba Client required for this task is not installed on the GateManager server.

Solution: To solve this problem you will have to contact your IT Administrator who installed the GateManager. The solution is to install the smb-client using the following command on the Linux command line:

```
# yum install samba-client
```

Follow the instructions on the command line. This process requires that the GateManager Server has access to the internet (TCP:80).

---

secomea

APPENDIX B, Upgrading GateManager firmware

Check the "About" tab in the GateManager Portal for the currently running version. If a newer version exists on the Secomea web site, you may want to continue with the following

- Firmware for GateManager model 9250 is in the format:

  V9250_xxxxx.ffs

- Firmware for GateManager model 8250 is in the format:

  Secomea_GateManager_Installer_x.x.xxxxx.tgz

(**xxxxx** denotes the firmware/build version)

1. Select **Files → Firmware** and press the plus Icon
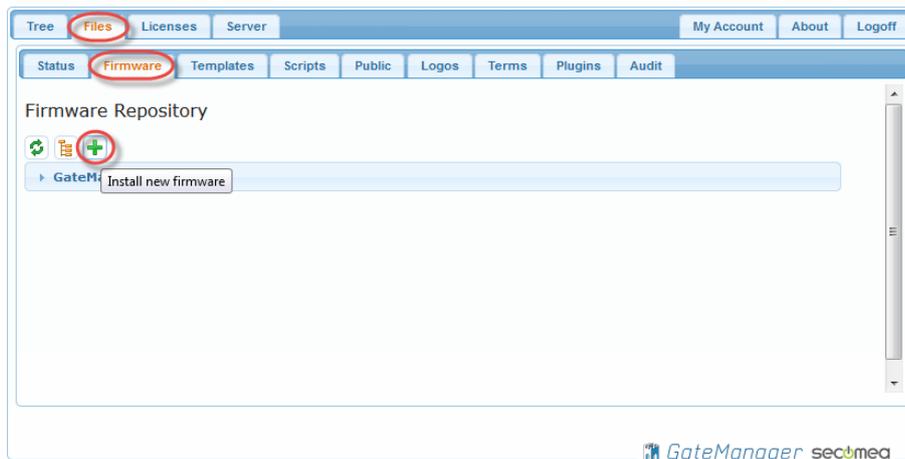
2. Press **Choose File** and browse for the file (.ffs file or .tgz file depending on GateManager model) and press **Upload:**
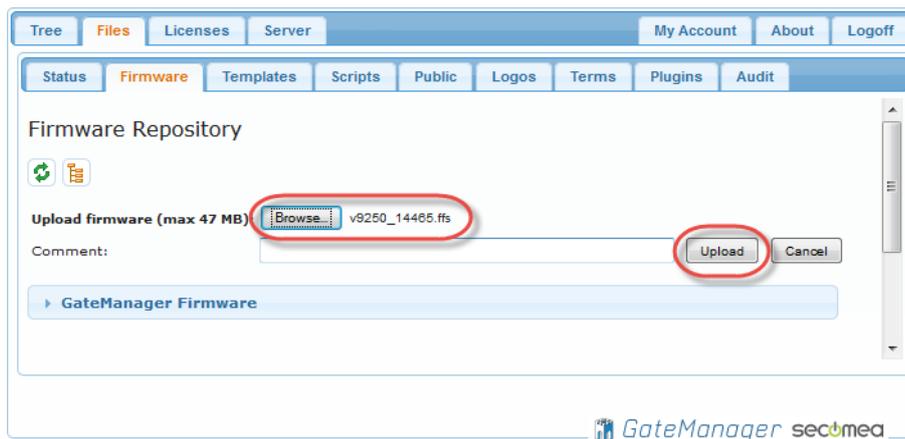
Wait for the firmware to be uploaded.

3. Select the **Tree** menu and click on the **"Show Appliances"** Icon in the top Icon-list, and the GateManager server should be listed. In this example it is called "gm.acme.com - …."

secomea

4. Press the **[Upgrade]** button
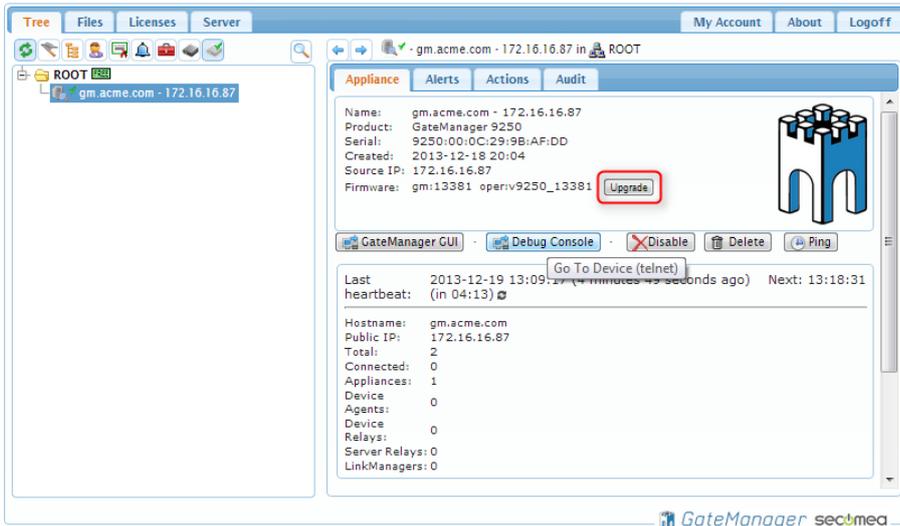
5. Press the **[Upgrade]** button next to the relevant firmware
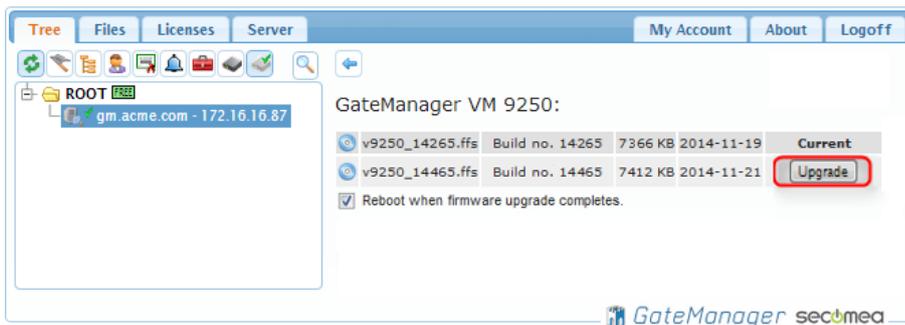
6. Upgrading the server will only take a few seconds and *Upgrade in progress* is shown on the screen.
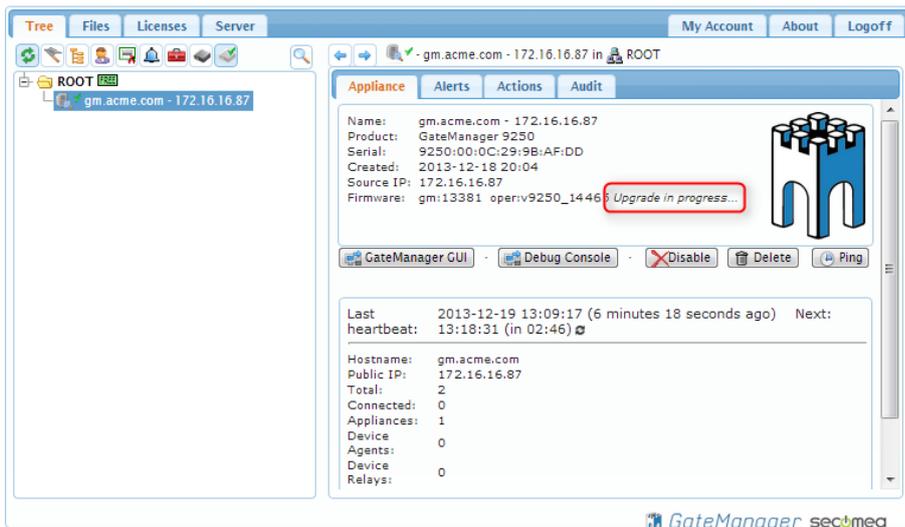
7. After that the server is upgraded, it is advisable to logoff and login again, and also click to refresh [F5] your browser cache.

secomea

APPENDIX C. GateManager Hosting License

About the Hosting license

The Hosting license is only used for a GateManager server of an appointed Secomea distributor, and where the GateManager is used as hosting server for customers of the distributor.

The Hosting license allows the distributor to define domains as **Customer Domains**. Subsequently the customer will be able to see the EasyService maintenance level on his domain (EasyService level is typically calculated based on the number of SiteManagers, LinkManagers and Domain Administrators in the customer domain)

On a monthly basis the administrator accounts in the customer domain, will receive an audit report of contents of the domain. Concurrently the upper level Distributor and Server administrators will receive a summary report of all customer domains.

This report is used to calculate the customer's EasyService level according to the Secomea price lists.

You can order a Hosting license for an already installed GateManager server in the License Portal. There is no specific order form for the Hosting license.

Installing the Hosting license

The license would typically have been automatically installed by the License Portal. If the GateManager was not connected to the Internet when ordering, you can follow the steps in **APPENDIX E. Manual installation of licenses**

Note that when in production the Hosting GateManager must be allowed to remain connected to the Secomea Audit GateManager.

Using the distributor license features.

You should always use the License Portal to order Starter Packages for your customers. This will automatically create domains and accounts

If you have reasons to add a customer manually without setting up a Starter Package, you can create the customer domain and check the Customer Domain box under Domain Configuration.

secomea
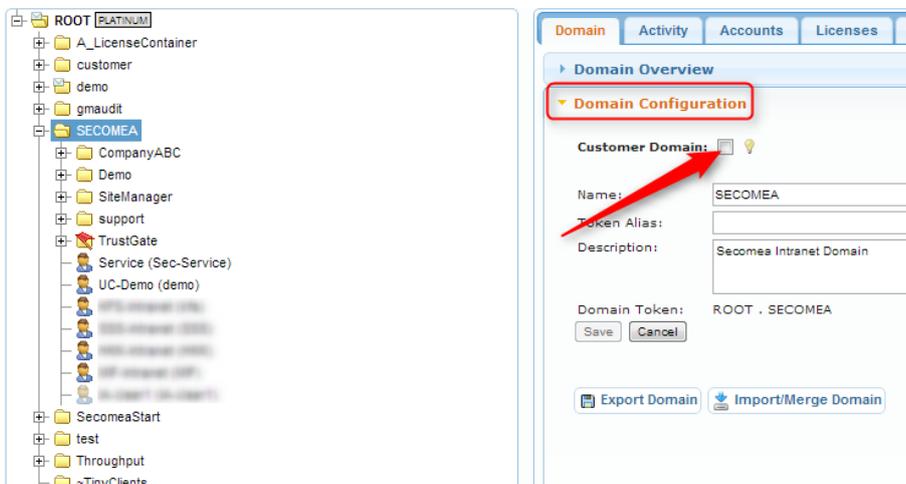
NOTE: This checkbox is only accessible for GateManager Administrator accounts created with the roles **Server Administrator** or **Distributor Administrator**.

Ordering Demo Licenses

You can, as Distributor, order Demo licenses via the License Portal. These licenses must NOT be used for production purposes, but are solely for demo, test and support purposes.

Demo licenses are automatically installed on your GateManager in a domain called **#License Container**. (If the domain does not exist, the License Portal will create the domain)
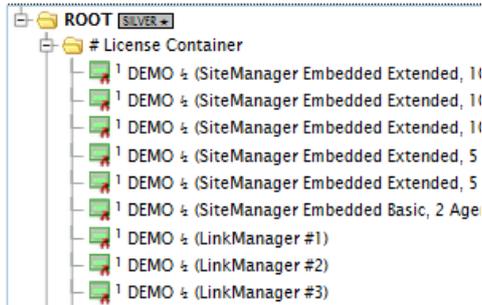
APPENDIX D. Recover lost Server Administrator password

If you have lost your root administrator account information, you can reactivate the default GateManager Server Administrator account via the GateManager line based console.

Recovery on GateManager model 9250

1. Access the Virtual host using the VMware player, vSphere client or if using HyperV then the HyperV Manager and connect to the console.

2. Initiate the recovery procedure by typing

    `recover`

3. The server has now created a recovery login. The account credentials are:
    Username: RecoveryAdmin **Password:** gatemanager

4. Login to the GateManager Web based GUI for changing account passwords, and resend certificates.

5. Once completed, delete the RecoveryAdmin from the Server > Status menu:
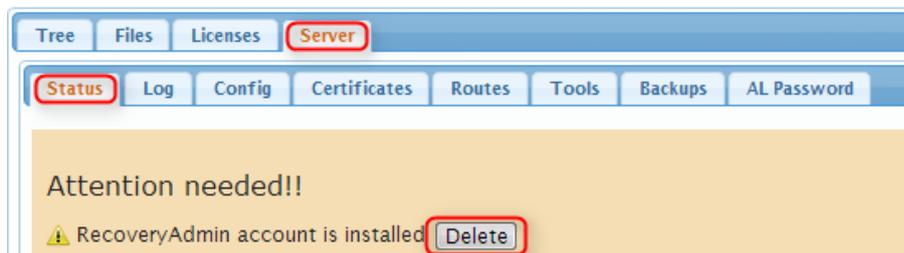
Recovery on GateManager model 8250

1. Connect to the GateManager SSH shell, and login with your Linux root account (See STEP 0 guide).

2. Initiate the recovery procedure by typing

    `# gm recover_admin`

secomea

```
[root@gm5ESXi ~]# gm recover_admin
Created RecoveryAdmin server account with well-known password.
Please change the password on Server > Admins page.
Use 'gm recover_admin remove' when done.
[root@gm5ESXi ~]#
```

3. The server has now created a recovery login. The account credentials are:
    Username: RecoveryAdmin **Password:** gatemanager

4. Login to the GateManager Web based GUI for changing account passwords, and resend certificates.

5. Once completed, remove the recovery user again, in the SSH shell by typing:

    # gm recover_admin remove

secomea

APPENDIX E. Manual installation of licenses

If the GateManager is located in a closed network, or was online when activation licenses were ordered, you may have to install the licenses manually.

Server Activation License (Soft Dongle)

Before a server activation license (Soft Dongle) has been installed, your License status will be as follows:
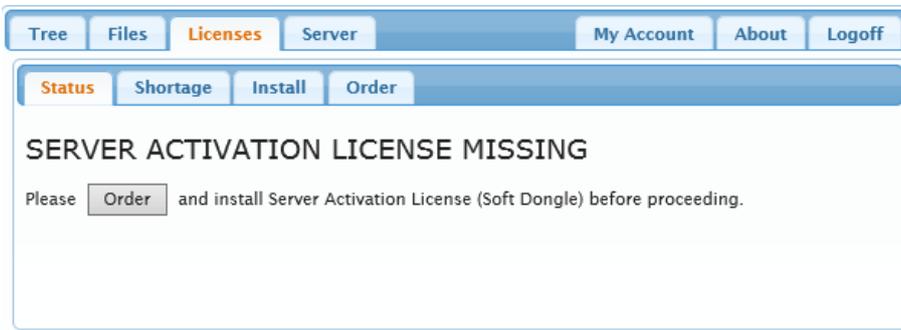

You will have received the ordered licenses as attachments to an email from the License Portal.

The license files may be zipped, so you will need to unzip them first. The unzipped text file(s) contains the license(s). Open the text file(s) with e.g. Notepad.

A license will look like this:

```
===============BEGIN DONGLE LICENSE==============
ya1HcPNuNudvepaE5Tc6gTMZl3T8kAqh
h1bINUs-c1pdn5tfQmE6Q-nrHLR2ic4b
NClta8BmGkBe4navWEph34wOezVx
===============END DONGLE LICENSE================
```

1. Copy this license text, and logon to the GateManager server. Go to the Licenses Tab, and select Install. Paste the license into the textbox, and click Install. When installing a Server Activation License (Soft Dongle), the server will restart to activate.
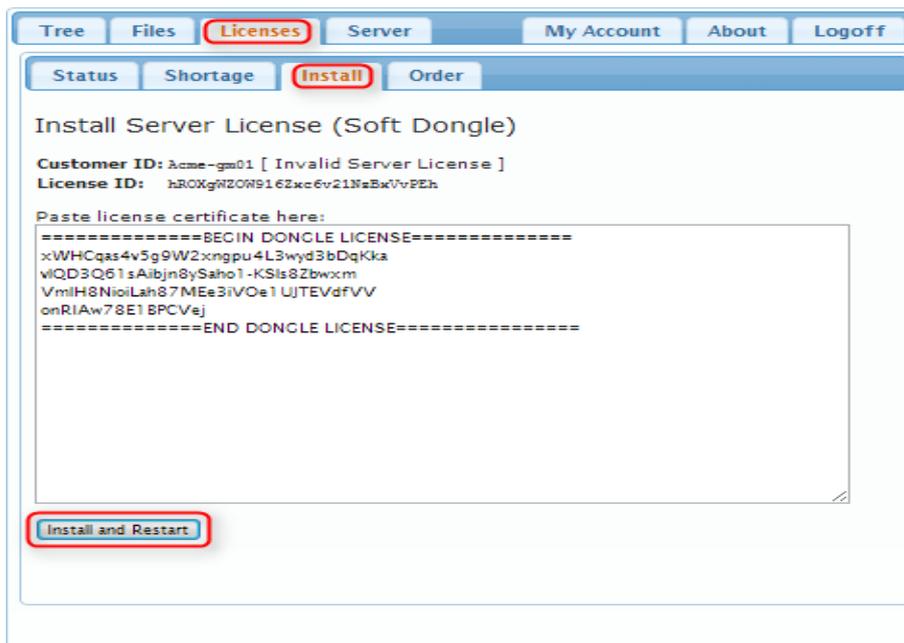
2. After the license upgrade your Licenses → Status will look like this:
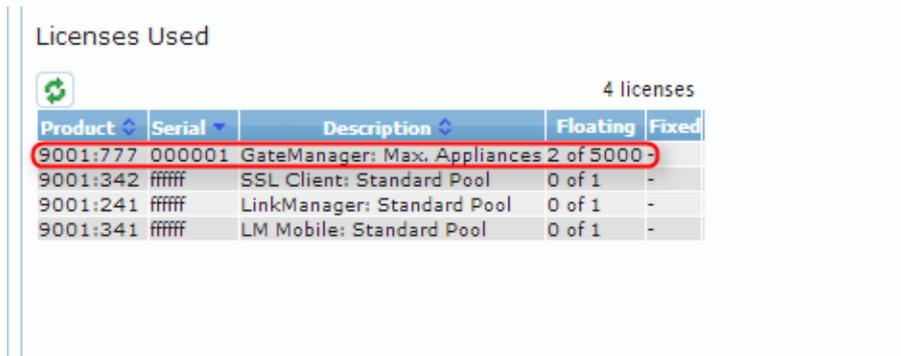
Licenses Used

Product	Serial	Description	Floating	Fixed
9001:777	000001	GateManager: Max. Appliances	2 of 5000	-
9001:342	ffffff	SSL Client: Standard Pool	0 of 1	-
9001:241	ffffff	LinkManager: Standard Pool	0 of 1	-
9001:341	ffffff	LM Mobile: Standard Pool	0 of 1	-

4 licenses

The soft dongle will always include a "Max. Appliances" license 9001:777 with a value from 25-5000 according to the ordered GateManager mainte- nance agreement. In the above screen license is based on EasyService terms indicated by a maximum of 5000.

If you have entered the "Limited Service" agreement, you would have started out with an Appliance license of 25. Upgrades can be purchased separately, and are installed the same way. A "Max. Appliance" license upgrade will have the following format:

```
======BEGIN LICENSE UPGRADE=====
YSNQlsPB26lKThI4nqNa2sbuByi1ddUZ
Bm-eYuHYMgX391FwnD1O-gYkhrhqj1Wa
51sk-ZFI
======END LICENSE UPGRADE======
```

Notices

Publication and Copyright

Trademarks

SiteManager™, LinkManager™, GateManager™ and TrustGate™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this document and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S.

Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following statements do not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

secomea