

GateManager™ model 4250 & 4260 Installation and Configuration



This document describes how to install the Secomea GateManager 4250 and 4260 hardware units.

The intended audience for this document is the person responsible for IT, or a person responsible for administration of the GateManager, and who can authorize the necessary network configuration for the GateManager to communicate via the Internet.

Version: 4.2, May 2018

Applicable to GateManager version 7.0 or later

Table of Contents

Document Version History	3
1. Introduction	4
1.1. Prerequisites for configuring according to this Guide	4
2. Initial GateManager installation and configuration	5
3. Firewall configuration (port forwarding)	9
3.1. Configuring your corporate firewall	9
3.1.1. Ingoing rules:	10
3.1.2. Outgoing rules:	10
4. Verify installation (first login)	11
5. Configuring GateManager environment settings	13
5.1. Set a Server Name and Browser Title	13
5.2. Enter/verify the Primary DNS server	14
5.3. Enter the Public Hostname	14
5.4. Configure mail settings.	16
5.5. Check sending of mails.	17
5.6. Specify the mail sender for Accounts and Alerts	18
5.7. Setup Server Administrator account(s)	18
5.8. Change password for Appliance Launcher access.	21
6. Ordering and installing production license	23
6.1. Order licenses	23
6.2. Example of an Info Form:	24
6.3. Installing licenses	25
6.4. Activation License(s)	25
6.4.1. Verifying if GateManager is Online	25
6.4.2. Verifying that activation was successful	26
APPENDIX A, Setting up backup	27
Backup to USB flash drive	27
Backup to FTP server	28
Verify that backup is working	29
APPENDIX B, Upgrading GateManager Firmware	31
APPENDIX C, SMS support	34
SMS modem physically connected to the GateManager	34
External SMS Gateways	35
APPENDIX D, Using Secomea TrustGate as firewall	36

D1. Configure Firewall rules	37
D2. Configure NAT rules	38
D3. Allow or limit access to the TrustGate WEB GUI	40
APPENDIX E. Recover lost Server Administrator password	41
Preparation	41
Recovery procedure	41
APPENDIX F. Manual installation of licenses	42
Server Activation License (Soft Dongle)	42
Notices	44

Document Version History

- 0.3 - Initial version
- 1.0 - Added TCP port 5800 in section 3.1.1 in relation to GateManager release 5.5 build 14123
- 1.1 - Added Appendix E - Recover lost Server Administrator password.
- 1.2 - Fixed disorder of appendices
- 1.3 - Changes relating to changes from version 5.7 to 5.8. Primarily related to new Mail setup, and security optimizations effecting operation with default password.
- 2.0 - Added GM model 4260 and modified Appendix C for more info on using SMS modems.
- 2.1 - Corrected section 4.3 to reflect v 6.0 configuration options.
- 3.7 - Section 5.6 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 Server Administrator role

1. Introduction

1.1. Prerequisites for configuring according to this Guide

This guide will assist you to plan for, and successfully complete the installation of the Secomea GateManager 4250/4260 hardware unit.

In principle you can install and run the GateManager 4250/4260 in a completely closed environment for testing. I.e. the GateManager will connect to your internal network as any other network device, and be used by LinkManager users and SiteManager devices connected within this closed network.

However, to operate the GateManager as intended, it must be accessible from the Internet.

Prerequisites for a fully functional install of the GateManager according to this guide are:

- You have the ability/authority to allocate a public Internet address for the GateManager.
- You have the ability/authority to adjust open necessary ports in an Internet firewall/NAT router to direct traffic to and from the server.
- You have the ability/authority to allow relaying of E-mails generated by the GateManager. (In worst case, you can relay via e.g. a Gmail account)
- The Internet bandwidth available for the GateManager must be at least 128Kb/s.

Model 4250



Model 4260 (NEW)



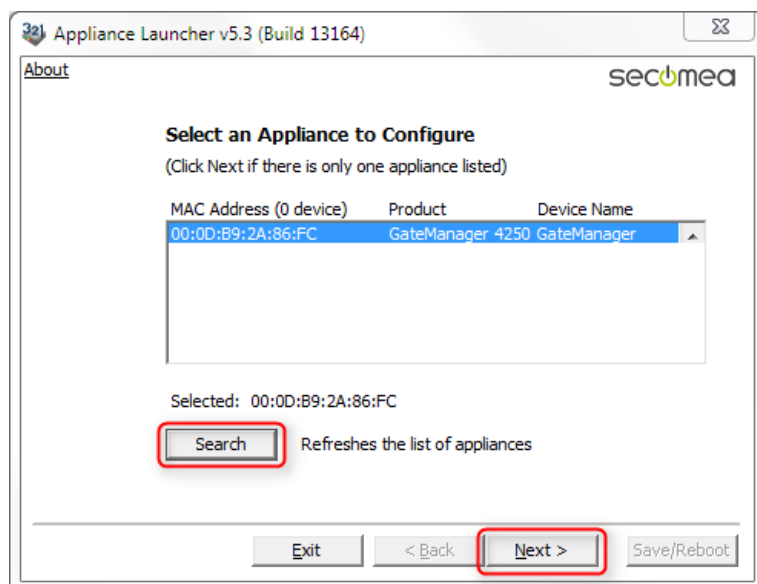
2. Initial GateManager installation and configuration

This section will make the basic configuration of the network settings for the GateManager. You can decide to move the GateManager to its intended physical location afterwards.

1. Download and install the **Secomea Appliance Launcher** from this location: <http://info.secomea.com/appliance-launcher> (Version 5.3 or newer is required)
2. Use a standard Ethernet cable (not a crossover cable) to connect the GateManager's **WAN port** to your internal network (same physical network where your PC is connected). The LAN port of the GateManager is currently not used.

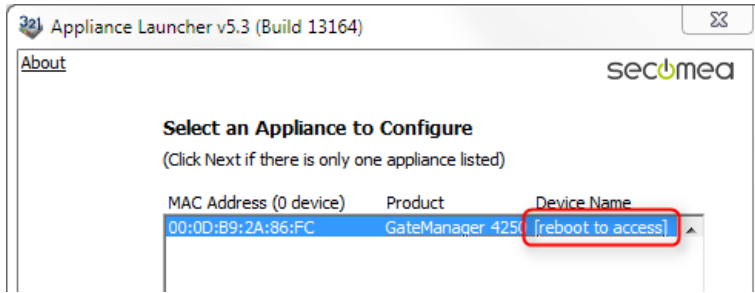
NB: If your PC is not located in the same physical network as the GateManager, you can alternatively connect your PC to the WAN or LAN port of the GateManager using the red cross-over cable

3. Apply power to the unit using the power supply delivered with the GateManager.
4. The red Error LED will blink during power on, and when ready it will continuously display 3 blinks followed by a pause. This indicates that the GateManager needs attention - in the case of first time installation it needs to be configured according to this guide.
5. If the GateManager has received an IP address from the DHCP server in the network, the green Status LED will turn on. This indicates that the GateManager web GUI is operational.
6. Start the Appliance Launcher. The GateManager should appear in the list immediately, or at least after pressing **Search** a few times.



If it does not appear, check that your PC is located on the same network segment as the GateManager, and check that you do not have a personal firewall or antivirus program that blocks for UDP broadcast.

NOTE: You may experience that the GateManager is marked with “reboot to access”.

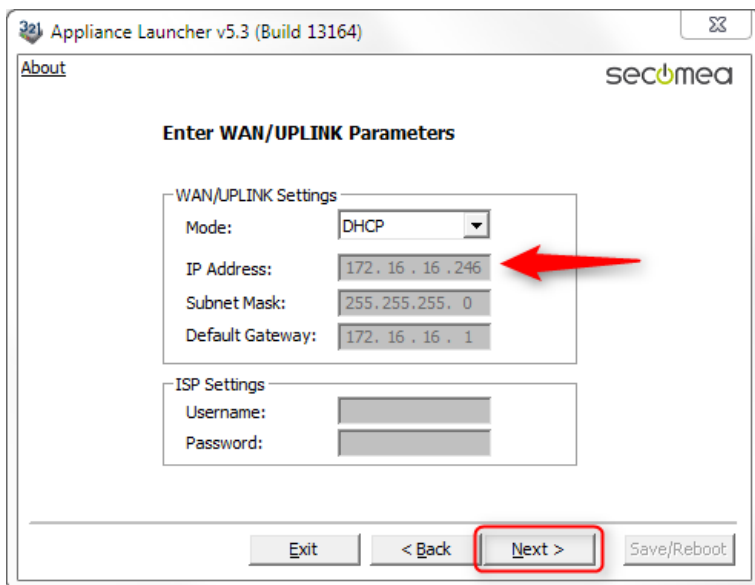


As a security precaution the GateManager will prevent access by the Appliance Launcher after 10 minutes, so that it will not be interrupted during normal operation.

Just repower the GateManager and press Search again until the GateManager appear with Device Name “GateManager”

7. Click **Next** to enter the WAN/UPLINK page. This will display the address received from the DHCP server.

Make note of this address, as you will need this to access the GateManager with a Web browser.



NOTE: If you intend to relocate the GateManager to a network without a DHCP server (such as a firewall DMZ), you should define a static IP address and the Default Gateway through which the GateManager can access the Internet.

- Click **Next** to get to the Optional Service Provider's GateManager page.

You should fill this page if you want the supplier of the GateManager to be able to establish remote access to the GateManager for assisting you in configuring or trouble shooting the GateManager configuration.

Appliance Launcher v5.3 (Build 13164)

About sec^omea

OPTIONAL: Your Service Provider's GateManager
(Leave fields empty to disable remote service and support)

Service Provider's GM Address*: 193.242.155.117 DNS

Domain Token*: Acme_Inc

Name of your GateManager*: Acme_GM01

Web-Proxy IP address: . . . DNS

Web-Proxy Account:

Web-Proxy Password:

* Contents for these fields are provided by your service provider.

Exit < Back **Next >** Save/Reboot

NOTE: Allowing remote access based on these settings, will make your GateManager establish an encrypted connection to the service provider's GateManager. Only authorized administrators on the service provider's GateManager will be able to obtain access, and only to the web log-in page on your GateManager (GateManager Administrator Web Portal) and they will have to login with an account that you control.

You can disable such access when the server is fully operational.

- Click **Next** to get to the Finish screen and select **Save/Reboot**:

Appliance Launcher v5.3 (Build 13164)

About

Finish

Press the [Save/Reboot] button to save your settings and reboot the appliance.

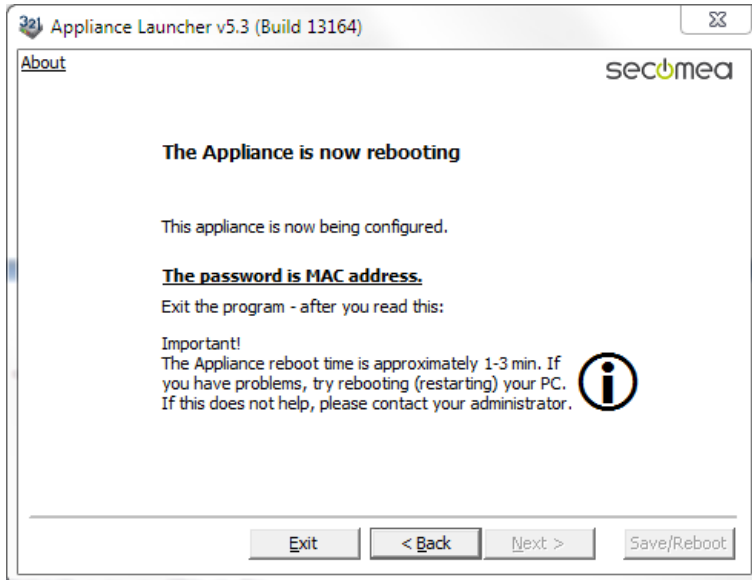
Pressing Exit will exit the Launcher and no changes will be saved.

Check here to preserve password {Default is not checked}

<Click> - copy current settings to clipboard

Exit < Back **Save/Reboot**

10. You will get the following dialogue, which means the initial network settings of the GateManager will be activated. You can now continue with the next section.



Note: You can disregard the message about the password being set to the MAC address.

This password is not used for accessing the GateManager Administrator web Portal, but used only for accessing a limited web GUI for the embedded OS on which the GateManager runs. Settings accessible via this web GUI can also be configured from within the GateManager Administrator web portal.

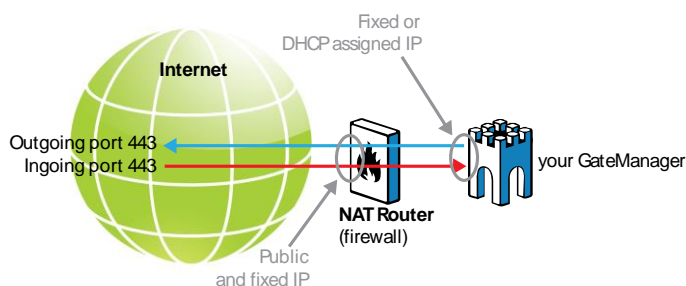
Setting the password to the MAC address is primarily to prevent unauthorized access to the underlying OS from the WAN port. The Appliance Launcher will not prompt for this password. In the GateManager Administrator web portal you can set a password for access by the Appliance Launcher (described later in this guide).

3. Firewall configuration (port forwarding)

The GateManager may not yet have been placed at the location where it is supposed to run in production. You may place it in your local network or in a DMZ zone of your firewall. In any case you will need to ensure the following:

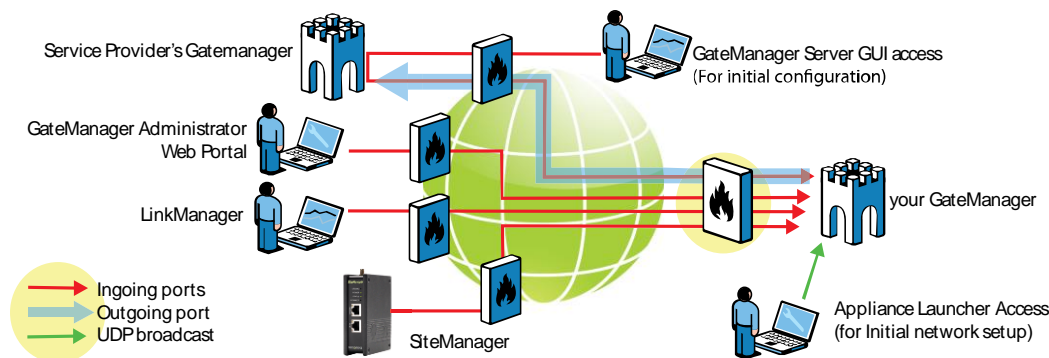
- Allocate a public IP address on your corporate firewall for use with the GateManager only. Alternatively order a new Internet connection from your ISP (e.g. an ADSL line), and specify that you need a fixed IP address.
- Configure the firewall to route the necessary incoming ports to the GateManager.
- The GateManager's WAN port must have the LAN side of the NAT Router / Firewall as its default gateway, so it can access the Internet.

Simplified illustration of the setup:



3.1. Configuring your corporate firewall

IMPORTANT: The GateManager MUST be protected by an external Firewall. The following ports must be forwarded or Destination NATed from the public IP address to the GateManager's WAN IP address. All other ports must be blocked by the corporate firewall to prevent unauthorized access.



In the sections below, the ports are marked as follows:

RED: Ports that must be opened for the system to work at all.

BLUE: Ports that must be opened for obtaining optimal functionality.

GREEN: Recommended, but only needed for special scenarios.

3.1.1. Ingoing rules:

TCP	80	--->	11444(or 80)	(Appliance)
	443	--->	11444(or 443)	(Appliance/Web GUI)
	11444	--->	11444	(Appliance)
	55000-59999	--->	55000-59999	(Go To Appliance)
	5900	--->	5900	(VNC support LM Mobile)
	5800	--->	5800	(JavaVNC support LM Mobile)
	3389	--->	3389	(RDP support LM Mobile)

Note: In case the GateManager Server will be accessed from inside the private network where it is located, the destination NAT rules must reflect that. This is the case if access from SiteManager, LinkManager or Administrator portal access is made from the same network as the local address of the GateManager.

Port 5800, 5900, 3389 is for "Go To Appliance" support using the Link-Manager Mobile. The ports are controlled and secured by the GateManager, so connection attempts on these ports by anything else than a LM Mobile will be rejected by the GateManager.

See also the example of setting up a firewall in **APPENDIX D, Using Secomea TrustGate as firewall.**

3.1.2. Outgoing rules:

TCP	21	(Optional: For FTP backup to external server)
	443	(For maintenance and Web Proxy)
	80	(Optional: WEB Proxy *)
TCP/UDP	53	(DNS)
	123	(NTP)

(*) The WEB Proxy allows a PC attached to the DEV port on a SiteManager to be able to browse the internet through the GateManager Server.

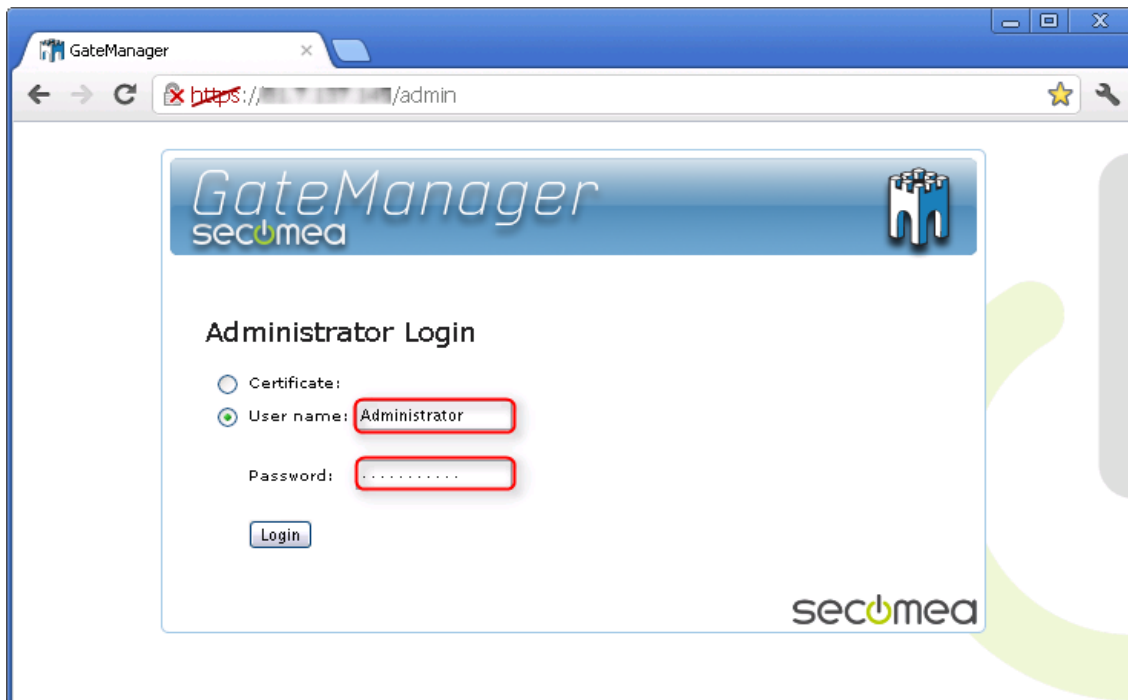
4. Verify installation (first login)

1. Open a browser and enter the IP address of the GateManager server. If logging in from inside the firewall, you should use the IP address of the WAN interface of the GateManager (from the WAN/UPLINK of the Appliance Launcher setup).

https://<GM Address>/admin

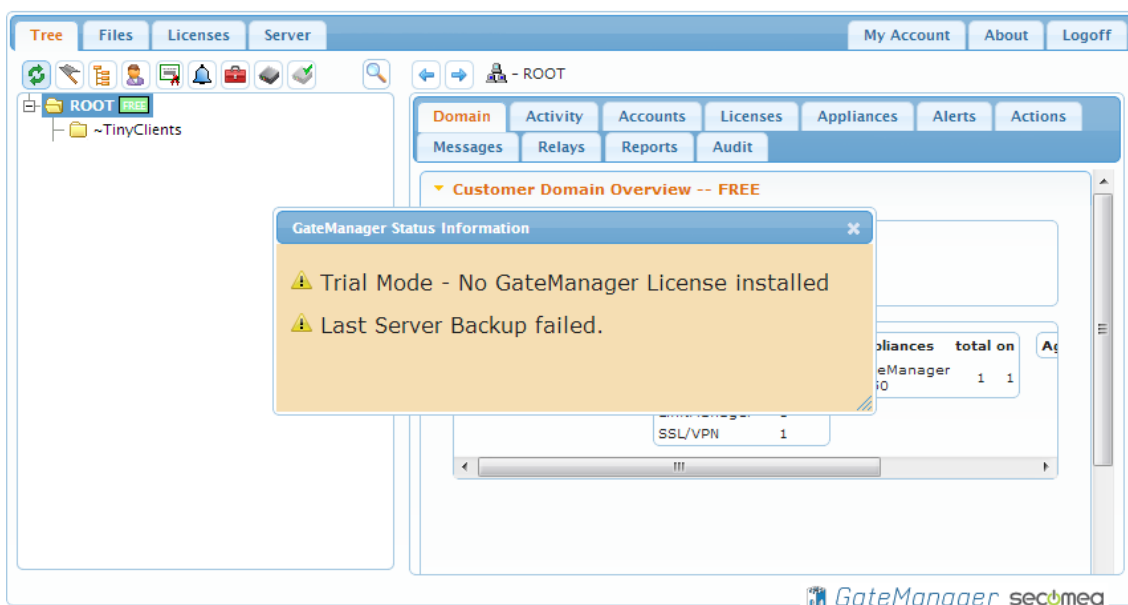
If connecting from the Internet, you should enter the public IP address that is routed to the GateManager.

The first screen you will see is:



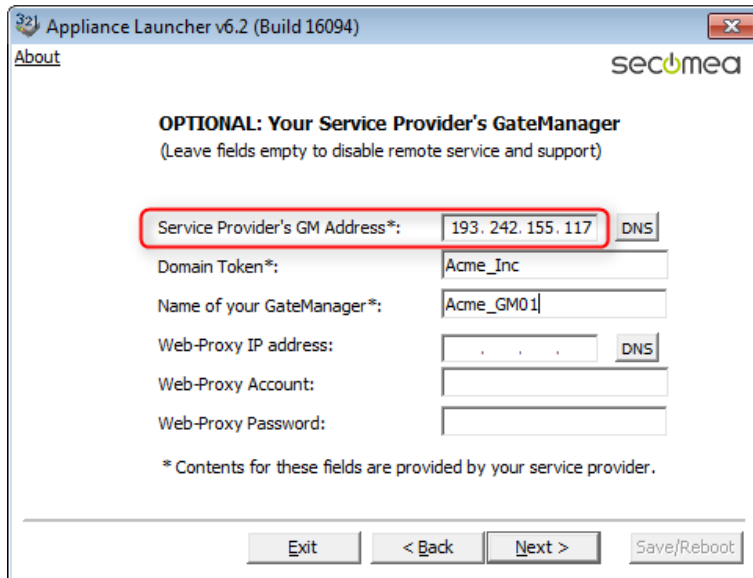
2. Login with the default settings:

- User name: **Administrator**
- Password: **gatemanager**

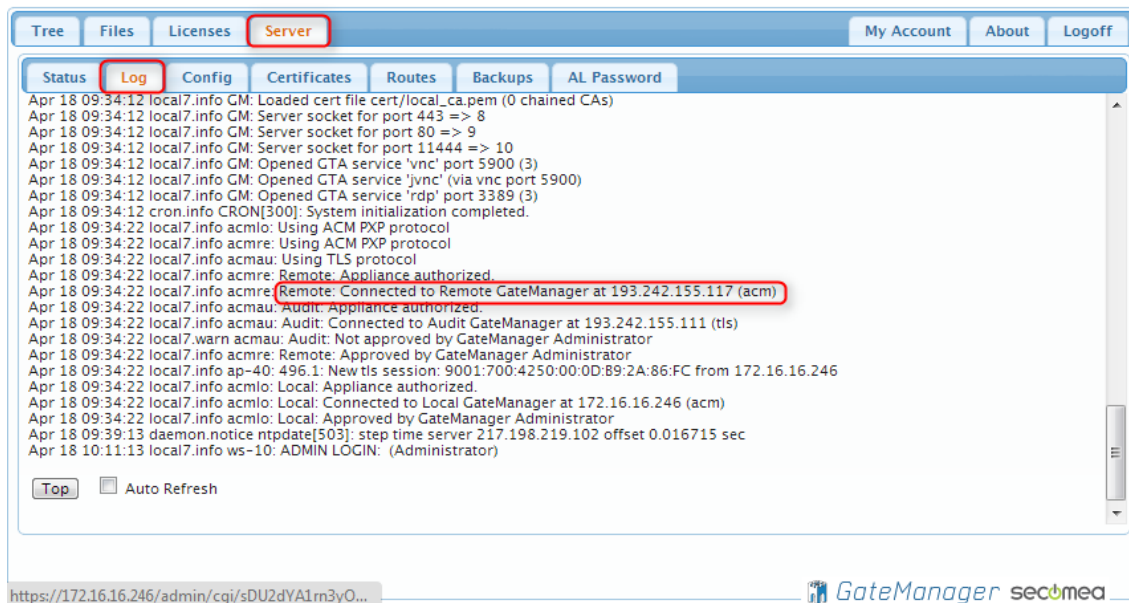


3. You can now configure the GateManager according to the next section.

NOTE: If, in the Appliance Launcher, you configured the GateManager to connect to a service provider's GateManager, your service provider should be able to securely access the same Web GUI from remote.



You can verify if the GateManager is in fact connected to your service providers GateManager by selecting Server and Log. If you can find the message "Connected to Remote GateManager <service provides GateManager>", the GateManager is accessible by the service provider:



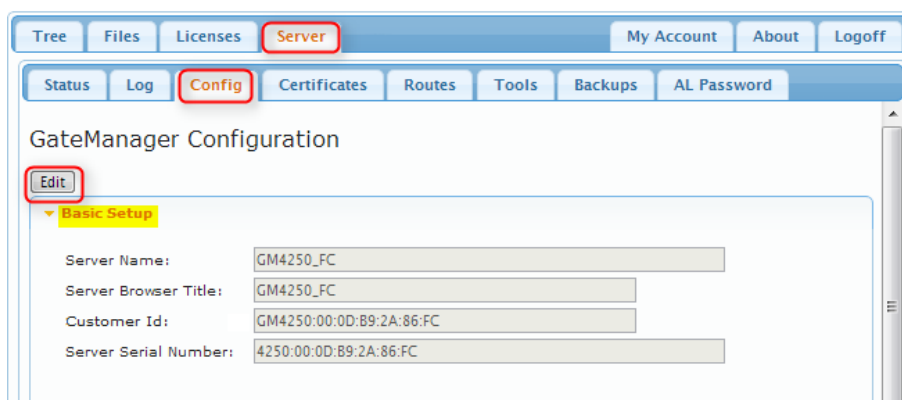
5. Configuring GateManager environment settings

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

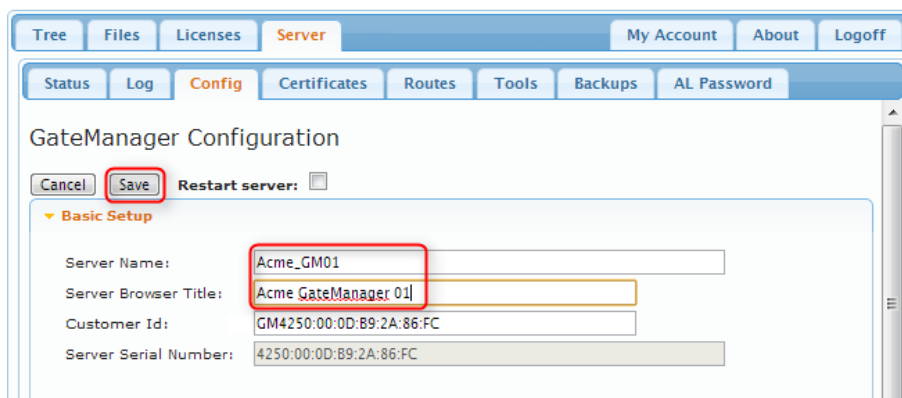
- Define a Server Name and web browser title.
- Enter/verify the primary DNS.
- Public DNS name or IP address that is port-forwarded to the GateManager.
- Setup and verify email relay settings.
- Create a new Server Administrator account and/or change the administrator account (new password and enable certificate). Also consider making a new server administrator account for access by your Service Provider.
- Consider defining a stronger password for Appliance Launcher access.

5.1. Set 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.



3. 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**.

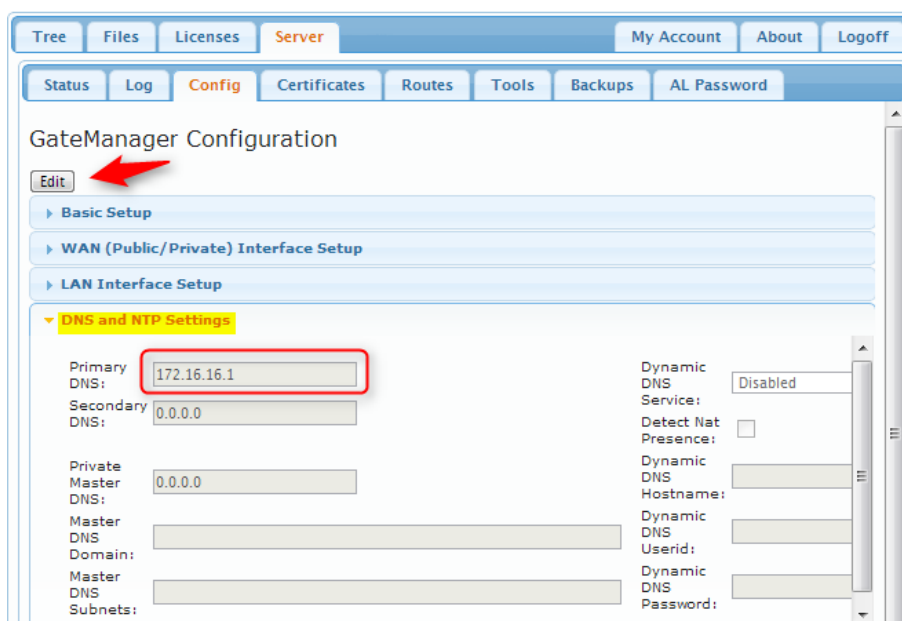


Note: It is a good idea to use the same name as defined for "Name of GateManager" in the appliance launcher (see page 7 step 8).

5.2. 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.

4. 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.



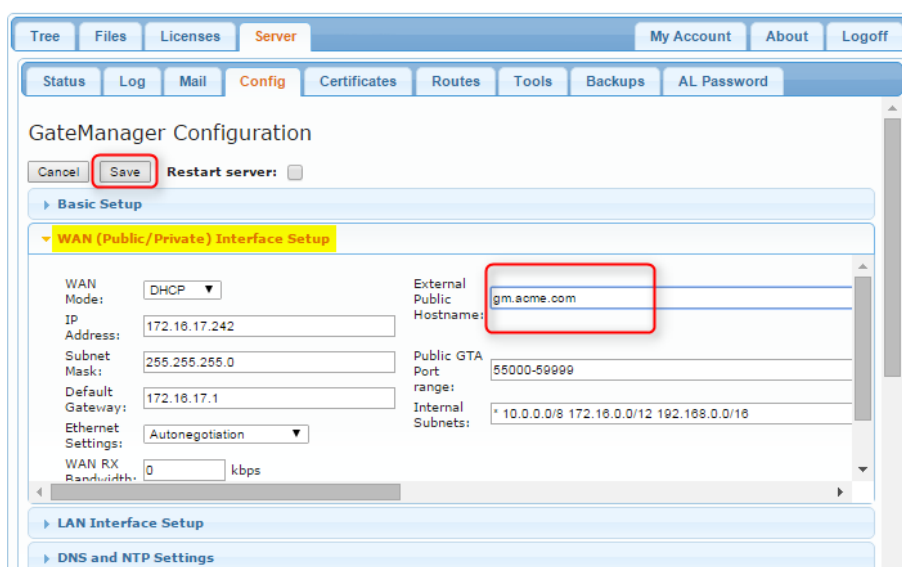
The screenshot shows the GateManager Configuration page. The 'Server' tab is selected. Under the 'DNS and NTP Settings' section, the 'Primary DNS' field is highlighted with a red box and contains the value '172.16.16.1'. A red arrow points to the 'Edit' button. Other fields include 'Secondary DNS' (0.0.0.0), 'Private Master DNS' (0.0.0.0), 'Master DNS Domain', 'Master DNS Subnets', 'Dynamic DNS Service' (Disabled), 'Detect Nat Presence' (checkbox), 'Dynamic DNS Hostname', 'Dynamic DNS Userid', and 'Dynamic DNS Password'.

5.3. Enter the Public Hostname

5. Under **WAN (Public/Private) Interface Setup** Enter the FQDN (Fully Qualified Domain Name) for this server and press **Save**.

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.

⚠ Do NOT select Restart Server yet!

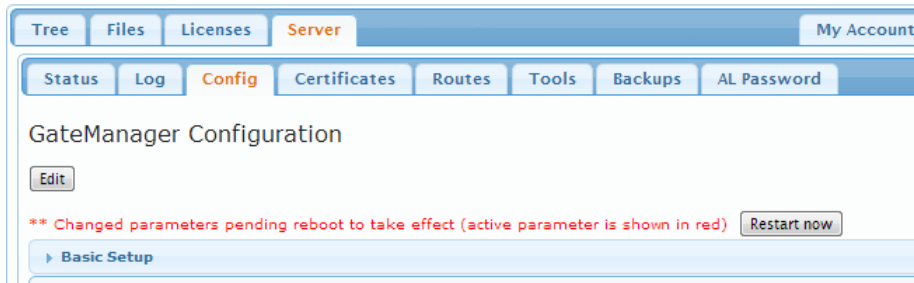


The screenshot shows the GateManager Configuration page. The 'Config' tab is selected. Under the 'WAN (Public/Private) Interface Setup' section, the 'External Public Hostname' field is highlighted with a red box and contains the value 'gm.acme.com'. Other fields include 'WAN Mode' (DHCP), 'IP Address' (172.16.17.242), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (172.16.17.1), 'Ethernet Settings' (Autonegotiation), 'WAN RX Bandwidth' (0 kbps), 'Public GTA Port range' (55000-59999), and 'Internal Subnets' (* 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16). The 'Save' button is highlighted with a red box.

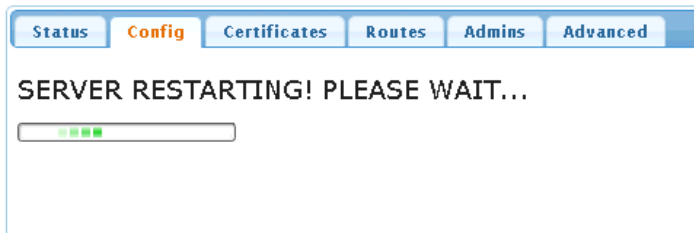
Possible error messages when saving:

- *Failed to resolve the DNS name.* This indicates that the DNS name (in this case gm.acme.com) is not valid. Your entered information will not be saved until the GateManager is able to resolve the host name.
- *Unknown hostname.* This indicates either that the DNS server has not been configured, or the DNS server is not working or not accessible.

6. When no error messages are displayed after saving the settings, you can click the “Restart now” button.



7. The GateManager server will restart, it will take about 60 seconds.



5.4. Configure mail settings.

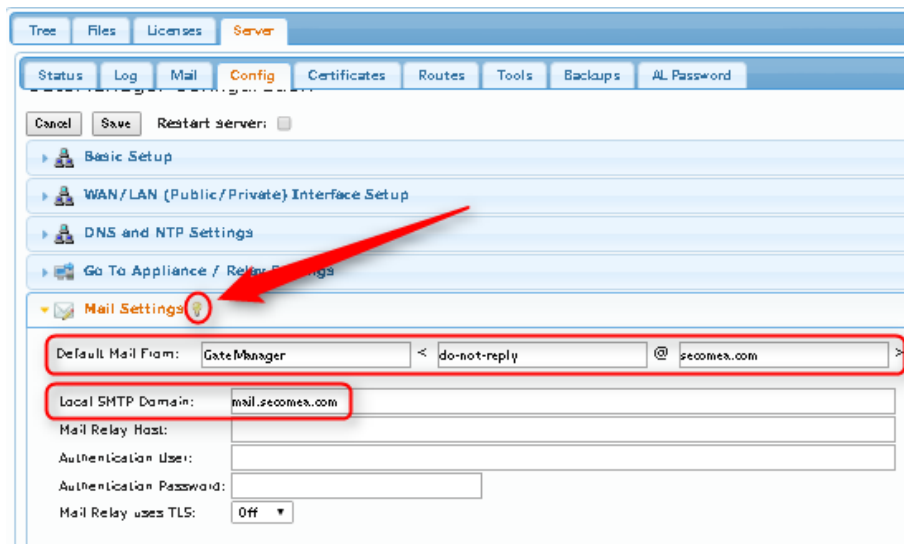
The ability to send email is absolutely essential to the GateManager!

The GateManager 4250/4260 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.

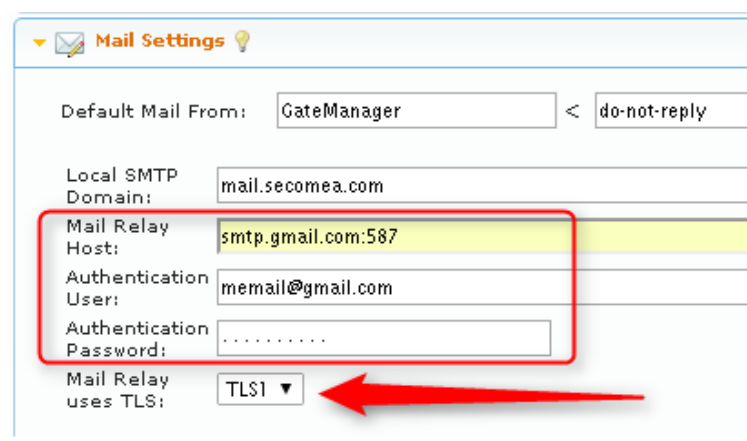
Here you should consider as a minimum the “Default Mail From” and the Local SMTP Domain.

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).

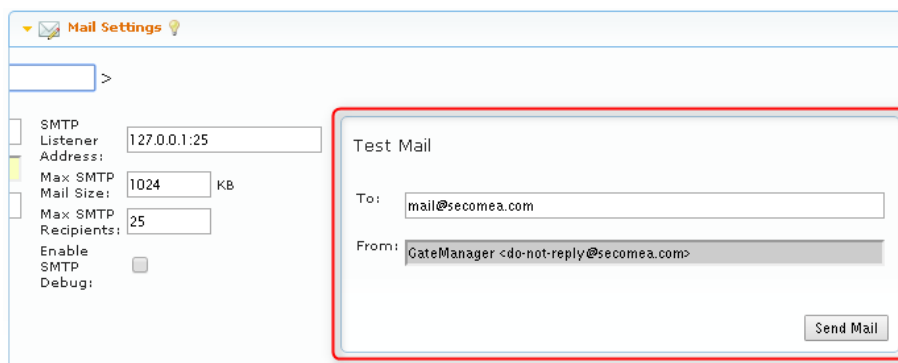


NOTE: It has not been verified if using e.g. Gmail for large volumes of emails would cause problems. So using such public mail services should only be used as an interim solution.

5.5. Check sending of mails.

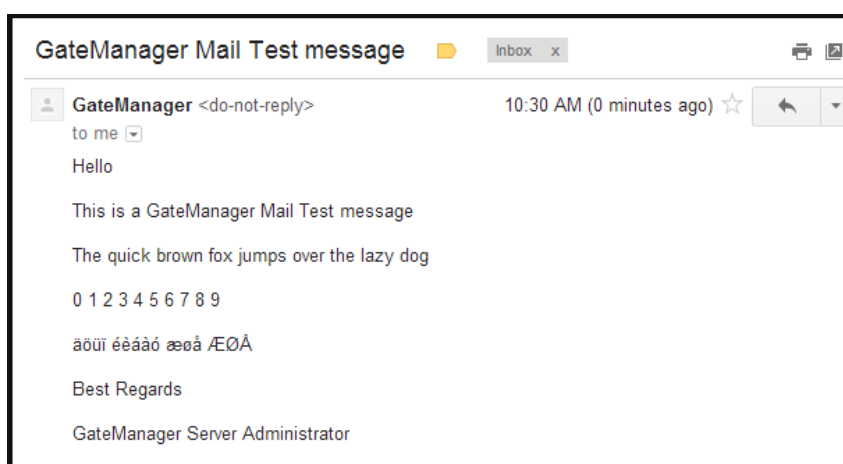
You should check with the Test Mail option that your settings are correct, and are accepted by recipient mail servers.

1. Enter the Mail Settings section and type your email and click Send Mail



The screenshot shows the 'Mail Settings' configuration window. On the left, there are several settings: 'SMTP Listener Address' is set to '127.0.0.1:25', 'Max SMTP Mail Size' is '1024 KB', and 'Max SMTP Recipients' is '25'. There are also checkboxes for 'Enable SMTP' and 'Debug'. On the right, the 'Test Mail' form is highlighted with a red box. It contains a 'To:' field with 'mail@secomea.com' and a 'From:' field with 'GateManager <do-not-reply@secomea.com>'. A 'Send Mail' button is located at the bottom right of the form.

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 account as described above, and always check your Spam filter.

5.6. Specify the mail sender for Accounts and Alerts

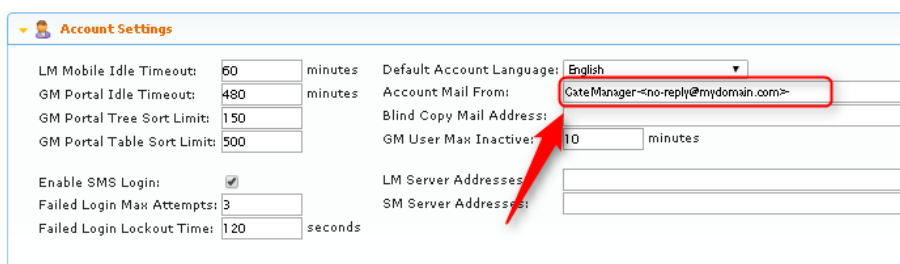
Starting from GateManager Release 7.0 there will no longer be any mail sender options to specify from the Accounts or Alerts Settings. All “Mail From” settings are handled from “Mail Settings”.

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.

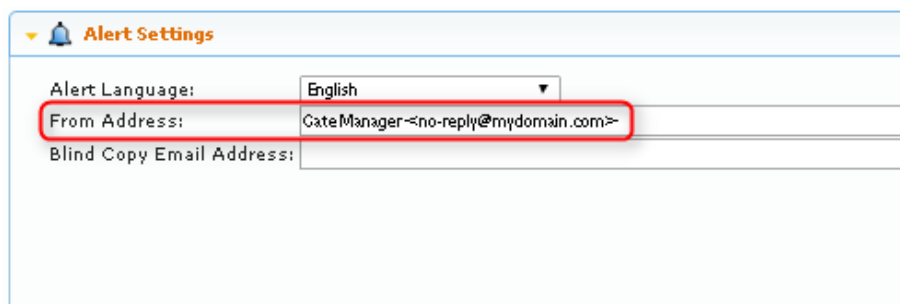
If you have a very special need for differentiating on the mails triggered by alerts and account mails, you can leave the fields as is, but you should still very strongly consider deleting the contents of the fields as shown below:

Delete “Account Mail From” if exists:



The screenshot shows the 'Account Settings' configuration page. The 'Account Mail From' field is highlighted with a red box and a red arrow pointing to it. The field contains the text 'GateManager <no-reply@mydomain.com>'. Other fields include 'LM Mobile Idle Timeout' (60 minutes), 'GM Portal Idle Timeout' (480 minutes), 'GM Portal Tree Sort Limit' (150), 'GM Portal Table Sort Limit' (500), 'Default Account Language' (English), 'Blind Copy Mail Address', 'GM User Max Inactive' (10 minutes), 'Enable SMS Login' (checked), 'Failed Login Max Attempts' (3), and 'Failed Login Lockout Time' (120 seconds).

Delete Alert “From Address” if exists:



The screenshot shows the 'Alert Settings' configuration page. The 'From Address' field is highlighted with a red box. The field contains the text 'GateManager <no-reply@mydomain.com>'. Other fields include 'Alert Language' (English) and 'Blind Copy Email Address'.

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.

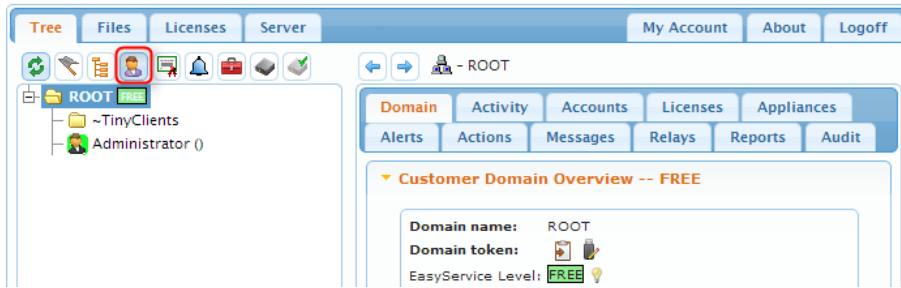
5.7. Setup Server Administrator account(s)

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..”.

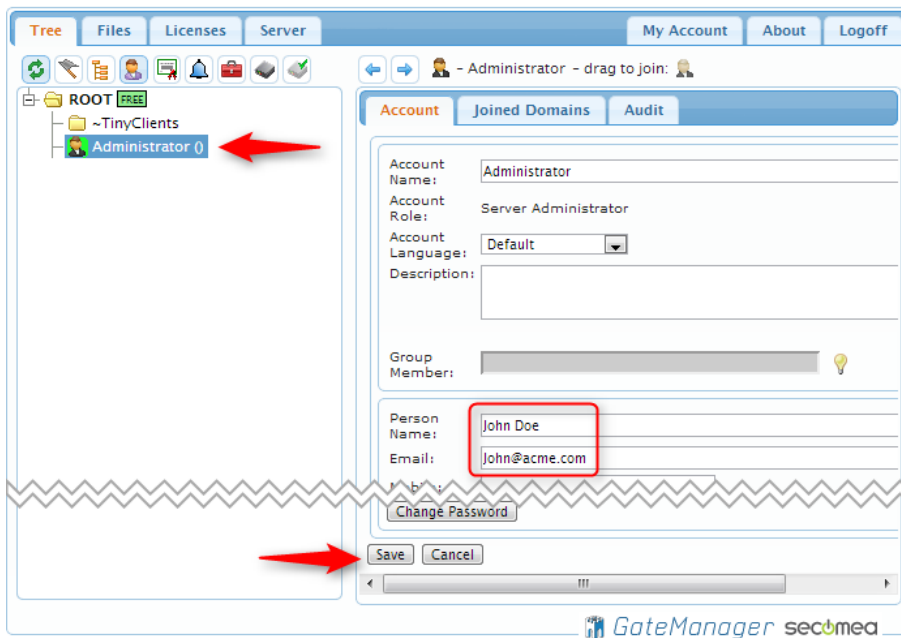
However, if the account is changed to use X.509 certificate, and the certificate is lost (e.g. it could be discarded by the email server that receives the email with the certificate attachment), you would lock yourself out of the server completely. Therefore, it is highly recommended to create a new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

The following explains the recommended steps:

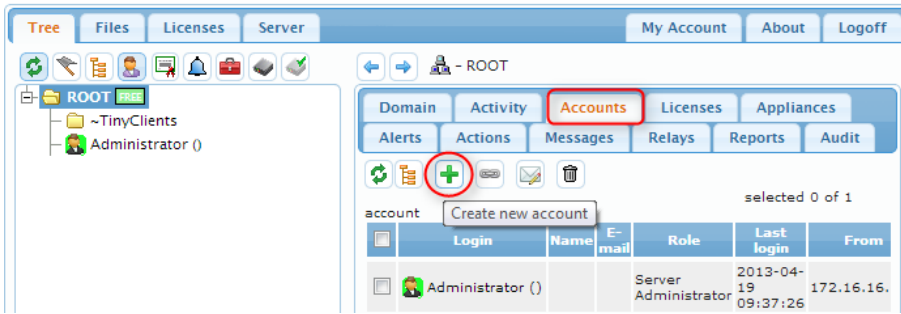
1. Select the Tree tab, and enable viewing of user accounts (in case they are not visible already), by clicking the account icon so its background turns light blue. You will now see the account that you are currently logged in with displayed with a green background.



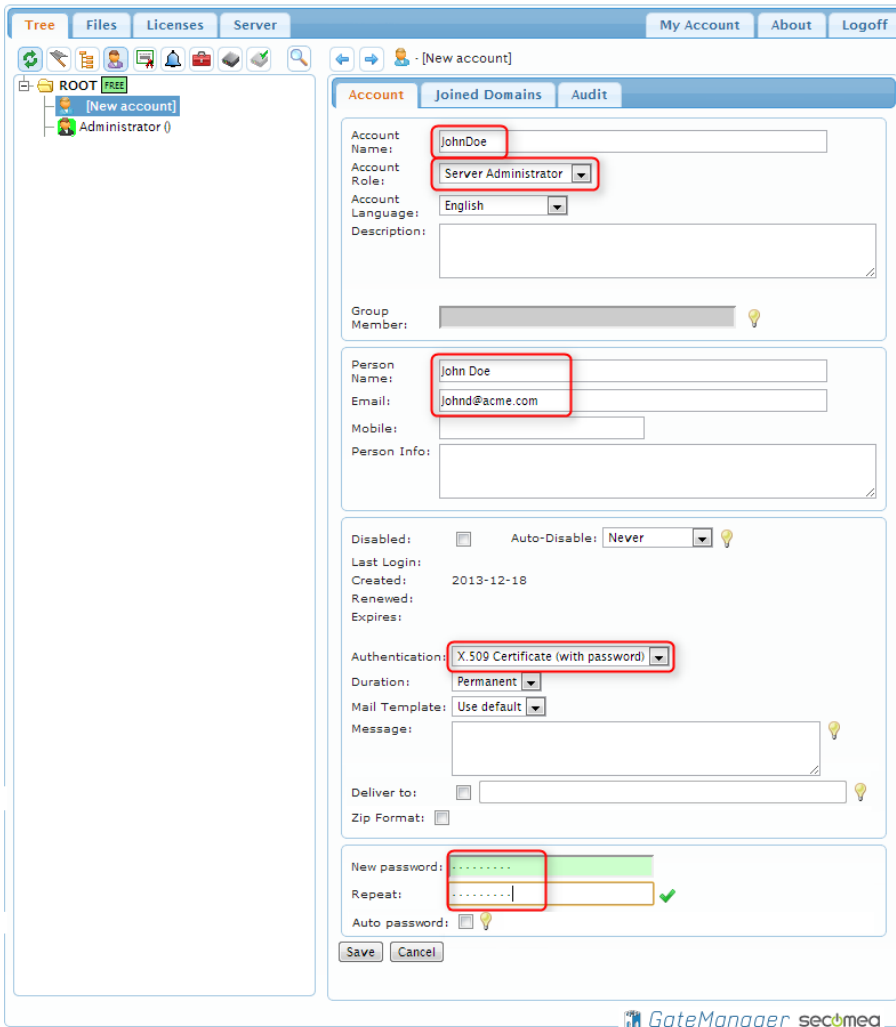
2. Click on the Administrator account, and insert your own name and email for the account. Select **Save**.



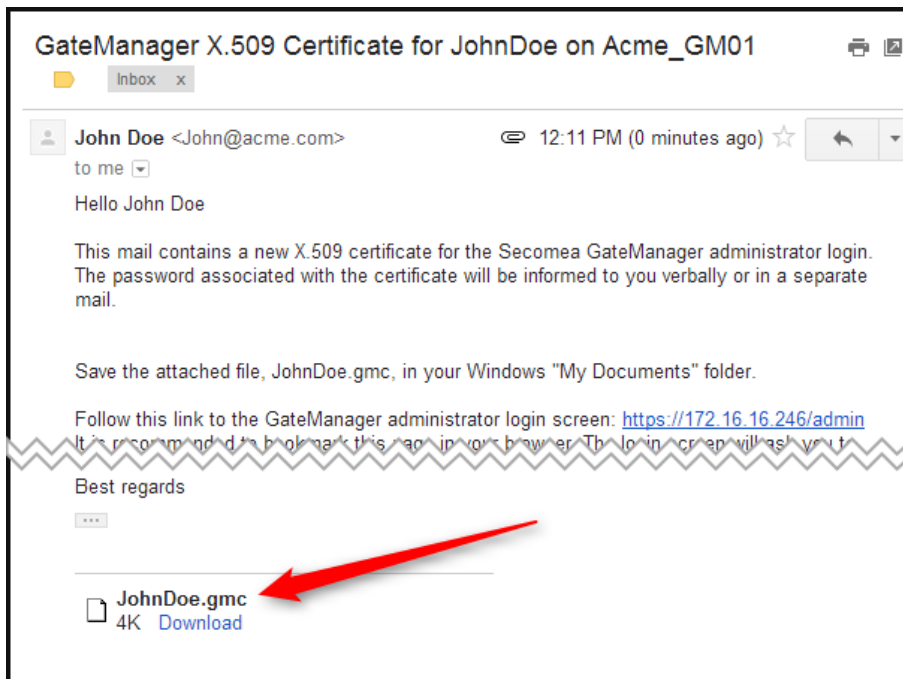
3. Standing in the Root domain, select **Accounts** and click the plus sign to create a new account:



4. Fill in the following minimum settings:



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



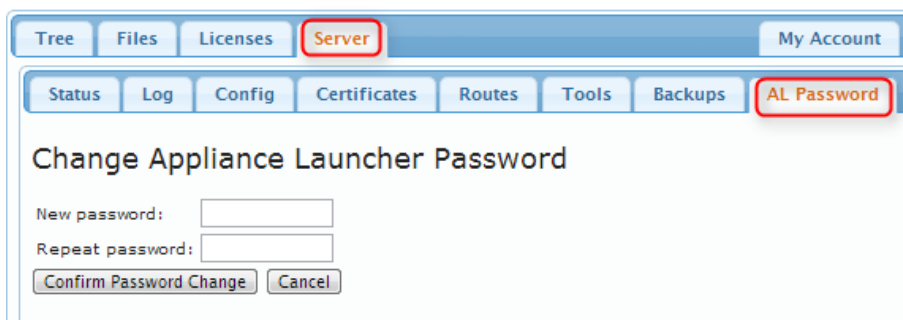
- You now have a backup Server Administrator account, and you can safely change the password of the default Server Administrator account, and also enable X.509 authentication for it, or you could even disable it.

⚠ 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.

5.8. Change password for Appliance Launcher access.

Select Server and 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 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>

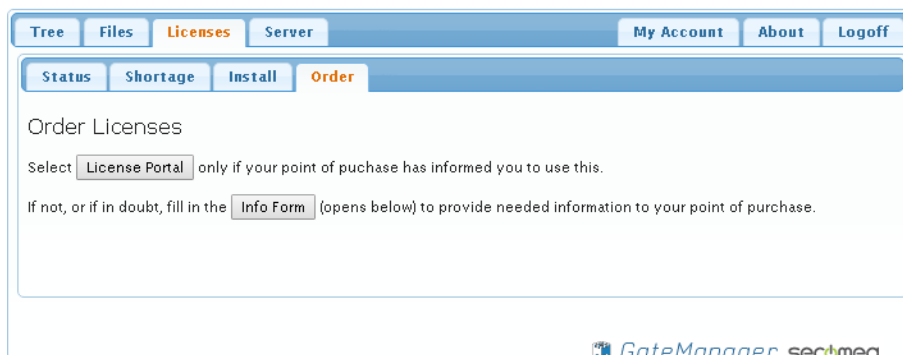
6. Ordering and installing production license

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

You will need to install a license certificate to increase the number of appliances to connect and to allow the GateManager to be used for production purposes.

6.1. Order licenses

1. 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.

6.2. Example of an Info Form:

Tree Files Licenses Server My Account About Logoff

Status Shortage Install Order

Order Licenses

Select only if your point of purchase has informed you to use this.

If not, or if in doubt, fill in the (opens below) to provide needed information to your point of purchase.

License Purchase Information

Use this form to submit information to your point of purchase in relation to your license order.
NOTE: This form is not your official purchase order, but only a specification of your current account status to ensure creation of the correct licenses.

Your point of purchase:

Company:

Contact:

E-mail:

Order Reference:

GateManager Model: 9250
Hostname (FQDN): gm.acme.com
LicenseID:: qRCjs3l0CRBycHNSlsoq7N2P-JEF

Order number:
Your own purchase order number related to this info submission

Your company:

Your name:

Your E-mail:

Comment:

Your current account and license status:

TLS Certificate: DEMO mode

6.3. Installing licenses

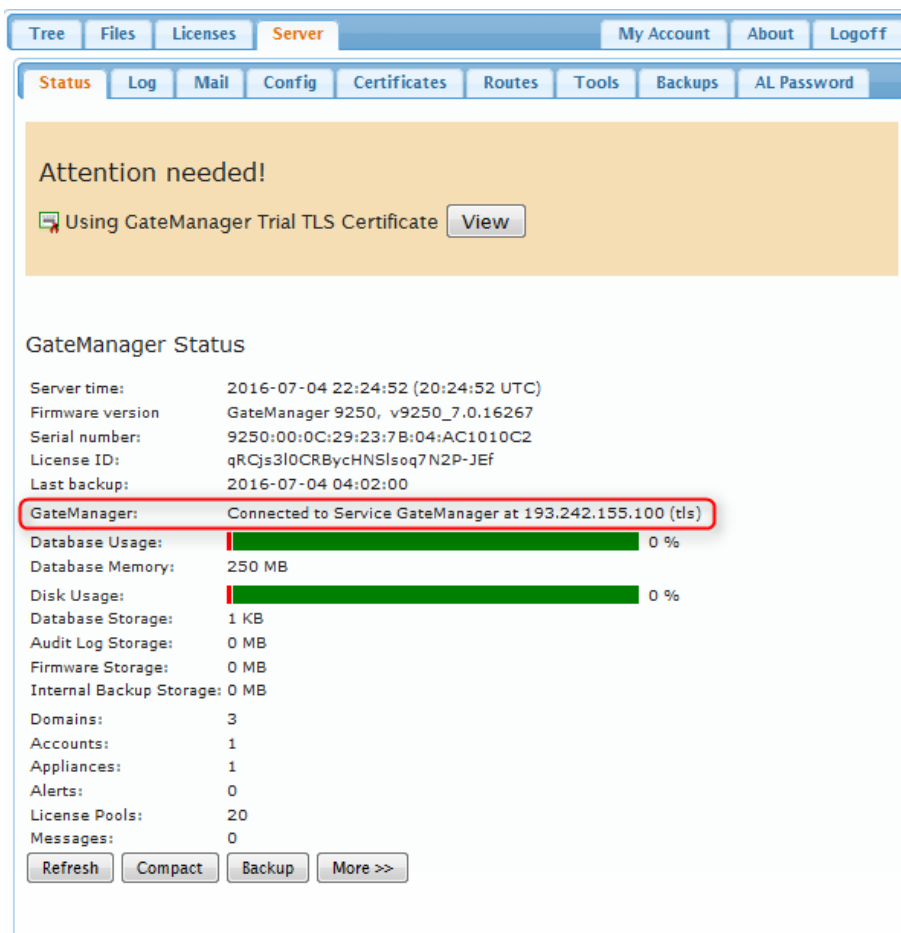
6.4. Activation License(s)

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)

6.4.1. Verifying if GateManager is Online

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

Check if the GateManager is Online Under Server → Status:



The screenshot shows the GateManager web interface. At the top, there are navigation tabs: Tree, Files, Licenses, Server (selected), My Account, About, and Logoff. Below this is a secondary set of tabs: Status (selected), Log, Mail, Config, Certificates, Routes, Tools, Backups, and AL Password. A yellow banner at the top of the main content area reads "Attention needed!" with a sub-message "Using GateManager Trial TLS Certificate" and a "View" button. Below the banner is the "GateManager Status" section, which contains the following information:

Server time:	2016-07-04 22:24:52 (20:24:52 UTC)
Firmware version:	GateManager 9250, v9250_7.0.16267
Serial number:	9250:00:0C:29:23:7B:04:AC1010C2
License ID:	qRCjs3l0CRBycHNSlsoq7N2P-JEF
Last backup:	2016-07-04 04:02:00
GateManager:	Connected to Service GateManager at 193.242.155.100 (tls)
Database Usage:	0 %
Database Memory:	250 MB
Disk Usage:	0 %
Database Storage:	1 KB
Audit Log Storage:	0 MB
Firmware Storage:	0 MB
Internal Backup Storage:	0 MB
Domains:	3
Accounts:	1
Appliances:	1
Alerts:	0
License Pools:	20
Messages:	0

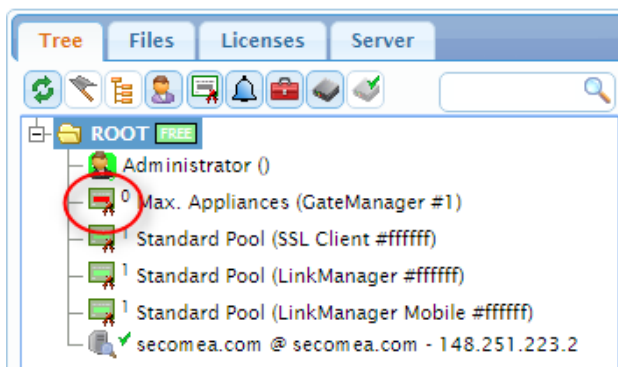
At the bottom of the status section are buttons for "Refresh", "Compact", "Backup", and "More >>".

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 F. Manual installation of licenses**

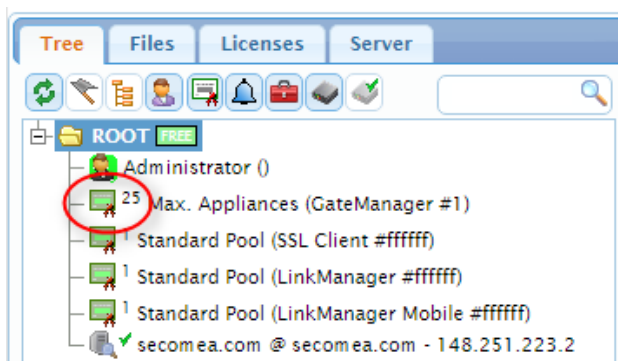
6.4.2. Verifying that activation was successful

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



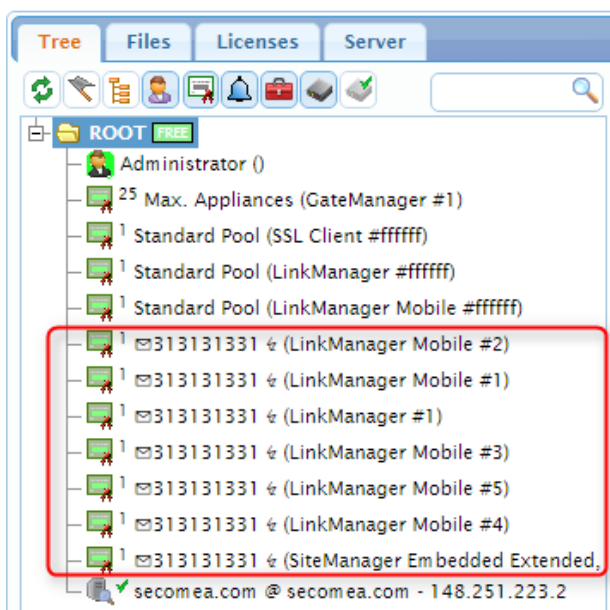
After activation this value will be 25-1000/5000 according to the ordered GateManager license agreement.

In ordering the GateManager with **EasyService** the value will show 1000 or 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 shown with the order number as description:



APPENDIX A, Setting up backup

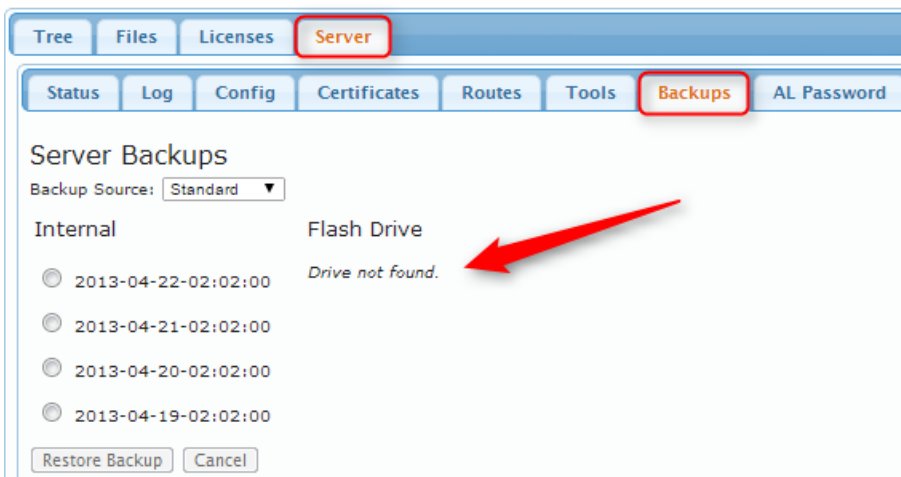
Backup will ensure that you can recover GateManager data including the database and the GateManager settings/licenses. This does not include a backup of the GateManager server firmware.

Backup to USB flash drive

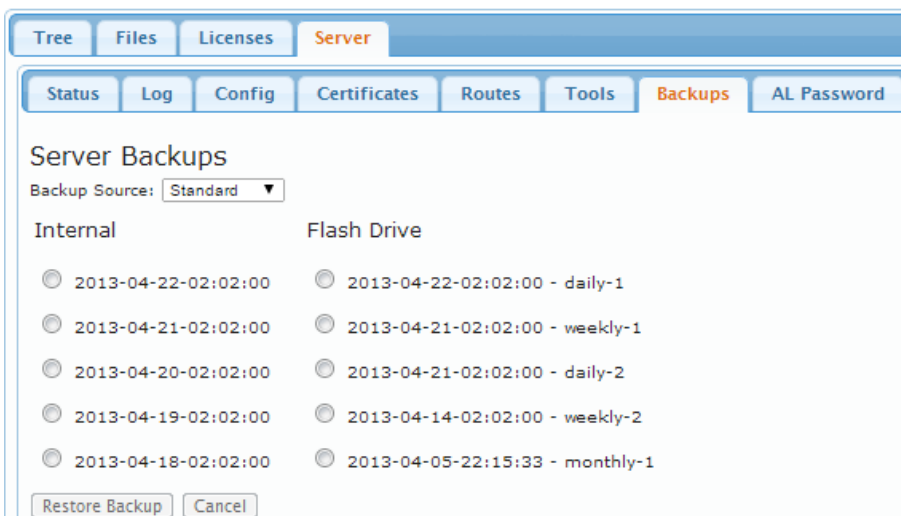
The primary backup is made on a USB flash drive. The backup is relatively compact, so a USB flash drive of e.g. 4GB would be sufficient. It is essential that the flash drive is formatted for FAT 32bit (NTFS formatted drives will not work).

(If you are formatting the USB flash drive in Windows open the control panel, then under administrative tools, select disk management. After right clicking, select the format on the USB flash drive.)

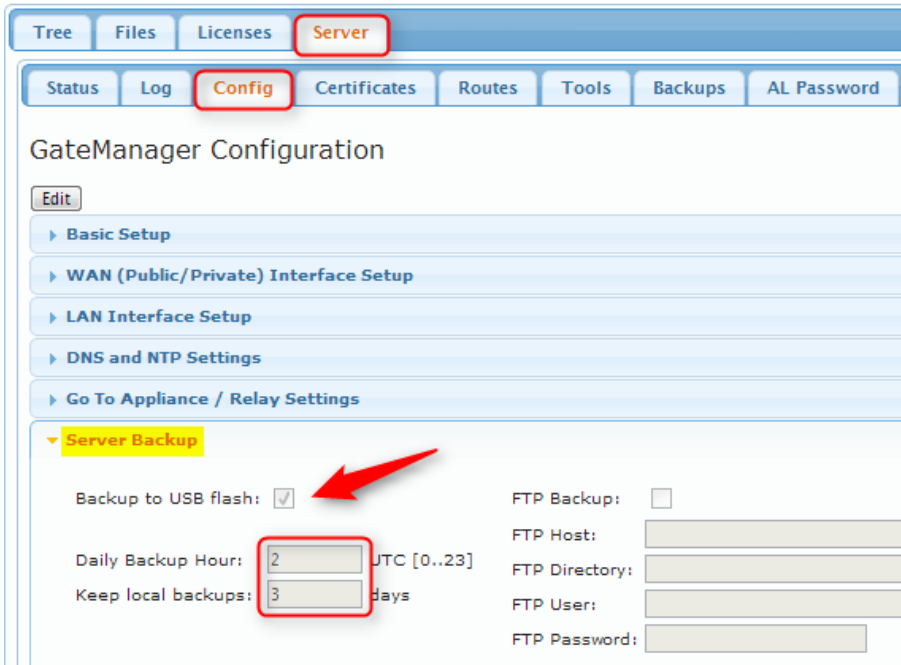
The GateManager will automatically assume there is a USB drive available for backup. If no USB drive is available you will see a warning under Server Status, and under Server Backups, you will see the following:



When inserting a properly formatted USB drive, this page will display the default backup intervals:



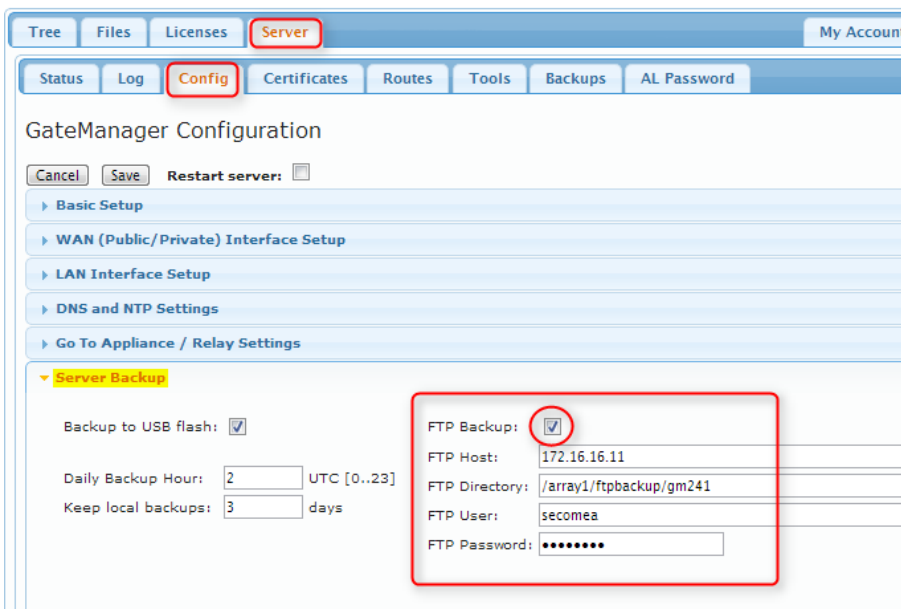
Under **Server** → **Config**, you will see that USB flash backup is default enabled, so unless you desire to change the backup intervals, you do not need to do anything:



Backup to FTP server

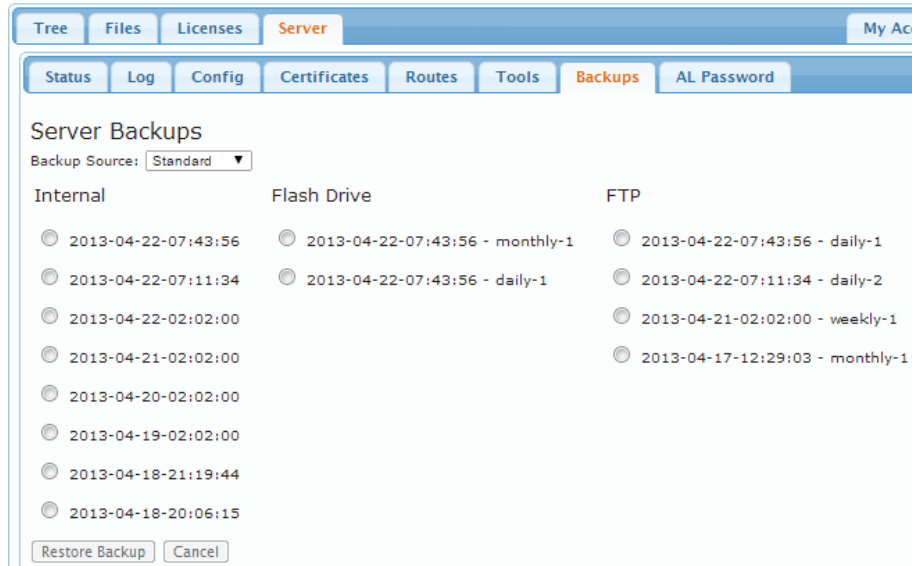
An advantage of a FTP backup is that the FTP server does not have to be in the same location as the GateManager server.

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



Note: If no USB drive is attached to the server you should uncheck the option "Backup to USB flash." Leaving it checked will result in the logon splash screen saying "Last Server Backup failed".

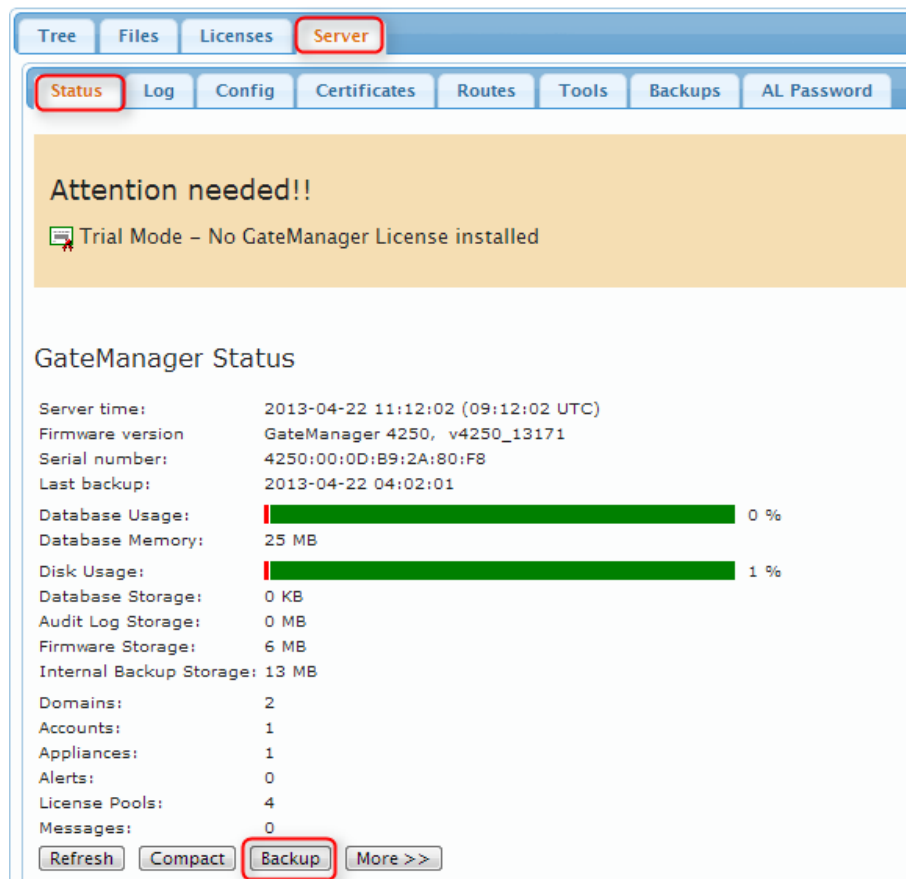
You can have several backup methods set up simultaneously. The following screenshot illustrates a GateManager that has been setup for both USB- and FTP backup:



Verify that backup is working

When a backup is configured, it would be wise to test the backup destination by making a manual backup.

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



A successful backup will be displayed as follows:

The screenshot shows a terminal window with a title bar that is partially obscured. Below the title bar, there are buttons for 'Refresh', 'Compact', 'Backup', and 'More >>'. The main content of the terminal is a log of backup operations. Two red callout boxes with white text are overlaid on the terminal output. The first callout, labeled 'USB flash backup', points to the lines: 'Copy/local to /mnt/sdb5/GMBACKUP/daily-1.tgz' and 'Eject USB flash drive: sdb5'. The second callout, labeled 'External FTP backup', points to the lines: 'Copy/FTP to 172.16.16.11:/array1/ftpbackup/gm241/daily-1.tgz' and 'FTP Backup succeeded'.

```
Messages: 0
[Refresh] [Compact] [Backup] [More >>]

Backup Done

Start Internal Backup: Mon Apr 22 09:51:19 UTC 2013
Database Snapshot (595KB): Mon Apr 22 09:51:32 UTC 2013
Compiling Backup file...
Internal Backup done: Mon Apr 22 09:51:44 UTC 2013

Backup File: backup/gm.2013-04-22-09:51:18.tgz (7MB)

Trim database storage...
Current audit log disk usage: 3 MB (4 months)
Removing backups older than 3 days

Start backup export

Export Backup Started ...
Mount USB flash drive: sdb5
Local auto-backup target: /mnt/sdb5/GMBACKUP
Copy/local to /mnt/sdb5/GMBACKUP/daily-1.tgz
Eject USB flash drive: sdb5
Copy/FTP to 172.16.16.11:/array1/ftpbackup/gm241/daily-1.tgz
delete daily-2.tgz
rename daily-1.tgz daily-2.tgz
FTP Backup succeeded
Export Backup Done: Mon Apr 22 09:52:35 UTC 2013
```

APPENDIX B, Upgrading GateManager Firmware

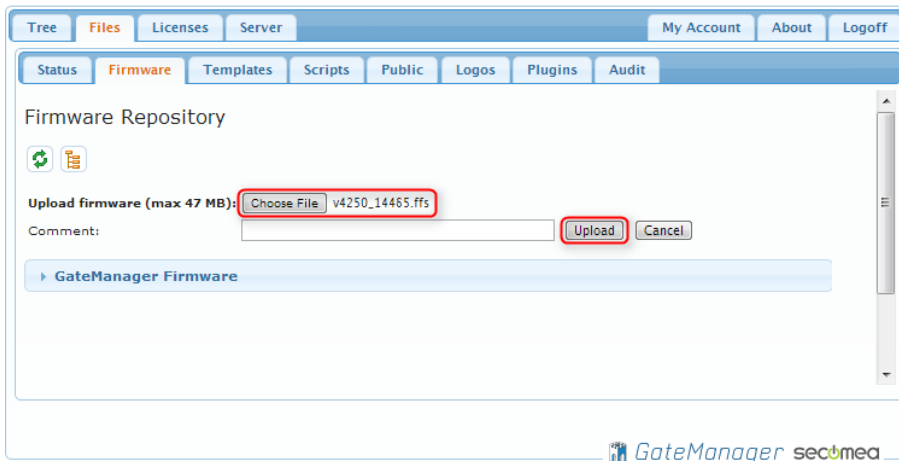
There may be a newer version of the GateManager firmware that introduces bug-fixes and new features.

Check the “About” tab in the GateManager portal for the currently running version. If a newer version exists on the Secomea web site, you can download and install it based on the following instructions.

1. Select **Files** → **Firmware** and press the plus icon.

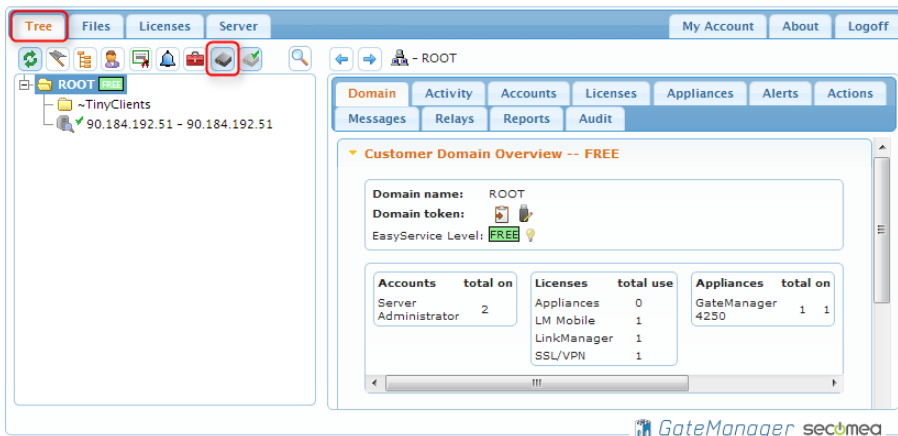


2. Press **Choose File** and browse for the file: (v4250_xxxx.ffs or v4260_xxxx.ffs) and press **Upload**:

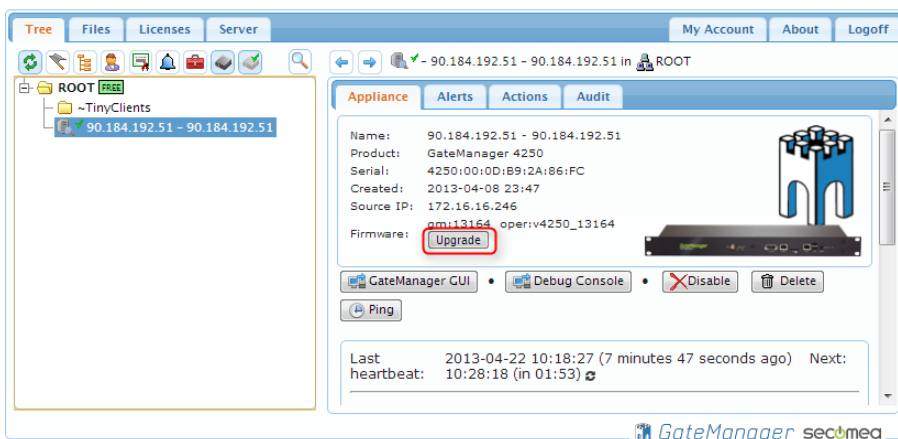


Wait for the firmware to be uploaded and saved.

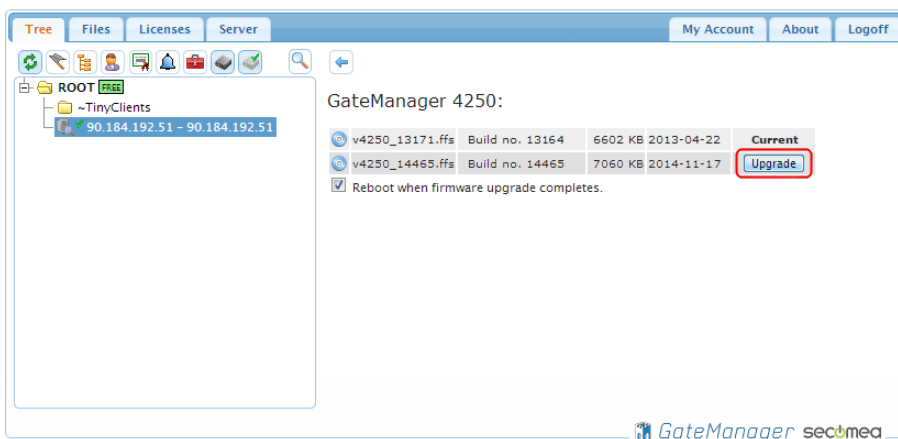
3. Select the **Tree** menu and click on the **“Show Appliances”** Icon in the top Icon-list, and the GateManager server will be listed (if not listed already). In this example it is named by the public IP address that is entered as the External Public Hostname in the WAN configuration.



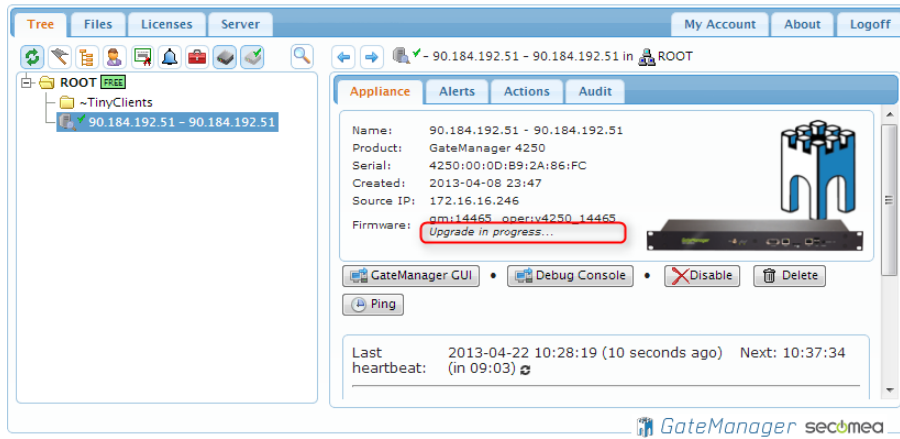
4. Select the GateManager Agent and press the **Upgrade** button.



5. Press the **Upgrade** button for the newly uploaded firmware.



6. While upgrading **Upgrade in progress** is shown on the screen. The upgrade will usually take less than 60 seconds.



7. After that the server is upgraded. You may want to log out and login again, in order to refresh your browser cache.

APPENDIX C, SMS support

The GateManager has support for sending SMS messages for the following purposes:

- Automatically sending the password for a newly created GateManager or LinkManager account (alternative to informing the password verbally or manually by email).
- Sending a SMS pass code in association with accounts configured for two-factor authentication by SMS.
- Sending SMS Alerts generated by the GateManager based on appliance status.
- Sending Alerts generated by a SiteManager (see separate guide "SiteManager Working with SMS and Email Alerts")

Note that a SMS modem associated with the GateManager is not used for data connections, and is not required for the GateManager to function, so the SMS feature can be considered optional.

SMS modem physically connected to the GateManager

GateManager 4250 has an integrated SMS modem. To enable the SMS feature you must insert a standard size SIM card with SMS subscription (NOTE: Power Off the GateManager when inserting and removing the SIM card).

GateManager 4260 needs a USB modem inserted in the USB port of the GateManager. Currently the GateManager supports a Huawei MS2131s only, which is a modem with increased temperature and moisture resistance specifications and thus suited for industrial use. This modem can be ordered from Secomea on P/N XXXXX.

The SMS modem is enabled in the Server Config. Make sure SMS #1 is set to "internal. Enter a SIM pin code (leave blank if the pin code has been removed from the SIM card). Enter a default country code prefix that will be used for mobile numbers that have been entered without a country code prefix.

The screenshot displays the GateManager configuration web interface. The 'Server' tab is selected in the top navigation bar. Under the 'Config' sub-tab, the 'SMS Settings' section is expanded. The 'Enable SMS' checkbox is checked. The 'SMS #1 Driver' is set to 'Internal'. The 'Default number prefix' is set to '+45'. The 'SIM Pincode' field is highlighted with a red box. A red arrow points to the 'Test SMS' button on the right side of the configuration panel.

Field	Value
Enable SMS	<input checked="" type="checkbox"/>
SMS #1 Driver	Internal
SMS #2 Driver	off
Default number prefix	+45
SIM Pincode	[Red Box]
Mobile	[Empty Field]
Flash SMS	<input checked="" type="checkbox"/>

External SMS Gateways

All GateManagers have support for using an external SMS gateway.

Refer to the document “Configuring SMS Gateways on GateManager” for detailed descriptions on setting up a SMS gateway.

APPENDIX D, Using Secomea TrustGate as firewall

Any firewall with NAT routing capabilities can be used in front of the GateManager. Presumably you will reconfigure your existing corporate firewall with the fixed IP address and forwarding rules, and maybe even place the GateManager in a DMZ of the firewall.

This appendix explains how to configure a Secomea TrustGate firewall as firewall for the GateManager. You can use the screenshots as guidelines for configuring your own firewall, or you could consider actually deploying a Secomea TrustGate for this purpose.

The TrustGate firewalls are professional firewalls that have been deployed in thousands of installations in more than a decade. The Secomea TrustGate products are based on the same design philosophy as the Secomea industrial solutions, namely to make it simple and yet highly secure. A big advantage of the TrustGate firewalls is the EasyTunnel VPN Server capability that enables traditional VPN tunnels to SiteManagers, in addition to access by the LinkManager client. Additionally the TrustGate can be managed from a GateManager (either another GateManager, or the one that the TrustGate is placed in front of). The GateManager will allow remote access to the TrustGate, and also manages firmware upgrades, backup and access logging.

You can read more about the TrustGate firewalls here under traditional VPN:

<http://www.secomea.com/>

Any TrustGate model will fulfill the firewall requirements of the GateManager. The choice of TrustGate model will depend on needs for fail-over, DMZ etc. We would recommend the TrustGate 62 as an entry point. You can always upgrade the model, by moving the entire configuration to a bigger model.

In the following example these IP addresses are used.

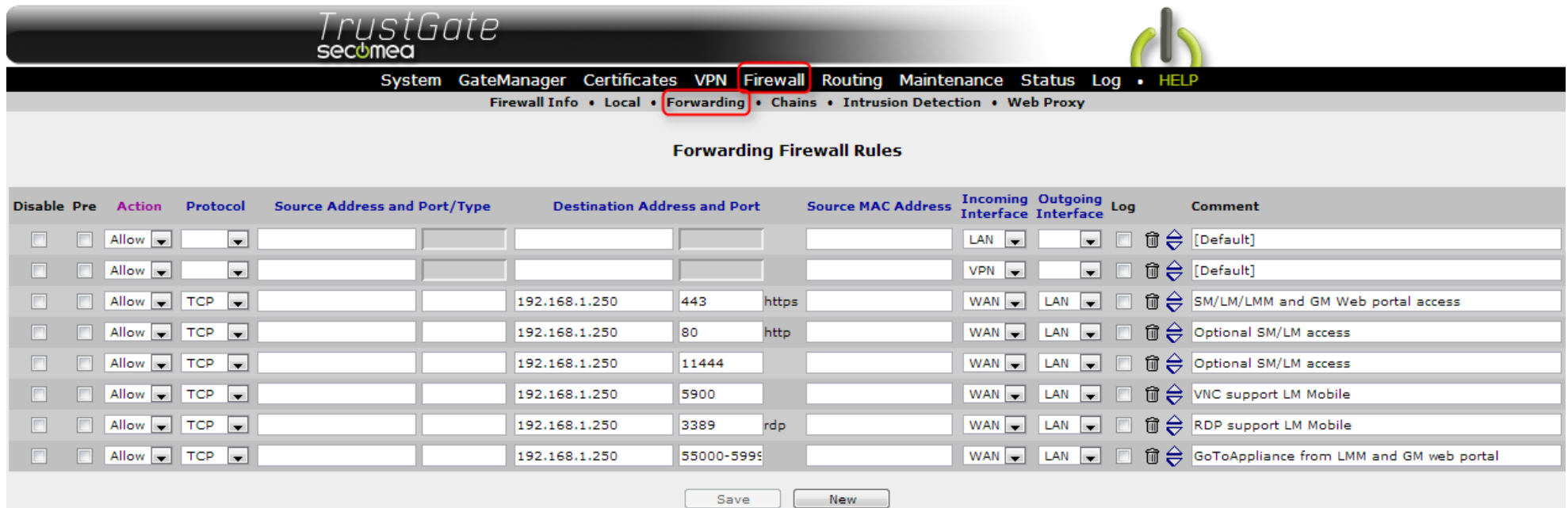
GateManager Server = 192.168.1.250

TrustGate LAN = 192.168.1.1

TrustGate WAN (GM public IP) = 80.212.2.8

D1. Configure Firewall rules

Create forwarding firewall rules for opening up access from the Internet to the GateManager WAN ports listed in section 3.1 **Configuring your corporate firewall**.



The screenshot shows the TrustGate Firewall configuration interface. The 'Firewall' menu item is highlighted in red. The 'Forwarding Firewall Rules' section displays a table of rules. The first rule is a default rule allowing all traffic from LAN to WAN. The subsequent rules are specific rules for allowing access to various ports on the WAN interface from the LAN interface.

Disable	Pre	Action	Protocol	Source Address and Port/Type	Destination Address and Port	Source MAC Address	Incoming Interface	Outgoing Interface	Log	Comment
<input type="checkbox"/>	<input type="checkbox"/>	Allow					LAN		<input type="checkbox"/>	[Default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow					VPN		<input type="checkbox"/>	[Default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 443	https	WAN	LAN	<input type="checkbox"/>	SM/LM/LMM and GM Web portal access
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 80	http	WAN	LAN	<input type="checkbox"/>	Optional SM/LM access
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 11444		WAN	LAN	<input type="checkbox"/>	Optional SM/LM access
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 5900		WAN	LAN	<input type="checkbox"/>	VNC support LM Mobile
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 3389	rdp	WAN	LAN	<input type="checkbox"/>	RDP support LM Mobile
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 55000-59999		WAN	LAN	<input type="checkbox"/>	GoToAppliance from LMM and GM web portal

Buttons: Save, New

- You could decide to replace the first rule that allow full access from the LAN to the Internet, with specific ports required by the GateManager according to the list of outgoing port in section 3.1 **Configuring your corporate firewall**.

D2. Configure NAT rules

Create Destination NAT rules that translate access to the TrustGate WAN port (GateManager Public IP address) to the GateManager's WAN port:

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Translation Address and Port	Comment
<input type="checkbox"/>	Translate	TCP		80.212.1.8 444	snpp WAN	192.168.1.1 443 https	TrustGate Web GUI
<input type="checkbox"/>	Translate	TCP		80.212.1.8 443	https WAN	192.168.1.250 443 https	SM/LM/LMM and GM Web portal
<input type="checkbox"/>	Translate	TCP		80.212.1.8 80	http WAN	192.168.1.250 80 http	Optional SM/LM access
<input type="checkbox"/>	Translate	TCP		80.212.1.8 11444	WAN	192.168.1.250 11444	Optional SM/LM access
<input type="checkbox"/>	Translate	TCP		80.212.1.8 55000-59999	WAN	192.168.1.250 55000-59999	GoToAppliance from LMM and GM Web portal
<input type="checkbox"/>	Translate	TCP		80.212.1.8 443	https LAN	192.168.1.250 443 https	SM/LM/LMM and GM Web portal from LAN
<input type="checkbox"/>	Translate	TCP		80.212.1.8 55000-59999	LAN	192.168.1.250 55000-59999	GoToAppliance from LMM and GM Web portal from LAN

- The first rule ensures that if you enter the address `http://80.222.1.8:444` in a browser, you can reach the WEB GUI of the TrustGate itself from the Internet.
- Rules number 2-5 ensure that you can reach the GateManager server from the Internet based on the ports described in section **3.1 Configuring your corporate firewall**.
- Rules number 6-7 ensure that you can reach the GateManager on the public IP address, from a PC or SiteManager in the LAN behind the TrustGate. You can add similar rules to also allow the remaining ports (80, 11444, 5900 and 3389)

Create Source NAT rules that translate access to the TrustGate WAN IP (GateManager Public IP address) to the GateManager.

TrustGate
secu^omea

System GateManager Certificates VPN Firewall **Routing** Maintenance Status Log • HELP

Routing Info • General • Static Routes • **Source NAT** • Destination NAT • QoS Classification

Source NAT

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface	Translation Address and Port	Comment
<input type="checkbox"/>	Translate				WAN*		[Default]
<input type="checkbox"/>	Translate	TCP	192.168.1.0/24	192.168.1.250 443	https LAN		SM/LM/LMM and GM Web portal from LAN
<input type="checkbox"/>	Translate	TCP	192.168.1.0/24	192.168.1.250 55000-59999	LAN		GoToAppliance from LMM and GM Web portal from LAN

Save New

- The first rule is default included in the TrustGate, and ensures that LAN devices (including the GateManager) can reach the Internet.
- The next rules ensure that you can reach the minimum ports of the GateManager from a PC or SiteManager in the LAN behind the TrustGate. You can add similar rules to also allow the remaining ports (80, 11444, 5900 and 3389).
- Note that the Source Address defines the LAN subnet as source (in this case 192.168.1.0 mask 255.255.255.0). If not limiting the source addresses to the LAN only, the connections from the WAN would be source NATed too, and the GateManager would risk confusing certain types of incoming connections for which it uses the source address to distinguish them.

D3. Allow or limit access to the TrustGate WEB GUI

You should decide if access should be allowed from the Internet to the TrustGate Web GUI. This is controlled by the last rule in this list (This is the factory default configuration of the Local Firewall Rules).

The screenshot shows the TrustGate web interface. The top navigation bar includes 'System', 'GateManager', 'Certificates', 'VPN', 'Firewall', 'Routing', 'Maintenance', 'Status', 'Log', and 'HELP'. The 'Firewall' menu item is highlighted with a red box. Below the navigation bar, the breadcrumb trail is 'Firewall Info > Local > Forwarding > Chains > Intrusion Detection > Web Proxy'. The main heading is 'Local Firewall Rules'. Below this is a table with the following columns: 'Disable', 'Pre', 'Action', 'Protocol', 'Source Address and Port/Type', 'Destination Address and Port', 'Incoming Interface', 'Log', and 'Comment'. There are four rows of rules. The last rule is 'Allow' on port 443 for https traffic, with the comment 'Enable TrustGate web GUI access'. At the bottom of the table are 'Save' and 'New' buttons.

Disable	Pre	Action	Protocol	Source Address and Port/Type	Destination Address and Port	Incoming Interface	Log	Comment
<input type="checkbox"/>	<input type="checkbox"/>	Allow				LAN	<input type="checkbox"/>	[Default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow				VPN	<input type="checkbox"/>	[Default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		113	ident	<input type="checkbox"/>	[Default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		443	https	<input type="checkbox"/>	[Default] Enable TrustGate web GUI access

- Even if you have defined the destination rule to access the Web GUI of the TrustGate on another port (such as 444 used in this example and defined in the translation NAT rule one), you should still use the translated port (443) in the local firewall rules to control the access.
- Even if you disable the last rule, or you set the incoming interface to WAN, which would prevent access to the TrustGate Web GUI from the Internet, you can still access the TrustGate Web GUI on the LAN address of the TrustGate on port 443. Also you can reach the TrustGate Web GUI via Go To Appliance from another GateManager regardless of the setting of this rule.

APPENDIX E. Recover lost Server Administrator password

If you have lost your root administrator account information (ref. section 5.7), you can reactivate the default GateManager Server Administrator account via the Serial port of the GateManager.

Preparation

You will need to connect a computer to the Console port on the front of the GateManager using a null-modem cable (DB9 Female to Female).

If you are using a Windows computer you can with advantage use the HyperTerminal application or a similar telnet application. If your computer does not have a physical COM port, you can use a USB-to-Serial adapter.

Serial parameters are: 4250-38400 4260-115200 baud, 8 bit, 1 stop bit, no parity, no flow control.

DB9-Female	DB9-Female
Pin 2	Pin 3
Pin 3	Pin 2
Pin 4	Pin 6
Pin 5	Pin 5
Pin 6	Pin 4

Null-modem cable pin layout

Recovery procedure

1. In your terminal application, press Enter and the menu will show on the screen if the application is configured and connected correctly.
2. Initiate the recovery procedure by typing:

recover

```
EXT3-fs (sdb1): mounted filesystem with ordered data mode
e2fsck 1.41.12 (17-May-2010)
/dev/boot: clean, 14/9984 files, 334/9969 blocks

Please press Enter to activate this console. pcnet32 0000:02:00.0 eth0: link up
>
The following commands are available:

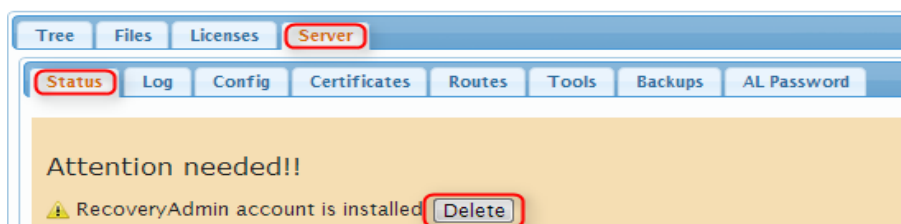
  recover      Install recover admin account
  reset        Reset the configuration to factory default
  reboot       Reboot the appliance
  status       Show system status
  ping        Ping a target

recover

-----
Created RecoveryAdmin account with well-known password.

Remember to delete the account on Server > Status page as soon
as you have recovered the server administrator account.
-----
>
```

3. The server has now created a recovery login. The account credentials are:
Username: RecoveryAdmin **Password:** gatemanager
4. Now, you are able to change any user's password, and resend their certificate. Once completed, delete the RecoveryAdmin from the Server > Status menu:

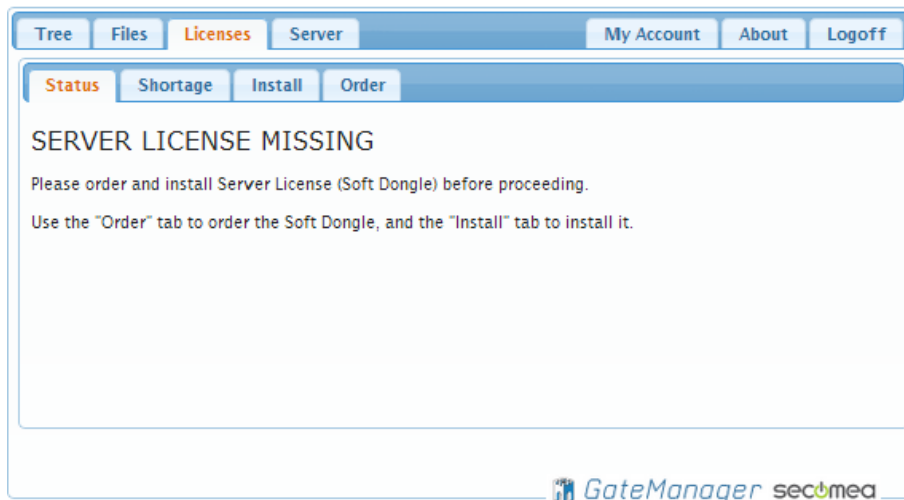


APPENDIX F. Manual installation of licenses

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:



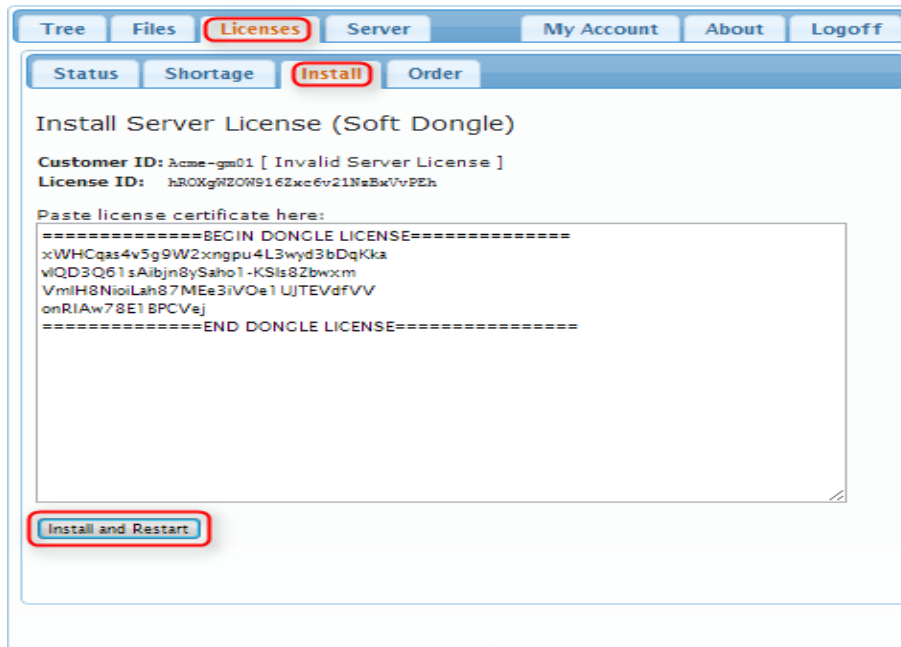
You will have received the ordered licenses as attachments to an email from the License Portal.

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=====
ya1HcPNuNudvepaE5Tc6gTMZ13T8kAqh
h1bINUs-clpdn5tfQmE6Q-nrHLR2ic4b
NC1ta8BmGkBe4navWEph34wOezVx
=====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

 4 licenses

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	-

The soft dongle will always include a “Max. Appliances” license 9001:777 with a value from 25-5000 according to the ordered GateManager maintenance 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=====  
YSNQ1sPB261KThI4nqNa2sbuByi1ddUZ  
Bm-eYuHYMgX391FwnD1O-gYkhrhqj1Wa  
51sk-ZFI  
=====END LICENSE UPGRADE=====
```

Notices

Publication and Copyright

© Copyright Secomea A/S 2013-2016. All rights reserved.

You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from the contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

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 A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com