

GateManager 8250 Setup Guide - Debian

Introduction

The following example of Linux preparation is based on a VM (Virtual Machine) using 64bit Debian 10.2.0, and a fully working internet connection with an IP address accessible from the Internet and all ports forwarded to the server.

System

Minimum system requirements

These are the minimum system requirements; these numbers include both Debian 10 (Buster) and GateManager Requirements.

Install Type	CPU	RAM	Storage
No Desktop	1.7 GHz - 2 Cores	2 Gigabytes	32 Gigabytes

Recommended system requirements

These are the recommended system requirements; these numbers include both Debian 10 (Buster) and GateManager Requirements. These requirements aim to ensure future proof stability.

Install Type	CPU	RAM	Storage
No Desktop	3 GHz - 2 Cores	4 Gigabytes	50 Gigabytes or more

GateManager domain requirements

A **Fully Qualified Domain Name** (FQDN) is required for a normal installation. The FQDN must be publicly registered (ex. gm.<your company>.com) and have a DNS A-Record pointing to the Public IP-Address of the GateManager Server.

If your GateManager is an "offline" GateManager, meaning you do not have a FQDN/Public IP, you must contact Secomea Support at support@secomea.com.

Downloading Debian 10 (Buster)

You may need to install a C++ 32-bit library (See more under "Package Requirements")

Debian can be downloaded for free [HERE](#) For this guide we will be using the "Small CDs or USB Sticks" 64-bit image files, more about the different versions can be found [HERE](#) and on the linked download page. (32-bit is also supported)

Getting Started

Change the Linux Password (Not Required)

This step is only required if you chose a generic or non-secure password during your install of Debian. If you chose a secure password or accept the risks of using an insecure password, please skip this step.

Login to the server with your SSH client. If configuring from Windows, we recommend [PuTTY](#).

Use the following command to initiate password reset:

```
passwd
```

Cleaning up Linux (Debian)

You should disable all per-installed non-critical services and remove non-critical packages, you can read more about Debian non-critical packages [HERE](#).

Services you should make sure is running are:

`crond`, `gatemanager`, `iptables**`, `network`, `ntpd`, `sendmail*`, `sshd`

(*) Or other mail service, such as postfix

(**) Only required if you do not have a firewall before the GateManager (May also be replaced with other firewall services)

Prepare Network Configuration / Physical Server Location

What ports are used by GateManager 8250

IMPORTANT

- Source NAT: The GateManager requires the source IP and therefore it's highly recommended to not use Source NAT on devices talking to the GateManager. This is especially true for the GTA Ports and account login logging.
- Proxies and Certificates: It is not possible to use Proxies like "Zscaler" that manipulates certificates, if you are using a proxy that manipulates certificates you might experience SiteManagers are unable to connect.
- Proxies and TLS: It is not possible to use proxies that manipulates TLS Client hello packets, if you use such proxy you might experience SiteManagers are unable to connect.
- Port Forwarding: Set appliance port as 443 in GateManager Configuration and Port Forward 80, 443 and 11444 to 443 in the Firewall towards the GateManager.

SiteManagers and LinkManagers connect to the GateManager Server public IP address on

TCP port 443 (standard https/TLS), 80 (standard TLS over http) or 11444 (Secomea ACM /TLS).

If using an outer Internet firewall / NAT router it must be configured to forward all incoming connections on a fixed public IP address, or at least connections to port 443, to the GateManager Server private IP address.

GateManager Administrator Web portal also connects to the GateManager Server on TCP port 443. **IMPORTANT:** If placed behind a NAT router, it must NOT do masquerading of incoming connections. The GateManager must be able to determine the original source IP. Through the administrator Web portal, the administrator can take access to the web interface of SiteManagers, LinkManagers and web enabled devices connected to the SiteManagers. This feature uses TCP port range 55000- 59999, and for this feature to work from the outside, the NAT router must be configured to forward incoming connections to these ports to the corresponding ports on the GateManager Server.

Local IP Address – If the Linux OS receives its IP address from a local DHCP server, the DHCP server must be configured to always provide the same local address.

Public IP Address - A publicly accessible IP address must be assigned to the GateManager Server. It is recommended that a Reverse-DNS record is assigned to this IP address. This will prevent most of the spam-filters/systems to block alert and account emails from the GateManager Server. Contact you ISP or IP address provider for details.

Configuring your Firewall

IMPORTANT: The GateManager **MUST** be firewall protected. If the GateManager Server is directly attached to the Internet, or all ports are forwarded to the GateManager from the Internet, then the build-in firewall on the Linux system must be enabled.

The following ports must be forwarded or "Destination NATed" from the public IP address to the Linux (Debian) System's local IP address. All other ports should be blocked to prevent unauthorized use.

The ports are marked as follows:

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

BLUE: Ports that must be opened for obtaining optimal functionality

GREEN: Recommended, but only needed for special scenarios

From *Outside* to *Inside*

Protocol	Outside	Inside	Description
TCP	80	11444 (or 80)	Appliance
TCP	443	11444(or 443)	Appliance/Web GUI
TCP	11444	11444	Appliance
TCP	55000-59999	55000-59999	Go To Appliance (GTA)
TCP	5900	5900	VNC Support LM Mobile
TCP	5800	5800	JavaVNC Support LM Mobile
TCP	3389	3389	RDP Support LM Mobile

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 used for LinkManager Mobile. The ports are controlled and secured by the GateManager and are NOT to be compared with common JVNC, VNC and RDP access to a PC. Only the validated LinkManager Mobile session that requests a connection will be allowed access.

From *Inside* to *Outside*

Protocol	Port	Description
TCP	25	SMTP/Mail*
TCP	21	For FTP backup to external server
TCP	443	For license control and Web Proxy**
TCP/UDP	53	DNS*
TCP/UDP	123	NTP*

(*) If the GateManager Server is using a DNS server or NTP server or an internal SMTP server for relaying emails – then these ports are not necessary to open.

(**) Can be restricted towards gm00.secomea.com (193.242.155.100)

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

You can follow the official guide on how to use Debian Firewall [HERE](#)

GateManager Installation

Package Requirements

These packages are the minimum required packages to run Debian and GateManager

You can see the table below for the different packages and how to install them or run the following command to install all packages.

```
apt-get install -y gawk gzip zip unzip tar grep coreutils perl
openssl net-tools telnet psmisc sendmail wget lib32stdc++6
```

Table of packages:

Package Name	Install Command	Link
--------------	-----------------	------

GNU awk	apt install -y gawk	https://packages.debian.org/buster/gawk
gzip	apt install -y gzip	https://packages.debian.org/buster/gzip
zip	apt install -y zip	https://packages.debian.org/buster/zip
unzip	apt install -y unzip	https://packages.debian.org/buster/unzip
tar	apt install -y tar	https://packages.debian.org/buster/tar
grep	apt install -y grep	https://packages.debian.org/buster/grep
uname	apt install -y coreutils	https://packages.debian.org/buster/coreutils
perl	apt install -y perl	https://packages.debian.org/buster/perl
base64	apt install -y coreutils	https://packages.debian.org/buster/coreutils
openssl	apt install -y openssl	https://packages.debian.org/buster/openssl
netstat	apt install -y net-tools	https://packages.debian.org/buster/net-tools
dirname	apt install -y coreutils	https://packages.debian.org/buster/coreutils
logger	apt install -y bsdutils	https://packages.debian.org/buster/bsdutils
telnet**	apt install -y telnet	https://packages.debian.org/buster/telnet
killall	apt install -y psmisc	https://packages.debian.org/buster/psmisc
sendmail	apt install -y sendmail	https://packages.debian.org/buster/sendmail
ip	apt install -y iproute2	https://packages.debian.org/buster/iproute2
wget	apt install -y wget	https://packages.debian.org/buster/wget
ftp*	apt install -y ftp	https://packages.debian.org/buster/ftp
lib32stdc++6	apt install -y lib32stdc++6	https://packages.debian.org/buster/lib32stdc++6

(*): The "ftp" package is only required if you are using FTP Backup

(**): The "telnet" package is only required during install and can safely be removed after.

Get the GateManager 8250 Installer and Install the GateManager

You need sudo/root permissions to run some of the following commands. If you are not root and do not have access to the "sudo" command. Please contact your IT-Department

Download the latest GateManager 8250 Installer (For Linux) file from the Secomea Firmware site found [HERE](#), and upload the file to the GateManager server (by using a program like WinSCP, FileZilla or alike).

You can also use "wget" to download the GateManager 8250 Installer to your server.

This can be done by using the following command:

```
wget --content-disposition https://firmware.secomea.com/download/gatemanager/8250/XX
```

To download the newest version of GateManager 8250 please run the following command instead:

```
wget --content-disposition https://firmware.secomea.com/download/gatemanager/8250
```

Once you have file on your server go to the folder where the file is located and run the following commands:

```
tar -xvzf Secomea_GateManager_Installer_x.x.xxxxx.tgz
```

Run the install script using the following command:

```
./RUN_GM_INSTALLER
```

```
lsadmin@SEC-GM-01 ~]$ sudo ./RUN_GM_INSTALLER
=====
GateManager (TM)
Copyright (c) 2003 - 2019, All rights reserved.
=====
Checking prerequisites...
Required programs:
GNU awk      : OK
id           : OK
gzip        : OK
zip         : OK
unzip       : OK
tar         : OK
gftp       : OK
uname      : OK
perl       : OK
base64     : OK
openssl    : OK
netstat    : OK
dirname    : OK
logger     : OK
telnet     : Not found
killall    : OK
ip         : OK
sendmail   : OK
===== ERROR =====
Required programs missing:
telnet
Please update your server before continuing.
=====
```

If any required programs are missing, you can find the list and how to install them under "Minimum Package Requirements".

In this example telnet is missing so we will need to install it before we can continue with the install.

Run the GateManager installer again to verify any other missing programs. When all programs are available the installer will prompt for continuing:

```
-----
| GENERAL TERMS
|
| In relation to general use of the Secomea solution, you should refer
| to the terms presented to you at first time login to the GateManager
| Portal.
|
| *** BY CONTINUING WITH THE INSTALLATION, YOU ACCEPT THESE TERMS. ***
|
|-----
Do GateManager installation found
Do you want to install GateManager 9.0.19405 [Y/n]
```

You will then be prompted to fill the Server identity information. This is the information the GateManager license will be based on, and if the information is insufficient your application for a license may be rejected.

```
Server Identity
-----
You must provide the following information to uniquely identify this
GateManager server for license and authorization purposes.
Company Name: The name of your company (e.g. Acme Inc.).
Department: The organizational unit running the server (e.g. Service).
Country Name: The name of your country (e.g. Denmark).
Country Code: The standard two-letter code for your country (e.g. DK).
City: The location of the server (e.g. Copenhagen).
Email: Email for the server administrator (e.g. support@acme.com).
Keyword(s): Description of the purpose of the server (e.g. Remote Service).
If you are running more than one GateManager server, you should use
different keywords for each server to uniquely identify each server.
```

Example:

```
Company name: [Secomea]
Department: [Support]
Country/state name: [Denmark]
Country code: [DK]
City: [Herlev]
Email: support@secomea.com
Keyword(s): Secomea GateManager Support
Please verify the information you have entered:
Company Name: Secomea
Department: Support
Country Name: Denmark
Country Code: DK
City: Herlev
Email: support@secomea.com
Keyword(s): Secomea GateManager Support
Is this information correct [Y/n]
```

When done, you will be prompted if you want to start the GateManager.

If you want to start the GateManager at a later point you can use the command:

```
gm start
```

```
Is this information correct [Y/n] y
Generated new local CA certificate.
Finalizing Software installation...
Installing /etc/init.d/gatemanager startup script
Scheduled daily backup of the database via cron
Software installation complete.
You must install a soft-dongle license for this server to complete
the software installation. See the installation notes for more information.
You can continue to use the server without a soft-dongle license, but you
cannot install any license upgrades to support additional users or devices.
Start GateManager now [Y/n]
```

Check the server is running with the following command.:

```
telnet localhost 777
```

Then run the following command:

```
status
```

```
~$ telnet localhost 777
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
Master: Management console opened from 127.0.0.1
GateManager version: 9.2.620087463
Server time: Mar 17 10:25:04 2020
+242425 31> status
GateManager version: 9.2.620087463
Database usage: 4897 KB of 250 MB
Connected: 31 (81 agents) of 528
Active UI conn: 28 (total 0)
UI servers: 44
WEB servers: 0 (total 5162)
Agent: Connected to Local GateManager at [redacted] (acm)
Agent: Connected to Service GateManager at 193.242.155.100 (t1s)
```

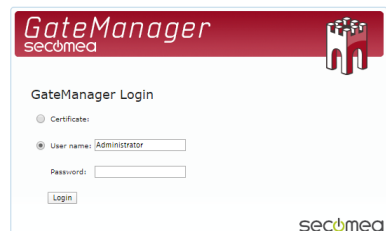
In this case you can see that the server is connected to the Secomea audit GateManager.

If you are connected to the same local network, you would now be able to connect to the GateManager Administrator Portal with a Web browser.

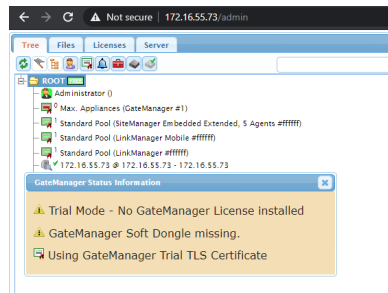
We recommend the web browser Chrome for best user experience or alternatively Firefox, Safari or Microsoft Internet Explorer (minimum version 9).



Write "Administrator" in the "User name" field and fill out the "Password" field with the default password "gatemanager".



The Portal window, will inform about missing licenses and certificates

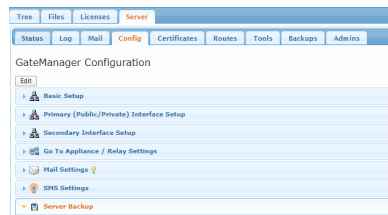


- **Trial Mode.** This indicates that the GateManager does not have a unique TLS certificate installed. The GateManager will be fully functional. Installing a TLS certificate will give your GateManager a unique identity, which increases the security, as your SiteManager will then be bound to this server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

Post Installation Tasks

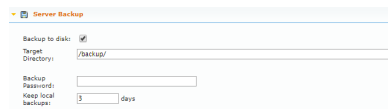
How to enable Backup

Go to Server > Config > Server Backup and click the "Edit" button.



Backup to a local disk

Ensure "Backup to disk" is enabled and then specify the target directory for the backup.



Backup to an FTP Server

Enable FTP Backup by check marking the "FTP Backup" field.

Fill out the following information:

FTP Host: The target FTP Server's FQDN or IP

FTP Directory: The folder where the backup is placed

FTP User

FTP Password

Checkmark "Toggle Passive" if *Passive FTP* mode is required.



Backup to an SMB Share

Enable “SMB Backup” by check marking the “SMB Backup” field.

Fill out the following information:

SMB Share: Path to the target share (e.g. //10.10.10.10/backup/)

SMB Directory: The sub folder where the backup is placed

SMB User

SMB Password

SMB Workgroup



SMB Backup:

SMB Share: //10.10.10.10/backup

SMB Directory: /gmbackup/

SMB User: smbuser

SMB Password: [REDACTED]

SMB Workgroup: [REDACTED]

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.

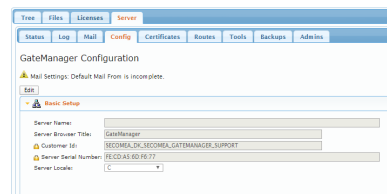
Configuring GateManager environment settings

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

Define a Server Name and Browser Title

Login with the default administrator account

Select **Server > Config** and select **Edit** for the **Basic Setup** section.



GateManager Configuration

Mail Settings: Default Mail From is incomplete.

Basic Setup

Server Name: [REDACTED]

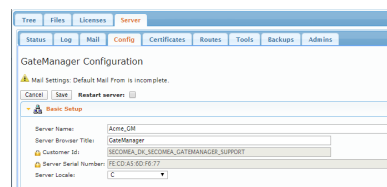
Server Browser Title: GateManager

Customer Id: SECOMEA_SIC_SECOMEA_GATEMANAGER_SUPPORT

Server Serial Number: RECDDA3-60D76-77

Server Locale: C

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**.



GateManager Configuration

Mail Settings: Default Mail From is incomplete.

Basic Setup

Server Name: Acme_GM

Server Browser Title: GateManager

Customer Id: SECOMEA_SIC_SECOMEA_GATEMANAGER_SUPPORT

Server Serial Number: RECDDA3-60D76-77

Server Locale: C

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.

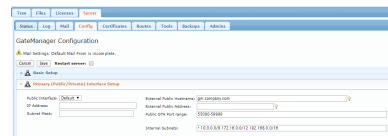
DNS and NTP settings are configured based on Linux (Debian) settings. To change these settings you must change the Linux settings. Read more about how to setup both here: [DNS Guide](#) - [NTP Guide](#).

Enter the Public Hostname

- 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.
- If there is no FQDN assigned to the server it is not possible for Secomea to automatically install new licenses – Contact Secomea for more Information

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

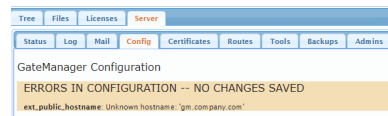
Do NOT select Restart server yet!



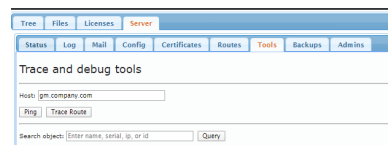
Possible error messages:

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.

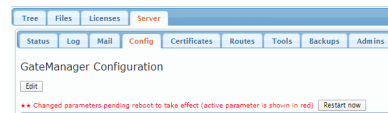
In this case, you will have to contact the IT administrator responsible for the GateManager installation and/or check the Linux (Debian) DNS and NTP Settings.



You can use the Tools menu to speed up the troubleshooting process



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

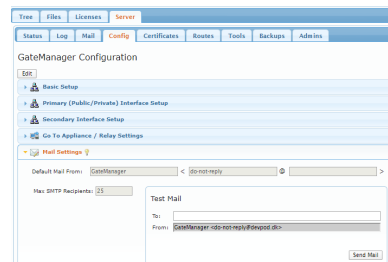


Configure mail settings

The ability to send email is required for the GateManager!

GateManager 8250 always uses the Linux systems mail client to either send or relay mails. It is not configured in the GateManager menus, normally sendmail or alike is used.

We recommend using Postfix, you can read more about configuring Postfix [HERE](#). For sendmail, you can find more at sendmail.org



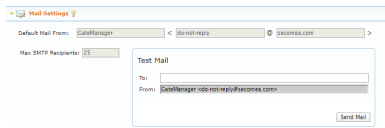
You can use the Test Mail to test your email configuration

Refer to the light bulb for further explanation.

Test mail settings.

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

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



The resulting email would look like this:



Hello

This is a GateManager Mail Test message

The quick brown fox jumps over the lazy dog

0 1 2 3 4 5 6 7 8 9

äöü êèáò æðå ÅÖÀ

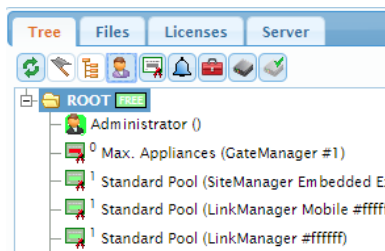
Best Regards

GateManager Server Administrator

Setup Server Administrator account(s)

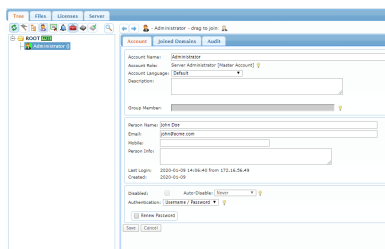
It is highly recommended to change the default Server Administrator account password (gatemanager), to something stronger. It is also advisable to enable two factor logins for the account by changing Authentication from "Username and Password" to "Certificate / Password".

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.



Click on the Administrator account and insert your own name and email for the account.

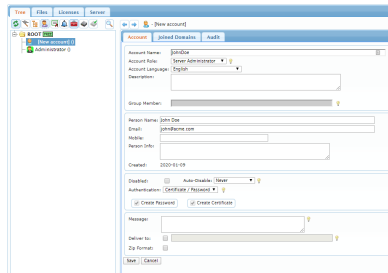
Select Save.



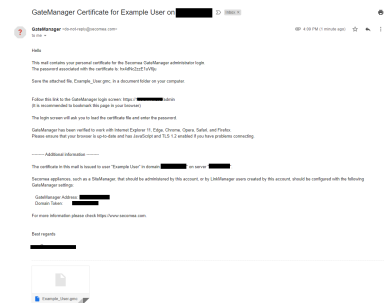
Standing in the Root domain, select Accounts and click the plus sign to create a new account:



Fill in the following minimum settings as shown below and click "Save":



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 enable certificate authentication for it, we do however recommend disabling the default Administrator account.

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

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).

You will need to install an activation license (aka Soft Dongle) to remove the trial pop-up and remove the appliance limit and allow the GateManager to be used for production purposes.

This is done by Contacting your Local Distributor or Point of Purchase.

Installing Licenses

Activation License(s)

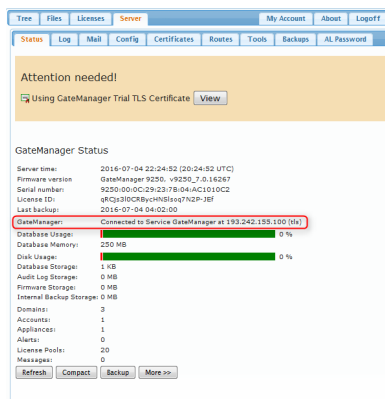
If the GateManager is online (connected to the Internet), Activation Licenses will automatically be installed on the GateManager by the License Portal.

Contact your local Distributor or Point of Purchase to purchase a GateManager license.

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.

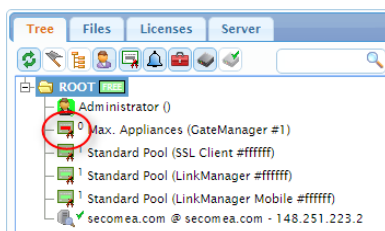
Check if the GateManager is Online Under Server Status:



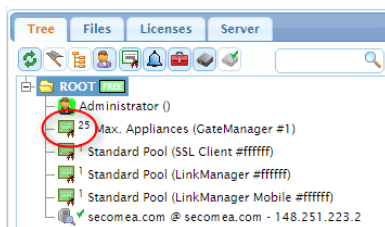
If your GateManager is not online, the email from the License Portal confirming the order will have the licenses attached for manual installation.

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.



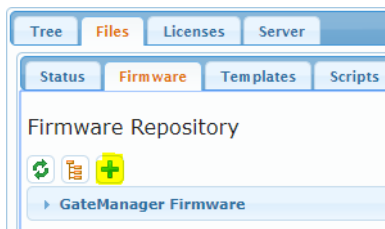
If additional licenses were ordered, they will also be visible in the “Tree” view

Updating your GateManager

Download the newest firmware for the GateManager 8250, which can be downloaded using the following link: <https://firmware.secomea.com/download/gatemanager/8250>

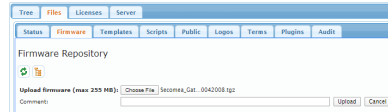
Upload the firmware to the GateManager Server via the web interface by doing the following:

Select Files > Firmware and then click green plus button



Then click “Choose file” button and select the firmware file you downloaded earlier.

Then click the "Upload" button.



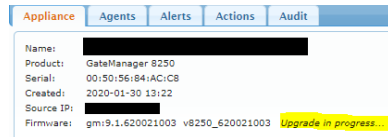
Then select the "Tree" menu and choose the GateManager server. Then click the "Upgrade" button.



Then click the "Upgrade" button next to the relevant firmware.



You will now notice the text "Upgrade in progress..." next to the Firmware version. Once the firmware is upgraded the GateManager Server will automatically reboot.



GateManager Commands

You can find all the GM Commands [HERE](#)