

GateManager™ Server 8250 Installation STEP 1

GateManager installation on Linux



This document describes how to install the Secomea GateManager 8250 software on a Linux platform.

The intended audience for this document is an IT administrator with intermediate Linux.

Version: 2.1, June 2014

Table of Contents

1. Introduction	3
1.1. Prerequisites for Installing According to this Guide	3
1.2. Difference between GateManager 8250 and 9250	3
1.3. Related Documents	3
2. Prepare Network Configuration / Physical Server Location	5
2.1. The principle of the solution (what ports are used for)	5
2.2. Configuring your Internet Firewall	6
2.2.1. From Outside to Inside:	6
2.2.2. From Inside to the Outside (Internet):	6
3. GateManager Installation Check List	7
4. GateManager 8250 installation	8
4.1. Verify Linux installation	8
4.2. Get the GateManager 8250 installer	8
5. Post Installation Tasks	12
5.1. Inform the appointed GateManager Administrator	12
5.2. Close the SSH configuration port (22)	12
5.3. Coordinate Backup of the Linux Server	12
APPENDIX A, Preserving the GateManager license	13
APPENDIX B, Nice to Know	14
Proper STOP and START of the server	14
Notices	15

1. Introduction

1.1. Prerequisites for Installing According to this Guide

This guide will assist you to plan for, and successfully complete the installation of the GateManager 8250 installer on a Linux platform.

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

- You have prepared and secured a Linux server. Refer to the guide GateManager Server 8250 Installation STEP 0, for requirements and information on the Linux platform.
- You have intermediate Linux skills.
- 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 your Internet firewall to direct traffic to and from the server.
- You have root access to a physical or virtualized Linux server.
- The Internet bandwidth available for the GateManager must be at least 128Kb/s.
- You have the ability/authority to arrange for outgoing mail traffic from the server.

1.2. Difference between GateManager 8250 and 9250

Secomea offers two versions of the software based GateManager:

- **Model 9250**, which is delivered as preinstalled virtual image based on a Linux platform that Secomea has adapted with the necessary services. This is the recommended version, but requires a VM platform (such as ESXi or HyperV) on which the image can be deployed. Some hosting centers do accept such customer provided images, others don't.
- **Model 8250**, subject for this guide, and which must be installed on a Linux platform, and where the Linux environment must be adapted to the GateManager. This version is required for installation on standalone servers, and for hosting centers that do not offer installation of a customer provided VM image, but instead provides a Linux OS with preinstalled services. Such hosting centers typically offer various Linux versions, among which Debian and CentOS are typical.

The following examples are based on a VPS (Virtual Private Server) with a 32bit CentOS 6.4, and fully working internet connection with an IP address accessible from the Internet and all ports forwarded to the server.

1.3. 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 centre, the VM image with a Linux installation with preinstalled hosting centre tools may be provided. This guide uses CentOS as example.

- **GateManager Server 8250 Installation STEP 1 (THIS GUIDE)**

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

- **GateManager Server Installation STEP 2**

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.

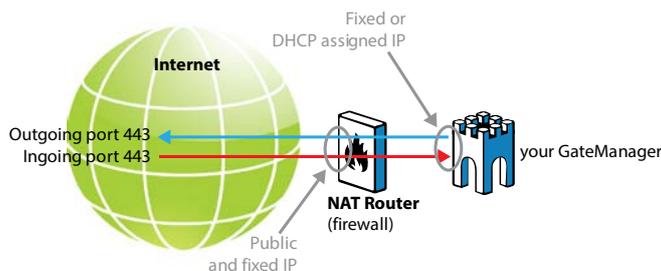
- **Customer and License Administration (for Secomea Distributors)**

This guide describes common daily tasks of creating accounts and how to manage LinkManager licenses.

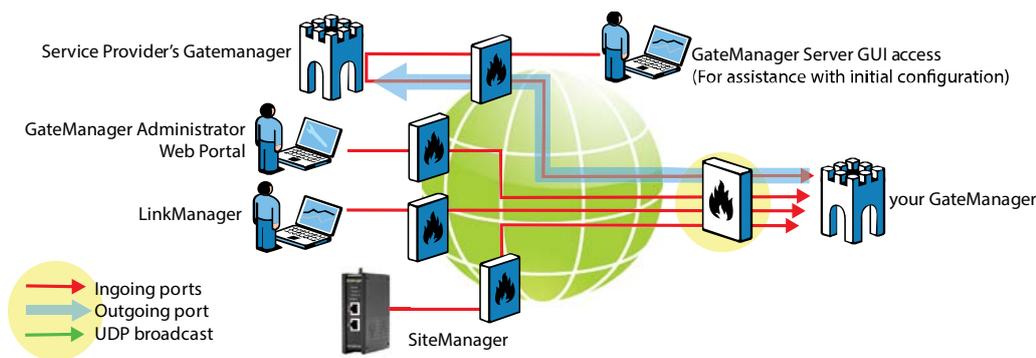
- **GateManager PREMIUM Domain Administration**

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

2. Prepare Network Configuration / Physical Server Location



2.1. The principle of the solution (what ports are used for)



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 public 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.

2.2. Configuring your Internet 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 (see the **STEP 0** guide for details).

The following ports must be forwarded or "Destination NATed" from the public IP address to the Linux 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 at all.

BLUE: Ports that must be opened for obtaining optimal functionality

GREEN: Recommended, but only needed for special scenarios

2.2.1. From	Outside	to	Inside:
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)

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.

2.2.2. From Inside to the Outside (Internet):

TCP	25	(SMTP/MAIL *)
	21	(For FTP backup to external server)
	443	(For license control and Web Proxy)
	80	(WEB Proxy **)
TCP/UDP	53	(DNS *)
	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.

(**) 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.

3. GateManager Installation Check List

Before you start the actual installation, it is advised to fill the following table so you have the minimum information ready at hand, and prevents you from getting stuck during the installation, and to not forget topics that should be followed up.

GateManager Installation Data		
<p>Information that must be informed to Secomea, for upgrading the built-in DEMO license to a Production license</p>	<p>The public Identification that the GateManager can be reached on from the Internet and which Secomea should create the Software License Dongle.</p> <p>Either a static IP address:</p> <p>Or a Fully Qualified Domain Name (FQDN), which has been publically registered (ex. gm.<yourcompany>.com).</p>	<p>_____</p> <p>_____</p>
	<p>During installation you will be promoted for a host-name for the GateManager Server. This must be formatted as FQDN but does not need to be publicly registered. (eg. gm.<yourcompany>.local)</p>	<p>_____</p>
	<p>Only if NOT using a mail server installed on the Linux OS with the GateManager: IP address of your SMTP(mail) server.</p> <p>You may also verify that the SMTP server is configured to allow relaying of emails from the GateManager server.</p>	<p>_____</p>
<p>Only if using a mail server on the Linux OS: Ensure that the public IP address - that has been assigned to the Linux System - has a reverse-DNS name appended (rDNS).</p> <p>It may work without, but there is a risk that mails from the GateManager Server will be considered as spam by the receiver.</p>		<p><input type="checkbox"/></p>
<p>NTP time server(s) if NOT using the ones pre-configured in the GateManager (pool.ntp.org):</p>	<p>_____</p> <p>_____</p>	
<p>DNS server(s) if NOT assigned by a DHCP server, and if NOT configured on in the Linux OS</p>	<p>_____</p> <p>_____</p>	
<p>Firewall has been opened with the required ports</p>		<p><input type="checkbox"/></p>

4. GateManager 8250 installation

4.1. Verify Linux installation

Verify that the proper firewall ports are open, that only the needed services are active, and that you have minimum 10GB available disk space for the GateManager installation (refer to the **STEP 0** guide for details)

The following illustrates the installation on Linux CentOS

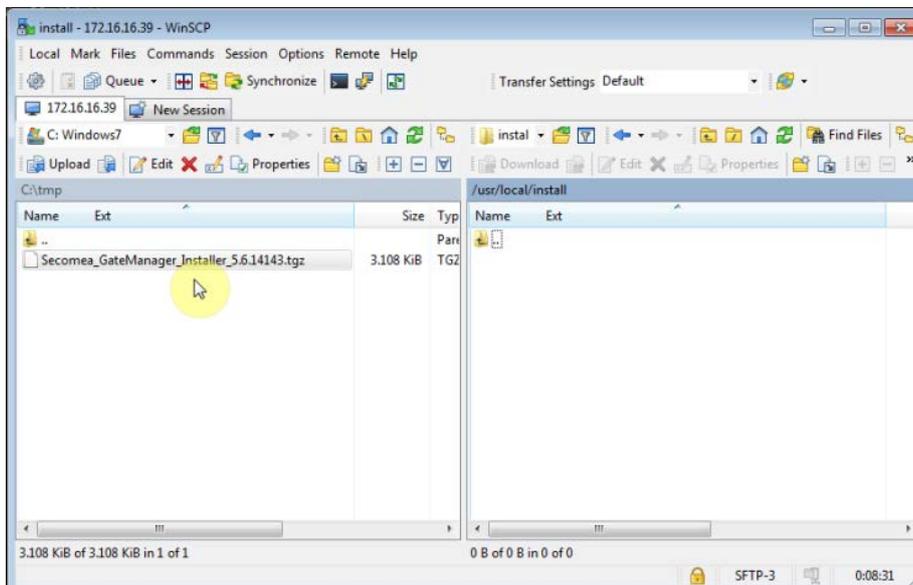
4.2. Get the GateManager 8250 installer

Download the latest GateManager v8250 Server Firmware tgz file from the Secomea support section:

<http://www.secomea.com/industry/support/gatemanager-software-and-documentation/>

Note that you must be logged in to the Secomea website for the download link to become active.

Copy the tgz file onto the server. There may be various ways to do that. One method is to use the freeware tool WinSCP, which is a combined SFTP, SCP and FTP client. With this you can create a folder on the server and simply drag the tgz file to the server (in this case we have made a folder called /usr/local/install):



On the server browse to the installation folder, and check that the file is present:

```
root@gm52:/usr/local/install
[root@gm52 /]# cd ..
[root@gm52 /]# cd usr/local/install/
[root@gm52 install]# ls
Secomea_GateManager_Installer_5.6.14143.tgz
[root@gm52 install]#
```

Unzip the file

```
# tar -xvzf Secomea_GateManager_Installer_5.6.14143.tgz
```

Run the install script

```
./RUN_GM_INSTALLER
```

The Installer will automatically check for needed programs.

```
[root@gm51 ins]# ./RUN_GM_INSTALLER
=====
                Secomea GateManager (TM)

        Copyright (c) 2003 - 2014, Secomea A/S, Denmark.
                All rights reserved.

=====

Checking prerequisites...

Required programs:
  GNU awk      :      OK
  id           :      OK
  gzip        :      OK
  zip         :      OK
  unzip       :      OK
  tar         :      OK
  grep        :      OK
  uname       :      OK
  perl        :      OK
  base64      :      OK
  openssl    :      OK
  netstat     :      OK
  dirname     :      OK
  logger      :      OK
  telnet      :      Not found
  ip          :      OK
  sendmail    :      OK

===== ERROR =====
Required programs missing:
  telnet
Please update your server before continuing.
=====
```

Install the needed programs. In this example telnet is missing:

```
# yum install telnet
```

Run the GateManager installer 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 read
| the General Terms here: http://info.secomea.com/terms-of-use
|
| *** BY CONTINUING WITH THE INSTALLATION, YOU ACCEPT THESE TERMS. ***
|
|-----
|
| No GateManager installation found
|
| Do you want to install GateManager 5.5.14143: [Y/n] █
```

Fill the Server identity information as accurate as possible. 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. Secomea).
Department:  The organisational unit running the server (e.g. Support).
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@secomea.com).
Keyword(s):  Description of the purpose of the server (e.g. Entry Backup).

If you are running more than one GateManager server, you should use
different keyword(s) for each server to uniquely identify each server.
```

```
Company name: Secomea
Department: Support
Country/state name: Denmark
Country code: DK
City: Kgs. Lyngby
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:        Kgs. Lyngby
Email:       support@secomea.com
Keyword(s):  Secomea GateManager Support

Is this information correct: [Y/n] _
```

When done, you will be prompted to start the GateManager

```
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] y
```

Check the running server with command line:

```
# telnet localhost 777
```

```
[root@gm52 install]# telnet localhost 777
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
master: Management console opened from 127.0.0.1

Gatemanager version: 5.5.14143
Server time: May 20 22:14:31 2014

+33 1> s
Gatemanager version: 5.5.14143
Database usage:      961 KB of 250 MB
Connected:          1 (0 agents) of 1
Active UI conn:     0 (total 0)
Audit ACM:          Connected to Audit GateManager at 193.242.155.111 (tls)
Local ACM:          Connected to Local GateManager at 172.16.16.39 (acm)
+39 1>
```

In this case you can see that the server is connected to the Secomea audit GateManager, and that the IP address of the local server is 172.16.16.39.

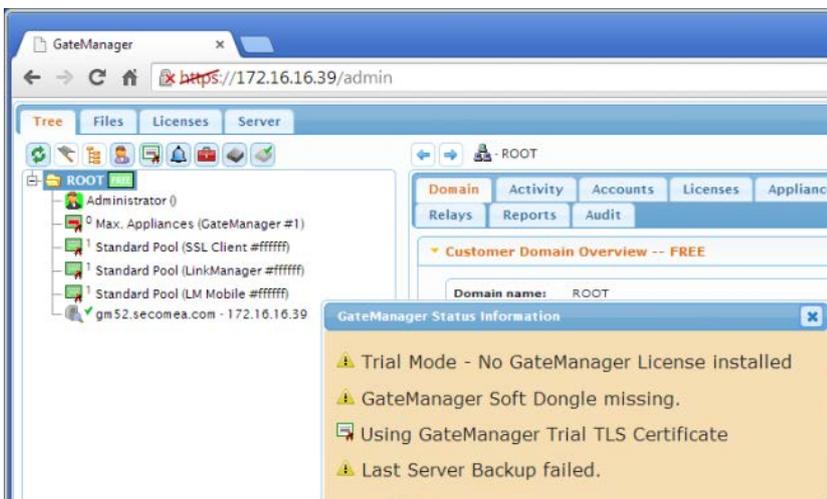
If you are connected to the same local network, you would now be able to connect to the GateManager Administrator Portal with a Web browser



Select user “Administrator” and login with the default password “gatemeager”



The Portal window, will inform about missing licenses and certificates



5. Post Installation Tasks

5.1. Inform the appointed GateManager Administrator

The server installation is finish and next step is for the GateManager Administrator to set up the GateManager server via the Web GUI.

You should pass on the following information:

1. The checklist sheet from section 3. This is needed in order to set up mail settings and determine the browser path to the GateManager
2. The new Linux password, ONLY if the GateManager administrator is intended to be administering the virtual image OS.

5.2. Close the SSH configuration port (22)

If the server was set up remotely, you may have opened for port 22 to the server from the public address. Ensure that this port is closed again, or that proper source IP check is made for connections to port 22.

5.3. Coordinate Backup of the Linux Server

The data of the GateManager itself is backed up by the integrated FTP backup feature configured in the GateManager Portal, and which is described in the STEP 2 guide.

You may have different preferences of backup depending on your usual backup strategies and is out of scope of this guide.

If you plan to backup a complete image of the server, you should ensure that the MAC address of the Linux installation does not change, as this is what the GateManager license is bound to. Refer to **APPENDIX A, Preserving the GateManager license** for details.

APPENDIX A, Preserving the GateManager license

GateManager licenses are associated with the MAC address of the GateManager Linux OS. So if you apply a backup strategy where you restore the entire Linux image, you should observe the following:

- If you are running directly on “bare metal”, and restore the Linux image including the GateManger on different hardware, the MAC address of the Linux image is likely to change. You should request your point of purchase for a replacement license based on the new MAC address. You may be subject for a sworn statement.
- If you are running a VPS in a hosting center, and you are restoring the backup image of the server, you would typically be able to preserve the binding to the MAC address of the virtual NIC (aka UUID). In the restore process you should make sure to keep the existing UUID, or define that the image was “moved” and not “copied”.

In order to ensure being able to preserve the UUID at restore, you may have to manually define a MAC address for the virtual machine, rather than letting it be auto assigned. On ESXi you may even have to manually edit the .vmx configuration file to define the MAC address as static.

NOTE: if the MAC address of the GateManager virtual image changes after the license key is applied (Ref. the STEP 2 guide), the GateManager will lose the licenses and only be operational in trial mode.

APPENDIX B, Nice to Know

Proper STOP and START of the server

If you need to stop or restart the host system it is recommended that the GateManager server is halted before the host system is taken down. See below.

Type:

```
# gm help
```

For a complete command list.

Note: As default the GateManager is installed as a service and will automatically start when the Linux system is started.

Stopping the GateManager Server:

```
# gm stop
```

Now you can safely take the Linux server down.

Notices

Publication and Copyright

© Copyright Secomea A/S 2012-2014. 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.

www.secomea.com

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. The combined body of work that constitutes CentOS™ is a collective work which has been organized by the CentOS™ Project, and the CentOS Project holds the copyright in that collective work; licensing is under the GPL. www.centos.org. 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 can not 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.