

GateManager™ Server model 9250 Installation STEP 1 for the IT department



This document describes how to install the Secomea GateManager Virtual Image.

The intended audience for this document is an IT administrator with intermediate Linux skills and knowledge about using virtual machines and TCP networking.

Version: 2.5, 2016

Applicable to GateManager version 5.8 or later

Table of Contents

1.	Prerequisites for Installing According to this Guide	3
1.1.	Related Documents	3
1.2.	Version history	3
2.	Prepare Network Configuration / Physical Server Location	4
2.1.	The principle of the solution (what ports are used for)	4
2.2.	Configuring your Corporate Firewall	5
2.2.1.	From Outside (*) to Inside:	5
2.2.2.	From Inside to the Internet:	5
3.	Fill in GateManager Installation Check List	6
4.	GateManager Virtual Images	7
4.1.	How to install:	7
4.2.	Successful installation	7
5.	Preserving the GateManager Licenses	8
6.	Local IP address of the GateManager	9
6.1.	DHCP assigned IP address	9
6.2.	Setting a Static IP address	9
6.2.1.	Using the GateManager Console	9
6.2.2.	Using the Appliance Launcher	9
7.	Verify Installation	12
8.	Post Installation Tasks	13
8.1.	Inform the appointed GateManager Administrator	13
8.2.	Coordinate Backup of the Server	13
APPENDIX A,	Backup and Restore	14
	Virtual image backup (one time event)	14
	Virtual image Restore	14
	VMware Player	14
	VMware ESXi Server:	14
	Hyper-V Server:	15
	Data backup (daily/weekly backup)	15
	Data restore (from the daily/weekly backup)	15
Notices		16

1. Prerequisites for Installing According to this Guide

This guide will assist you to plan for, and successfully complete the installation of a Virtual Image containing preinstalled GateManager server software.

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

- You have downloaded a virtual image from Secomea as either the OVA format (VMware, ESXi) or VHD format (Hyper-V) according to your chosen server platform.
- 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 access to a physical Workstation or Server, or a virtualized Server on which you have full administrator rights to install the image.
- 32 GB dynamic storage available for the image, and you have 1-2GB RAM allocated for the image.
- The Internet bandwidth available for the GateManager must be at least 128Kb/s.
- 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).

1.1. Related Documents

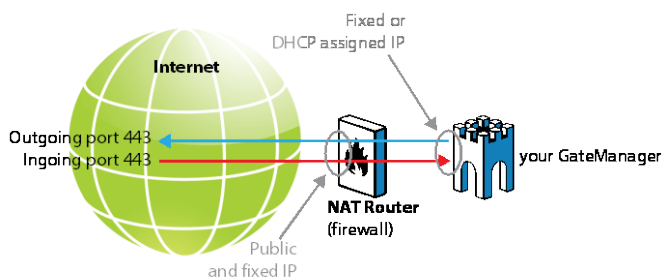
The following guides are available from the Secomea support website – support.secomea.com

- **GateManager Server 9250 STEP 1 (THIS GUIDE)**
Describes the installation of the server performed by the IT department.
- **GateManager Server 8250-9250 STEP 2**
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.

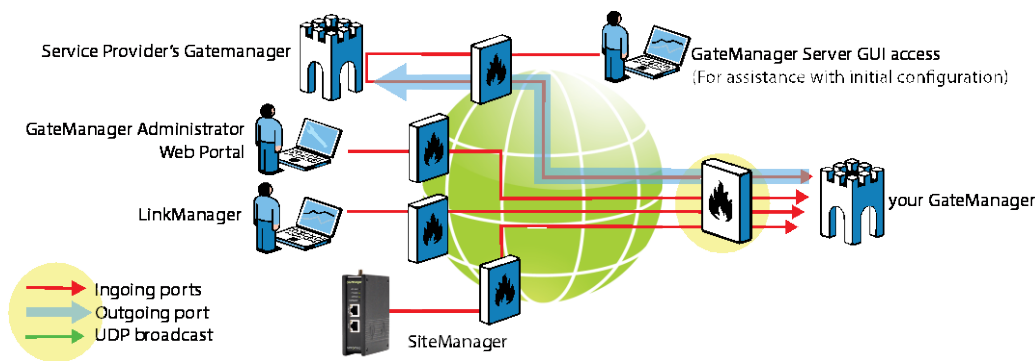
1.2. Version history

- 2.2 Initial version
- 2.3 Added TCP port 5800 in section 2.2.1 in relation to GateManager release 5.5 build 14123.
- 2.4 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.
- 2.5 New update to section 4 GateManager Virtual Image

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).

The Corporate firewall / NAT router must be configured to forward connections to preferably all, or at least port 443 to the GateManager Server private IP address.

GateManager Administrator Web portal connects to the GateManager Server on TCP port 443. A **NAT router** must be configured to forward connections to port 443 on the GateManager Server. **IMPORTANT:** The NAT router 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 through 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 port on the GateManager Server. The installation script will allow you to select a different port range.

DHCP Server - The GateManager System is by default configured as DHCP Client. Both DNS and default gateway is assumed to be provided by the company DHCP server. The DHCP server must provide the GateManager System with the same fixed private IP address that is used by the port forwarding rules in the NAT router. (A static IP can be set using the Appliance Launcher. See section 6 Local IP address of the GateManager).

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 Corporate Firewall

IMPORTANT: The GateManager MUST be protected by an external Firewall. If the GateManager Server is directly attached to the Internet then the build in firewall must be enabled. This is not part of this document.

The following ports must be forwarded or Destination NATed from the public IP address to the Linux System local IP address. All other ports should be blocked by the corporate firewall 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 for connecting by LinkManager Mobile. The port is controlled and secured by the GateManager and is NOT to compare with a common JVNC, VNC and RDP access to a PC. Only the LinkManager Mobile that request the connection will be allowed using this.

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

4. GateManager Virtual Images

The GateManager 9250 virtual images are provided as OVA and VHD files.

The OVA image supports most common systems compatible with the Open Virtualization Format. These are Hypervisor systems such as Virtual Box (www.virtualbox.org) and most VMware products (e.g. Player, Workstation, Fusion and ESXi)

The VHD image is specific to Microsoft Hyper-V products.

4.1. How to install:

For installing the OVA image simply follow the instructions according to the actual Hypervisor system.

For instance on VMware Player you select File > Open and follow the instructions on the screen. For VMware ESXi select from the vSphere Client the File and Deploy menu and follow the instructions on the screen.

For installing the VHD image look up the GateManager_Hyper-V-image.txt file contained in the GateManager9250-vhd-x.x.xxxx.zip file downloaded from the support.secomea.com web site. More information like supported Windows systems are maintained in this file.

4.2. Successful installation

Installing on any of the Hypervisor systems should result in showing the GateManager console.

```
/dev/flash: clean, 391/8388608 files, 571732/8387930 blocks
kjournald starting. Commit interval 5 seconds
EXT3-fs (sdb1): using internal journal
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. e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
random: tgdrandom read with 30 bits of entropy available

>
Unknown command.

The following commands are available:

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

random: nonblocking pool is initialized
```

From here you can continue to the next section.

5. Preserving the GateManager Licenses

Make sure that proper measures are taken to ensure that the MAC address of the GateManager virtual machine image does not change during operation. This could happen in case of fail-over setups, where the backup machine may assign a different MAC address to the virtual NIC. In rare cases it may also occur for a single server installation when recovering from a power failure.

Especially for ESXi - you should consider at this point to manually define a MAC for the virtual machine, but typically you would leave it at "Auto" and let VMware assign it automatically, which will in most cases work fine. If you want to ensure that the currently auto assigned MAC address is guaranteed for this virtual machine, you may consider manually editing the .vmx configuration file to define the MAC address as static. Consult the VMware knowledge base for procedures and syntax specific to your ESXi product and version. The same actions and considerations should be taken concerning any Hyper-Visor system.

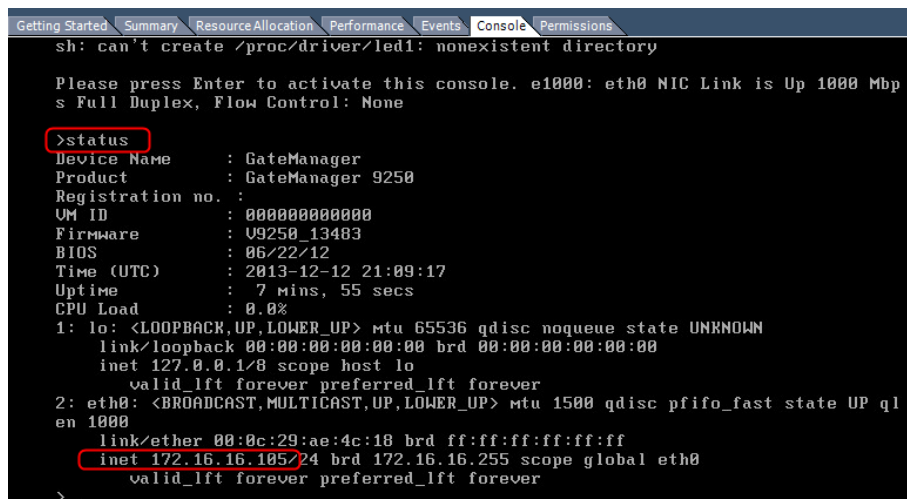
NOTE: if the MAC address of the GateManager virtual image changes after the license key is applied (Ref. the STEP 2 guide), the GateManager will lose the licenses and only be operational in trial mode.

6. Local IP address of the GateManager

6.1. DHCP assigned IP address

The GateManager is default configured as DHCP client and from the GateManager Console it is now possible to read the IP address:

Press <ENTER> and type **status**



```
Getting Started Summary Resource Allocation Performance Events Console Permissions
sh: can't create /proc/driver/led1: nonexistent directory

Please press Enter to activate this console. e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None

>status
Device Name      : GateManager
Product         : GateManager 9250
Registration no. :
UM ID           : 000000000000
Firmware        : U9250_13483
BIOS            : 06/22/12
Time (UTC)      : 2013-12-12 21:09:17
Uptime         : 7 mins, 55 secs
CPU Load        : 0.0%
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 00:0c:29:ae:4c:18 brd ff:ff:ff:ff:ff:ff
   inet 172.16.16.105/24 brd 172.16.16.255 scope global eth0
       valid_lft forever preferred_lft forever
>
```

6.2. Setting a Static IP address

If there is no DHCP server available for the GateManager installation or the IP address needs to be statically assigned, you can either use the GateManager Console or the Appliance Launcher to set a static IP address on the GateManager.

6.2.1. Using the GateManager Console

Pressing a key in the GateManager Console will bring up the console menu. From here you type 'config' <enter> and follow the instruction on the screen to set a static IP address.

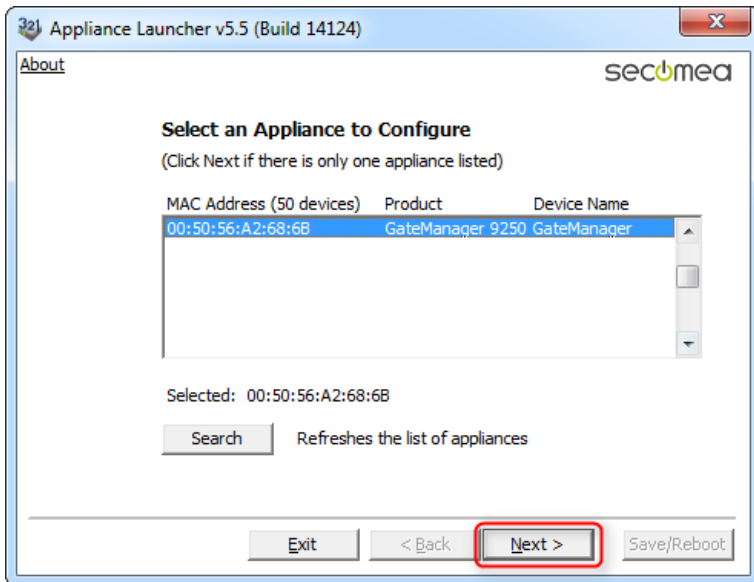
The 'factoryreset' command will reset the IP address back to DHCP mode.

6.2.2. Using the Appliance Launcher

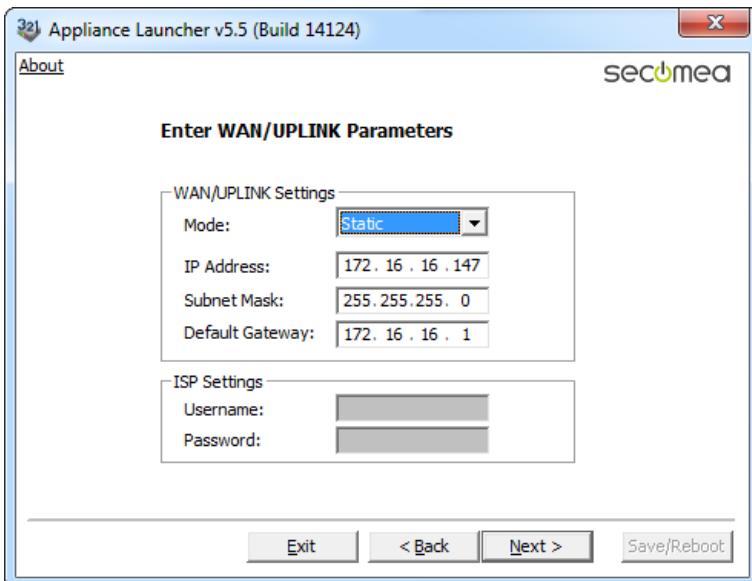
Download the free Appliance Launcher from support.secomea.com

(Appliance Launcher version 5.4 or newer is needed.)

For the Appliance Launcher to reach the GateManager it needs to be launched from a Windows PC on the same broadcast network as the GateManager.

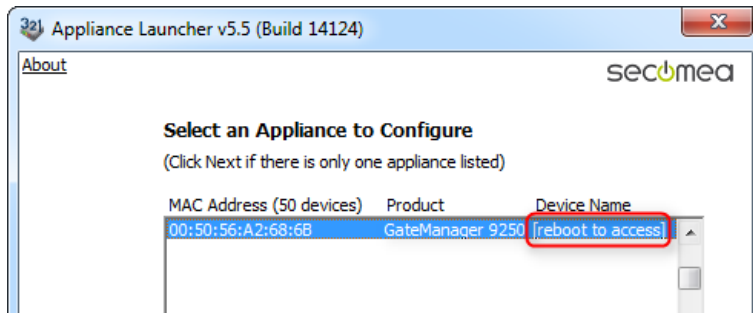


The Local GateManager IP address is entered as the WAN/Uplink address.



Troubleshooting hints

- If the GateManager is not shown when searching, it may indicate that you are not launching Appliance Launcher from a computer located in the same network as the GateManager, subsequently the broadcast cannot reach the GateManager.
- If the GateManager prompts for password, it may indicate that the GateManager has been operational and the Appliance Launcher (AL) password has been changed as described in the GateManager Portal (see the STEP 2 guide)
- The Appliance Launcher may show the GateManager marked with "reboot to access".



This is a security precaution that prevents access by the Appliance Launcher after 10 minutes, so the GateManager will not be interrupted during normal operation.

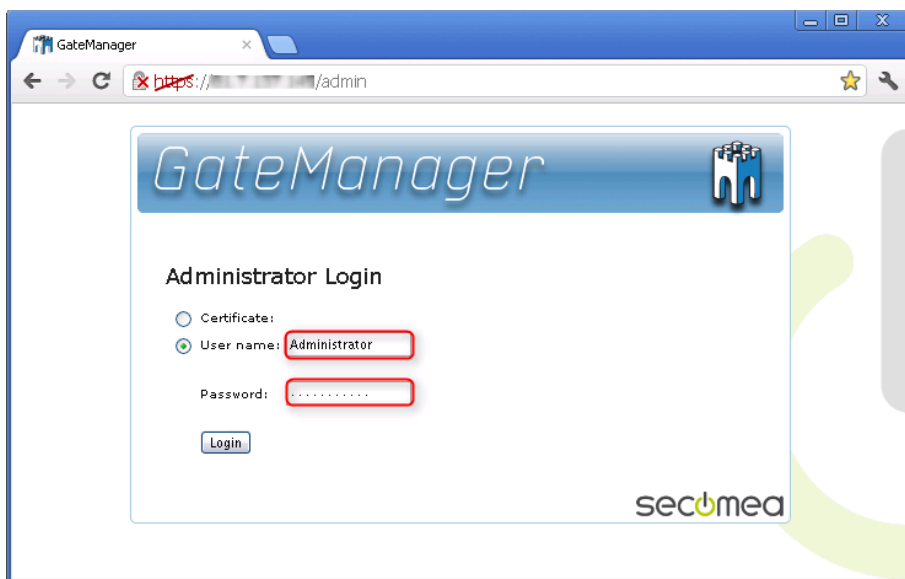
Just restart the GateManager virtual machine and press Search again until the GateManager appear with Device Name "GateManager"

Note: for Appliance Launcher versions older than 5.6, you will still be able to click Next and get the login prompt. This will, however, have no effect.

7. Verify Installation

The basic installation of the GateManager is complete and the GateManager Administration Web Portal should be possible to launch using the local IP address (see previous chapter):

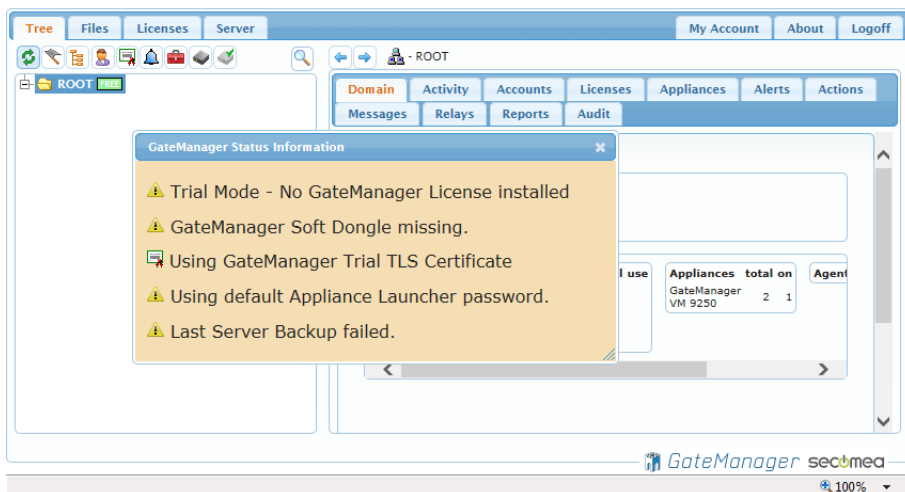
https://<local IP>/admin



Default login is

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

You should see a screen like this, which means the server is running as expected.



8. Post Installation Tasks

8.1. Inform the appointed GateManager Administrator

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

You should pass on the checklist sheet from section 3. This is needed in order to set up mail settings and determine the browser path to the GateManager

8.2. Coordinate Backup of the Server

Refer to Appendix A on how to coordinate a backup strategy with your appointed GateManager administrator.

APPENDIX A, Backup and Restore

Two different backups should be prepared:

1. One time backup of the virtual image
2. Daily/weekly backup of data

A full restore or reestablishing of the server would require reinstalling the backup version of the virtual image, followed by a restore of the latest data backup via the GateManager Administrator Web portal.

Virtual image backup (one time event)

Because the License key is bound to the UUID of the virtual image it is important that a copy of the virtual image is made just after the GateManager administrator has received the GateManager Soft Dongle from Secomea and installed it via the GateManager Administration Web Portal.

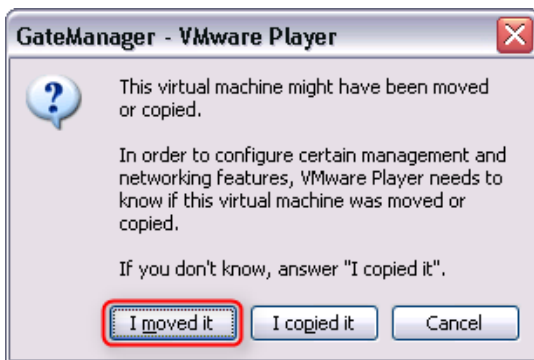
You must therefore coordinate with your appointed GateManager administrator that he informs you when this has been done.

Virtual image Restore

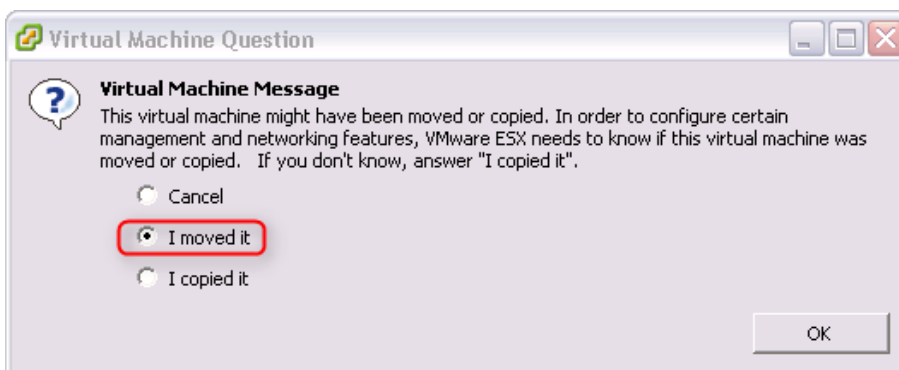
It is important to select the “move” option and NOT the “Copy”.

Following is screenshots from the various Virtual server products:

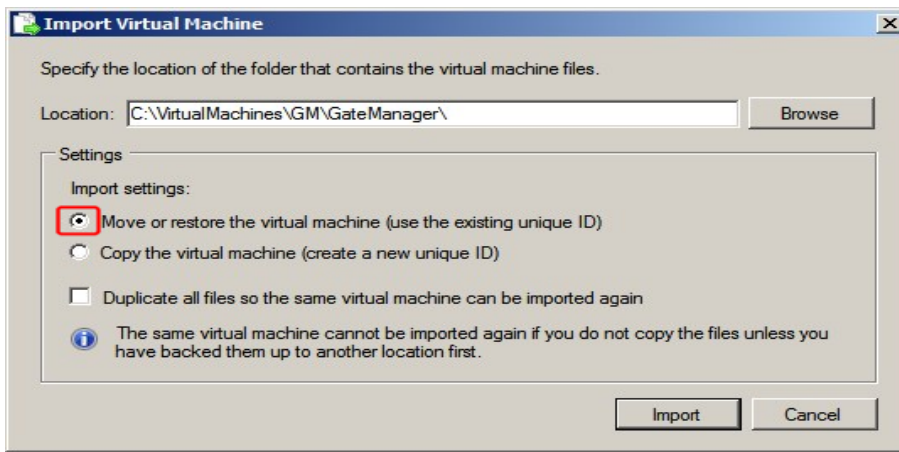
VMware Player



VMware ESXi Server:



Hyper-V Server:



Data backup (daily/weekly backup)

The Backup and Restore of the GateManager data is setup by the GateManager administrator in the GateManager Administrator Web Portal (ref. the STEP 2 guide)

This backup is based on a schedule that submits an archive of the database to a FTP server.

The GateManager administrator may ask for you help to establish a FTP server.

Data restore (from the daily/weekly backup)

Data restore is done by your appointed GateManager administrator by retrieving the latest backup file from the FTP server, and restore it via the GateManager Administrator Web Portal.

Notices

Publication and Copyright

© Copyright Secomea A/S 2012-2016. 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