

# Secomea GateManager BASIC Guide

## *Learning Secomea Remote Access*

### (Using SiteManager Embedded for Windows)







This guide is intended for first time users of the Secomea remote access solution, who need a practical introduction to the **Secomea GateManager BASIC** solution in relation to the **SiteManager Embedded (SM-E)** for Windows software

This guide will lead you through different roles and processes related to installing and configuring the **SiteManager**, **GateManager** Administration of users and using **LinkManager**.

**Version: 1.1. March 2015**

---

# Table of Contents

<b>1. Introduction</b>	<b>3</b>
1.1. Prerequisites for This Guide	3
1.2. Component Analogies	3
1.3. About Roles referred to in this Guide:	4
1.4. Illustration of Role locations	4
1.5. If something should not work out as expected	5
<b>2. Basic Setup and connection</b>	<b>6</b>
2.1. ROLE: SiteManager Embedded (SM-E) Installer 	6
2.1.1. SM-E Installation	6
2.1.2. Configure the GateManager settings.	7
2.2. ROLE: GateManager BASIC Admin 	10
2.2.1. Install the GateManager Administrator certificate	10
2.2.2. Create LinkManager user account	11
2.2.3. Create LinkManager Mobile user account.	13
2.2.4. Assign License to the the SM-E	14
2.3. ROLE: LinkManager User 	15
2.3.1. Install and login to the LinkManager	15
2.3.2. Connect to the PC via the SM-E	17
2.4. ROLE: LinkManager Mobile User 	20
2.4.1. Login and connect to a web GUI with LinkManager Mobile	20
<b>3. SM-E Basic - Adjusting Agents</b>	<b>23</b>
3.1. Connect to Device Agents section in the SiteManager GUI	23
3.2. Enable standard connect buttons for Agents	25
3.2.1. Example: Enable VNC button for the default Full Access agent	25
3.2.2. Connect to VNC Server with LinkManager Mobile	26
3.3. Using Agents with custom LinkManager Mobile connect buttons	27
3.3.1. Example: Create a new Pro-face Agent	27
3.3.2. Configure the Pro-face Remote HMI APP to connect via the Agent	28
3.3.3. Connect to the Pro-face agent with LinkManager Mobile	29
3.3.4. Connect with the Pro-face Remote HMI APP	30
<b>4. SM-E Extended – Accessing external devices</b>	<b>31</b>
4.1. Ordering SM-E Extended license (and other licenses)	31
4.2. Installing licenses on (own) GateManager	32
4.3. Upgrading SM-E Basic to SM-E Extended	33
4.4. Define device agent for external device	34
<b>5. Additional Features</b>	<b>37</b>
5.1. Upgrading your GateManager Administrator account from BASIC to PREMIUM (P/N 26473)	37
<b>Notices</b>	<b>38</b>



## 1. Introduction

### 1.1. Prerequisites for This Guide

Prerequisites for this guide are:

- You have administrator privileges to install a program on your Windows PC or laptop.
- Your PC has outgoing access to the Internet via https. This applies for both your corporate firewall and any personal firewall installed on your PC.
- You have a SiteManager Embedded (SM-E) license.
- You have a Windows machine to install SM-E on (supported platforms: Windows XP/7/8, Standard or Embedded)
- You have received, by email, a GateManager administrator certificate with a link to the GateManager web portal.
- Preferably you have a login account for the Secomea partner web site, for download of supplementary information on <http://info.secomea.com/RDM-documentation>. (if not choose **Register** at the top right of the Secomea web site)

### 1.2. Component Analogies

With the Secomea Remote Access solution you are introduced to three components. To place them into a context that you may be familiar with, we have made analogies to traditional modem solutions:




- **SiteManager.** This component compares to the traditional dial-up modem attached to the machine at the customer site. The big difference is that SiteManager utilize the existing network infrastructure to obtain Internet connection.
- **LinkManager Client Software.** This compares to the modem dial-up software on the service engineers' PC. The big difference is that the service engineer does not need to administer a list of phone numbers. The list of devices that the service engineer can connect to, is automatically updated when a new SiteManager and its configured "Device agents" are connected. Point and click and the LinkManager user get instant access to the device over the Internet.
- **GateManager Server.** This component acts as a switch-board for connections between LinkManagers and SiteManagers, and ensures that neither LinkManagers nor SiteManagers need to have public addresses on the Internet. For the BASIC package the GateManager is used only for administering users, but you can upgrade to a domain administrator account that allows you to check logs, fine grain LinkManager access to certain devices etc. (read more in section **5. Additional Features**)
- **Upgrading your GateManager Administrator account from BASIC to PREMIUM (P/N 26473)**



### 1.3. About Roles referred to in this Guide:

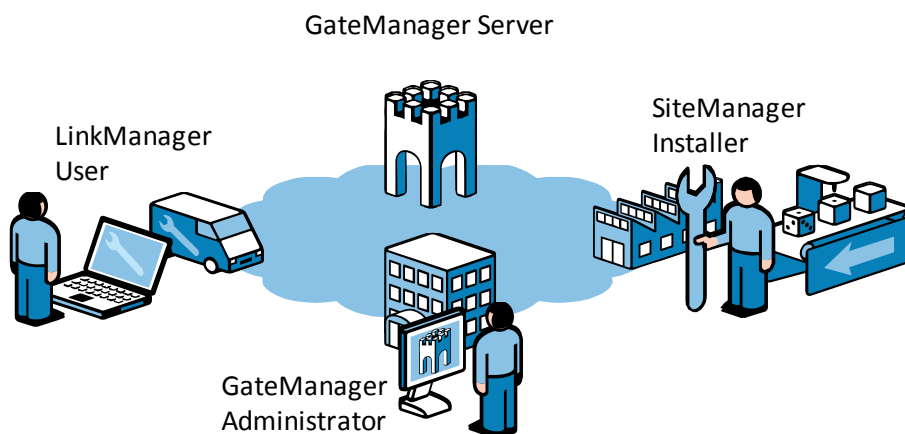
Through the document the header will indicate the role you are undertaking.

Roles will be marked as follows:

	<p><b>SiteManager Installer.</b></p> <p>This role covers the following tasks:</p> <ul style="list-style-type: none"><li>■ Physically Install SiteManagers (often done by the service engineer or the customer)</li><li>■ Configure network settings (primarily initial GateManager access)</li></ul>
	<p><b>GateManager BASIC administrator.</b></p> <p>This role covers the following tasks:</p> <ul style="list-style-type: none"><li>■ Assign licenses to connected SM-Es</li><li>■ Create and administering LinkManager user accounts.</li></ul>
	<p><b>LinkManager User.</b></p> <p>This role is held by the PLC programmer or service engineer:</p> <ul style="list-style-type: none"><li>■ Connect remotely to equipment for servicing/programming the equipment.</li><li>■ Optionally configure the SiteManager and devices agents on the SiteManager, if not done by the SiteManager Installer role.</li></ul>

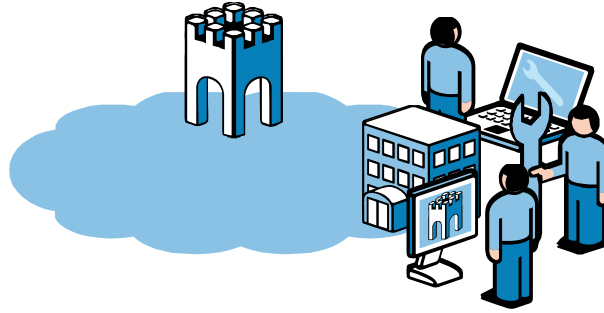
### 1.4. Illustration of Role locations

The typical setup of the relative to the Internet would be like this:





However, following this guide for the first time, you will probably play all roles and be physically located more like this:



### 1.5. If something should not work out as expected

We experience that this guide works for 95% of all users, whereas the last 5% may be subject for a little more advanced configurations depending on special infrastructure setup.

The solution does allow for adaptation to highly complex and security restricted infrastructures involving e.g. a Web proxy or NTLM authorization server, but it is out of scope of this guide to elaborate on.

If you run into problems, then do not hesitate to contact us a call and we will guide you in the right direction, or help you troubleshoot.

You can also consult our document library here:

<http://www.secomea.com/industry/support/documentation/>

or the FAQ section here:

<http://www.secomea.com/industry/support/faq/>



## 2. Basic Setup and connection

This section explains the basic installation and configuration of SM-E and accounts, for making full access to the PC on which the SM-E is installed.

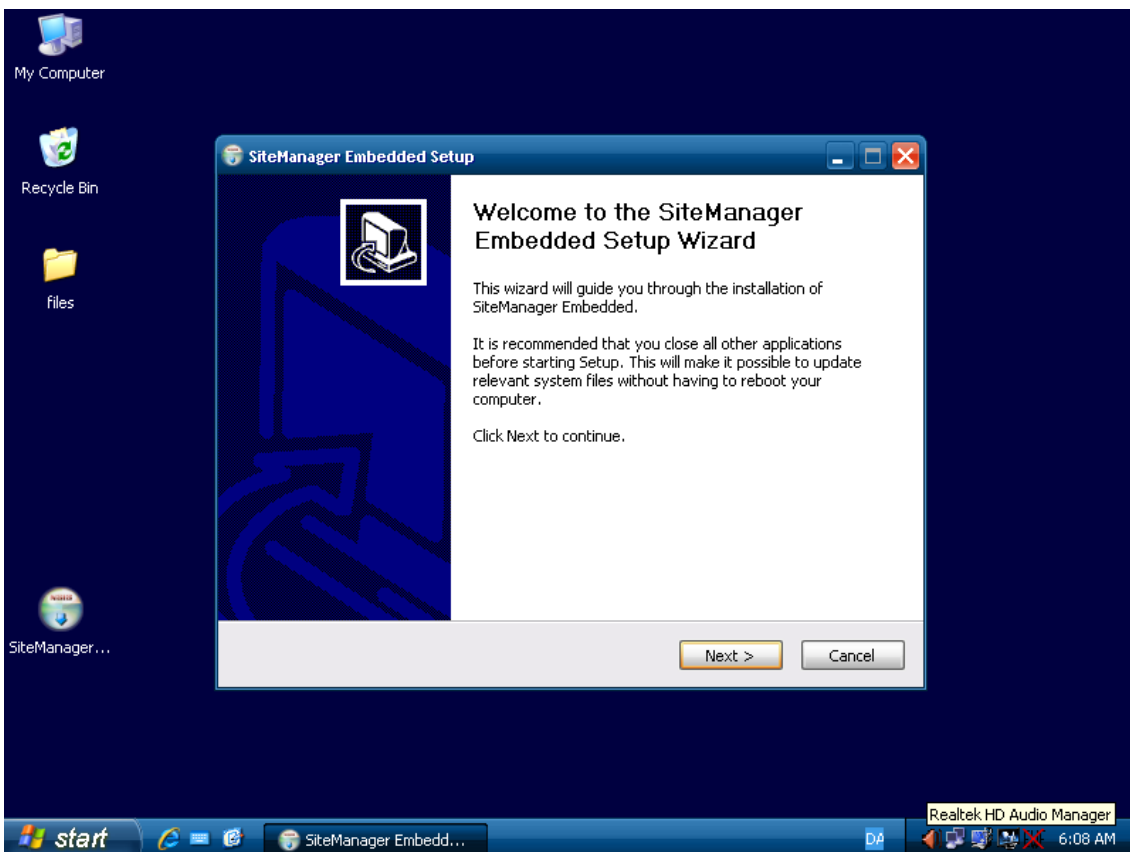
### 2.1. ROLE: SiteManager Embedded (SM-E) Installer

Download the SM-E from this location:

<http://info.secomea.com/sme>

#### 2.1.1. SM-E Installation

1. Copy the SiteManager Embedded exe files onto the Windows machine on which it should be installed.
2. Run the exe file and click Next > until finished.



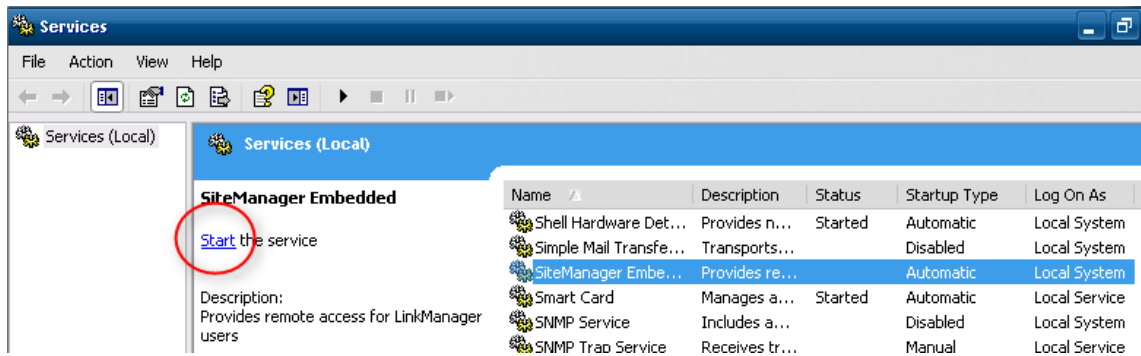
3. A Web browser should open automatically with the SM-E SETUP Assistant.

**NOTE:** If a browser does not automatically open, it may be that the SM-E service has not started (this may happen on Windows XP Embedded).

- a. In that case you should restart the Windows machine, which will automatically start the service, or you can start the service manually. Select Start -> Run and type the command `services.msc`.



- b. Scroll to the SiteManager Embedded and click **start**

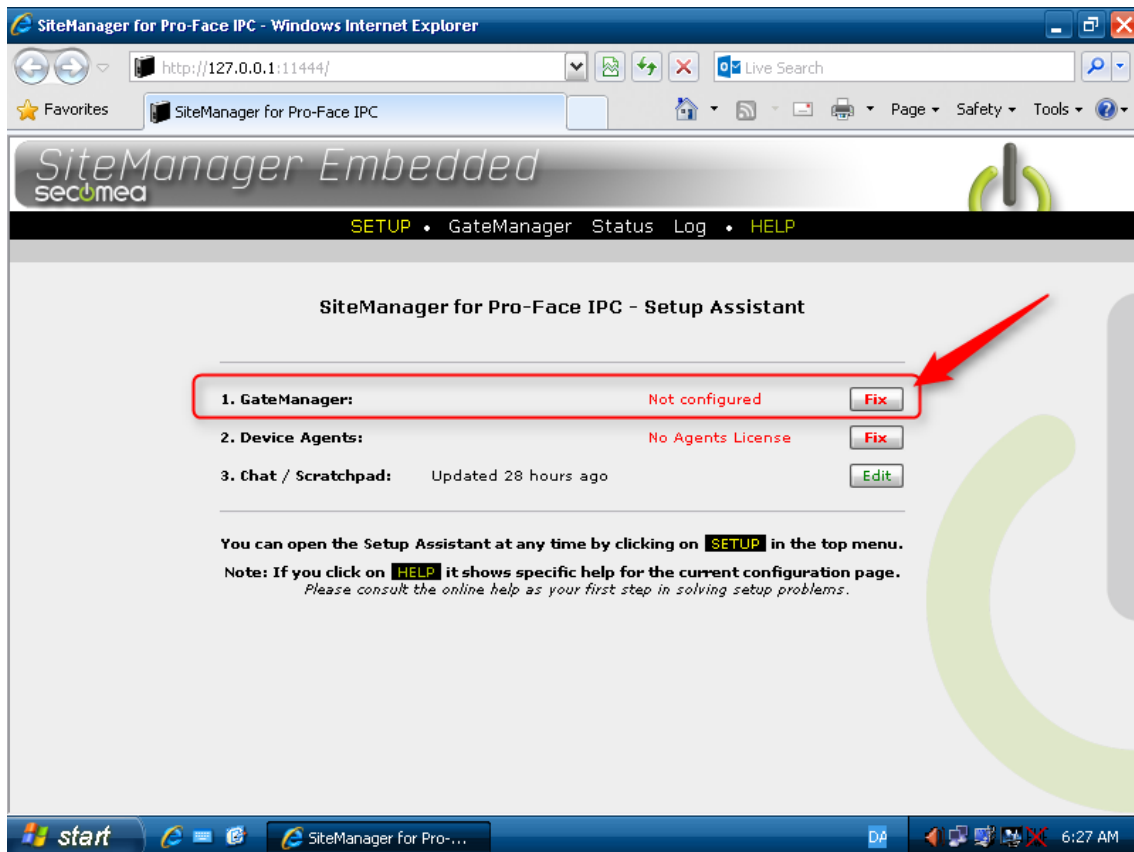


- c. Now click the SM-E shortcut on the desktop to open the SM-E Web GUI:



### 2.1.2. Configure the GateManager settings.

4. In the SM-E Web click the Fix button for the GateManager settings:





5. Enter the GateManager Server name and Token.

SiteManager Embedded  
secomea

SETUP • GateManager Status Log • HELP

GateManager **not** connected.

Remote Management: Enabled

Go To Appliances: Automatic Login

Appliance Name: SiteManager

Domain Token: \* SecomeaVar **2**

GateManager Address: \* 193.242.155.117 **1**

Web-proxy Address:

Web-proxy Account:

Web-proxy Password:

**IMPORTANT:** The information to enter in this screen is found in the lower section of the email you received from the GateManager with the GateManager X.509 Certificate.

**GateManager X.509 Certificate for JohnJohn on Secomea VPNLAB GM5\_ESXi**  
do-not-reply@secomea.com  
Sent: 09-02-2014 21:23  
To: [redacted]

Message | JohnJohn.gmc (3 KB)

Hello John John

This mail contains a new X.509 certificate for the Secomea GateManager administrator login. The password associated with the certificate will be informed to you verbally or in a separate mail.

Save the attached file, JohnJohn.gmc, in your Windows "My Documents" folder.

Follow this link to the GateManager administrator login screen:  
<https://gm07.secomea.com/admin> (or alternatively:  
<https://193.242.155.117/admin>).

It is recommended to bookmark this page in your browser. The login screen will ask you to load the certificate file and enter the password.

GateManager has been verified to work with Internet Explorer 9 (IE8 also works), Google Chrome, Apple Safari, and Mozilla Firefox. Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

----- Additional information -----

The certificate in this mail is issued to user "JohnJohn" in domain "SecomeaVar" on server "Secomea VPNLAB GM5\_ESXi".

Secomea appliances, such as a SiteManager that should be administered by this account or by LinkManager users created by this account, should be configured with the following GateManager settings:

GateManager Server: 193.242.155.117 **1**  
GateManager Token: SecomeaVar **2**

For more information please check [www.secomea.com](http://www.secomea.com)





- Click **Save** and **Connect**, and click the **refresh** icon periodically

GateManager **not** connected. 3

Remote Management: Enabled

Go To Appliances: Automatic Login

Appliance Name: SiteManager

Domain Token: \* SecomeaVar

GateManager Address: \* 193.242.155.117

Web-proxy Address:

Web-proxy Account:

Web-proxy Password:

1 \* = Mandatory field 2

Save More >> Connect

- After a short while the status should change to this:

GateManager connected: 193.242.155.117:443 (LAN) Not Attached!

Remote Management: Enabled

Go To Appliances: Automatic Login

Appliance Name: SiteManager

Domain Token: \* SecomeaVar

GateManager Address: \* 193.242.155.117

Web-proxy Address:

Web-proxy Account:

Web-proxy Password:

*You do not need to do more local to the SM-E.*

*In reality you could now ship the Windows machine to a new site.*

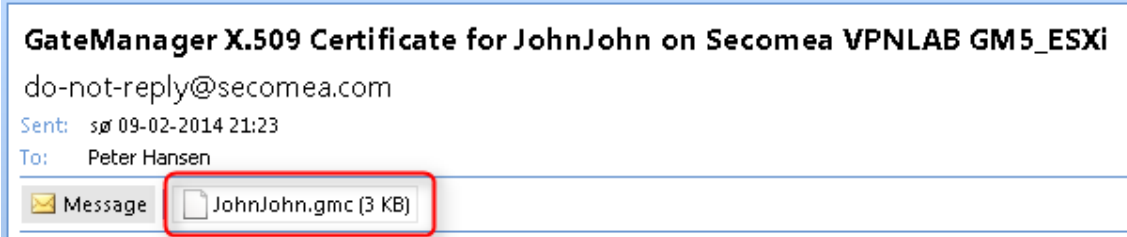
*Once the Windows machine is connected to a network that has Internet access, the SM-E will automatically connect to the GateManager*




## 2.2. ROLE: GateManager BASIC Admin

### 2.2.1. Install the GateManager Administrator certificate

8. Locate the email you received from the GateManager with the **GateManager Certificate**, and save the attached file to your hard disk:



**GateManager X.509 Certificate for JohnJohn on Secomea VPNLAB GM5\_ESXi**  
do-not-reply@secomea.com  
Sent: sø 09-02-2014 21:23  
To: Peter Hansen

Message  JohnJohn.gmc (3 KB)

Hello John John

This mail contains a new X.509 certificate for the Secomea GateManager administrator login.  
The password associated with the certificate will be informed to you verbally or in a separate mail.

Save the attached file, JohnJohn.gmc, in your Windows "My Documents" folder.

Follow this link to the GateManager administrator login screen:  
<https://gm07.secomea.com/admin> (or alternatively:  
<https://193.242.155.117/admin>).

It is recommended to bookmark this page in your browser. The login screen will ask you to load the certificate file and enter the password.

GateManager has been verified to work with Internet Explorer 9 (IE8 also works), Google Chrome, Apple Safari, and Mozilla Firefox.  
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

9. Open the link in the same email. (There may be two links with a DNS name and IP address respectively and you can use either of them)



This will open the login screen of the GateManager:



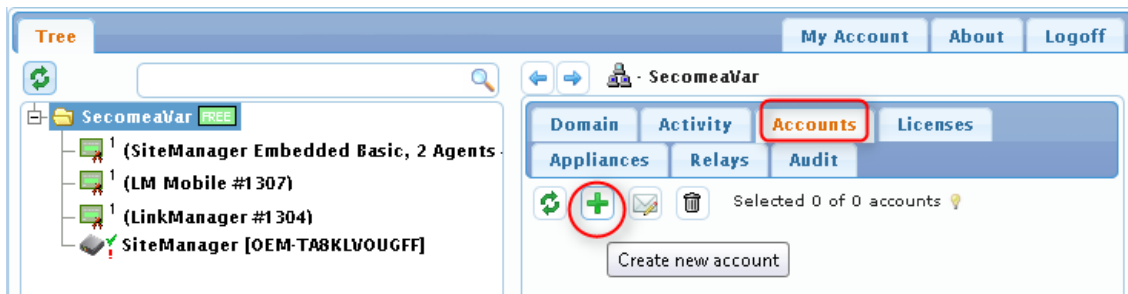
**Note:** The GateManager administrator portal requires minimum MS Internet Explorer 9, Apple Safari, FireFox or Google Chrome.

10. Browse for the certificate you just saved, and enter the password you were informed by the administrator.

If you have not yet received the password via email, SMS or verbally, you should take contact the person that is listed in the **signature section** of the email with the certificate (do not hit reply on the email, as it is auto-generated from the GateManager)

### 2.2.2. Create LinkManager user account

11. When logged in select the **Accounts** tab, and select the “+” icon to create a new account





12. Fill in the following information

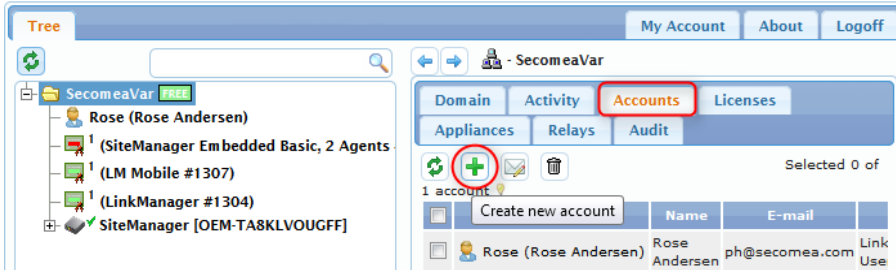
- ❶ The **Account name**. This will become the file name of the LinkManager certificate file (in this case Rose.lmc)
- ❷ **Person Name, Email** and optionally **Mobile** number. In this exercise you will likely issue the account to yourself. You can later create accounts for other users. (All users will share the same LinkManager floating license)
- ❸ Type a **Password**. If you create the account for another use, you should inform this password to the user verbally or in a separate email. Alternatively select “Auto password”, which will automatically create a password and include in a separate mail to the user.
- ❹ When pressing **Save**, the email is automatically sent from the GateManager.



### 2.2.3. Create LinkManager Mobile user account.

The account is created identically to the LinkManager account

13. Login to the GateManager portal and select **Accounts** and **Create new account**



14. Now fill in the following details

Account Name: **Rose LMM** 1

Account Role: **LinkManager Mobile** Assign license:  2

Account Language: **English**

Description:

Group Member:

Person Name: **Rose Andersen** 3

Email: **rose@acmeinc.com**

Mobile:

Person Info:

Disabled:  Auto-Disable: **Never**

Last Login:

Created: 2014-02-10

Renewed:

Expires:

Authentication: **Username and Password** 4

Duration: **Permanent**

Mail Template: **Use default**

Message:

New password: **.....** 5

Repeat: **.....**

SMS new password:  Auto password:

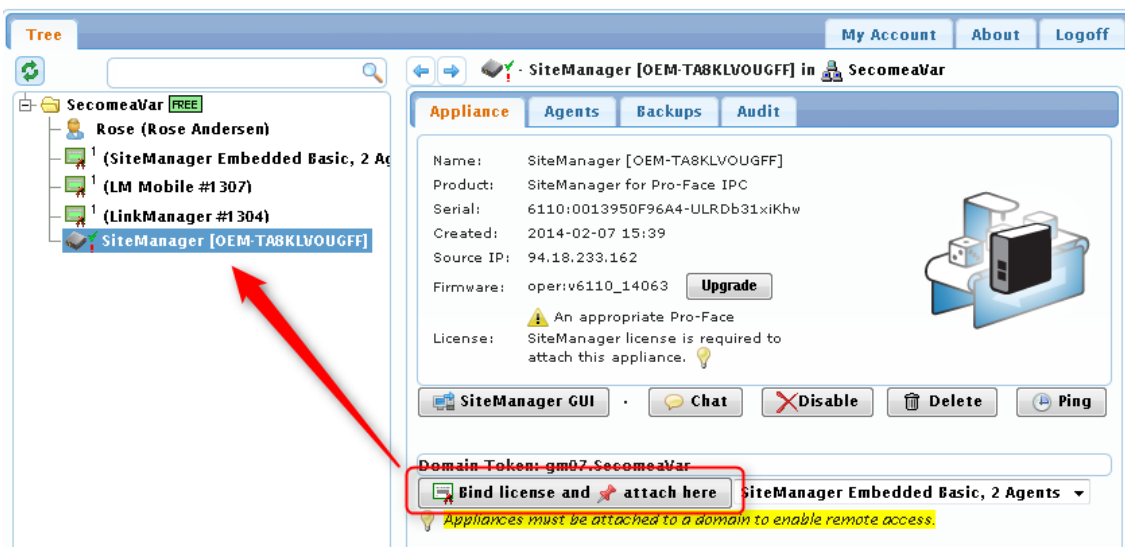
**Save** 6 **Cancel**



- 1 The **Account name**. This will become the login ID for the account
- 2 Role **LinkManager Mobile**. Note that the check box “Assign License” appears when selecting this role. When checking this box, this account will allocate the free LinkManager Mobile license and subsequently allow remote access by this account (if not checking the box, the account will still be working, but remote access is blocked)
- 3 **Person Name, Email** and optionally **Mobile**. The Mobile number is relevant if using Two-factor security with SMS code.
- 4 If the GateManager has a SMS modem associated, you would have the option to select SMS code in combination with the login ID and password and thereby ensure two-factor login. Otherwise the only option will be **Username and Password**
- 5 Type a **Password**. If you create the account for another use, you should inform this password to the user verbally or in a separate email. Alternatively select “Auto password”, which will automatically create a password and include in a separate mail to the user.
- 6 When pressing **Save**, an email with a link to the LinkManager Mobile login page is automatically sent from the GateManager

#### 2.2.4. Assign License to the the SM-E

15. If the SM-E has been configured correctly according to section 2.1.2 **Configure the GateManager settings**, the SM-E should appear in the tree view. Place your cursor on it and press **Bind license and attach here**.

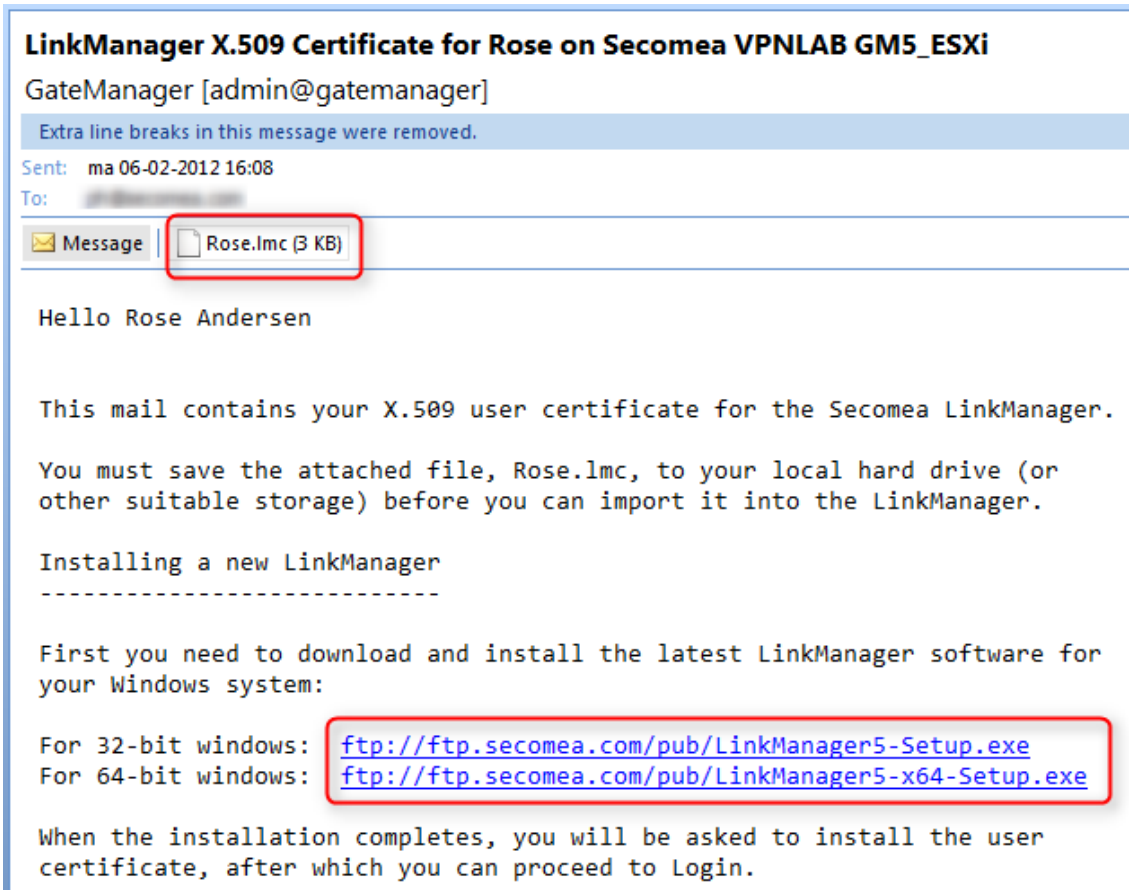




## 2.3. ROLE: LinkManager User

### 2.3.1. Install and login to the LinkManager

16. The previous step has generated an email from the GateManager that includes a LinkManager certificate (.lmc). Save the attached certificate to your computer.



17. Download and install the LinkManager software by clicking the appropriate link in the email.


**IMPORTANT:** You *must* have administrator privileges on the PC in order to install LinkManager.

**HINT:** You can also install LinkManager inside a VMWare virtual machine if the host OS is Windows 7 and the CPU supports virtualization. You can also run your programming software inside a virtual machine and connect to devices via LinkManager installed on the host OS if the virtual machine is configured for "NAT".

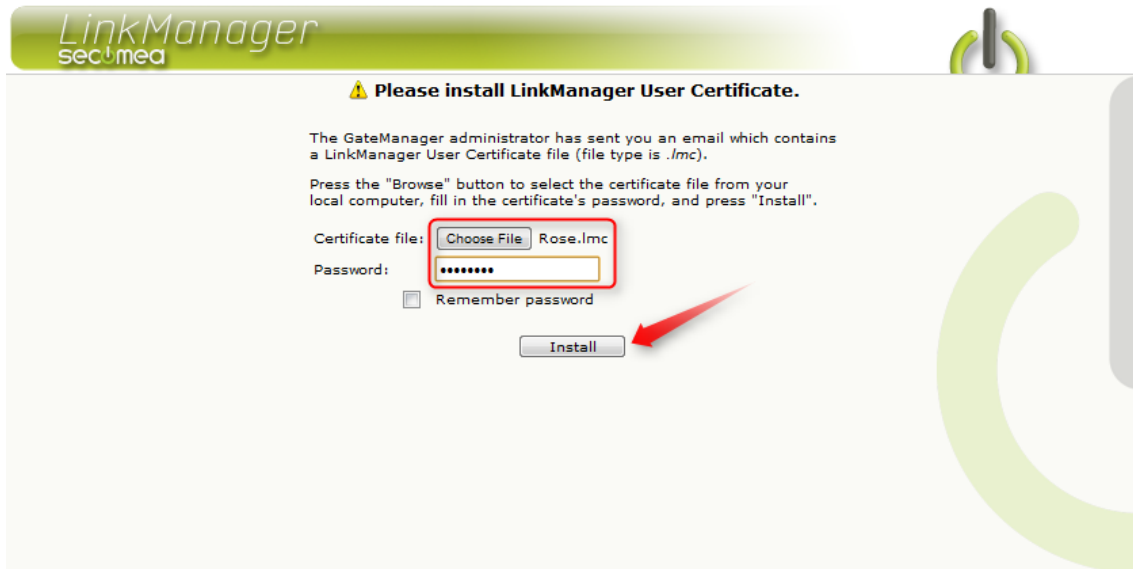
18. Eventually, when you click Finish in the installation wizard, the LinkManager icon will after a while turn green in your Windows system tray, and your default web browser will open, showing the LinkManager Web GUI.



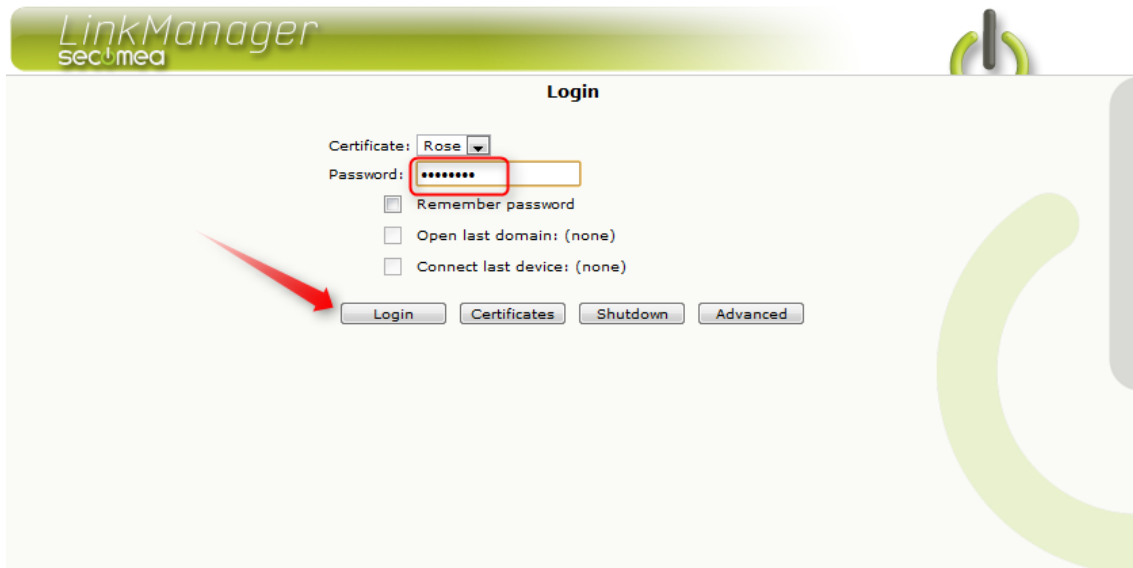


**Hint:** If The LinkManager icon remains yellow  for a long while, it could indicate that something on the PC is preventing the LinkManager from starting correctly. Consult the FAQ here for trouble shooting info: <http://www.secomea.com/industry/support/faq/>

19. **Browse** for the certificate you just saved and enter the password you specified for the account in step 12:

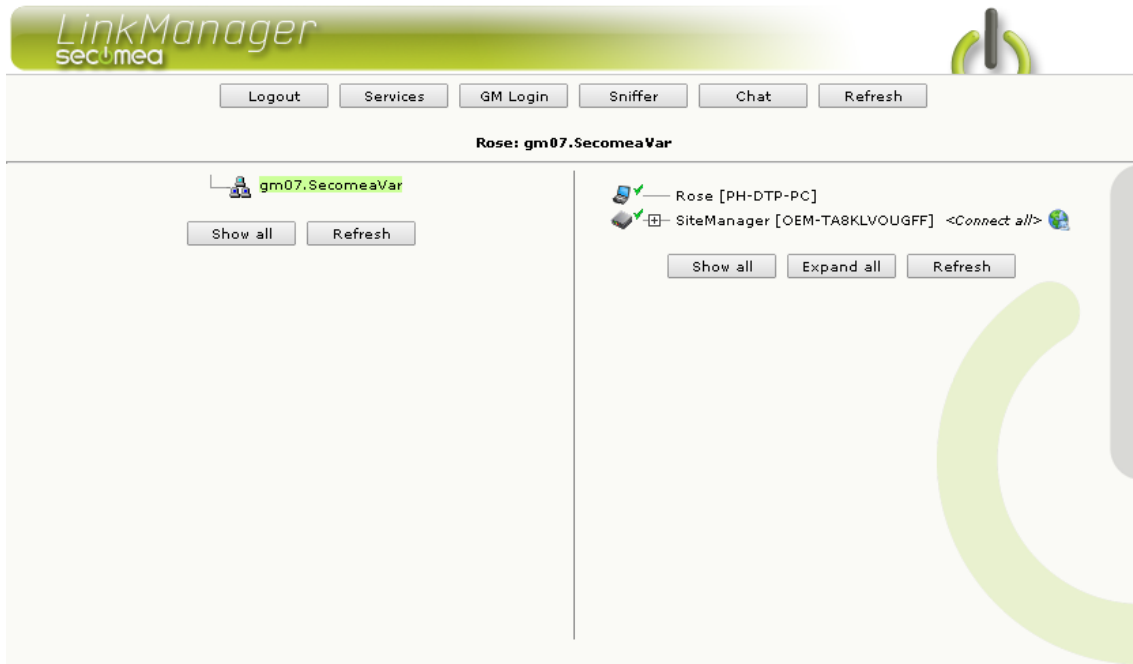


20. When clicking **Install**, you will be prompted to login. Repeat the password from above, and click **Login**:



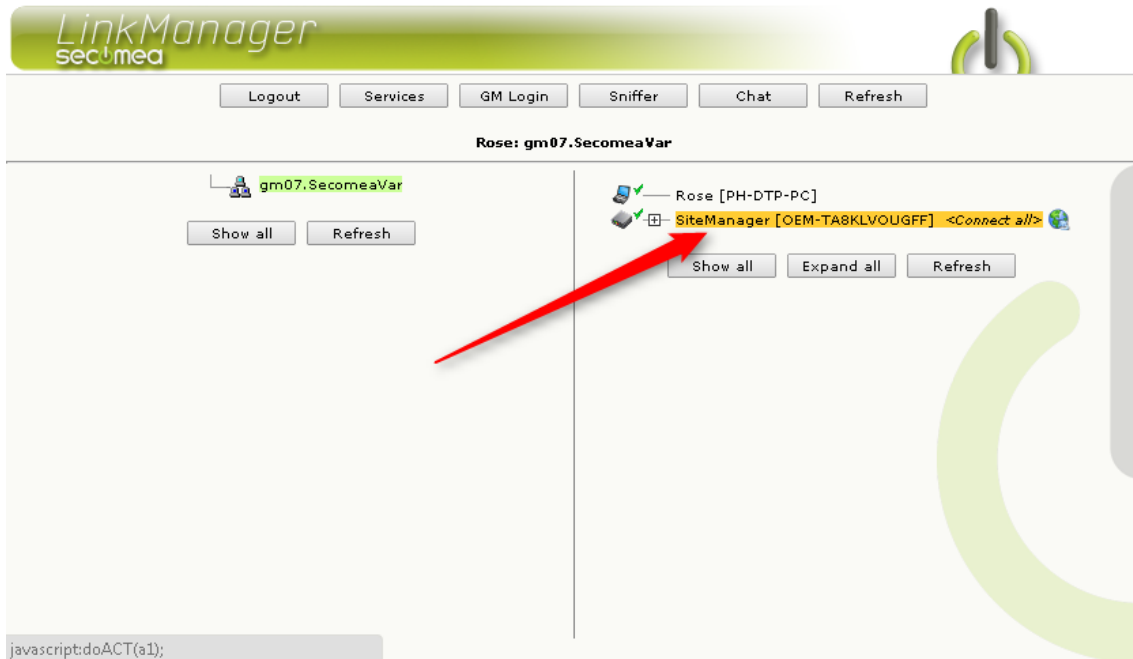
You are now logged in





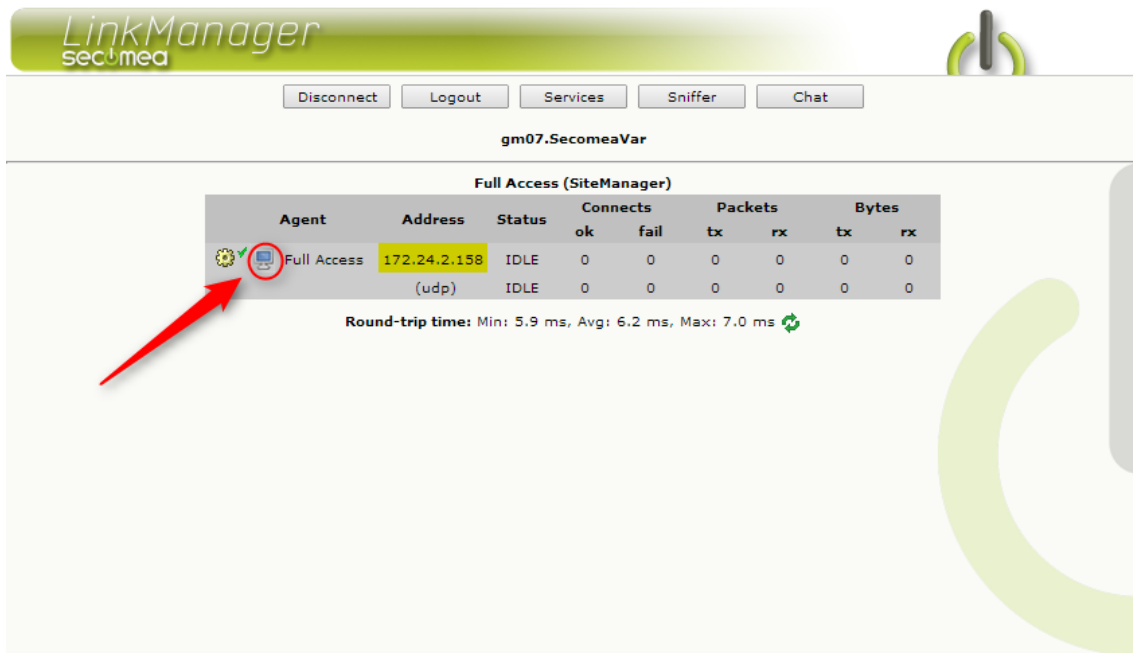
### 2.3.2. Connect to the PC via the SM-E

21. Click on the SiteManager <Connect All>

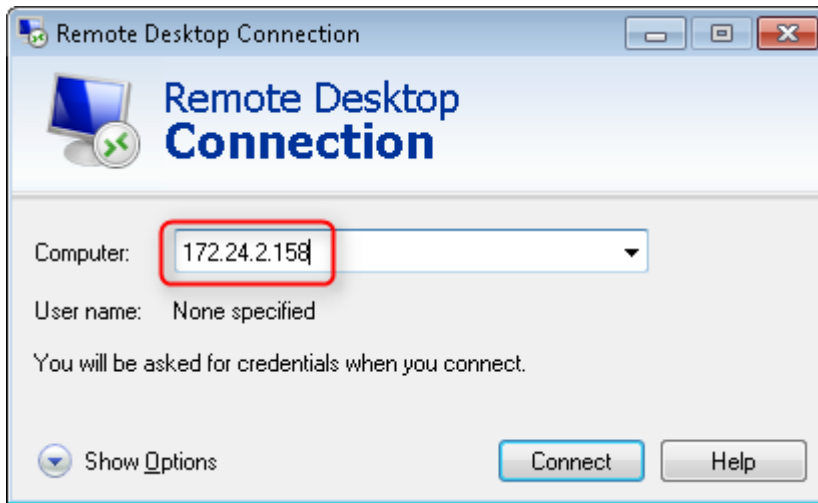




22. You are now connected to the IP address of the PC.

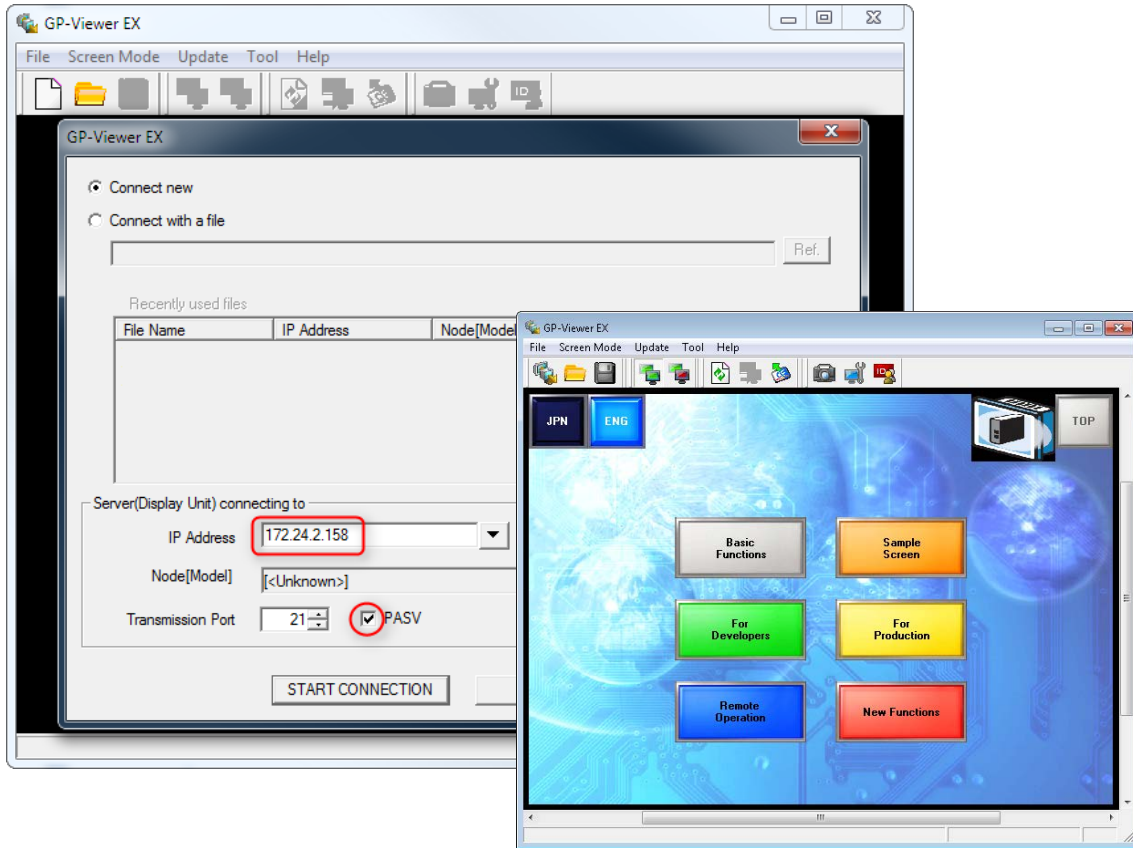


23. You can now connect to any application on that IP address. (Note that MS Remote Desktop can be auto-started with the screen icon)

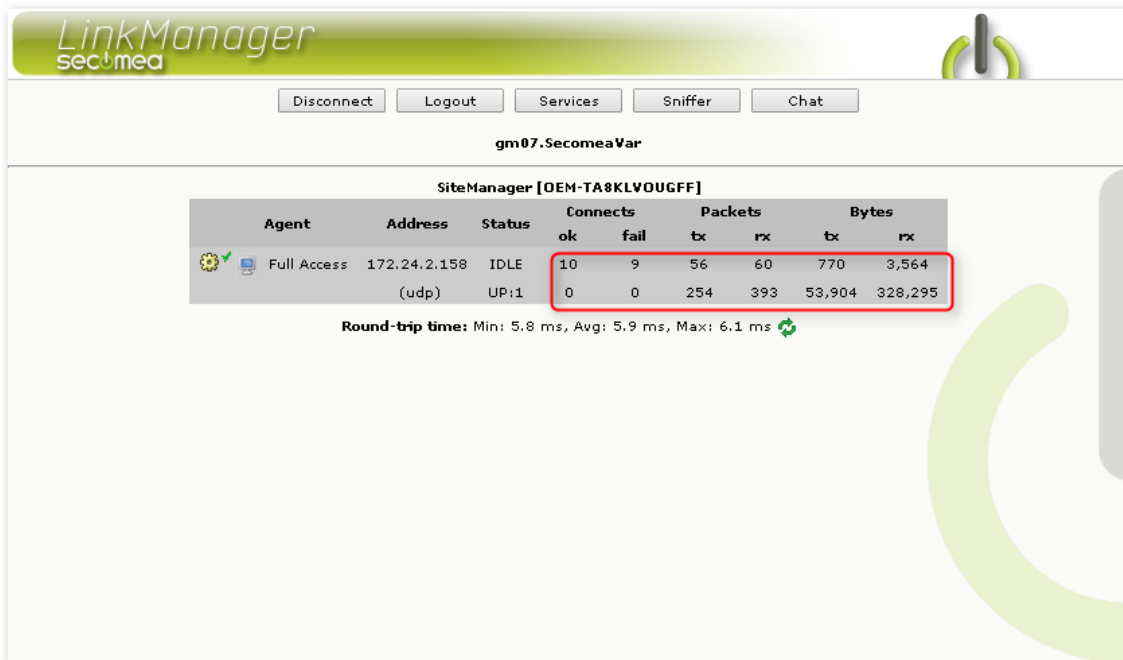




24. Or you could connect to a special service running on the Windows machine. In this example where the connection is made with GP-Viewer to the WinGP server on the machine:



**HINT:** You will notice that the LinkManager shows that the data counters reflects the transferred data.





## 2.4. ROLE: LinkManager Mobile User

LinkManger Mobile can be seen as a “light-weight” version of LinkManager that can be used from most devices with a web browser, such as PCs, Smartphones and tablets.

With LinkManager mobile you can connect to the following services on a device:

1. Web GUI (http/https)
2. RDP (MS Remote Desktop) on port 3389
3. VNC Servers on port 5900
4. Selected APP access mapped via port 5900

### 2.4.1. Login and connect to a web GUI with LinkManager Mobile

25. As result of creating the account in section 2.2.3, you will have received an email with a link to the LinkManager Mobile login screen.

You can activate the link from most platforms with a suitable web browser supporting https and java script.

#### **LinkManager Mobile password-only account for Rose LMM on Secomea VPNLAB GM5\_ESXi**

do-not-reply@secomea.com

Sent: ma 10-02-2014 13:53

To: 

Hello Rose Andersen

This mail is a notification that the LinkManager Mobile account "Rose LMM" has been created for login to the Secomea GateManager server. The password associated with the account will be informed to you verbally or in a separate mail.

Follow this link to the LinkManager Mobile login screen:

<https://gm07.secomea.com> (or alternatively: <https://193.242.155.117>).

(It is recommended to bookmark this page in your browser)

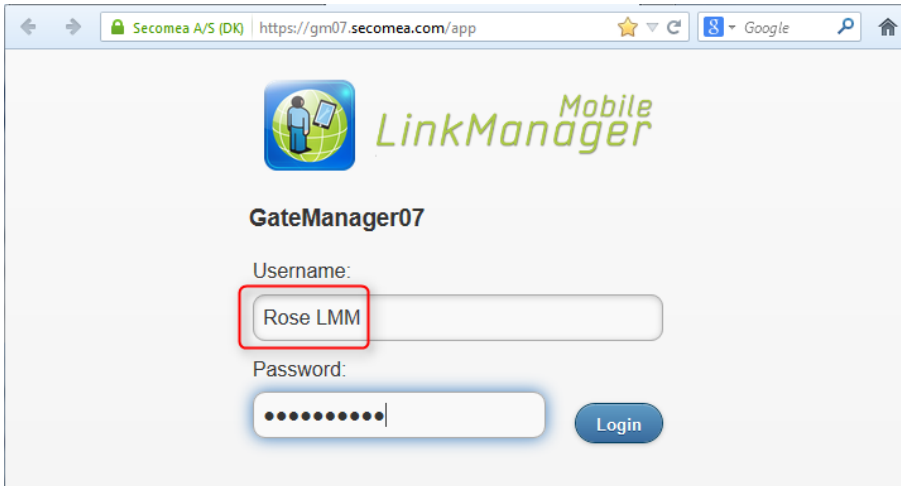
In the Login screen type your username "Rose LMM" and the password.

LinkManager Mobile has been verified to work with iPhone, iPad, and Android smart phones, as well as Internet Explorer 8, Google Chrome, Apple Safari, and Mozilla Firefox.

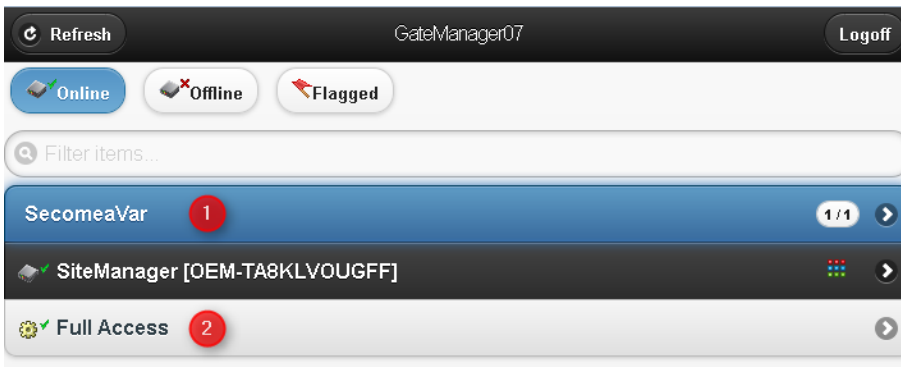
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.



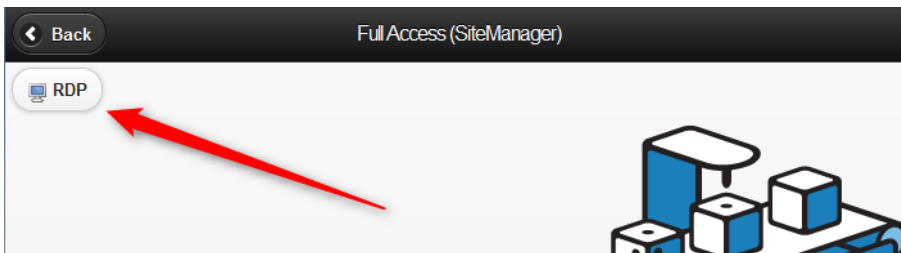
26. Login with the user name from the email. The password is either provided in a separate email, or verbally, depending on how the administrator created the account.



27. Click on the blue bar to unfold devices in the root domain, and connect to the Full Access agent.

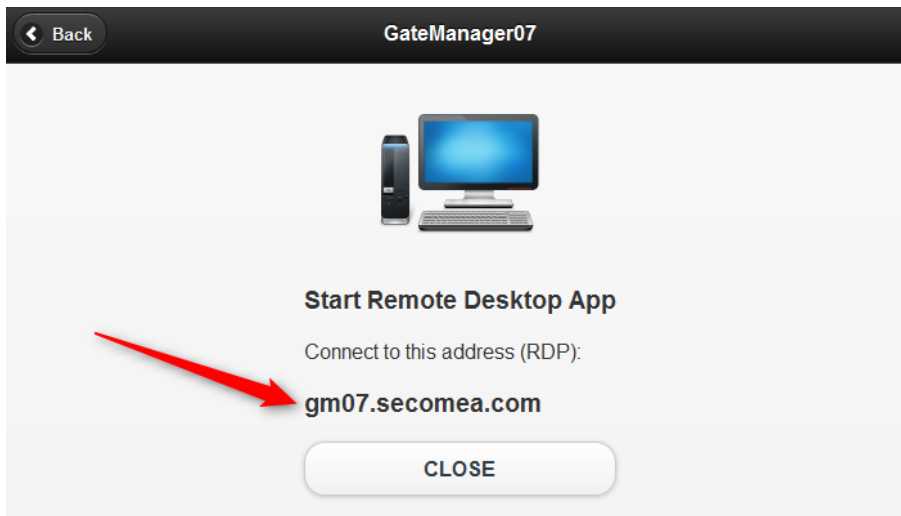


28. Now click on the RDP button.





29. You are now connected to the computer with the RDP protocol:



30. You can now start your RDP Client to the address shown.



**HINT:** If you are operating LinkManager Mobile from a tablet or smart phone, you can use your favorite remote desktop app.



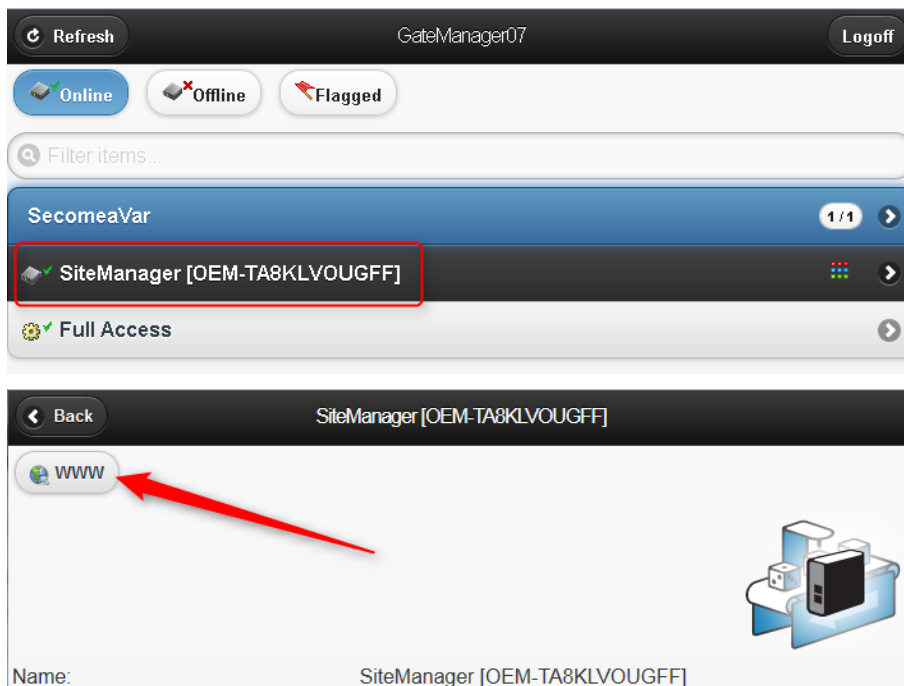
### 3. SM-E Basic - Adjusting Agents

This section describes how to extend SM-E Basic to allow access to selected services on the windows computer.

In extension to the default Full Access agent on SM-E you can create agents that allow access to specific services on the computer. This can be used to limit remote access to the computer, or to enable connection buttons on LinkManager or LinkManager Mobile for accessing the selected services.

#### 3.1. Connect to Device Agents section in the SiteManager GUI

1. Connect to the Web GUI of the SM-E. this can be done either from the LinkManager Mobile, LinkManager or from the GateManager Portal:
  - a. From **LinkManager Mobile** Select the SiteManager and click WWW:

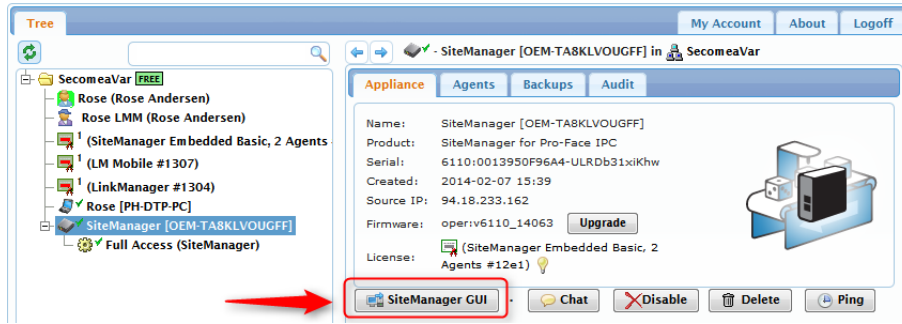


- b. or from **LinkManager**. Select the globe next to the SM-E

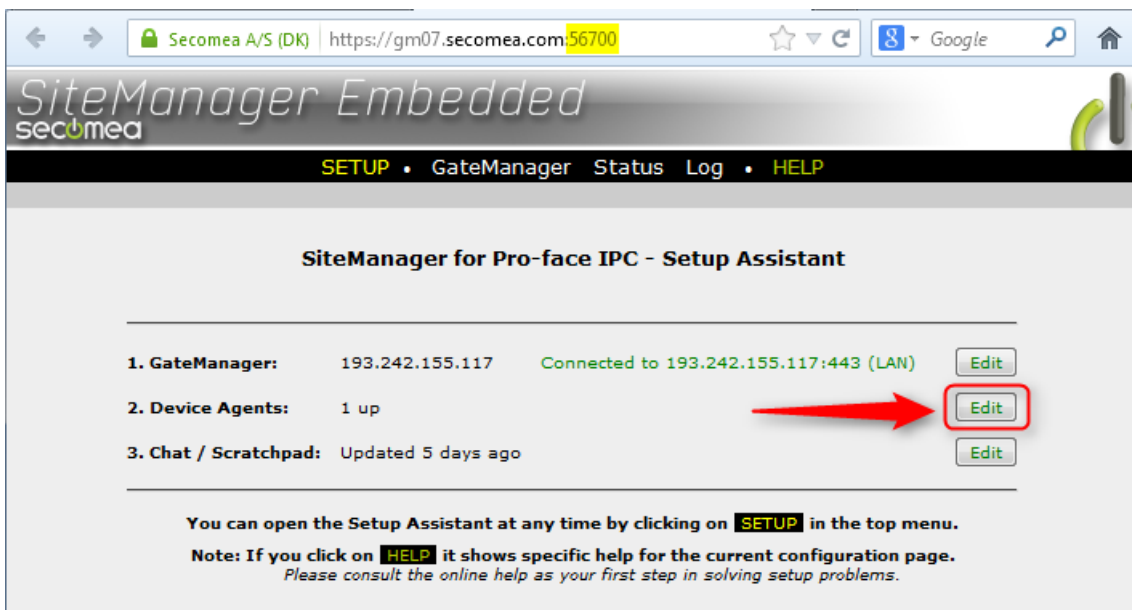




- c. or from the **GateManager Portal**, click the SiteManager GUI button.



- 2. When connected, the first screen is the Setup Assistant, where you click the **Edit** button for Device Agents:



**Note:** The connection is made as a proxy connection via the Gate-Manager, and is using a randomized port number. (in this case 55700 as indicated in the address line). You outgoing firewall must support http and https access via the port range 55000-59999 for remote web access to work.





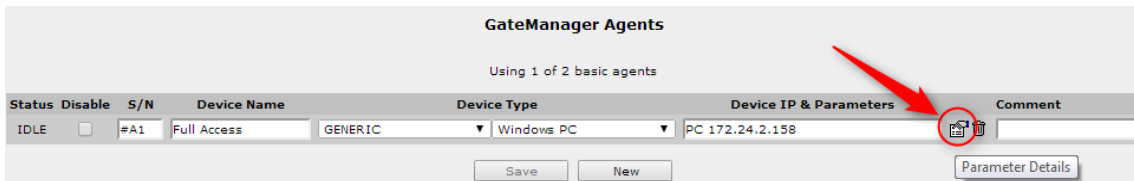
### 3.2. Enable standard connect buttons for Agents

For a SiteManager Agent you can enable buttons for WWW, VNC and RDP access that will appear in LinkManager and LinkManager Mobile for connecting to the device.

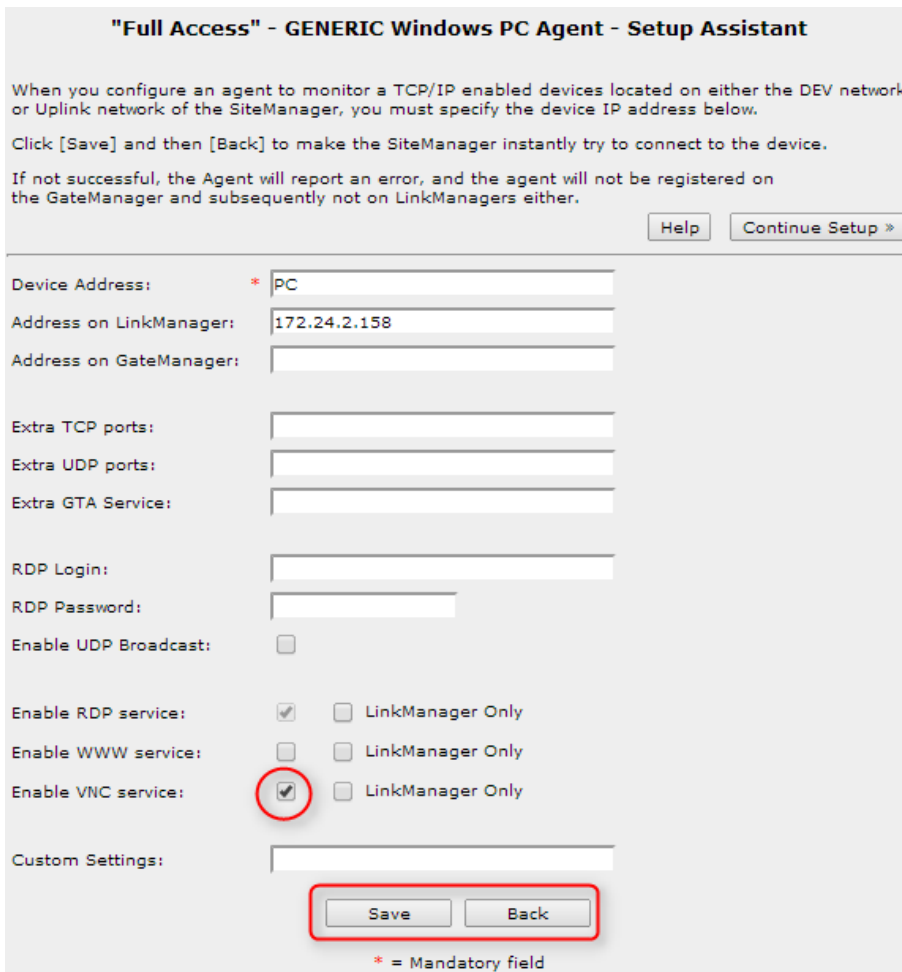
Typically these buttons are not enabled default , as the corresponding service (listen socket), may not be available for the device that the Agent represents.

#### 3.2.1. Example: Enable VNC button for the default Full Access agent

1. Click the Parameter details for the Full Access agent.



2. Check "VNC", and select **Save** and **Back**



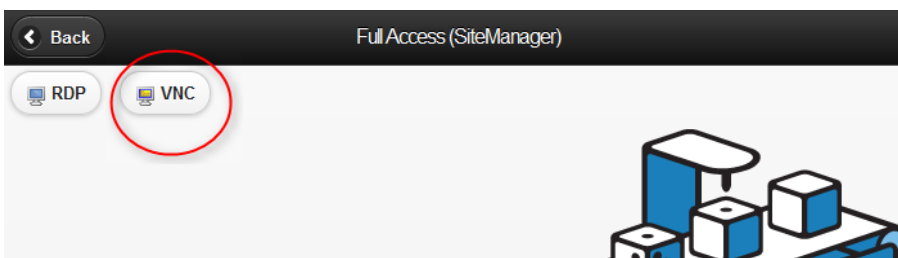


### 3.2.2. Connect to VNC Server with LinkManager Mobile

3. In the LinkManager Mobile connect to the Full Access agent.

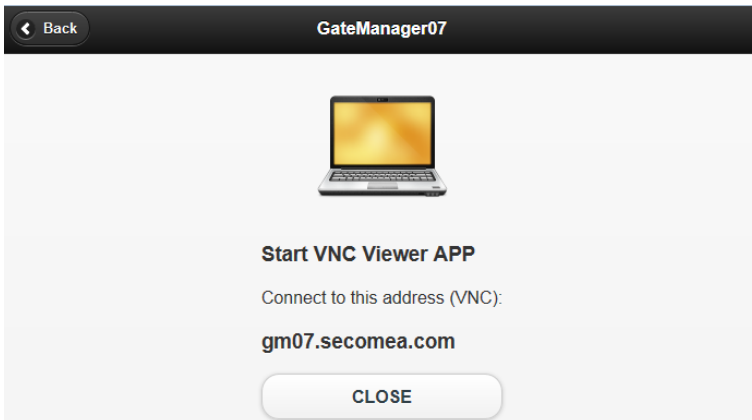


4. You will now see the VNC button.

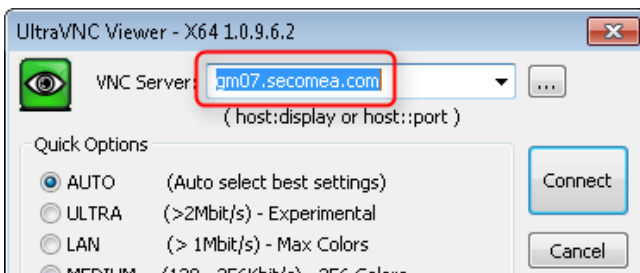


**NOTE:** The VNC button is only displayed if the agent can detect that the VNC server is started.

5. When pressed, LinkManager Mobile will create a connecting to the device:



6. Within 60 seconds you should connect with ae VNC Client, otherwise the connection is closed again, and you would need to repeat the above procedure.





### 3.3. Using Agents with custom LinkManager Mobile connect buttons

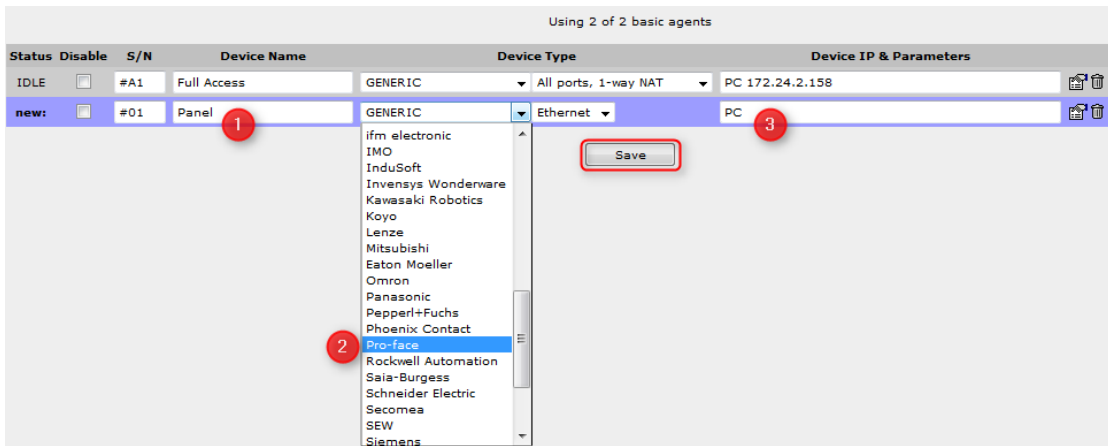
Some agents, such as Pro-face and Schneider, includes own custom connect buttons. These do not need to be defined specifically for the agent

#### 3.3.1. Example: Create a new Pro-face Agent

1. Select New.



2. Fill in the information:



1 Type a meaningful name that will describe the agent when logged into LinkManager or LinkManager Mobile

2 Select the **Pro-face** agent from the scroll bar. In case of SM-E the only connection type will be **Ethernet**.

**Hint:** Other options could have been **Generic / Web access**, which would have limited access to a web server on the computer

3 By just stating PC, the SM-E will just leave it up to Windows which IP address should be used when remote accessing from LinkManager. If the computer had multiple network adapters, you may wish to associate a specific address.



3. Select **Save** and observe that the Status of the agent goes “idle”

Status	Disable	S/N	Device Name	Device Type	Device IP & Parameters	
IDLE	<input type="checkbox"/>	#A1	Full Access	GENERIC	All ports, 1-way NAT	PC 172.24.2.158
IDLE	<input type="checkbox"/>	#01	Panel	Pro-face	Ethernet	PC

4. You can now close the SiteManager web GUI window

### 3.3.2. Configure the Pro-face Remote HMI APP to connect via the Agent

You probably already have downloaded and installed the Pro-face app from Apple APP Store or Google Play, in which case you would just need to create a new connection profile.

5. Log into the Pro-face Remote HMI, and select "+" to create a new connection profile.



6. Enter the following settings:



**1 Server Name.** Define a name of choice. In this case we have just entered the name of the GateManager through which the LinkManager Mobile connects.

**2 IP Address:** Enter the IP address of the GateManager server. You can find this in any mail received from the GateManager (see example in section 2.1.2)

**3 Port.** Enter Port **5900**.

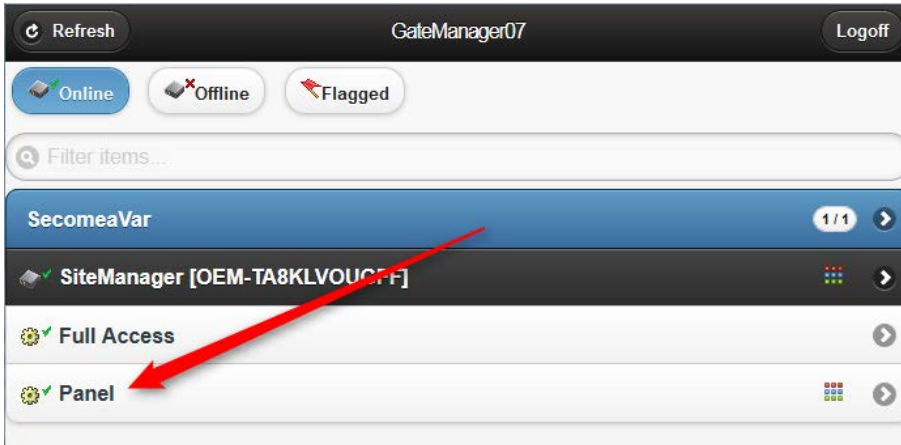
**NOTE:** You should always use port 5900, even if the panel is using such as port 10000, as the case is for Proface. GateManager will automatically map port 5900 from the LinkManager Mobile to the port used by the agent towards to the device.



- 7. Click **Done** in the Pro-face app to save the settings.

### 3.3.3. Connect to the Pro-face agent with LinkManager Mobile

- 8. In the LinkManager Mobile view, you will discover the new Vendor agent.

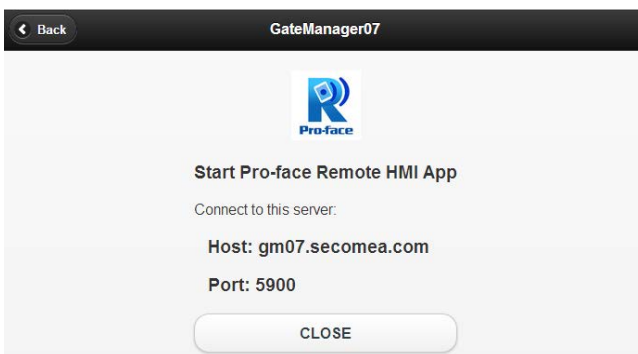


- 9. If you select the agent, you will see the HMI button specific for the Pro-face agent.



**NOTE:** The HMI button is only displayed if the agent can detect that the HMI server application is started.

- 10. Clicking the HMI button will establish a connection to port 5900 on the GateManager, which is mapped to the WinGP port (10000) on the Pro-face panel:



**NOTE:** Within 60 seconds you should connect with the Pro-face Remote HMI app, otherwise the connection is closed again, and you would need to repeat the above procedure.



### 3.3.4. Connect with the Pro-face Remote HMI APP

11. Click the home button on your tablet or smart phone to return to the home screen and select the Pro-face Remote HMI app. Login and click the connection profile you just created in section 3.3.2.



12. You will now be prompted for the password for the panel itself



**Note:** Reaching the above screen means that everything is setup correctly.

13. Entering the correct password will bring you to the Panel view:



You can now operate the panel as you would do if connected to the panel from the local network.



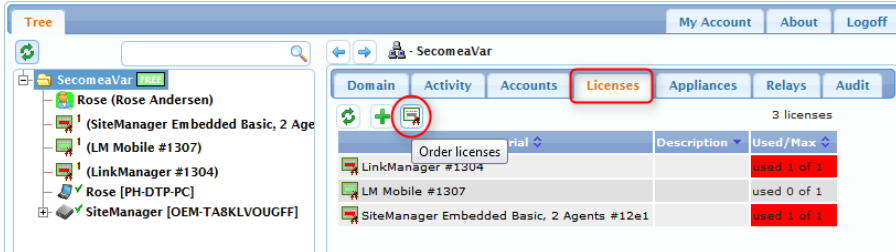
## 4. SM-E Extended – Accessing external devices

By upgrading to SiteManager extended, you can use SM-E to access other devices in the same network as the computer running SM-E

### 4.1. Ordering SM-E Extended license (and other licenses)

**NOTE:** If you already received and assigned a **SiteManager Extended** license as part of your start package, you can skip this section, and continue with section 4.4 **Define device agent for external device**

1. Standing on the root domain, select the Licenses tab, and click the Order Licenses icon.



2. Fill in the following information (descriptions next page)

**Billing information:**

Company: Acme Inc  
Address: Automationstreet  
ZIP/City: 2140 Copenhagen  
Country: Denmark  
Contact: John John  
Email: Johnjohn@Secomeavar.com

**Send order to:**

Company: Secomea A/S  
Contact: GM07-Demo Server  
Country: Denmark  
E-mail: support@secomea.com  
Cc: licenseservice@secomea.com

**Order Details:**

Order date: 2014-02-10 08:45:53  
Order ID: 4453-33553-514  
My Order ref.: Acme-01-2014  
My name: John John  
My E-mail: Johnjohn@Secomeavar.com

**Number of licenses ordered:**

LinkManager Mobile Licenses: \_\_\_\_\_ pools of \_\_\_\_\_ licenses  
LinkManager Floating Licenses: \_\_\_\_\_ pools of \_\_\_\_\_ licenses  
SiteManager Embedded Basic (2 agents): \_\_\_\_\_ pools of \_\_\_\_\_ licenses  
SiteManager Embedded Extended (5 agents): 2 pools of 1 licenses  
SiteManager Embedded Extended (10 agents): \_\_\_\_\_ pools of \_\_\_\_\_ licenses

I confirm that I have read the [terms and conditions](#)

1. Insert your own billing information here.



- 2 This information reflects your point of purchase and cannot be altered if you are running on a hosted GateManager.
- 3 This ID should be included if an order is placed without using this form. The information is used only for securing that Secomea license generators can cross reference the details in order ensure creation of the licenses with the exact information.
- 4 This is your order details, and should include your company's order number (if you use such)
- 5 This is where you fill in the desired licenses. In this example you will get a license consisting of two logical license files with one SM-E Extended license in each.

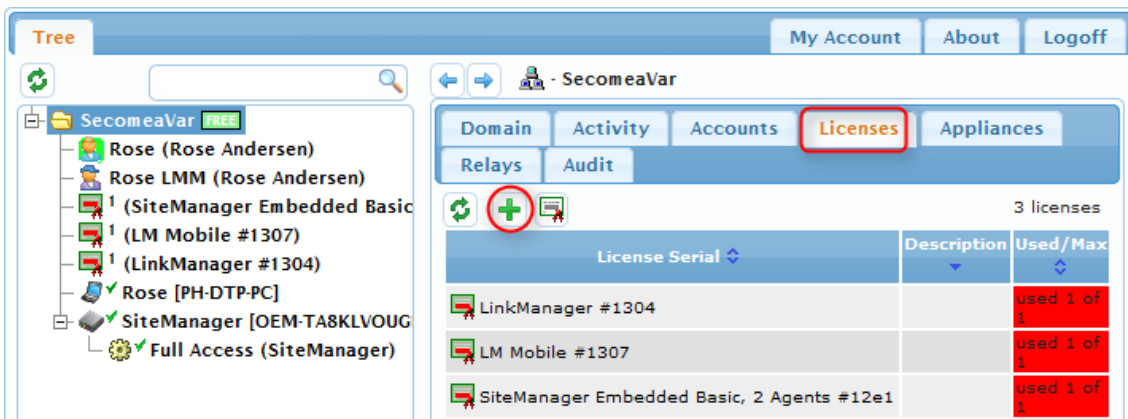
### 4.2. Installing licenses on (own) GateManager

**NOTE:** If you running on a hosted server, your hosting provider will place the ordered license in your domain, and you can continue with section 4.3 Upgrading SM-E Basic to SM-E Extended

- 3. If you have your own GateManager server, you will receive the license as a text file attached to an email. Open the text file and copy the contents to the clipboard.

```
1 =====BEGIN LICENSE UPGRADE=====
2 yCkk1JJN5GIVjjMLktdK005ScSo5EoCA
3 h50F-4pdgf23yZw7VbTGzzvmU3X5bGfQ
4 XUwT4IT6
5 =====END LICENSE UPGRADE=====
6
```

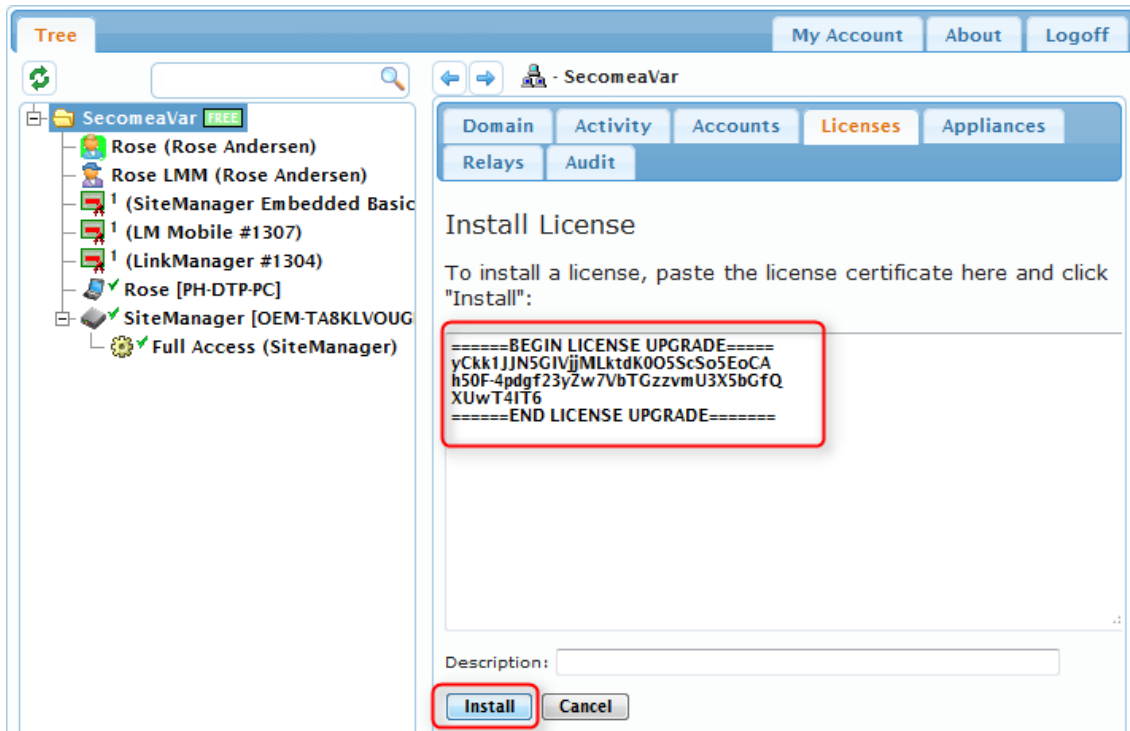
- 4. Select Licenses and the “+” sign.







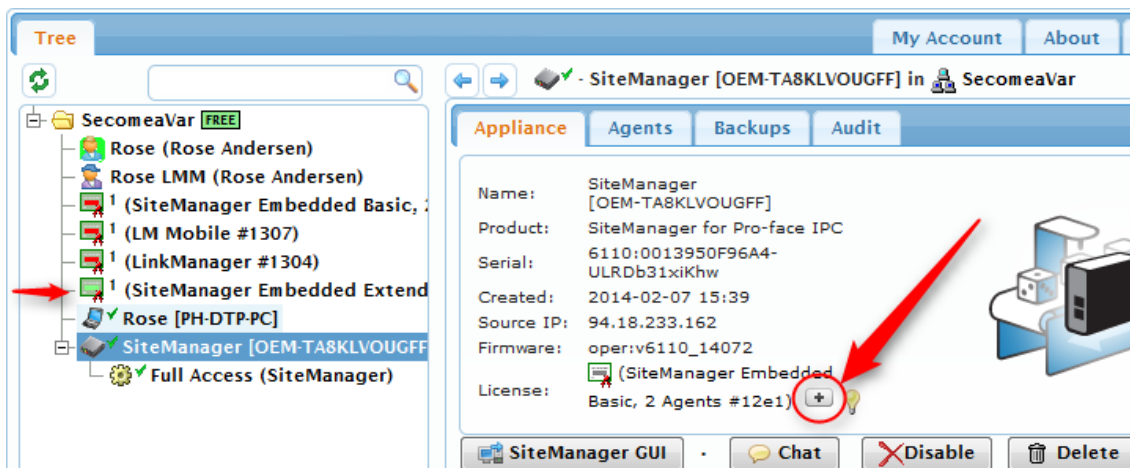
- Past the license into the text field, and click Install.



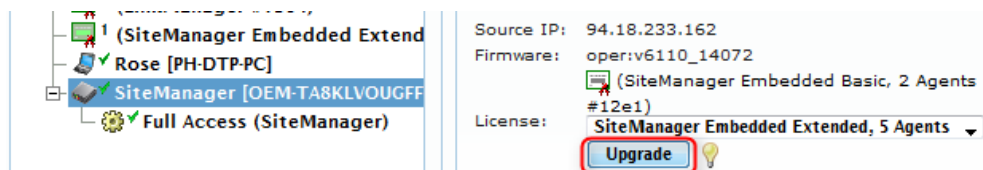
### 4.3. Upgrading SM-E Basic to SM-E Extended

**NOTE:** This section assumes you have a SM-E with a BASIC license attached to it, and have received a SM-E Extended license. If your SM-E already has a SM-E Extended license, you can jump to section 4.4 **Define device agent for external device**

- Locate the SiteManager in the GateManager Portal, and click the “+” sign to upgrade the license.



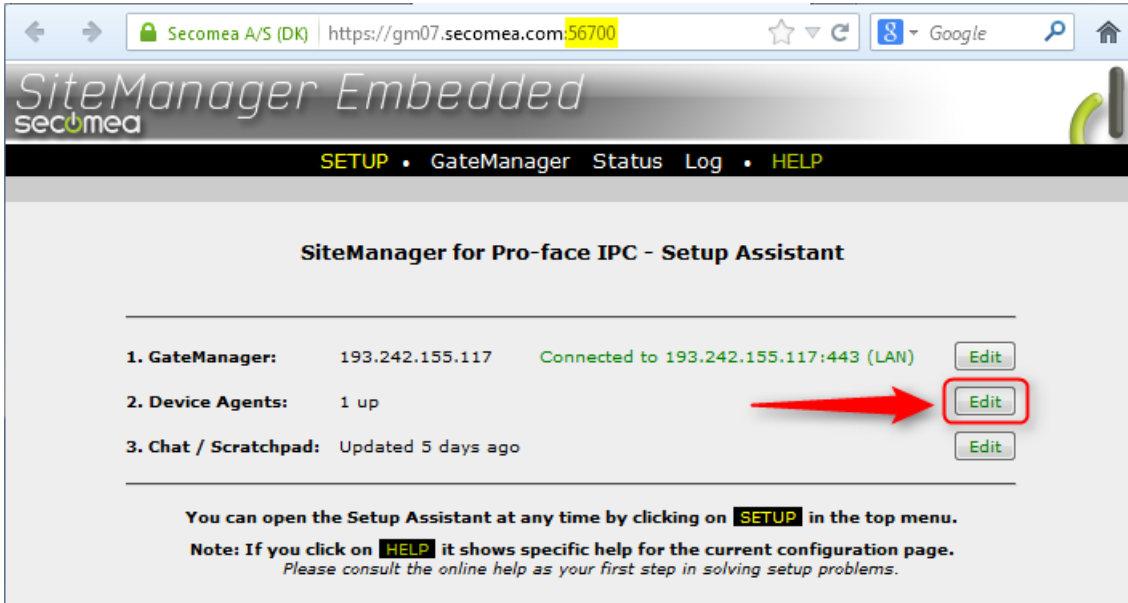
- Available licenses will be listed. Click **Upgrade** to bind the license



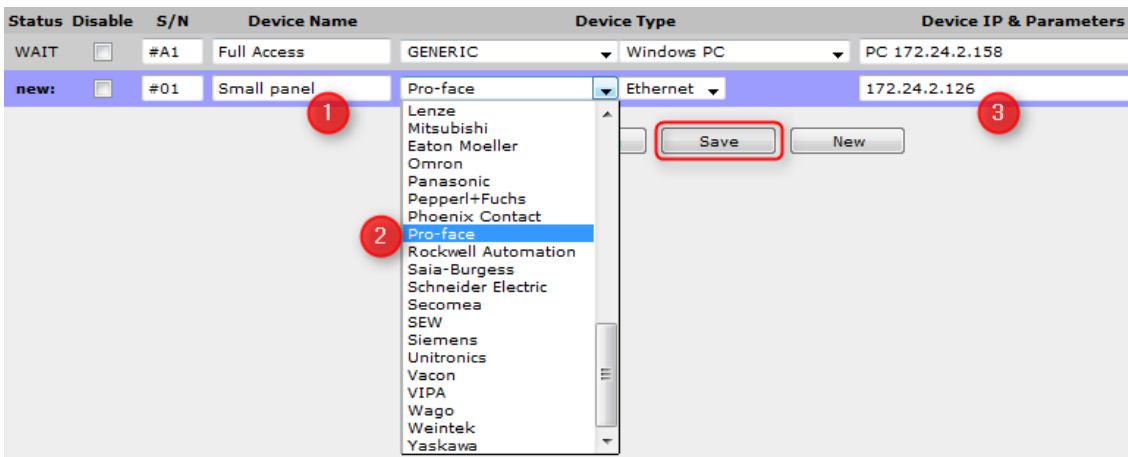


### 4.4. Define device agent for external device

8. Connect to the SiteManager GUI, and select Edit for 2. Device Agents

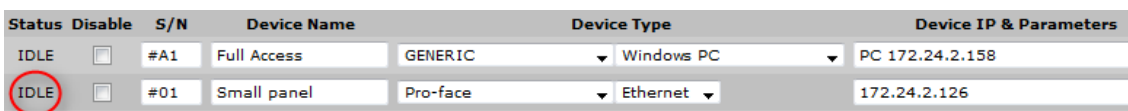


Select New and fill in the details



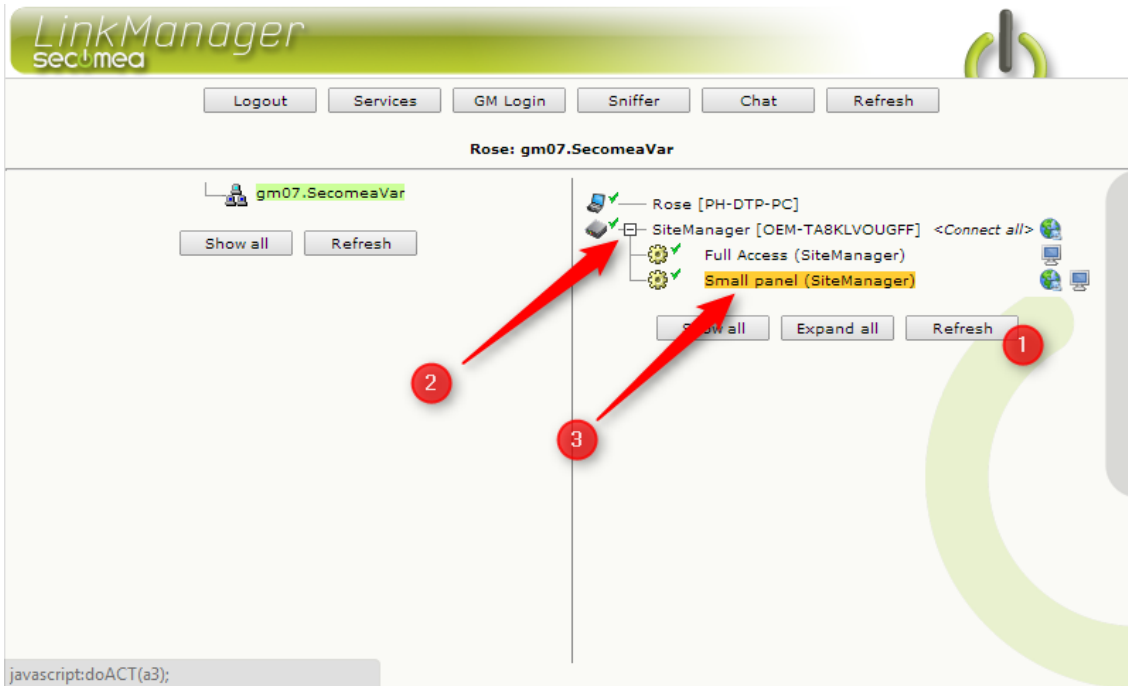
- ① Fill in the name that will appear in LinkManager
- ② Select the type of device. In this example we will connect to an Ethernet attached Pro-face panel
- ③ Enter the IP address of the device. The IP address must be accessible from the computer on which SM-E is installed.

9. Click Save and Refresh a couple of time until the Agent becomes idle, which indicates that SM-E can reach the device.

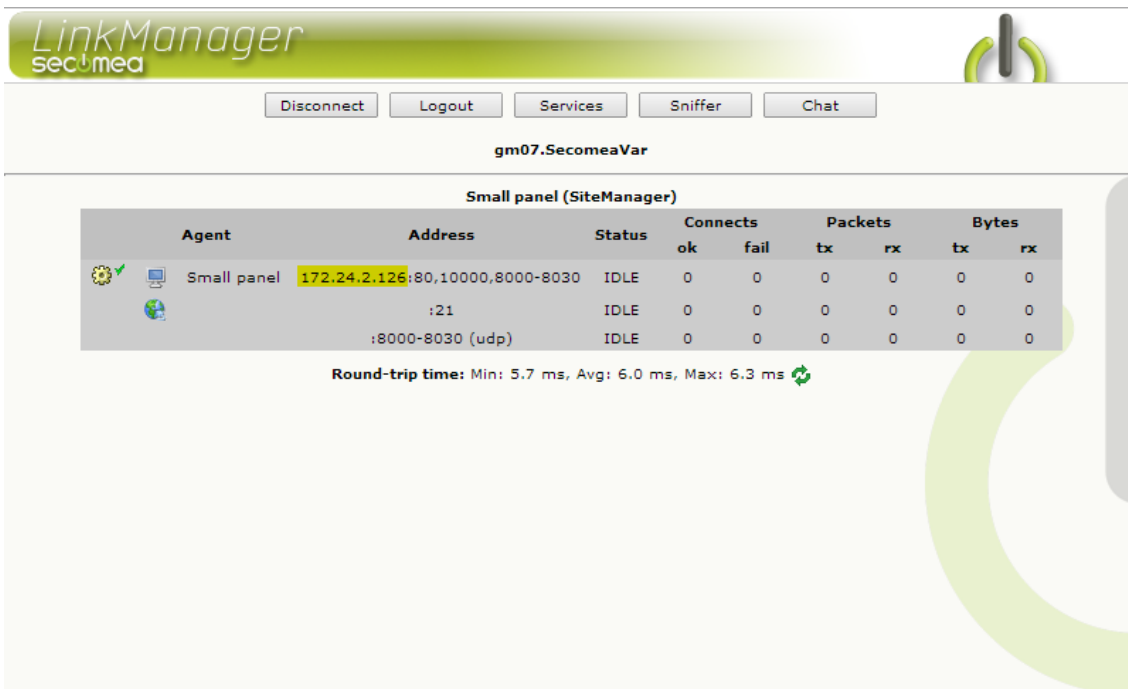




10. Login to LinkManager, click **Refresh** to update changes, Click “+” to unfold the agents on the SiteManager, and connect to the new agent, by clicking the agent description.

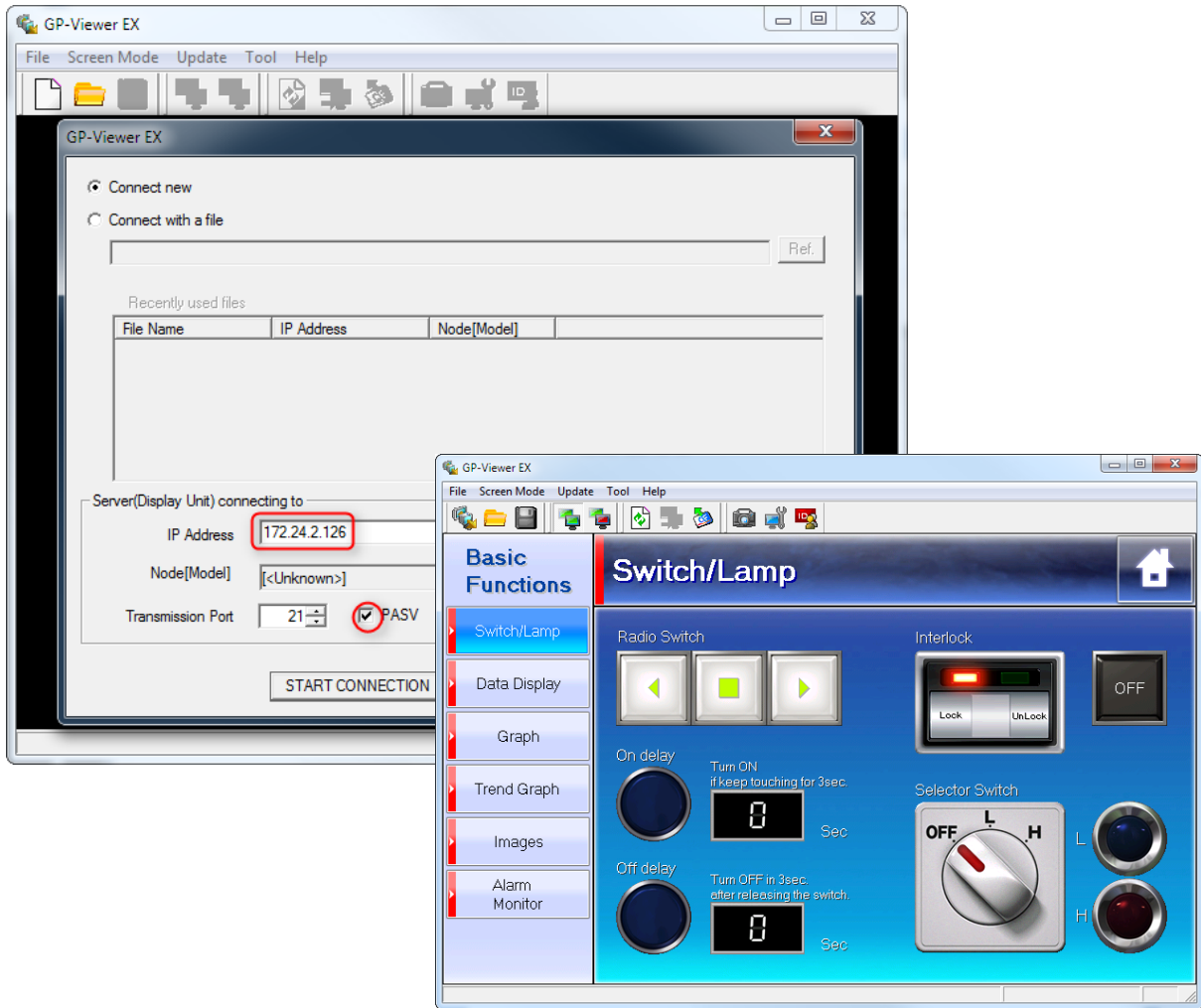


11. You are now connected directly to the IP address of the device.





12. Now start the native application for the device and define the target IP address:





## 5. Additional Features

### 5.1. Upgrading your GateManager Administrator account from BASIC to PREMIUM (P/N 26473)

With your current GateManager BASIC account, you are only using the GateManager administrator account to manage your LinkManager accounts.

You can, however, upgrade to **GateManager PREMIUM** and receive a Full GateManager administrator account.

This upgrade will add the following features to your current account:

- Organize equipment in domains per customer, factory, access levels or other logical structure (create domains and drag and drop devices and SiteManagers into relevant domains)
- Give LinkManager accounts individual access to domains (all LinkManager accounts will, when logging in, pull a license from the same LinkManager floating license pool on the server)
- Access the LinkManager GUI of your users, so you can provide remote assistance by looking at the same LinkManager screen that the user sees locally.
- Distribute messages for LinkManager users, that are automatically displayed to the users when logging into LinkManager (it could notification of server maintenance)
- Have the possibility to apply alert rules that will result in email reports when triggered (such as failed, connected etc.)
- Create and administer co-administrators for GateManager Console access.

You can order a GateManager PREMIUM account on Secomea part number 26473.

---

## Notices

### Publication and copyright

© **Copyright Secomea A/S 2014-2015**. 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 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™ and GateManager™ 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 publication 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 paragraph does 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](mailto:sales@secomea.com)  
[www.secomea.com](http://www.secomea.com)