

# Secomea GateManager5 BASIC Leitfaden

## Secomea Remote Access erlernen



Dieser Leitfaden ist für Erstanwender der Secomea Remote Access-Lösung für Fernzugriff, die eine praktische Einführung für die **Secomea GateManager BASIC** Lösung suchen, die spezifisch auf den **GateManager 5** Server zugeschnitten ist.

Dieser Leitfaden stellt Ihnen die verschiedenen Rollen und Prozesse im Zusammenhang mit der Installation und Konfiguration des **SiteManager**, **GateManager** Administration von Benutzern und die Verwendung des **LinkManagers** vor.

**Version: 1.1. Mai 2012**

---

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>3</b>
1.1. Voraussetzungen für diesen Leitfaden	3
1.2. Komponentenanalogien	3
1.3. Über Rollen, auf die sich in diesem Leitfaden bezogen wird:	4
1.4. Illustration der Rollenstandorte	5
1.5. Wenn etwas nicht funktioniert wie erwartet	5
<b>2. ROLLE: SiteManager Installierer.</b> 	<b>6</b>
2.1. Konfigurieren Sie die GateManager Einstellungen mithilfe des Appliance Launchers	6
2.2. Sich für eine Geräteanschlussmethode entscheiden	12
<b>3. ROLLE: GateManager BASIC Admin</b> 	<b>13</b>
3.1. Das GateManager Administrator-Zertifikat installieren	13
3.2. LinkManager Benutzer erstellen	14
<b>4. ROLLE: LinkManager Nutzer</b> 	<b>15</b>
4.1. LinkManager installieren	15
4.2. Verbindung zum SiteManager GUI	17
4.3. Die SiteManager Netzwerkeinstellungen konfigurieren	18
4.4. Den SiteManager Geräte-Agenten konfigurieren	20
<b>5. Zusammenfassung</b>	<b>24</b>
<b>6. Ihr GateManager Administrator-Konto von BASIC PREMIUM (P / N 26777) aktualisieren</b>	<b>25</b>
<b>Hinweise</b>	<b>26</b>

---

# 1. Einleitung

## 1.1. Voraussetzungen für diesen Leitfaden

Voraussetzungen für diesen Leitfaden sind:

- Sie verfügen über Administratorrechte, um ein Programm auf Ihrem Windows-PC oder Laptop zu installieren.
- Vorzugsweise befinden Sie sich in einem Netzwerk, das IP-Adressen per DHCP zuweist (auch für andere Anlagen als PCs).
- Ihr PC verfügt über ausgehenden Zugriff auf das Internet via https. Dies gilt sowohl für Ihre Unternehmens-Firewall als auch für jede persönliche Firewall, die auf Ihrem PC installiert ist.
- Sie haben eine SiteManager Hardware-Appliance erhalten.
- Sie haben Zugang zu einem freien Anschluss an einen Ethernet-Switch oder einer Steckdose, an die Sie den SiteManager anschließen können (kann auf dem gleichen Netzwerk wie Ihr PC aber auch in einem anderen Netzwerk sein - solange er ausgehenden Zugriff auf das Internet hat). Alternativ kann die Uplink2 3G-Verbindung verwendet werden.
- Sie haben ein netzwerkfähiges Gerät in Ihrem Netzwerk, das Sie als "fernüberwachtes Gerät" verwenden können. Dies könnte ein SPS oder ähnliches sein, oder einfach nur ein internetfähiges Netzwerkgerät wie z.B. Ihr Netzwerkdrucker.
- Sie haben per E-Mail ein GateManager-Zertifikat mit einem Link zum webbasierten GateManager-Administrator-Portal erhalten.
- Vorzugsweise haben Sie ein Benutzerkonto auf der Secomea Partner-Website zum Download von Zusatzinformationen <http://info.secomea.com/RDM-documentation> (wenn nicht, wählen Sie **Registrieren** in der oberen rechten Ecke auf der Secomea Website)

## 1.2. Komponentenanalogien

Mit der Secomea Remote Access-Lösung werden Sie in drei Komponenten eingeführt. Um sie in einen Zusammenhang zu stellen, mit dem Sie möglicherweise vertraut sind, haben wir Analogien zu traditionellen Modem-Lösungen gefunden:

- **SiteManager Hardware-Appliance.** Dies kann mit einem traditionellen Wählleitungsmodem verglichen werden, das mit dem Rechner beim Kunden vor Ort verbunden ist. Der große Unterschied besteht darin, dass ein SiteManager Zugriff auf mehrere Maschinen gewährleisten kann (sowohl IP, serielle und ausgewählte USB-Geräte) und er kann die vorhandene Netzwerk-Infrastruktur nutzen, um eine Internetverbindung herzustellen (einige Modelle unterstützen auch 3G).
- **LinkManager Client Software.** Dies ist vergleichbar mit der Modem-Software auf dem PC der Servicetechniker. Der große Unterschied besteht darin, dass der Servicetechniker keine Liste mit Telefonnummern verwalten muss. Die Liste der Geräte, die der Service-Techniker anschließen kann, wird automatisch aktualisiert, wenn ein neuer SiteManager angeschlossen wird und wenn der SiteManager mit neuen Geräte-Agenten konfiguriert ist. Zeigen und klicken Sie und der LinkManager Nutzer erhält sofortigen Zugriff auf das Gerät über das Internet.

- **GateManager Server.** Diese Komponente dient als Switchboard für Verbindungen zwischen LinkManagern und SiteManagern und sorgt dafür, dass weder LinkManager noch SiteManager öffentliche Adressen im Internet haben müssen. Für das BSIS-Paket wird der GateManager nur für das Verwalten von Nutzern verwendet, aber Sie können mit einem Domain-Administrator-Konto erweitern, mit dem Sie Protokolle überwachen können, feinkörniger LinkManager Zugriff auf bestimmte Geräte etc. (lesen Sie mehr dazu in Abschnitt 6 . Ihr GateManager Administrator-Konto von BASIC PREMIUM (P / N 26777) aktualisieren)

### 1.3. Über Rollen, auf die sich in diesem Leitfaden bezogen wird:

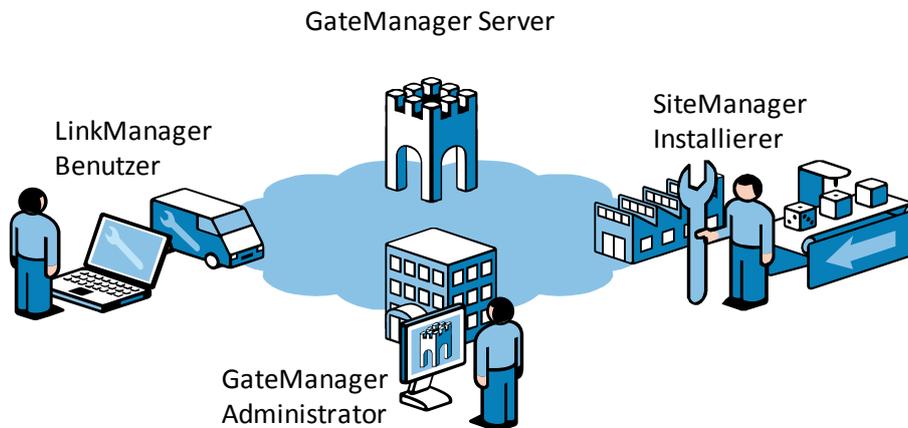
Im Dokument wird im Titel die Rolle angezeigt, die Sie einnehmen.

Die Rollen werden wie folgt gekennzeichnet:

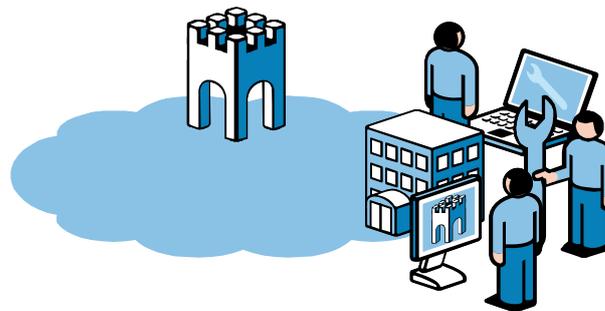
	<p><b>SiteManager Installierer.</b></p> <p>Diese Rolle umfasst folgende Aufgaben:</p> <ul style="list-style-type: none"><li>▪ SiteManager physisch installieren (oft vom Servicetechniker oder dem Kunde ausgeführt)</li><li>▪ Netzwerkeinstellungen konfigurieren (zuerst GateManager-Zugang initialisieren)</li><li>▪ Optional Geräteagenten auf dem SiteManager konfigurieren, wenn dies nicht vom LinkManager-Nutzer getan wird.</li></ul>
	<p><b>GateManager BASIC-Administrator.</b></p> <p>Diese Rolle umfasst folgende Aufgaben:</p> <ul style="list-style-type: none"><li>▪ Erstellen und Verwalten von LinkManager-Benutzerkonten.</li></ul>
	<p><b>LinkManager-Nutzer</b></p> <p>Diese Rolle wird von dem SPS-Programmierer oder Servicetechniker übernommen:</p> <ul style="list-style-type: none"><li>▪ Geräte für die Wartung / Programmierung der Geräte aus der Ferne anschließen.</li><li>▪ Den SiteManager und die Geräte-Agenten auf dem SiteManager optional konfigurieren, wenn dies nicht von dem SiteManager-Installierer übernommen wird.</li></ul>

## 1.4. Illustration der Rollenstandorte

Der typische Aufbau gegenüber dem Internet würde wie folgt aussehen:



Wenn Sie diese Anleitung zum ersten Mal befolgen, werden Sie wahrscheinlich alle Rollen spielen und physisch wie folgt angeordnet sein:



## 1.5. Wenn etwas nicht funktioniert wie erwartet

Wir wissen, dass dieser Leitfaden für 95% aller Anwender funktioniert, wobei 5% eine etwas erweiterte Konfiguration benötigen, die abhängig von der speziell eingerichteten Infrastruktur ist.

Die Lösung ermöglicht die Anpassung an hochkomplexe und von Sicherheitsvorkehrungen eingeschränkte Infrastrukturen mit z.B. einem Web-Proxy oder NTLM Autorisierungsserver, aber diesbezügliche Erklärungen liegt außerhalb der Aufgabe dieses Leitfadens.

Wenn Sie auf Probleme stoßen, zögern Sie nicht uns per Telefon zu kontaktieren und wir werden Sie in die richtige Richtung lenken oder Ihnen bei der Fehlerbehebung helfen.

Sie können hier auch unsere Dokumentbibliothek abrufen:

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

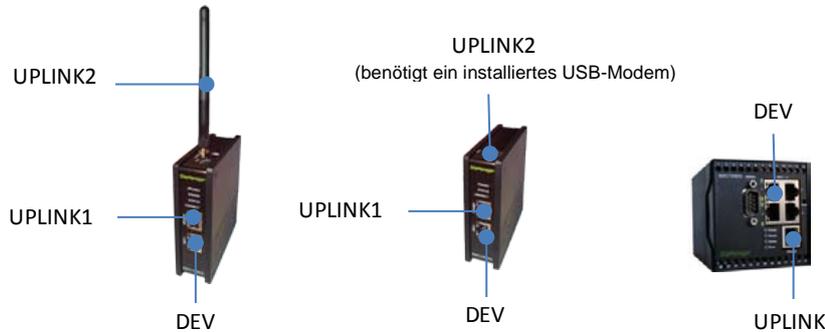
oder den FAQ-Bereich hier:

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



## 2. ROLLE: SiteManager Installierer.

Sie sollten einen neuen, unkonfigurierten SiteManager erhalten haben.



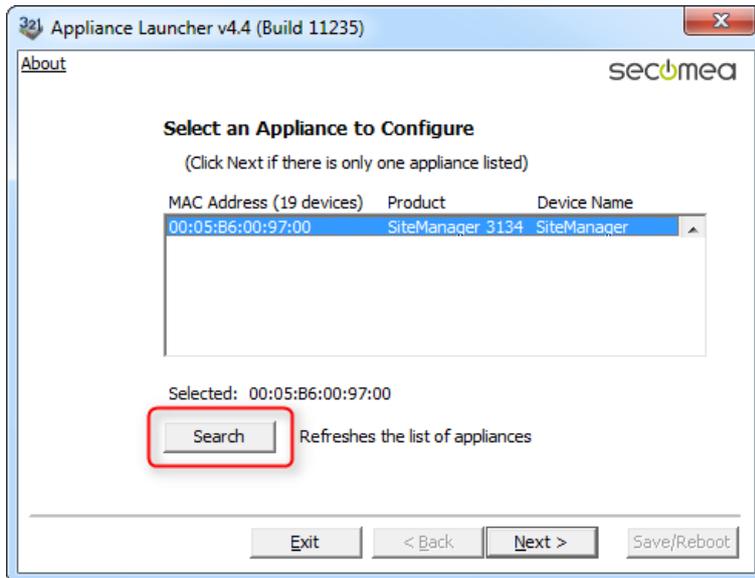
### 2.1. Konfigurieren Sie die GateManager Einstellungen mithilfe des Appliance Launchers

**Tipp:** Die Schritte in diesem Abschnitt können im Grunde durchgeführt werden, bevor der SiteManager an seinen endgültigen Bestimmungsort gesendet wird.

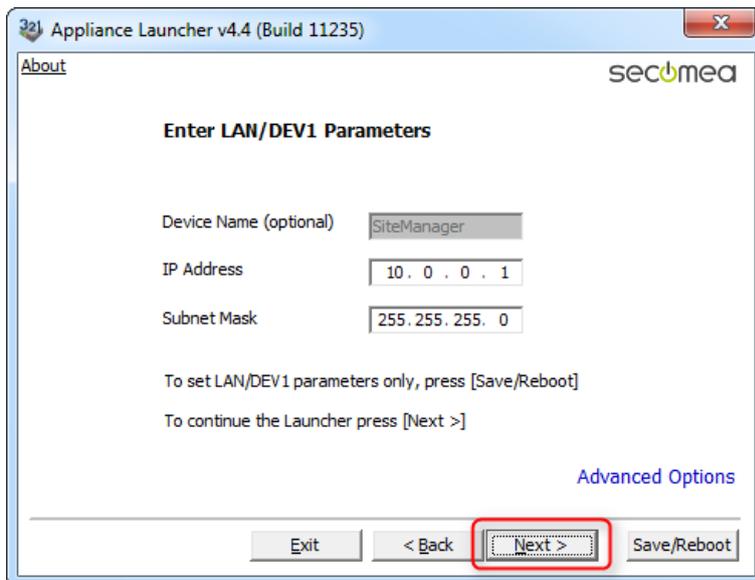
1. Laden Sie den Secomea Appliance Launcher hier herunter und installieren Sie ihn: <http://info.secomea.com/appliance-launcher>
2. Verwenden Sie ein Standard-Ethernet-Kabel, um den Ethernet Uplink/Uplink1 Port des SiteManager mit Ihrem lokalen Netzwerk zu verbinden.  
  
(Alternativ können Sie Ihren PC-LAN-Port mit einem Ethernet-Kabel direkt an den Uplink-Port des SiteManagers anschließen. Sowohl Standard- als auch gekreuzte Internetkabel können dafür verwendet werden.)
3. Schließen Sie die Stromkabel an die Schraubklemmen des SiteManagers nach Anleitung an, die im SiteManager Paket enthalten ist.
4. Schalten Sie den SiteManager ein und warten Sie etwa 30 Sekunden.



5. Starten Sie das Programm Appliance Launcher. Wenn der SiteManager nicht sofort angezeigt wird, drücken Sie die Taste **Search (Suchen)** so oft, bis der SiteManager erscheint.



6. Klicken Sie auf **Next (Nächste)** um auf die **LAN/DEV1** Konfigurationsseite zu gelangen. Bis jetzt müssen wir hier nichts zu tun. Wir können dies per Fernzugriff über den LinkManager später im Bedarfsfall konfigurieren.





7. Klicken Sie auf **Next (Nächste)** um die **WAN/UPLINK** Seite zu öffnen. Da wir annehmen, dass der SiteManager an Ihr Firmennetzwerk angeschlossen ist, können Sie die Einstellung auf DHCP lassen und es wird automatisch eine IP-Adresse und ein Standard-Gateway von Ihrem Unternehmen-DHCP-Server eingeholt.

Appliance Launcher v4.4 (Build 11235)

About sec<sub>o</sub>mea

### Enter WAN/UPLINK Parameters

WAN/UPLINK Settings

Mode:

IP Address:

Subnet Mask:

Default Gateway:

ISP Settings

Username:

Password:

8. Klicken Sie auf **Next (Nächste)** um die **WAN2/UPLINK2** Seite zu öffnen. Dies wird nur für die Konfiguration eines 3G/GPRS drahtlosen Uplink verwendet, der derzeit nur von den SiteManager Modellen 1029, 1039, 3129, 3229 und 3239 unterstützt wird.

Appliance Launcher v4.4 (Build 11235)

About sec<sub>o</sub>mea

### Enter WAN2/UPLINK2 Parameters

WAN2/UPLINK2 Settings

Mode:

IP Address:

Subnet Mask:

Default Gateway:

ISP Settings

SIM PIN Code:

APN:

**Tip:** Wenn Sie jetzt bereits beschlossen haben, die 3G/GPRS Option zu nutzen, sollten Sie hier nur den PIN-Code der SIM-Karte eingeben. Beachten Sie, dass Sie diese Information später immer noch über das SiteManager Web-GUI eingeben können.



9. Klicken Sie auf **Next (Nächste)** um zur Seite **GateManager Parameters** zu gelangen.

Appliance Launcher v4.4 (Build 11235)

About secomea

**Enter GateManager Parameters**

GateManager IP address: 1 130.226.210.167 DNS

GM Domain Token: 2 SecomeaVar

GM Appliance Name:

Web-Proxy IP address: . . . DNS

Web-Proxy Account:

Web-Proxy Password:

To disable the GateManager functionality - clear the GM Address field.

Exit < Back Next > Save/Reboot

**WICHTIG:** Die Informationen, die Sie in diesem Bildschirm eingeben, werden in der E-Mail mitgeteilt, die Sie vom GateManager zusammen mit dem GateManager X.509-Zertifikat erhalten haben.

**GateManager X.509 Certificate for JohnJohn on Secomea VPNLAB GM5\_ESXi**

GateManager [admin@gatemanager]

Extra line breaks in this message were removed.

Sent: so 05-02-2012 12:18

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: <http://130.226.210.167/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.

-----Additional info-----

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: 130.226.210.167 1

GateManager Token: SecomeaVar 2

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

Best regards  
Peter Hansen  
Mobile: +45 11223344



10. Für den **GM Appliance-Name** sollten Sie einen aussagekräftigen Namen auswählen, wie z.B. die Lage des SiteManagers. Beispielsweise **SiteA**

Appliance Launcher v4.4 (Build 11235)

About sec<sup>o</sup>mea

### Enter GateManager Parameters

GateManager IP address:

GM Domain Token:

GM Appliance Name:

Web-Proxy IP address:

Web-Proxy Account:

Web-Proxy Password:

To disable the GateManager functionality - clear the GM Address field.

11. Klicken auf **Next (Nächste)** um zum Bildschirm **Finish (Fertig)** zu gelangen. Aktivieren Sie das Kontrollkästchen, um das Passwort aufzubewahren:

Appliance Launcher v4.4 (Build 11235)

About sec<sup>o</sup>mea

### Finish

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

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

Check here to preserve password (Default is not checked)

[<Click> - copy current settings to clipboard](#)

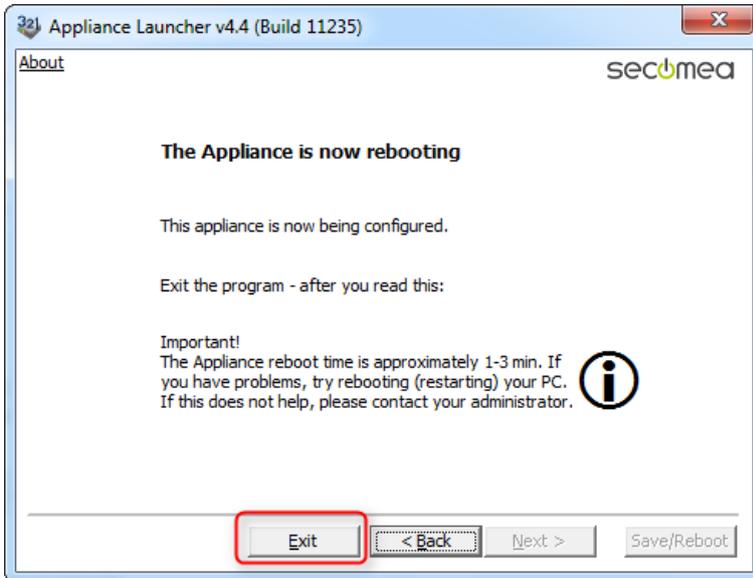
**Anmerkung:** Wenn Sie "Passwort aufbewahren" auswählen, bleibt das Passwort für die lokale Anmeldung für die Verwaltung der Web-Schnittstelle des SiteManagers **admin**.

Wenn diese Option deaktiviert wird, wird das Passwort zur der MAC-Adresse des SiteManager geändert.

Eine Anmeldung im SiteManager über den LinkManager erfordert kein Passwort.



12. Beim Klicken auf **Save/Reboot** sollten Sie die folgende Seite erhalten (wenn nicht, können Sie versuchen, auf **Back (Zurück)** auf die erste Seite zu klicken; klicken Sie dann erneut auf **Next (Nächste)**, bis der Save/Reboot Bildschirm erscheint).



13. Wenn der SiteManager eine DHCP zugewiesene IP-Adresse erhalten hat und entweder Port 11444, 443 oder 80 Internet-Zugang mit SSL/TLS-Verschlüsselung durch die Netzwerk-Firewall gewährt wird, wird der SiteManager nun mit dem GateManager verbunden.

Überprüfen Sie in der Broschüre Ihres SiteManagers das LED-Signal "GateManager Verbunden".

Wenn Sie über ein 3G/GPRS Modem an den Uplink2 USB-Port angeschlossen sind, gilt die gleiche LED-Status-Signalisierung.

*Das ist alles, was Sie lokal auf dem SiteManager ausführen müssen.*

*In Wirklichkeit könnten Sie nun den SiteManager an einen neuen Standort bewegen.*

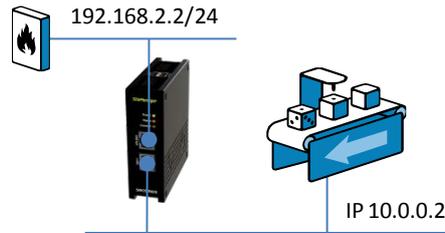
*Sobald der Ethernet-Uplink1 Port am neuen Standort verbunden ist oder der Uplink2 Port mit dem 3G/GPRS Providers verbunden ist, wird der SiteManager eine neue DHCP-Adresse erhalten und versuchen, sich mit dem GateManager über das Internet zu verbinden.*



### 2.2. Sich für eine Geräteanschlussmethode entscheiden

**Anmerkung:** SiteManager kann auch Zugriff auf serielle Geräte oder USB-Geräte herstellen, indem er an den RS232 DB9-Anschluss oder den USB-Anschluss des SiteManagers angeschlossen wird. Im Folgenden konzentrieren wir uns nur auf Ethernet-Geräte.

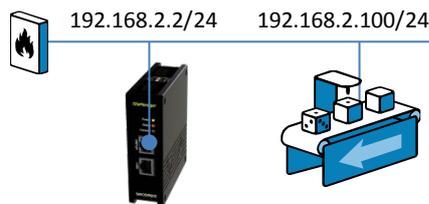
14. Beim Einsatz eines SiteManagers und der zu verwaltenden Geräte beruft man sich normalerweise auf die Fähigkeit des SiteManagers zur vollständigen Trennung der Geräte vom Unternehmensnetzwerk, wie folgt (IP-Adressen sind nur Beispiele):



**HINWEIS:** Die Maschine dargestellt als 10.0.0.2, kann über einen Schalter oder direkt mit einem Ethernet-Kabel an einen **DEV**-Port angeschlossen werden. Optional kann der SiteManager so konfiguriert werden, dass er die Adresse an die Geräte auf den DEV Ports über DHCP DEV zuweist.

(/24 notiert, nachdem die IP-Adresse nur die Standard-TCP Notation einer Subnetzmaske 255.255.255.0 ist)

15. Sie können jedoch auch ein Gerät überwachen, das sich bereits auf dem Firmennetz (Ethernet **Uplink**-Seite) befindet. Dabei sind keine weiteren Netzwerkkonfigurationen von Ports auf dem SiteManager erforderlich (wenn Sie Uplink2 verwenden, um ein 3G/GPRS Modem anzuschließen, müssen Sie Geräte auf dem DEV-Port wie oben gezeigt anschließen und die DEV-Port IP-Einstellungen entsprechend konfigurieren)



**BITTE BEACHTEN:** Die abgebildete Maschine stellt das Netzwerk-Gerät dar, das Sie als "fernüberwachtes Gerät" für diese Übung verwenden möchten. Sie können aber auch jedes IP-fähige Gerät, wie z. B. SPS, HMI oder sogar einen PC oder einen Drucker verwenden. Im Folgenden arbeiten wir mit einer auf der DEV-Seite des SiteManagers angebrachten SPS.

16. **WICHTIG:**





### 3. ROLLE: GateManager BASIC Admin

#### 3.1. Das GateManager Administrator-Zertifikat installieren

- Suchen Sie die E-Mail, die Sie vom GateManager mit dem **GateManager X.509-Zertifikat** erhalten haben und speichern Sie die angehängte Datei im Ordner "Meine Dokumente":



- Öffnen Sie den Link in der gleichen E-Mail. (Es können auch zwei Links mit jeweils einem DNS-Namen und einer IP-Adresse angegeben sein, wobei Sie einen davon verwenden können)

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

Follow this link to the GateManager administrator login screen:  
<http://130.226.210.167/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.

- Dies öffnet den Login-Bildschirm des GateManagers:



**Anmerkung:** Das GateManager Administrator-Portal erfordert mindestens MS Internet Explorer 9, Apple Safari, Firefox oder Google Chrome.

- Suchen Sie nach dem Zertifikat, das Sie gerade gespeichert haben, und geben Sie das Passwort ein, das Ihnen vom Administrator mitgeteilt wurde.

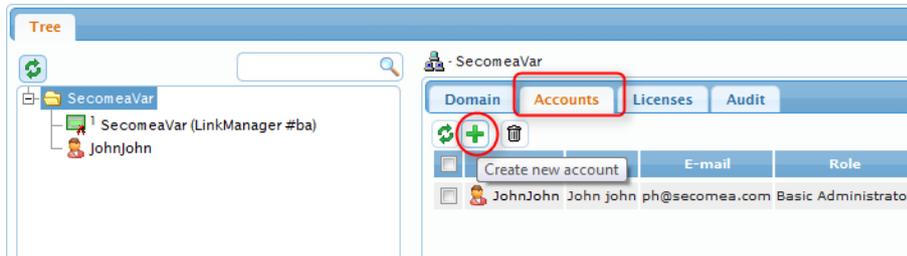
Wenn Sie das Passwort noch nicht per E-Mail, SMS oder mündlich erhalten haben, sollten Sie sich an die Person wenden, die im **Abschnitt Unterschrift** der E-Mail mit dem Zertifikat aufgeführt ist



(antworten Sie nicht auf die E-Mail, da sie automatisch vom GateManager erstellt wurde)

### 3.2. LinkManager Benutzer erstellen

21. Wenn Sie eingeloggt sind, wählen Sie die Registerkarte **Konten** und wählen Sie das "+" Symbol, um ein neues Konto zu erstellen



22. Füllen Sie die folgenden Informationen aus

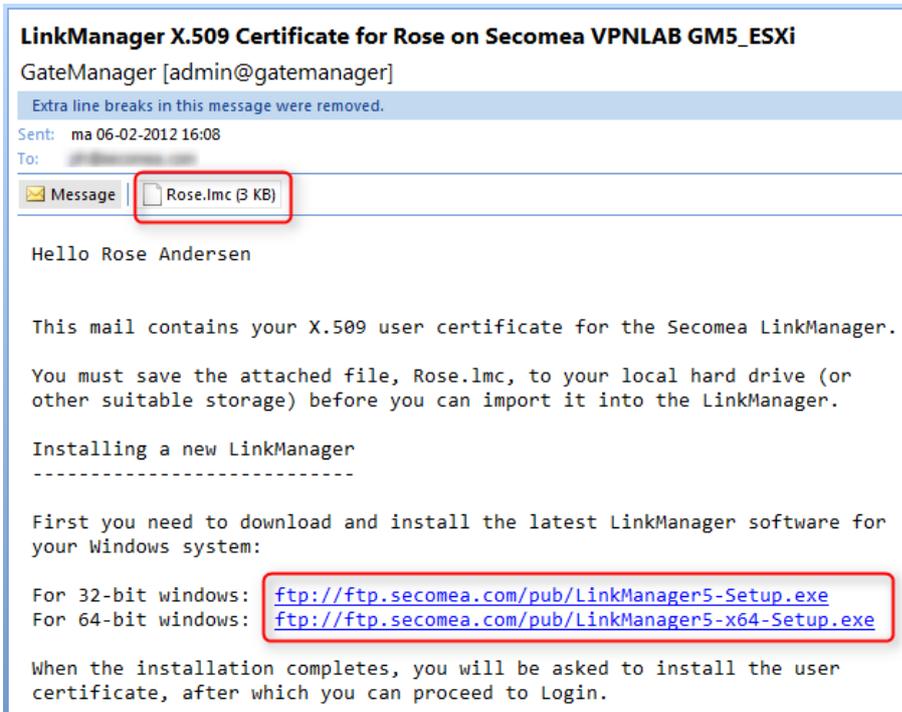
- 1 Der **Kontoname**. Dies wird der Dateiname der LinkManager Zertifikats-Datei (in diesem Fall Rose.lmc)
- 2 **Personenname, E-Mail** und gegebenenfalls **Mobiltelefon**. In dieser Ausübung werden Sie das Konto für sich selbst ausstellen. Sie können später Konten für andere Benutzer erstellen. (Alle Benutzer werden die gleiche LinkManager Floating License verwenden)
- 3 Geben Sie ein **Passwort** ein. Wenn Sie das Konto für einen anderen Zweck erstellen, sollten Sie dieses Passwort dem Benutzer mündlich oder in einer separaten E-Mail mitteilen.
- 4 Beim Klicken auf **Speichern** wird die E-Mail automatisch vom GateManager gesendet.



### 4. ROLLE: LinkManager Nutzer

#### 4.1. LinkManager installieren

23. Beim vorherigen Schritt wurde eine E-Mail vom GateManager erstellt, der ein LinkManager Zertifikat beinhaltet (.lmc). Speichern Sie das angehängte Zertifikat auf Ihrem Computer.



24. Laden Sie die LinkManager Software herunter, indem Sie auf den entsprechenden Link in der E-Mail klicken und installieren Sie sie.

**WICHTIG:** Sie müssen über Administratorrechte auf dem PC verfügen, um LinkManager zu installieren.

*LinkManager wird nicht funktionieren, wenn er auf Windows installiert ist, das in einer VMWare oder VBox virtuellen Maschine läuft. Installieren Sie LinkManager immer auf dem Host-Betriebssystem. Sie können Ihre Programmiersoftware trotzdem innerhalb einer virtuellen Maschine laufen lassen und mit Geräten über den LinkManager auf dem Host-Betriebssystem verbinden, wenn die virtuelle Maschine für "NAT" konfiguriert ist.*

25. Schließlich, wenn Sie im Installations-Assistenten auf Fertigstellen klicken, wird das LinkManager Symbol in der Windows-Taskleiste nach einer Weile wieder grün angezeigt und Ihr Standard-Web-Browser öffnet sich und zeigt den LinkManager Web GUI an. 

**Tipp:** Wenn das LinkManager-Symbol  für eine lange Zeit gelb bleibt, könnte dies darauf hindeuten, dass etwas auf dem PC den korrekten Start des LinkManagers verhindert. Konsultieren Sie die FAQ hier für Fehlersuche-Info: <http://www.secomea.com/industry/support/faq/>



26. **Browse (Suchen)** Sie nach dem Zertifikat, das Sie gerade gespeichert haben und geben Sie das Passwort ein, das Sie für das Konto in Schritt 22 angegeben haben:

The screenshot shows a dialog box titled "Please install LinkManager User Certificate." with a warning icon. The text inside reads: "The GateManager administrator has sent you an email which contains a LinkManager User Certificate file (file type is .lmc). Press the 'Browse' button to select the certificate file from your local computer, fill in the certificate's password, and press 'Install'." Below this, there are two input fields: "Certificate file:" with a "Choose File" button and the text "Rose.lmc", and "Password:" with a masked password field. A checkbox labeled "Remember password" is also present. At the bottom, there is an "Install" button, which is highlighted with a red arrow.

27. Beim Anklicken von **Install (Installieren)** werden Sie aufgefordert, sich anzumelden. Wiederholen Sie die Eingabe des obigen Passworts und klicken Sie auf **Login**:

The screenshot shows a dialog box titled "Login" with the LinkManager logo. It contains a "Certificate:" dropdown menu set to "Rose", a "Password:" masked input field, and three checkboxes: "Remember password", "Open last domain: (none)", and "Connect last device: (none)". At the bottom, there are four buttons: "Login", "Certificates", "Shutdown", and "Advanced". A red arrow points to the "Login" button.

**Tip:** Wenn Sie zuerst eine Fehlermeldung erhalten, versuchen Sie es noch einmal. Dies passiert in einigen Fällen mit neuen Konten.



### 4.2. Verbindung zum SiteManager GUI

28. Wenn Sie sich erfolgreich über die LinkManager-Konsole angemeldet haben, erhalten Sie ein Menü, wo der linke Rahmen Ihre Domain auf dem GateManager anzeigt.

Sie werden feststellen, dass es die gleiche Domain ist wie Sie zuvor als "GM Domain Token" im SiteManager definiert haben.

Anschließend sollte der SiteManager auch im rechten Rahmen mit dem von Ihnen definierten Namen angezeigt werden. In diesem Fall **SiteA**



29. Klicken Sie auf das **Globus** Symbol neben dem SiteManager, um eine Verbindung mit der Konfiguration-GUI des SiteManagers herzustellen.



Zum ersten Mal wählen Sie die "SiteManager GUI"-Taste für ein bestimmtes Gerät. Sie werden mit einer Browsermeldung begrüßt, die besagt, dass das Zertifikat der Website unsicher ist (der genaue Wortlaut ist vom Browser abhängig).



Das liegt daran, dass das SiteManager Zertifikat und die temporäre IP-Adresse um es zu erreichen, von einem öffentlichen Zertifikat-



Authentifizierungsdienst nicht erkannt werden. Sie können beruhigt auf **Continue (Weiter)** drücken.

### 4.3. Die SiteManager Netzwerkeinstellungen konfigurieren

**Anmerkung:** Wenn Sie sich mit einem Gerät im selben Netzwerk wie die Uplink-Schnittstelle (vgl. Abschnitt 2.2) verbinden möchten oder wenn Sie ein serielles oder USB-Gerät an den SiteManager anschließen wollen, brauchen Sie nichts zu konfigurieren oder an den DEV-Port des SiteManagers anzuschließen, sondern können direkt zu **Abschnitt 4.4** auf **Seite 20** gehen.

In den folgenden Schritten nehmen wir an, wir wollen ein Gerät an den **DEV-Port** des SiteManagers anschließen und ein separates Gerät-Netzwerk erstellen.

30. Sofern Ihr Gerät bereits über eine IP-Adresse im Standard-DEV-Netzwerk des SiteManagers (10.0.0.0/24) verfügt, müssen Sie die IP-Adresse des DEV-Ports auf dem SiteManager ändern.

**WICHTIG:** Diese IP-Adresse muss mit der Subnetzmaske des Geräts übereinstimmen und darf sich nicht im gleichen IP-Subnetz wie der Uplink-Port befinden.

Wählen Sie **Edit (Bearbeiten)** auf dem DEV-Port:

SiteManager  
secomea

SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

SiteManager 3134 - Setup Assistant

1. GateManager:	130.226.210.167	Connected to 130.226.210.167:11444 (UPLINK)	Edit
2. Uplink port:	172.16.15.109/24 (DHCP)	Up	Edit
3. DEV port:	10.0.0.1/24 [default]		Edit
4. Device Agents:		No agents defined	Fix
5. Admin Password:		Using default password	Fix

You can open the Setup Assistant at any time by clicking on **SETUP** in the top menu.  
Note: If you click on **HELP** it shows specific help for the current configuration page.  
Please consult the online help as your first step in solving setup problems.

31. Die SPS in unserem Beispiel hat die IP-Adresse 172.24.2.129/24 (/24 bedeutet, sie hat Subnetzmaske 255.255.255.0). So muss die Adresse für den DEV-Port eine freie Adresse in diesem Subnetz (172.24.2.x) sein, zum Beispiel 172.24.2.128.

Wählen Sie **Save (Speichern)** und **Continue Setup (Installation fortsetzen)**

Help Continue Setup >>

1

IP Address: 172.24.2.128

Subnet Mask: 255.255.255.0

Auto Subnet Agent: Enabled

Proxy ARP: Disabled

2 Save DHCP >> DNS >>

3



**Tipp:** Wenn Ihr Gerät so konfiguriert ist, um eine IP-Adresse von einem DHCP-Server zu erhalten, könnten Sie DHCP in diesem Menü aktiviert haben, was zur Folge hätte, dass der SiteManager als DHCP-Server agiert, der IP-Adressen an Geräte auf dem DEV-Netzwerk zuweist.

Sie können sogar die DHCP-Lease an ein Gerät mit MAC-Adresse sperren, so dass Ihr Gerät immer die gleiche IP-Adresse erhält.

32. Zurück im Bildschirm Setup Assistent werden Sie feststellen, dass der SiteManager einen Neustart benötigt, um die Änderungen (die neue DEV IP-Adresse) zu aktivieren.

Wählen Sie **Fix (Beheben)** und aktivieren Sie den Neustart:

SiteManager  
sec<sup>o</sup>mea

SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

SiteManager 3134 - Setup Assistant

1. GateManager:	130.226.210.167	Connected to 130.226.210.167:11444 (UPLINK)	Edit
2. Uplink port:	172.16.15.109/24 (DHCP)	Up	Edit
3. DEV port:	172.24.2.128/24		Edit
4. Device Agents:		No agents defined	Fix
5. Admin Password:		Using default password	Fix
6. Reboot:		Need Reboot	Fix

You can open the Setup Assistant at any time by clicking on **SETUP** in the top menu.  
Note: If you click on **HELP**, it shows specific help for the current configuration page.  
Please consult the online help as your first step in solving setup problems.

SiteManager  
sec<sup>o</sup>mea

SETUP • System GateManager VPN Routing Maintenance Status Log • HELP

Rebooting...

■■■■

Your browser will automatically reconnect when the appliance has rebooted.

**Tipp:** Falls Ihr Browser sich nicht automatisch wieder verbindet, drücken Sie **F5** einige Male um zu sehen, ob er online ist.



### 4.4. Den SiteManager Geräte-Agenten konfigurieren

33. Der SiteManager Setup-Assistent zeigt an, dass keine Agenten konfiguriert sind.

Wählen Sie **Fix (Beheben)**

**SiteManager 3134 - Setup Assistant**

1. GateManager:	130.226.210.167	Connected to 130.226.210.167:11444 (UPLINK)	Edit
2. Uplink port:	172.16.15.109/24 (DHCP)	Up	Edit
3. DEV port:	10.0.0.1/24 [default]		Edit
4. Device Agents:	No agents defined		Fix
5. Admin Password:	Using default password		Fix

You can open the Setup Assistant at any time by clicking on **SETUP** in the top menu.  
**Note:** If you click on **HELP** it shows specific help for the current configuration page.  
*Please consult the online help as your first step in solving setup problems.*

34. Klicken Sie **New (Neu)** um einen neuen Agent zu erstellen.

**GateManager Agents - Setup Assistant**

You can configure an agent to monitor a device connected to the SiteManager Serial port and TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager.

Click [New], and give the Agent a name (this name will be what the LinkManager user will see), and select a suitable device type (first vendor, then model). Then click on to specify the device address and other relevant parameters.

The SiteManager will instantly try to connect to the device, and if successful the Agent will go IDLE and appear on the GateManager and any LinkManager that have been granted access to the domain of the SiteManager.

If not successful, the Agent will report an error, and the agent will not be registered on the GateManager and subsequently not on LinkManagers either.

Help Continue Setup >>

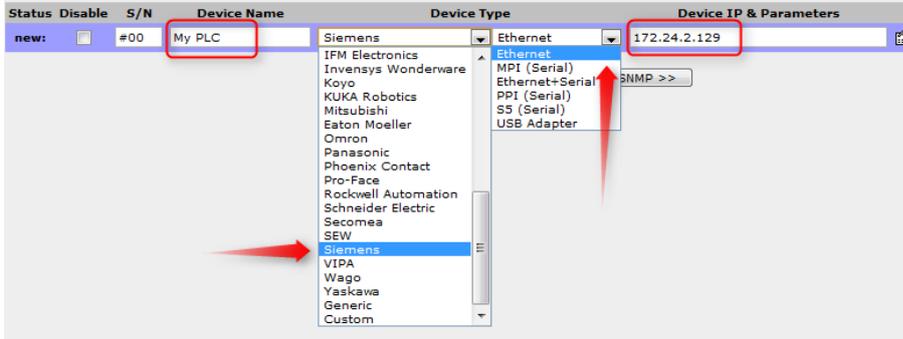
Using 0 of 50 agents

New SNMP >>

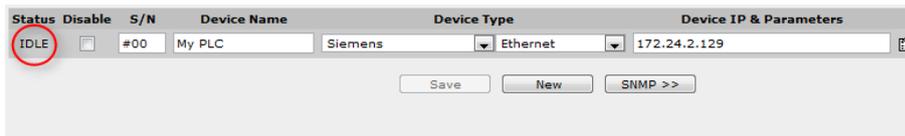


35. In diesem Beispiel haben wir ein Siemens S300 SPS gewählt und der **Gerätetyp** sollte daher "Siemens / Ethernet" lauten.

Geben Sie einen passenden **Gerätenamen** ein und geben Sie die **IP-Adresse** des Geräts ein.



36. Klicken Sie auf **Save (Speichern)** und klicken Sie auf die Schaltfläche **Refresh (Aktualisieren)**, bis Sie sehen, dass der Agent auf **IDLE (Leerlauf)** übergeht:



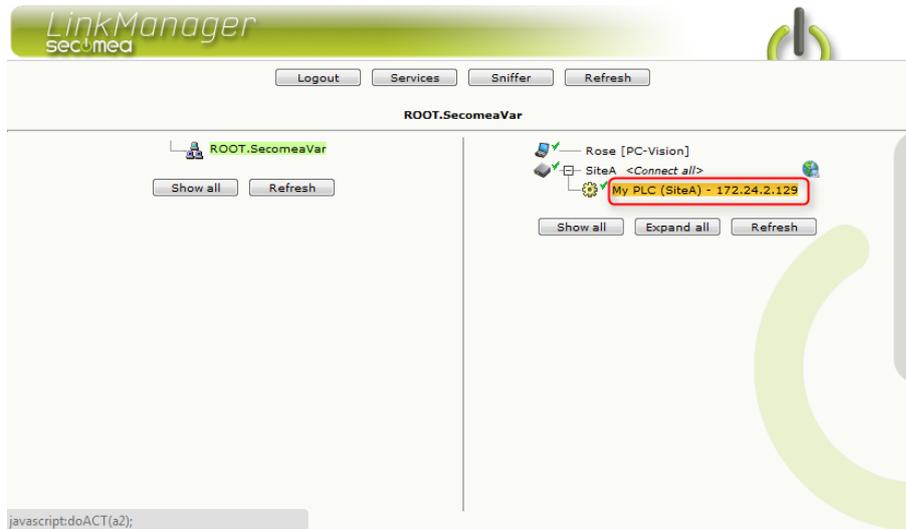
**Tipp:** Wenn es nicht in den Leerlauf übergeht, bedeutet dies, dass der SiteManager keine Antwort vom Gerät erhält und Sie sollten die konfigurierten IP-Adressen und Ethernet-Verkabelungen erneut prüfen.

37. Suchen Sie das Browser-Fenster mit dem LinkManager. Klicken Sie auf **Aktualisieren** im oberen Menü, und Sie werden nun ein "+" Zeichen feststellen, das den SiteManager erweitert:

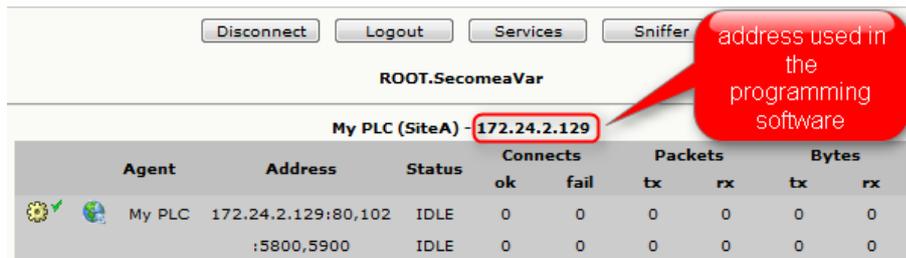




38. Erweitern Sie es und **Klicken Sie auf den Text** des Agenten, um eine Verbindung herzustellen.



39. Der Agent wird nun alle Ports öffnen, die für die Programmierung dieser Art von SPS wichtig sind.



Sie haben nun von Ihrem PC aus TCP/IP Zugriff auf das Gerät durch den LinkManager über den GateManager und den SiteManager. Sie können sich jetzt daher direkt an die IP-Adresse des Geräts unter Verwendung der nativen SPS-Software verbinden (in diesem Beispiel Siemens Step7 oder TIA Portal).

Für weitere Informationen, lesen Sie die Anleitungen für die verschiedenen Arten von Geräten in Abschnitt D hier: <http://info.secomea.com/quick-start>



40. Abhängig vom Agententyp, können Sie auch eine **Globus-Symbol** erhalten, mit dem Sie sich mit der Web-GUI des Gerätes verbinden können:

Agent	Address	Status	Connects		Packets		Bytes	
			ok	fail	tx	rx	tx	rx
 My PLC	172.24.2.129:80,102	IDLE	0	0	0	0	0	0
	:5800,5900	IDLE	0	0	0	0	0	0

41. Dies bringt Sie direkt zur lokalen Web-Schnittstelle der SPS:





## 5. Zusammenfassung

Wenn die IP-Adresse aus dem obigen Beispiel eine SPS in Ihrem Netzwerk darstellen würde, müssen Sie diese Adresse nur in Ihrer SPS-Programmiersoftware konfigurieren; so als befänden Sie sich dazu lokal.

Wenn Sie diese Übung mit Ihrem LinkManager, dem SiteManager und dem verwalteten Gerät durchgeführt haben, das an das selbe Netzwerk angeschlossen ist, können Sie denken: "wird die Verbindung nicht gerade direkt ausgeführt und nicht über LinkManager, GateManager und SiteManager?"

In der Tat, die gesamte Kommunikation über den GateManager wird immer verschlüsselt, so dass, egal wo Sie SiteManager und SPS-Gerät auf dem Internet platzieren, wird Ihre Erfahrung die gleiche sein: das Gerät scheint lokal auf Ihrem PC zu sitzen und mit seiner wahren lokalen IP-Adresse vertreten.

Sie könnten sogar alle Geräte eines bestimmten Typs, die an verschiedenen Orten platziert sind, die gleiche lokale IP-Adresse nutzen lassen. Damit können Sie ein SPS-Projekt mit der gleichen IP-Adresse für alle SPS haben.

Wenn Sie feststellen, dass die Dinge wie in dieser Anleitung beschrieben funktionieren, empfehlen wir Ihnen, weiter zu gehen und den SiteManager in einer wirklichen Produktionsstätte einzusetzen, reale industrielle Geräten zu konfigurieren und Sie mit Ihrer eigenen Programmiersoftware auszuprobieren.

Alles ist voll funktionsfähig und bereit für den Einsatz in der Produktion!

## 6. Ihr GateManager Administrator-Konto von BASIC PREMIUM (P / N 26777) aktualisieren

Mit Ihrem aktuellen GateManager BASIC Konto nutzen Sie nur das GateManager Administrator-Konto um Ihre LinkManager Konten zu verwalten.

Sie können jedoch auf **GateManager PREMIUM** aufrüsten und ein Full GateManager Administrator-Konto erhalten.

Dieses Upgrade wird Ihrem aktuellen Benutzerkonto die folgenden Funktionen hinzufügen:

- Organisieren Sie Ausrüstung in Domains pro Kunde, Werk, Zugriffsebenen oder einer anderen logischen Struktur (erstellen Sie Domains und Drag & Drop-Geräte und SiteManagers in relevanten Domains)
- Geben Sie LinkManager-Konten individuellen Zugriff auf Domains (alle LinkManager-Konten werden bei der Anmeldung eine Lizenz aus dem gleichen LinkManager Floating-Lizenz-Pool auf dem Server ziehen)
- Verwalten Sie alle SiteManager aus der Ferne (Konfiguration, Backup, Firmware-Upgrade)
- Besuchen Sie die LinkManager-GUI Ihrer Benutzer, so können Sie Fernassistenz anbieten, indem Sie den gleichen LinkManager Bildschirm ansehen, den der Benutzer lokal sieht.
- Verteilen Sie Nachrichten für LinkManager-Nutzer, die den Benutzern automatisch angezeigt werden, wenn sie sich im LinkManager angemeldet haben (z.B. eine Meldung zur Server-Wartung)
- Holen Sie sich einen Überblick über den Status aller angeschlossenen Geräte und haben Sie die Möglichkeit, Alarmregeln anzuwenden, die zu E-Mail-Berichten führen, wenn dieser ausgelöst wird (z. B. nicht verbunden etc.)
- Erhalten Sie Zugriff auf Audit-Protokolle für alle Geräte (wer hat was, wann getan)
- Erstellen Sie eine unbegrenzte Anzahl von Co-Administratoren für den Zugriff auf die GateManager Console.
- Verwalten Sie alle GateManager Console und LinkManager Konten und entziehen Sie ausgeschiedene Mitarbeitern zum Beispiel den Zugriff oder definieren Sie einen zeitlich begrenzten Zugang für bestimmte Konten.

Sie können ein GateManager PREMIUM-Konto mit der Secomea Teilenummer 26777 bestellen.



## Hinweise

### Veröffentlichung und Urheberrechte

© **Copyright Secomea A/S 2008-2012.** Alle Rechte vorbehalten. Sie können eine Kopie für den eigenen Gebrauch herunterladen und drucken. Als Administrator auf hoher Ebene können Sie jeden beliebigen Inhalt dieses Dokuments dazu nutzen, eine eigene Anleitung für den Einsatz unserer Produkte zu erstellen. Andernfalls darf kein Teil dieses Dokuments ohne die schriftliche Zustimmung der Secomea A/S vervielfältigt oder in irgendeiner Weise reproduziert werden. Wir würden uns freuen, eine Kopie des von Ihnen produzierten Materials zu erhalten, um unser eigenes Material zu verbessern und - wenn Sie uns die Erlaubnis dazu geben - andere Nutzer zu inspirieren.

### Handelsmarken

SiteManager™, LinkManager™ und GateManager™ sind Warenzeichen von Secomea A/S. Alle anderen Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

### Haftungsausschluss

Secomea A/S behält sich das Recht vor, ohne Vorankündigung Änderungen an diesem Dokument und an den hierin beschriebenen Produkten vorzunehmen. Die Veröffentlichung dieses Dokuments stellt keine Verpflichtung seitens Secomea A/S dar. Erhebliche Anstrengungen wurden unternommen, um sicherzustellen, dass diese Veröffentlichung keine Ungenauigkeiten enthält und Auslassungen vorweist, aber wir können nicht garantieren, dass es keine gibt.

Der folgende Abschnitt gilt nicht für Länder oder Staaten, in denen die nachstehenden Bestimmungen nicht mit dem jeweils dort geltenden Recht vereinbar sind:

SECOMEA A/S LIEFERT DIESE VERÖFFENTLICHUNG OHNE JEDLICHE GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, ABER NICHT AUSSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

SECOMEA A/S HAFTET NICHT FÜR DIREKTE, INDIREKTE, FOLGE- ODER ANDERE SCHÄDEN IN VERBINDUNG MIT ODER DIE VERWENDUNG VON DIESEN INFORMATIONEN.