HIRSCHMANN
A BELDEN BRAND

GateManager BASIC Guide

Using SiteManager Embedded for Windows

GateManager™ BASIC

GateManager™ Basic
Release 01 02/2016

Technical Support
https://hirschmann-support.belden.eu.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

This guide is intended for first time users of the Secure Remote Access Solution, who need a practical introduction to the Hirschmann GateManager Basic Administration solution together with the SiteManager Embedded (SM-E) for Windows software.

The same configuration steps are used for hardware-based SiteManagers, such as the GECKO.

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

Contents

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 an available SiteManager license on your GateManager.
- You have a Windows machine to install SiteManager Embedded (SM-E) on (supported platforms: Windows XP/7/8, Standard or Embedded). Alternatively, you could use a hardware SiteManager such as a GECKO, running at least v02.0.00 software.
- You have received, by email, a GateManager administrator certificate with a link to the GateManager web portal.

1.2 Component Analogies

With the Hirschmann 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 is comparable with the traditional dial-up modem attached to the machine at the customer site. The big difference is that SiteManager utilizes the existing network infrastructure to obtain an Internet connection.

LinkManager Client Software. This is comparable with the modem dial-up software on the service engineer's 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 gets instant access to the device over the Internet.

GateManager Server. This component acts as a switchboard 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).

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:

SiteManager Installer.

This role covers the following tasks:

Physically Install SiteManagers (often done by the service engineer or the customer)

Configure network settings (primarily initial GateManager access)

GateManager BASIC administrator.

This role covers the following tasks:

Assign licenses to connected SM-Es (Windows PCs running SM-E software or hardware devices)

Create and administering LinkManager user accounts.

LinkManager User.

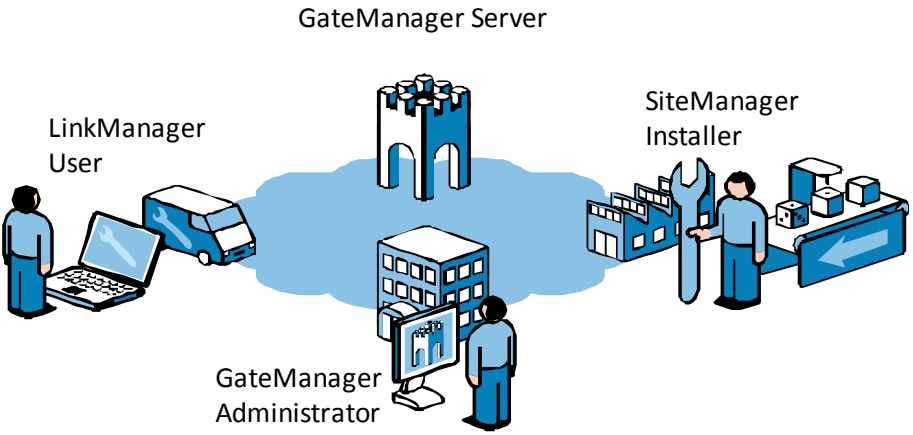
This role is held by the PLC programmer or service engineer:

Connect remotely to equipment for servicing/programming the equipment.

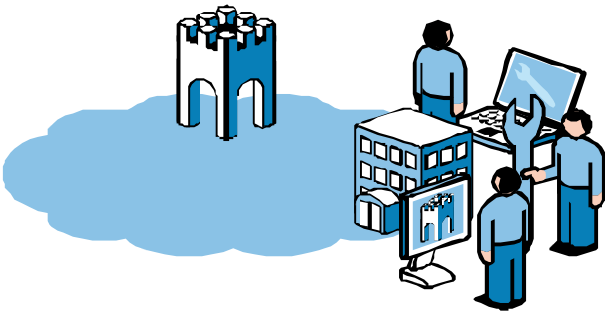
Optionally configure the SiteManager and devices agents on the SiteManager, if not done by the SiteManager Installer role.

1.4 Illustration of role locations

The typical setup 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 require a little more advanced configuration depending on special infrastructure setup.

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

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

2 Basic Setup and connection

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

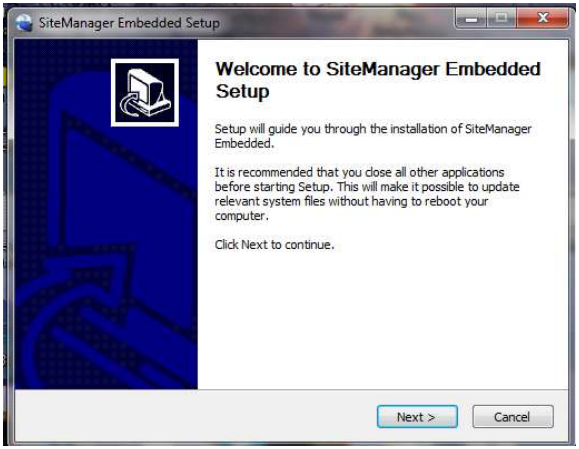
2.1 ROLE: SiteManager Embedded (SM-E) Installer

Download the SM-E from this location:

http://www.hirschmann.com/en/QR/SRA-SiteManager-Download

2.1.1 SM-E Installation

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

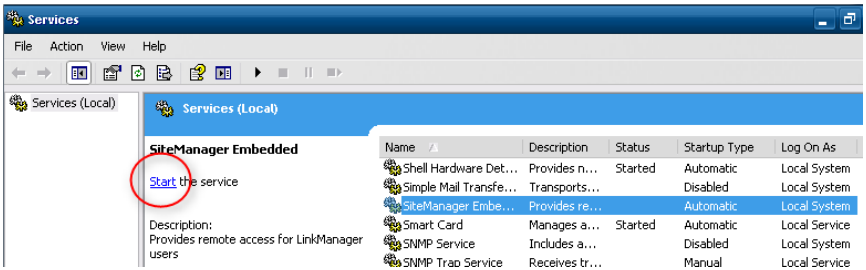


A Web browser should open automatically with the SM-E Setup Assistant.

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).

In that case you should restart the Windows machine, which will automatically start the service, or you can start the service manually.

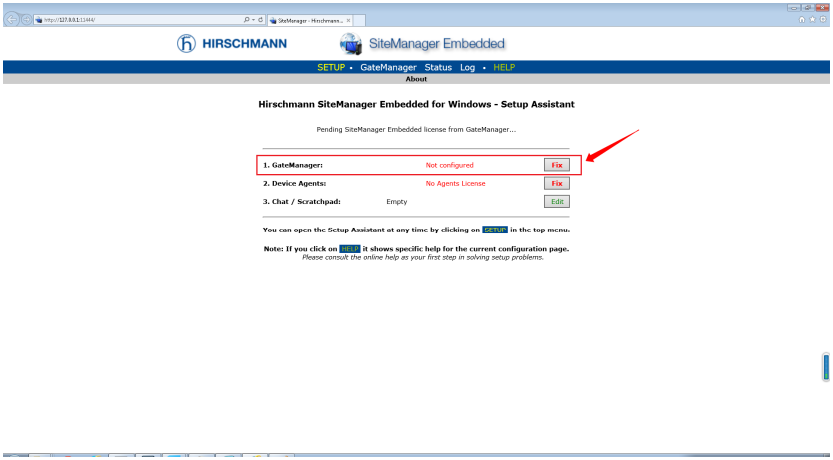
- Select Start -> Run and type the command services.msc.
- Scroll to the SiteManager Embedded and click start



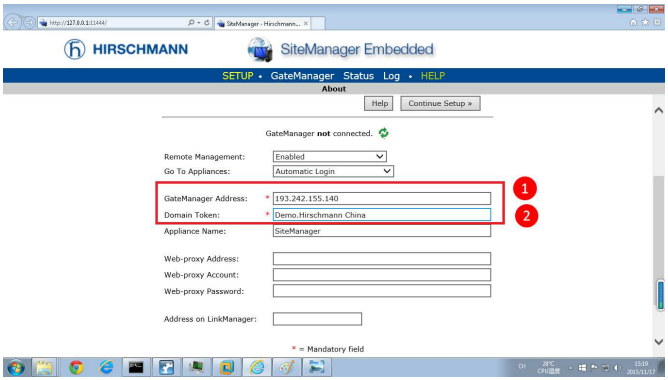
Now click the SM-E shortcut on the desktop to open the SM-E Web GUI:

2.1.2 Configure the GateManager settings

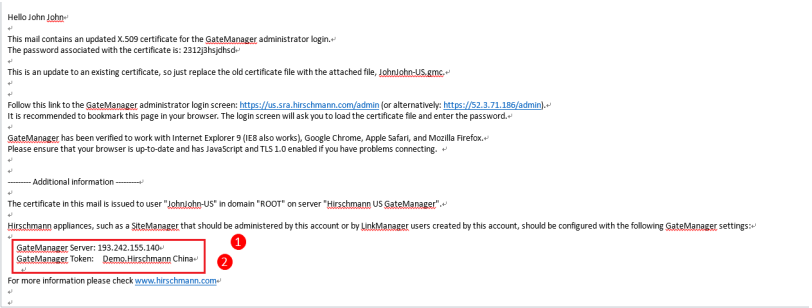
The following steps are the same for SM-E and a hardware-based SiteManager such as the GECKO. In the SM-E Web click the Fix button for the GateManager settings:



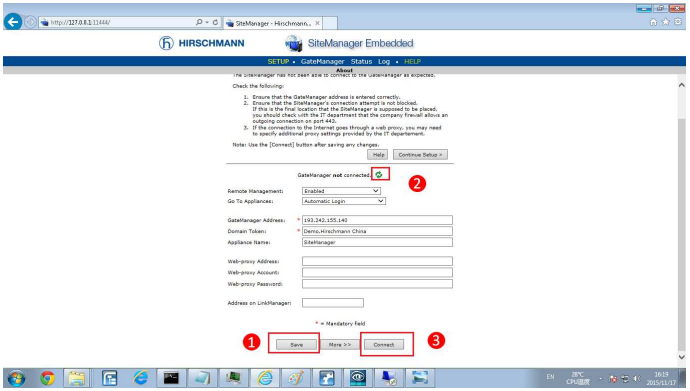
Enter the GateManager Server name and Token.



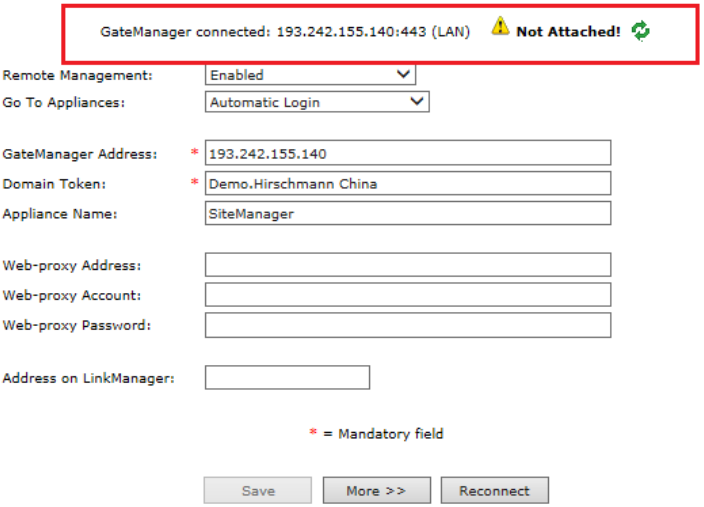
IMPORTANT: The information to enter in this screen is found in the lower section of the email you received from the GateManager with the GateManager X.509 Certificate.



Click Save and Connect, and click the refresh icon periodically.



After a short while the status should change to this:



You do not need to do more locally to the SM-E.

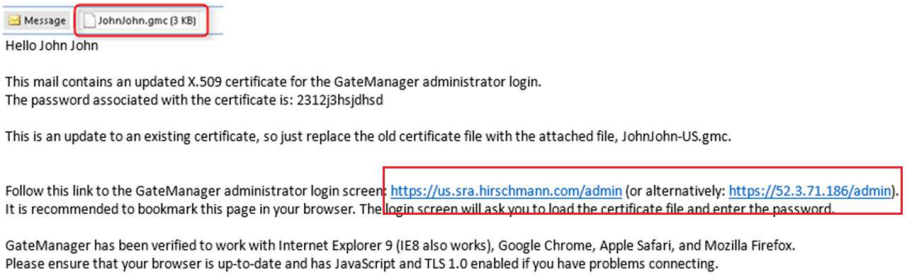
In reality you could now ship the Windows machine or GECKO to a new site.

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

2.2 ROLE: GateManager BASIC Admin

2.2.1 Install the GateManager Administrator certificate

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



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.*

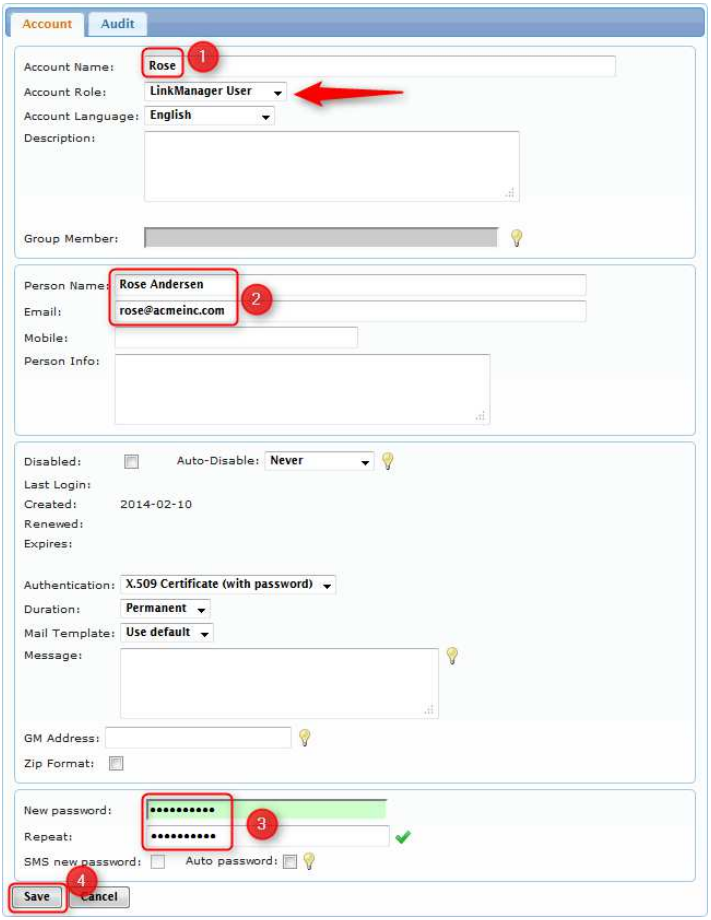
Browse for the certificate you just saved, and enter the password you were informed of by the administrator.

If you have not yet received the password via email or verbally, you should 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

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

Fill in the following information:

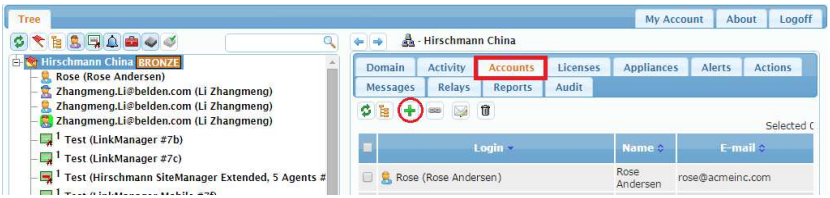


1. The **Account Name**. This will become the file name of the LinkManager certificate file (in this case Rose.lmc)
2. **Person Name, Email** and optionally **Mobile** number. In this exercise you will likely issue the account to yourself. You can later create accounts for other users. (All users will share the same LinkManager floating license)
3. Type a **Password**. If you create the account for another user, 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 it in a separate mail to the user.
4. When pressing **Save**, the email is automatically sent from the GateManager.

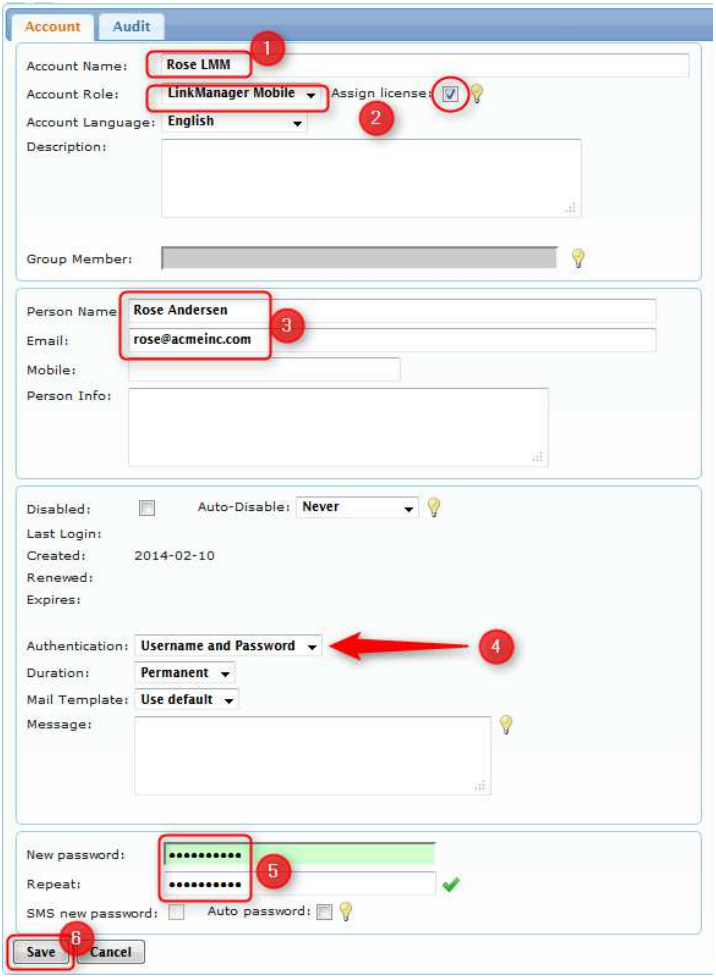
2.2.3 Create LinkManager Mobile user account

The account is created identically to the LinkManager account.

Login to the GateManager portal and select Accounts and Create new account:



Now fill in the following details:

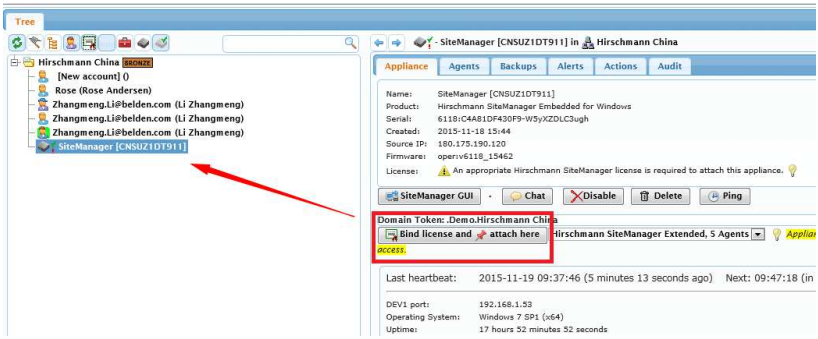


1. The **Account Name**. This will become the login login ID for the account
2. Role **LinkManager Mobile**. Note that the check box “Assign License” appears when selecting this role. When checking this box, this account will allocate the free LinkManager Mobile license and subsequently allow remote 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 user, 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 it 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 SM-E or Hardware SiteManager

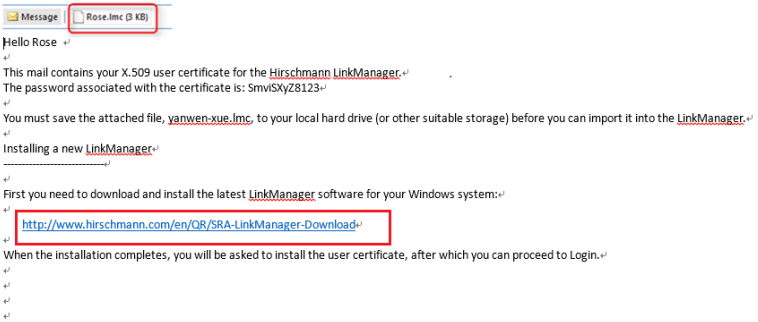
If the SM-E has been configured correctly according to section 2.1.2 Configure the GateManager settings, the SM-E or hardware SiteManager should appear in the tree view. Place your cursor on it and press **Bind license and attach here**. A SiteManager license will then be bound to the SM-E.



2.3 ROLE: LinkManager User

2.3.1 Install and login to the LinkManager

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


Message | Rose.lmc (3 KB)

Hello Rose

This mail contains your X.509 user certificate for the Hirschmann LinkManager.
The password associated with the certificate is: SmviSXyZ8123

You must save the attached file, yanwen-xue.lmc, to your local hard drive (or other suitable storage) before you can import it into the LinkManager.

Installing a new LinkManager

First you need to download and install the latest LinkManager software for your Windows system:

http://www.hirschmann.com/en/QR/SRA-LinkManager-Download

When the installation completes, you will be asked to install the user certificate, after which you can proceed to Login.

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.

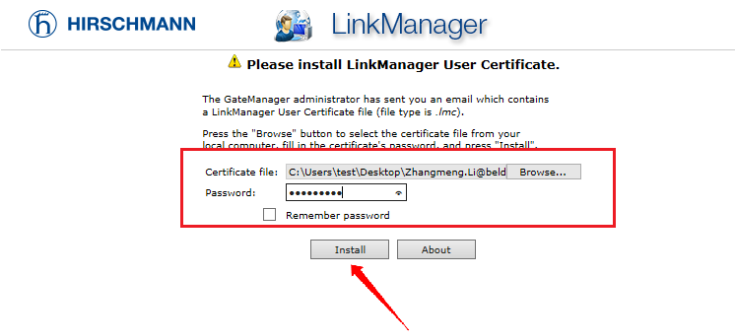
HINT: You can also install LinkManager inside a VMWare virtual machine if the host OS is Windows 7 and the CPU supports virtualization. You can also run your programming software inside a virtual machine and connect to devices via LinkManager installed on the host OS if the virtual machine is configured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

Eventually, when you click Finish in the installation wizard, the bubble help of the LinkManager icon will show the IP address of the GateManager to which it is connected. Your default web browser will open, showing the LinkManager Web GUI.

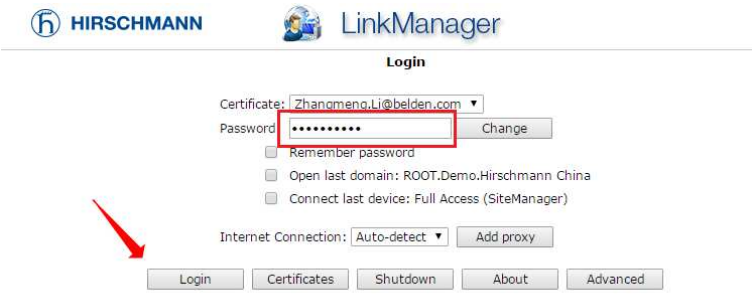
Hint: If The LinkManager icon does not display the GateManager IP address for a long while, it could indicate that something on the PC is preventing the LinkManager from starting correctly. Consult the FAQ here for trouble shooting info:

http://www.hirschmann.com/en/QR/SRA-LinkManager-Download

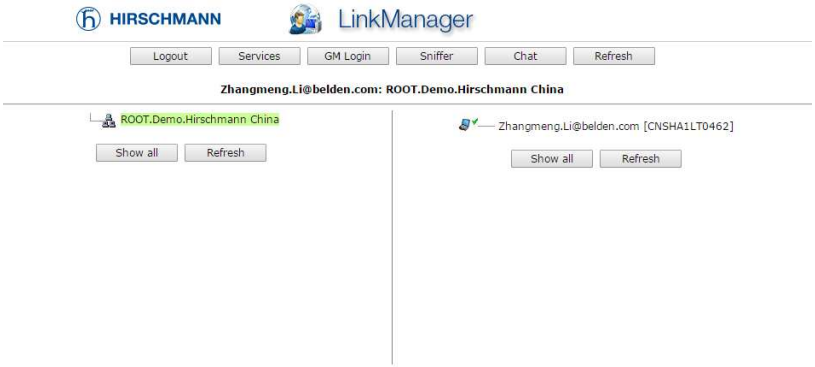
Browse for the certificate you just saved and enter the password you specified for the account earlier:



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

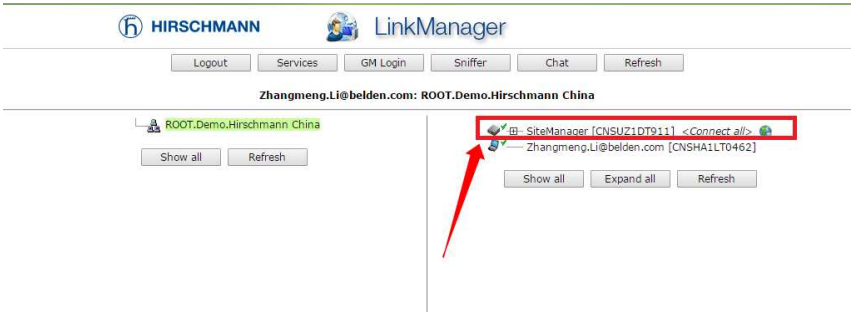


You are now logged in.

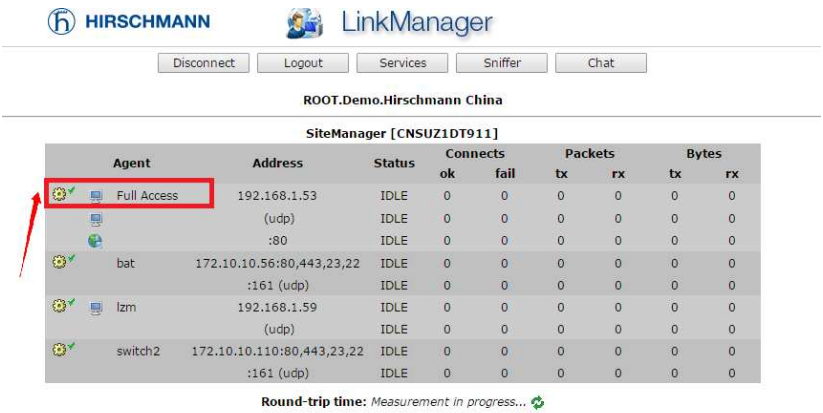


2.3.2 Connect to the PC via the SM-E

Click on the SiteManager <Connect All>

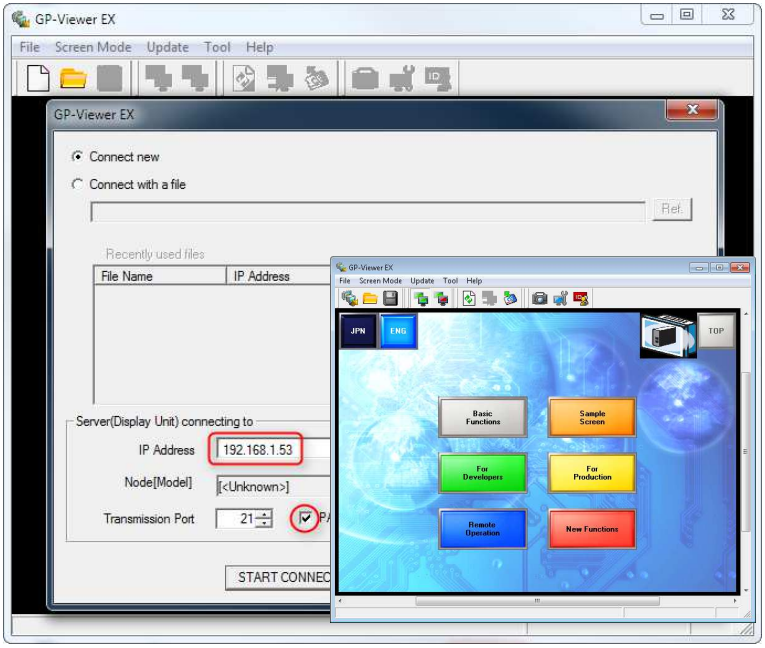


You are now connected to the IP address of the PC.

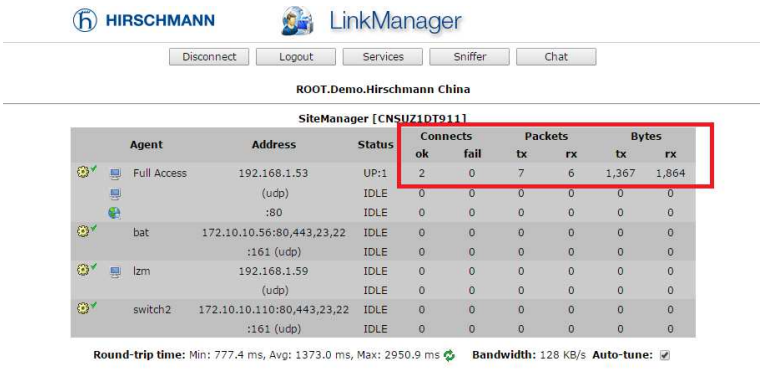


You can now connect to any application on that IP address. (Note that MS Remote Desktop can be auto-started with the screen icon).

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 reflect the transferred data.



2.4 ROLE: LinkManager Mobile User

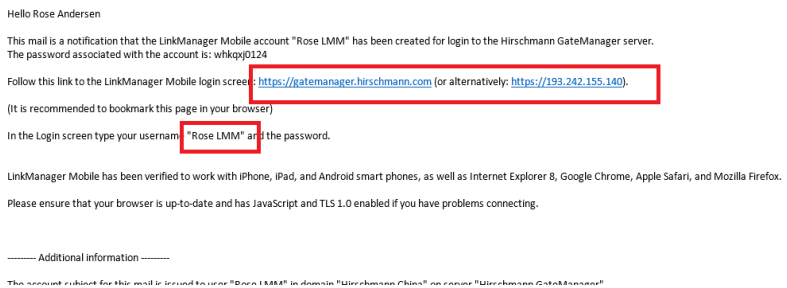
LinkManger Mobile can be seen as a “light-weight” version of LinkManager that can be used from most devices with a web browser, such as PCs, Smartphones and tablets.

With LinkManager mobile you can connect to the Web GUI (http/https) on a device.

2.4.1 Login and connect to a web GUI with LinkManager Mobile

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.



Hello Rose Andersen

This mail is a notification that the LinkManager Mobile account "Rose LMM" has been created for login to the Hirschmann GateManager server.
The password associated with the account is: whkqxj0124

Follow this link to the LinkManager Mobile login screen: https://gatemanager.hirschmann.com (or alternatively: https://193.242.155.140).

(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.

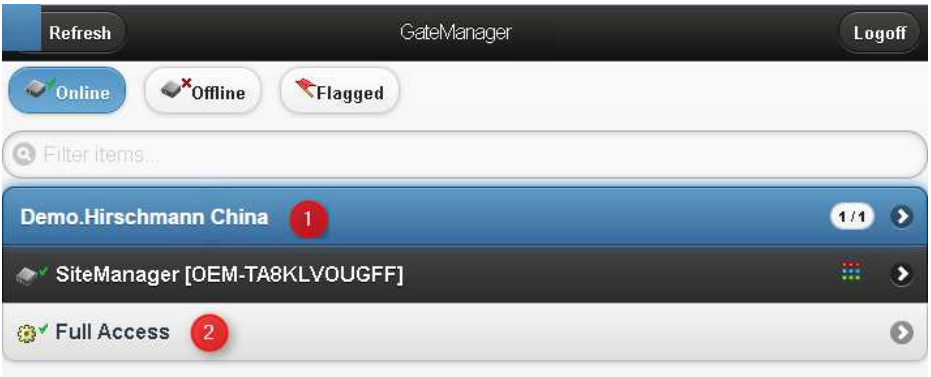
Please ensure that your browser is up-to-date and has JavaScript and TLS 1.0 enabled if you have problems connecting.

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

The account subject for this mail is issued to user "Rose LMM" in domain "Hirschmann China" on server "Hirschmann GateManager"

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.

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



3 SM-E Basic - Adjusting Agents

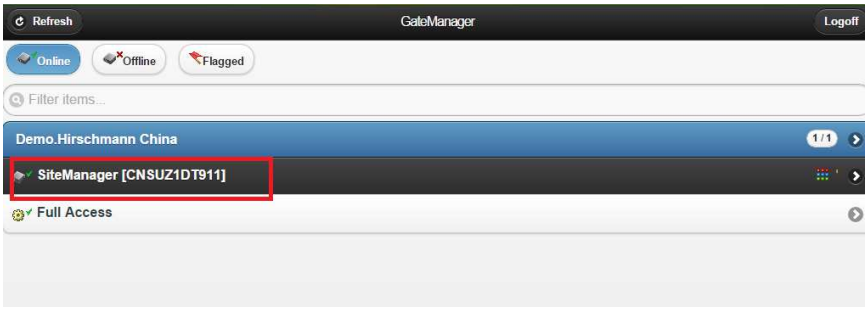
This section describes how to extend SM-E Basic to allow access to selected services on the windows computer.

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

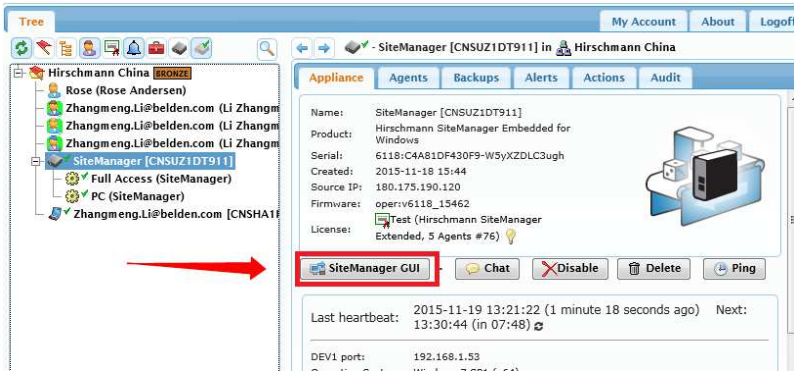
Connect to the Web GUI of the SM-E. This can be done either from the LinkManager Mobile, LinkManager or from the GateManager Portal:

From **LinkManager Mobile**: Select the SiteManager and click WWW:

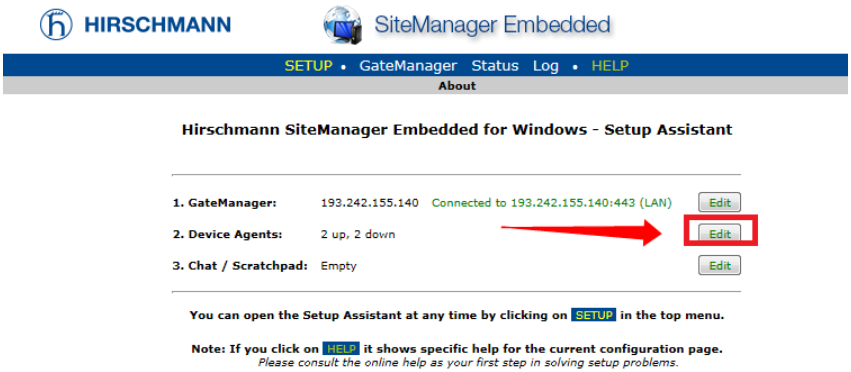


Or from LinkManager: Select the globe next to the SM-E

Or from the GateManager Portal: Click the SiteManager GUI button.



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 GateManager, and is using a randomized port number, (in this case 55700 as indicated in the address line). Your outgoing firewall must support http and https access via the port range 55000-59999 for remote web access to work.

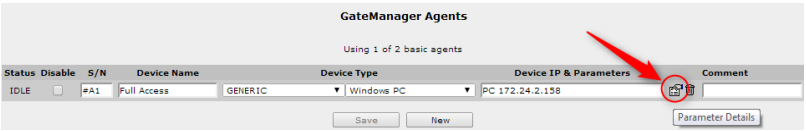
3.2 Enable standard connect buttons for Agents

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.

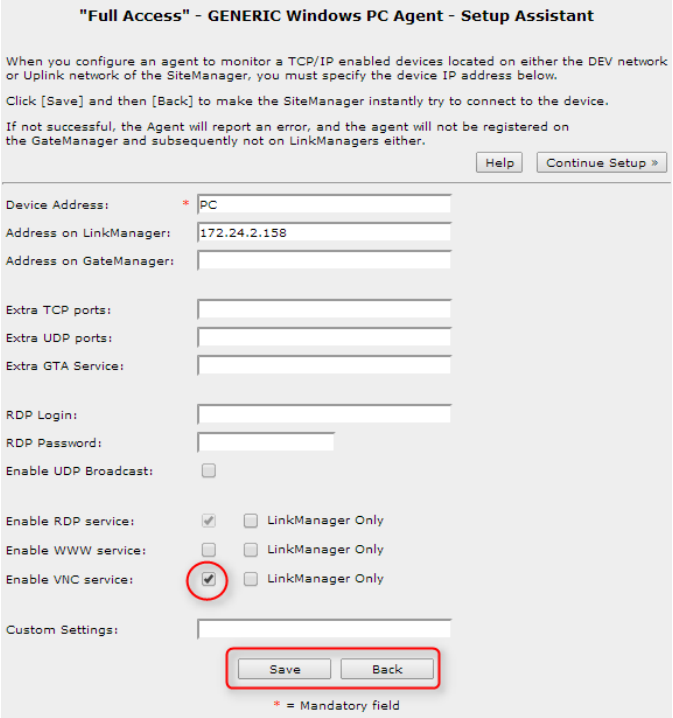
Typically these buttons are not enabled default, as the corresponding service (listen socket), may not be available for the device that the Agent represents.

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

Click the Parameter details for the Full Access agent.



Check “VNC”, and select Save and Back.

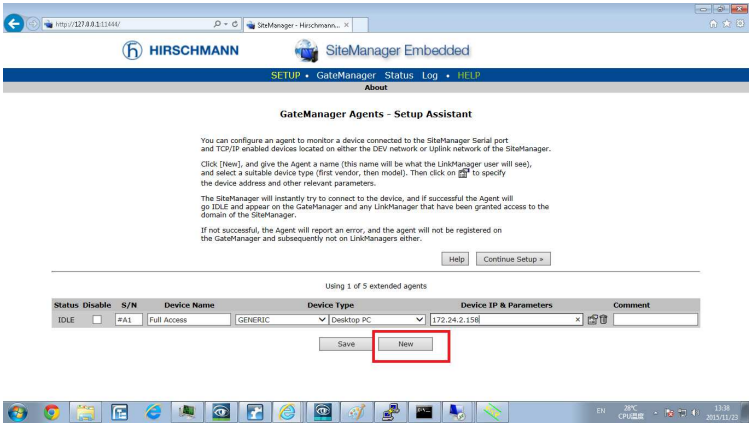

"Full Access" - GENERIC Windows PC Agent - Setup Assistant
When you configure an agent to monitor a TCP/IP enabled devices located on either the DEV network or Uplink network of the SiteManager, you must specify the device IP address below.
Click [Save] and then [Back] to make the SiteManager instantly try to connect to the device.
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 »
Device Address:
PC
Address on LinkManager:
172.24.2.158
Address on GateManager:
Extra TCP ports:
Extra UDP ports:
Extra GTA Service:
RDP Login:
RDP Password:
Enable UDP Broadcast:
Enable RDP service:
LinkManager Only
Enable WWW service:
LinkManager Only
Enable VNC service:
LinkManager Only
Custom Settings:
Save
Back
* = Mandatory field

3.3 Using Agents with custom LinkManager Mobile connect buttons

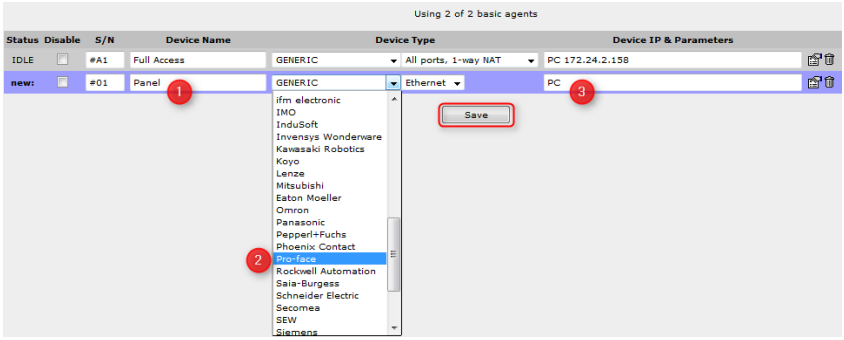
Some agents, such as Pro-face and Schneider, includes own custom connect buttons. These do not need to be defined specifically for the agent

3.3.1 Example: Create a new Pro-face Agent

Select New.

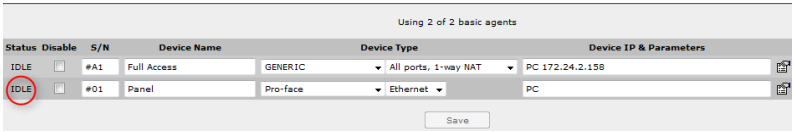


Fill in the information:



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.
3. Hint: Other options could have been Generic / Web access, which would have limited access to a web server on the computer
4. 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.

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



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.

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

Enter the following settings:

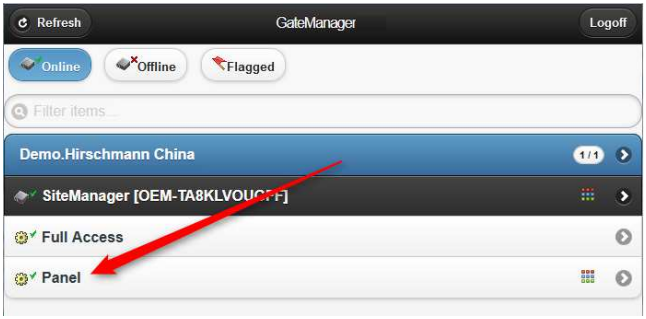
1. **Server Name**. Define a name of choice. In this case we have just entered the name of the GateManager through which the LinkManager Mobile connects.
2. **IP Address**: Enter the IP address of the GateManager server. You can find this in any mail received from the GateManager (see example in section 2.1.2)
3. **Port**. Enter Port **5900**.

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

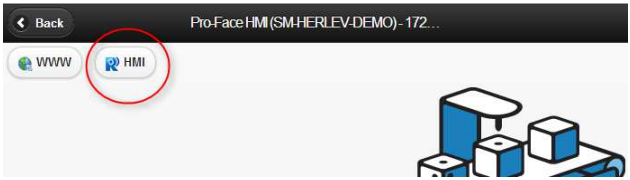
Click **Done** in the Pro-face app to save the settings.

3.3.3 Connect to the Pro-face agent with LinkManager Mobile

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



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.

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

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.

You will now be prompted for the password for the panel itself:

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

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.

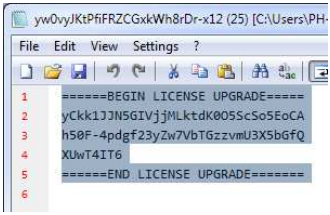
4 SM-E Extended – Accessing external devices

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 Installing licenses on (own) GateManager

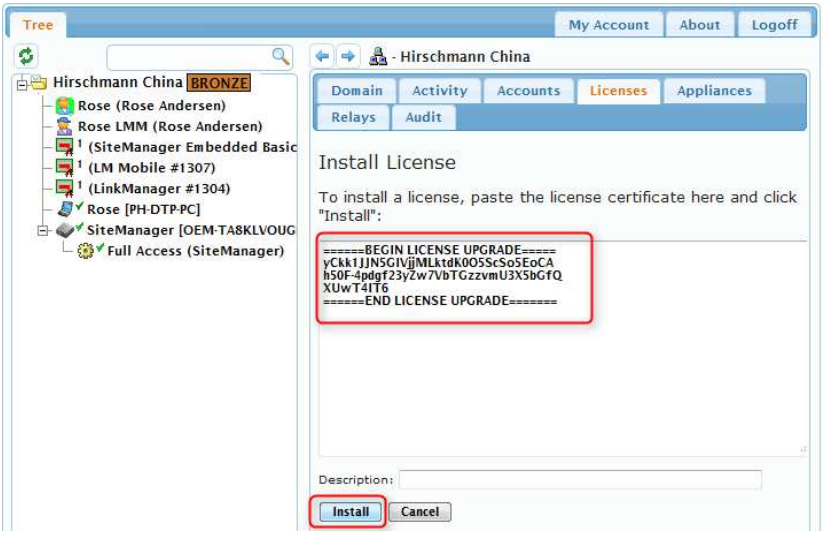
NOTE: If you running on a hosted server, your hosting provider will place the ordered license in your domain, and you can continue with section **4.2 Upgrading SM-E Basic to SM-E Extended**.

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.



Select Licenses and the “+” sign.

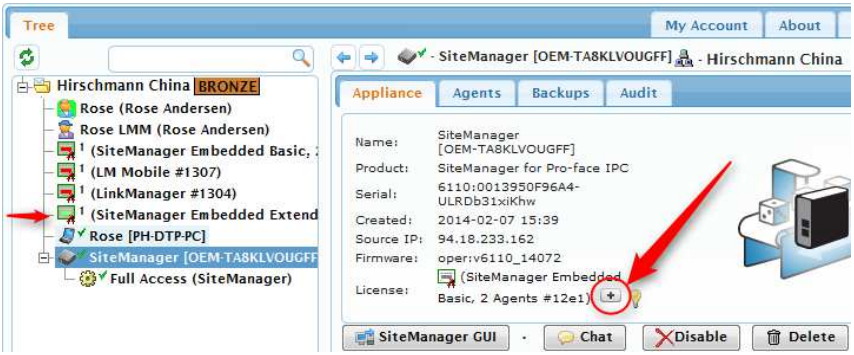
Paste the license into the text field, and click Install.



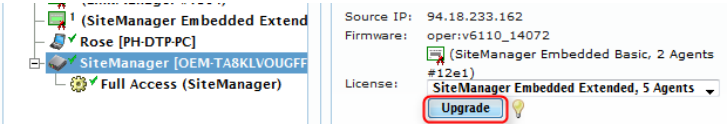
4.2 Upgrading SM-E Basic to SM-E Extended

NOTE: This section assumes you have a SM-E or hardware SiteManager with a SiteManager Basic license attached to it, and have received a SiteManager 5 or 10 Node License. If your device already has a 5 or 10 Node License, you can jump to section **4.3 Define device agent for external device**

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

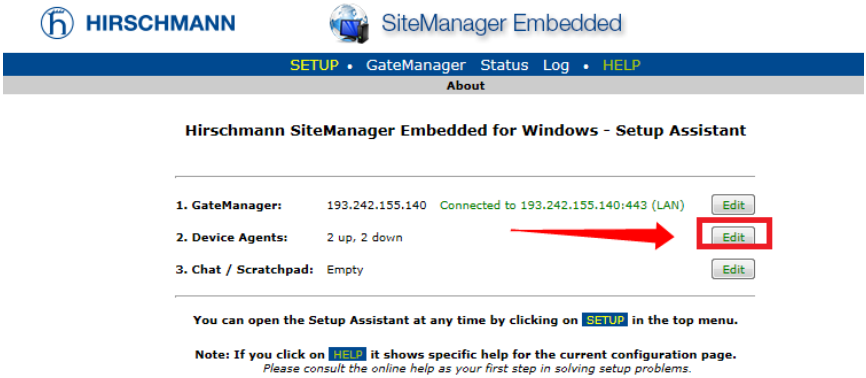


Available licenses will be listed. Click **Upgrade** to bind the license.

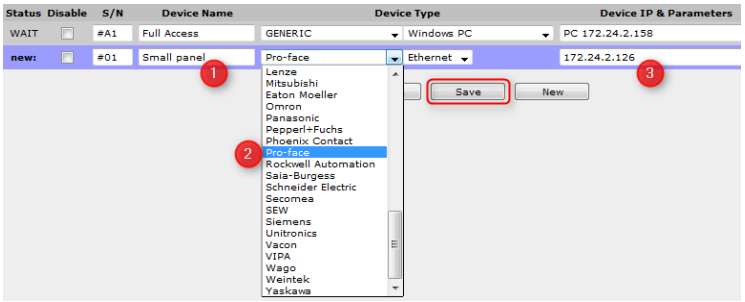


4.3 Define device agent for external device

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

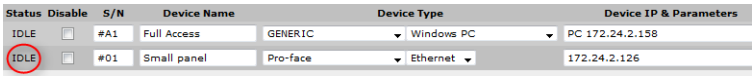


Select New and fill in the details.

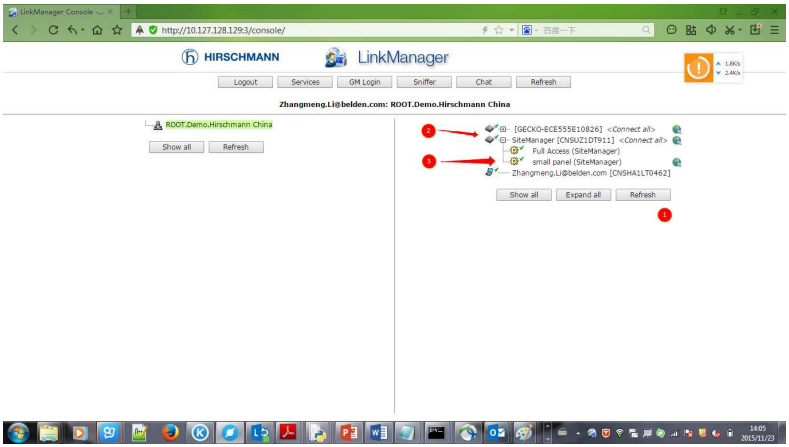


1. Fill in the name that will appear in LinkManager
2. Select the type of device. In this example we will connect to an Ethernet attached Pro-face panel
3. Enter the IP address of the device. The IP address must be accessible from the computer on which SM-E is installed.

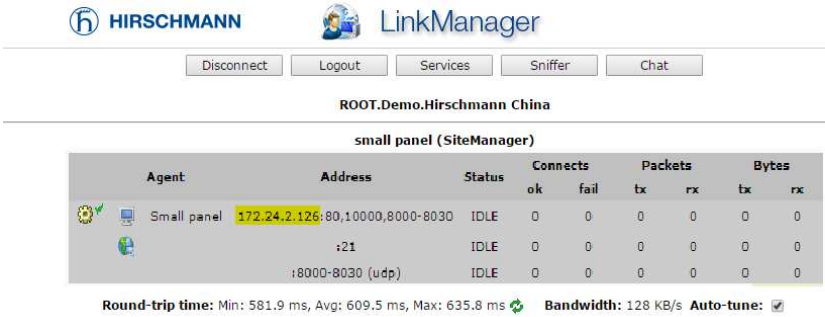
Click Save and Refresh a couple of times until the Agent becomes idle, which indicates that SM-E can reach the device.



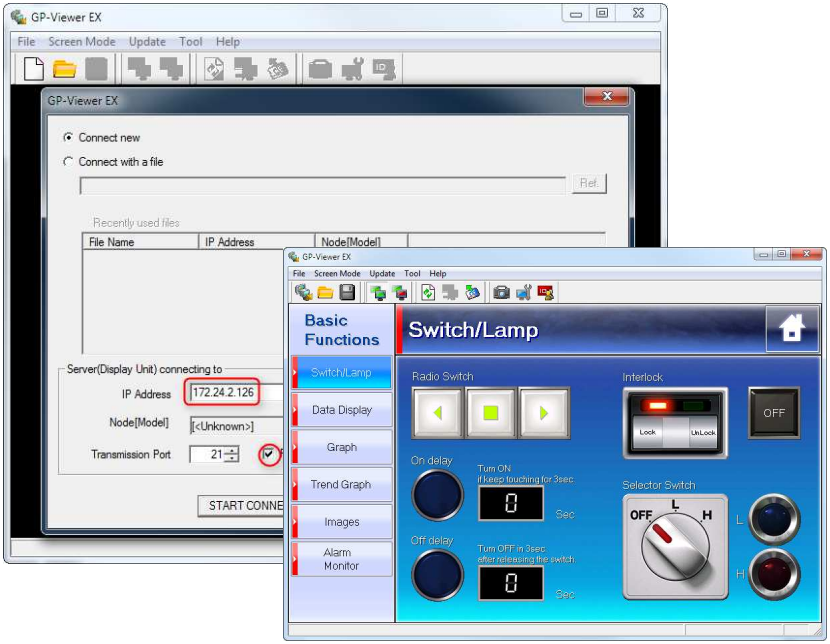
Login to LinkManager, click Refresh to update changes, Click “+” to unfold the agents on the SiteManager, and connect to the new agent, by clicking the agent description.



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



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

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 be 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.

6 Appendix A: Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.
You will find the addresses of our partners on the Internet at
http://www.hirschmann.com
Contact our support at
https://hirschmann-support.belden.eu.com

You can contact us in the EMEA region at

- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at

- Tel.: +1 (717) 217-2270
- E-mail: inet-support@belden.com

in the Asia-Pacific region at

- Tel.: +65 68549860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- The current training courses for technology and products can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet: http://www.hicomcenter.com

7 Appendix B: Third-Party Software

The software solution uses open source software originated from third parties that is subject to their respective licenses.

Firmware/Software for SiteManager, LinkManager and GateManager

(NOTE: The list below represents a common denominator for all product categories. Each of the products contains only a subset of these software components)

Linux – http://www.kernel.org
Apache httpd – http://httpd.apache.org
OpenSSL – http://www.openssl.org
mod_ssl – http://www.modssl.org
axTLS (originating from BSD) – http://axtls.sourceforge.net
busybox – http://www.busybox.net
tinylogin – http://tinylogin.busybox.net
ISC DHCP – http://www.isc.org/software/dhcp
DNRD – http://dnrd.sourceforge.net/
ethtool – http://freshmeat.net/projects/ethtool
expat – http://expat.sourceforge.net
FreeS/WAN – http://www.freeswan.org
hping – http://www.hping.org
hwclock – http://freshmeat.net/projects/hwclock
iproute2 – http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2
traceroute – http://www.linuxfoundation.org/collaborate/workgroups/networking/traceroute
bridge-utils – http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge
vconfig – http://www.candelatech.com/~greear/vlan.html
iptables – http://www.netfilter.org
OSSP mm – http://www.ossp.org/pkg/lib/mm
Net-SNMP – http://net-snmp.sourceforge.net
ntpdate – http://www.eecis.udel.edu/~mills/ntp/html/index.html
pppd – http://freshmeat.net/projects/pppd
RP-PPPoE – http://www.roaringpenguin.com/products/pppoe
e2compr – http://e2compr.sourceforge.net
lilo – http://freshmeat.net/projects/lilo
U-Boot – http://www.denx.de/wiki/U-Boot
lm_sensors – http://www.lm-sensors.org
pcmcia_cs – http://pcmcia-cs.sourceforge.net

ez-ipupdate – http://ez-ipupdate.com
Open1X – http://open1x.sourceforge.net
FreeRADIUS – http://freeradius.org
ser2net – http://sourceforge.net/projects/ser2net
Squid – http://www.squid-cache.org
glibc – http://www.gnu.org/software/libc
libGD – http://www.libgd.org
uClibc – http://www.uclibc.org
SquashFS – http://squashfs.sourceforge.net
UnionFS – http://www.fsl.cs.sunysb.edu/project-unionfs.html
VirtualBox – http://www.virtualbox.org
SDL – http://www.libsdl.org
com0com – http://com0com.sourceforge.net
gSOAP – http://gsoap2.sourceforge.net
NSIS – http://nsis.sourceforge.net
AES crypto routines – http://www.gladman.me.uk/
Cntlm – http://cntlm.sourceforge.net/
wcecompat (SM-E for WinCE only) http://wcecompat.sourceforge.net