Pro-face
by Schneider Electric

Pro-face Connect
User Guide for GateManager

Preface

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Pro-face nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information that is contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Pro-face software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Trademark Rights

All company or product names used in this manual are the trade names, trademarks (including registered trademarks) of those respective companies.

This document omits individual descriptions of each of these rights.

Microsoft, Windows, Windows Vista, Windows Server, Internet Explorer, Windows Media, Excel, Visio, DirectX, Visual Basic, Visual C++, and Visual Studio are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Intel, Pentium, and Xeon, are trademarks of Intel Corporation in the United States and/or other countries.

The following terms differ from the formal trade names and trademarks indicated in this document.

Term used in this manual	Formal Trade Name or Trademark
Windows 10	Microsoft(R) Windows(R) 10 Operating System
Windows 8.1	Microsoft(R) Windows(R) 8.1 Operating System
Windows 8	Microsoft(R) Windows(R) 8 Operating System
Windows 7	Microsoft(R) Windows(R) 7 Operating System
Windows Vista	Microsoft(R) Windows Vista(R) Operating System
Windows Embedded 8.1	Microsoft(R) Windows(R) Embedded 8.1 Industry
Windows Embedded Standard 7	Microsoft(R) Windows(R) Embedded Standard 7 Runtime (WS7P)(ESD)
Internet Explorer	Microsoft(R) Internet Explorer(R)
Google Chrome	Google Chrome (TM) browser
Mozilla Firefox	Firefox (R)
Apple Safari	Safari (R)

Manual Symbols and Terminology

Safety Symbols and Terms

This manual uses the following symbols and terms to identify important information related to the correct and safe operation of display units and Pro-face Connect. The notes shown here describe important information on safety.

Symbols and descriptions are as follows.

	The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.
	This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

General Information Symbols and Terms

This manual uses the following symbols and terms for general information.

Display	Description
IMPORTANT	States precautions and restrictions that must be followed.
NOTE	Provides tips on correct product use or supplementary information.

Terminology

This manual uses the following terms and acronyms in its descriptions:

Term used in this manual	Description
Screen Editor & Logic Program Software	Indicates GP-Pro EX or BLUE software.
Display Unit	Indicates a touch panel display unit manufactured by Pro-face for displaying the screen interface designed in Screen Editor & Logic Program Software.

Term used in this manual	Description
Device/PLC	Indicates a device, such as a PLC, that connects to a display unit.
Pro-face Connect GateManager (hereafter called "GateManager")	GateManager is used for user administration and access control for LinkManagers, and acts as communication broker between LinkManagers and SiteManagers.
Pro-face Connect SiteManager (hereafter called "SiteManager") Pro-face Connect SiteManager Embedded (hereafter called "SiteManager Embedded ")	SiteManager Embedded is the software installed on the display unit. A display unit with SiteManager Embedded running is called SiteManager.
Agent	Generic term for display units and external devices that SiteManager Embedded allowed connecting to the network. The access methods (agent) you can register differ depending on your license.
Pro-face Connect SiteManager Embedded Basic (hereafter called " SiteManager Embedded Basic ")	One of the license formats required to use SiteManager Embedded.
Pro-face Connect SiteManager Embedded Extended (hereafter called " SiteManager Embedded Extended ")	One of the license formats required to use SiteManager Embedded.
Pro-face Connect LinkManager (hereafter called " LinkManager ")	LinkManager, the software installed on your computer, allows remote access to SiteManager and/or devices represented by agents on the SiteManager.
Pro-face Connect LinkManager Mobile (hereafter called " LinkManager Mobile ")	LinkManager Mobile, a service on the GateManager, allows remote access.

About Screen Images

Depending on your operating environment, screen images presented in this document may differ from the actual screen you see.

Please keep this in mind when reading the document.

Global Code

A global code is assigned to every Pro-face product as a universal model number.

For more information on product models and their matching global codes, please refer to our Web site.

http://www.pro-face.com/trans/en/manual/1003.html

Inquiry

If you cannot solve the problem after reading this manual or other references, you can access our homepage to find a solution.

http://www.pro-face.com/trans/en/manual/1001.html

This site will help you contact the closest Pro-face office.

http://www.pro-face.com/trans/en/manual/1015.html

NOTE

- The latest manuals are available at our home page.

Table of Contents

1. Introduction

1.1. Prerequisites on Using This Guide

Prerequisites on using this guide are:

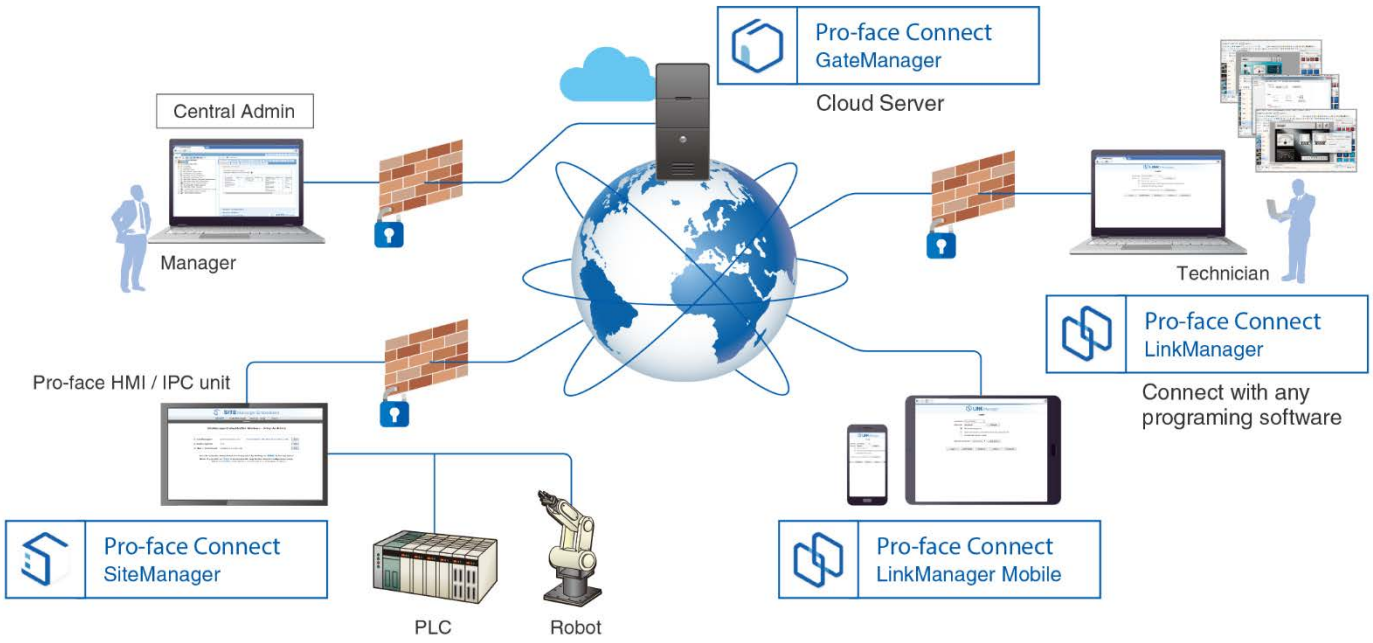
- You have administrator privileges to install a program on your Windows PC or laptop.
- Your PC has outgoing access to the Internet via https. This applies to both your corporate firewall and any personal firewall installed on your PC.
- You have a SiteManager Embedded license.
- You have received, by e-mail, a GateManager Administrator certificate with a link to the GateManager Web portal.

1.2. Concept of Pro-face Connect

1.2.1.What is Pro-face Connect?

When you want to display or operate on a personal computer or tablet, the screens of display units in remote locations, you need a system that can prevent unauthorized access from external sources.

With Pro-face Connect serving the role of router, as long as you have an Internet connection, you can construct such a system.



Pro-face Connect is structured to safely connect display units on the work site (SiteManager), with computers or smart devices in the office (LinkManager), over a server (GateManager).

- GateManager
  Server for creating a safe encrypted connection between display units on the work site (SiteManager) and personal computers or smart devices in the office (LinkManager). You can use GateManager to check the network connection status of SiteManager and LinkManager. The GateManager Administrator registers the SiteManager and LinkManager and allows access to the network.

- SiteManager
  Display unit having SiteManager Embedded running is called SiteManager. Setup for accessing the network is handled from the software; SiteManager Embedded.

- LinkManager
  Software installed on the computers. It allows remote access to SiteManager and/or devices represented by agents on the SiteManager. Setup for accessing the network is handled by GateManager. For the purpose of remote monitoring and operation, you can use data collection and remote monitoring software as the LinkManager.
  Different configurations are possible depending on the package you purchase. Refer to the license that comes with each package.

⚠ WARNING
EQUIPMENT DAMAGE ● Before performing maintenance, ensure by phone that you have on-site agreement. ● Before any update, ensure that you have a stable internet and electrical environment. ● More particularly, don't use 3G through a cell phone setup as tethering hotspot for any update. Failure to follow these instructions can result in death, serious injury, or equipment damage.

1.3. Operating Environment

The following table lists the system requirements for Pro-face Connect.

IMPORTANT

- If you receive a notification that a LinkManager update is available, install the update. Otherwise, the system may not function properly.

Models for SiteManager	For a list of the display unit models that support Pro-face Connect, see Supported Model List.
PC for GateManager / LinkManager	Windows PC/AT compatible machine
Operating System	• GateManager / LinkManager Windows 10/Windows 8/Windows 8.1/Windows 7/Windows Vista (All editions for 32/64 bit versions) • SiteManager For information about the operating system installed on a display unit, refer to its corresponding hardware manual.
Other non-operating-system programs	• Browsers Internet Explorer 9 or later, Google Chrome, Apple Safari, Mozilla Firefox
Network Settings	• Port / Protocol SiteManager runs all its communication using one of the following ports or protocols. Use in an environment that supports the port or protocol. Port 11444 Port 443 with HTTPS/TLS Port 80 with TLS over HTTP TLS via Web Proxy For details, refer to Pro-face Connect Troubleshooting for LinkManager (LinkManager connection methods).

Supported Functions and Drivers

For information on supported software, features, and drivers, refer to the following URL.

http://www.pro-face.com/trans/en/manual/1049.html

1.4. Supported Model List

You can register the following display units as SiteManager.

GP4000 Series

SP5000 Series

IPC Series

NOTE

- Available models differ depending on the screen editing software you are using.
  For more information, refer to the manuals that came with your screen editing software.

GP4000 Series

Series	Model	Model Numbers
GP-4200	GP-4201T	PFXGP4201TAD
	GP-4203T	PFXGP4203TAD
GP-4300	GP-4301T	PFXGP4301TAD
		PFXGP4301TADC
		PFXGP4301TADR
	GP-4301TW	PFXGP4301TADW
		PFXGP4301TADWC
	GP-4303T	PFXGP4303TAD
	GP-4311HT	PFXGP4311HTAD
		PFXGP4311HTADER
		PFXGP4311HTADERK
		PFXGP4311HTADEYK
		PFXGP4311HTADEGK
GP-4400	GP-4401T	PFXGP4401TAD
		PFXGP4401TADR
	GP-4401WW	PFXGP4401WADW
GP-4500	GP-4501T(Analog Touch Panel)	PFXGP4501TAD
		PFXGP4501TADC
		PFXGP4501TADR
		PFXGP4501TAA
		PFXGP4501TAAC
	GP-4501T(Matrix Touch Panel)	PFXGP4501TMD
		PFXGP4501TMA
	GP-4501TW	PFXGP4501TADW
	GP-4503T	PFXGP4503TAD
	GP-4521T	PFXGP4521TAA
GP-4600	GP-4601T(Analog Touch Panel)	PFXGP4601TAD
		PFXGP4601TADC
		PFXGP4601TADR
		PFXGP4601TAA
		PFXGP4601TAAC
	GP-4601T(Matrix Touch Panel)	PFXGP4601TMD
		PFXGP4601TMA
	GP-4603T	PFXGP4603TAD
	GP-4621T	PFXGP4621TAA
		PFXGP4621TAD

SP5000 Series

	Model	Model Numbers
Standard Box	SP-5B00	PFXSP5B00
Power Box	SP-5B10	PFXSP5B10
eXtreme Box	SP-5B90	PFXSP5B90
Open Box	SP-5B40	PFXSP5B40
	SP-5B41	PFXSP5B41

NOTE

- For the display modules you can mount, refer to the “Hardware Manual”.

IPC Series

Model	Model Numbers
PS-5000, PS/PE-4000	PS5000 Series, PS4000 Series, PE4000 Series (For details about the models, refer to the corresponding hardware manual for your display unit.)

1.5. License and System Configuration

License formats are divided largely into two groups: SiteManager Embedded Basic and SiteManager Embedded Extended.

The combination of licenses you purchase changes what sort of system configurations you can have.

For information on licenses, see the following URL.

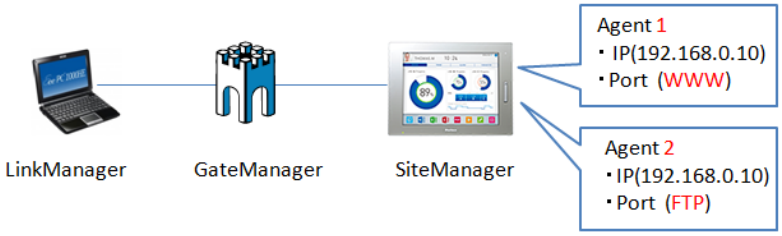
http://www.pro-face.com/trans/en/manual/1061.html

SiteManager Embedded Basic

Only for accessing a display unit itself, license for registering up to 2 Agents (access methods) per display unit.

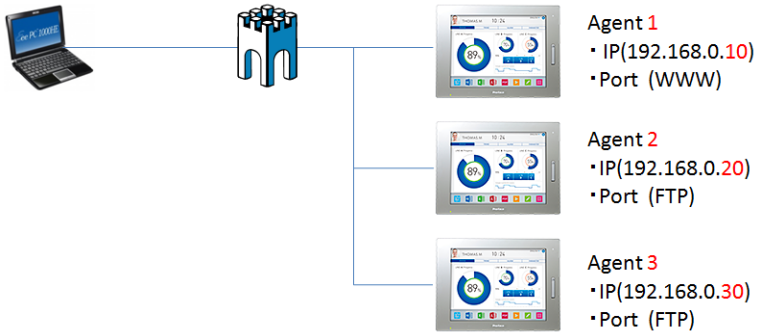
When the display unit has multiple Ethernet interfaces, you can set up an Agent for each interface.

When different ports are used with a single interface, you can set up an Agent for each port.



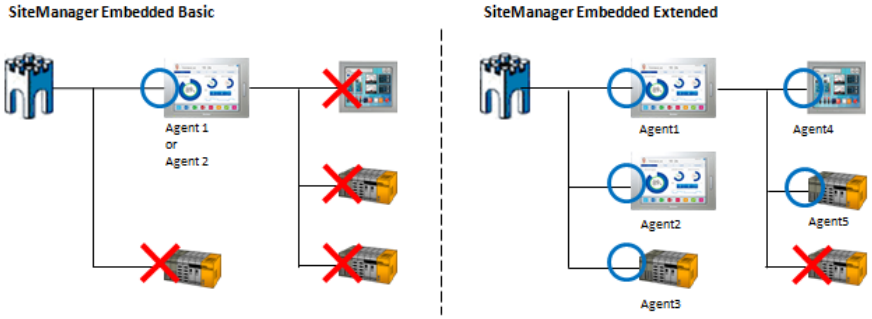
SiteManager Embedded Extended

You can access external IP devices (such as PLCs, IPCs, Server, Web camera, and so on) on the same network as the display unit and register Agents.
As you can connect multiple devices with different IP addresses, you can also register multiple Agents.



NOTE

- The default is for all the ports to be open. Change to the port as used by your application. Make changes to settings from the SiteManager GUI (**Edit** from **Device Agents**).
- Display units without a registered Agent are not accessible from Pro-face Connect.



1.6. Restrictions

See our website for details on restrictions.

http://www.pro-face.com/trans/en/manual/1072.html

2. Basic Setup and Connection

2.1. Building Your Environment

On purchase of your Pro-face Connect license, build your environment using the following workflow.

Creating SiteManager Environment *1	Creating GateManager Environment *2	Creating LinkManager Environment *3	Creating LinkManager Mobile Environment *4
Set up the GateManager accessed from SiteManager	Authentication and Logging into GateManager	Authentication and Installing LinkManager	Login and connect to LinkManager Mobile
	Create LinkManager user account	Connect to the display unit	
	Create LinkManager Mobile user account		
	Assigning the license to SiteManager		

*1 Tasks for SiteManager User or GateManager Administrator.

*2 Tasks for GateManager Administrator.

*3 Tasks for LinkManager User.

*4 Tasks for LinkManager Mobile User.

NOTE

- Using Windows Embedded models as SiteManager
  When using Windows Embedded models, you can set the write filter (write protection) on drives installed with the operating system. If the write filter settings are enabled, disable the write filter settings before installation.
  If you are using Windows XP Embedded, disable EWFSettingTool.exe. If you are using Windows Embedded Standard 7, and Windows Embedded Standard 2009, disable EWF Manager.
  For details, refer to the User Manual/Reference Manual for your unit.

2.2. Creating the SiteManager Environment

2.2.1.Set up the GateManager accessed from SiteManager

The setup method for SiteManager differs depending on your display unit.

Display Unit	Setup Method
With GP-Pro EX, models other than the SP5000 Series Open Box or IPC Series	Set up in Offline Mode
With BLUE, models other than the SP5000 Series Open Box or IPC Series	Set up in Hardware Configuration
SP5000 Series Open Box, IPC Series	Set up in browser

Set up in Offline Mode

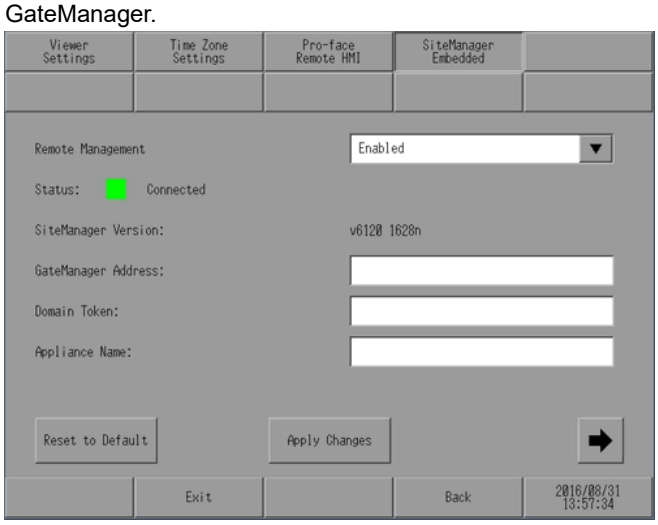
The following are the steps for models that support setting up SiteManager from the display unit's offline mode.

NOTE

- For information on how to enter offline mode, or details about each setup item, refer to the GP-Pro EX Reference Manual. You can download the manual from the Pro-face support site (http://www.pro-face.com/trans/en/manual/1001.html).

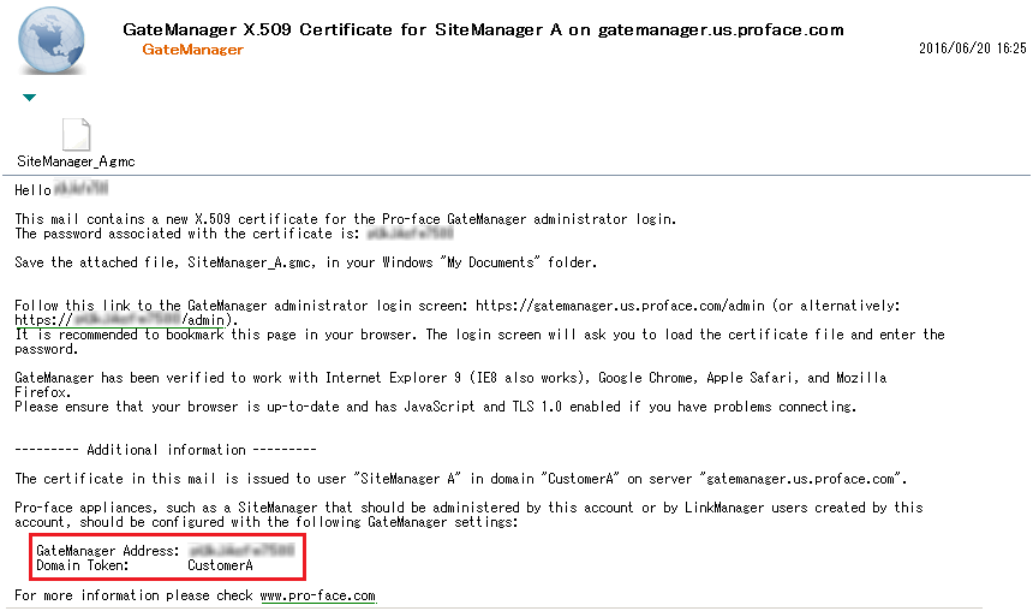
1. Enter offline mode, then on the menu touch Main Unit Settings – Remote Viewer Settings, and select SiteManager Embedded. When SiteManager Embedded is not available, use GP-Pro EX Ver.4.07.100 or later to transfer the system to the display unit.

2. Check that **Remote Management** is set to **Enabled**. Enter the IP address of the GateManager to access, the password (token) required for connection, and the SiteManager name. The defined SiteManager name appears on the GateManager.



IMPORTANT

- The information required in this screen is found in the lower section of the e-mail you received from the GateManager with the GateManager X.509 Certificate.


GateManager X.509 Certificate for SiteManager A on gatemanager.us.proface.com

GateManager

2016/06/20 16:25

SiteManager_A.gmc

Hello [redacted]

This mail contains a new X.509 certificate for the Pro-face GateManager administrator login.
The password associated with the certificate is: [redacted]

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

Follow this link to the GateManager administrator login screen: https://gatemanager.us.proface.com/admin (or alternatively: https://[redacted]/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 ---------

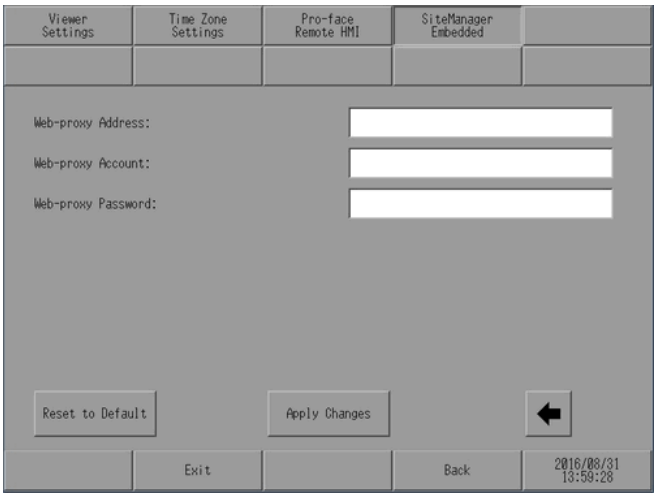
The certificate in this mail is issued to user "SiteManager A" in domain "CustomerA" on server "gatemanager.us.proface.com".

Pro-face 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 Address: [redacted]
Domain Token: CustomerA

For more information please check www.pro-face.com

3. If necessary, confirm the IP address of the proxy server with the network administrator, and enter it in the **Web-proxy Address** field.



4. Click **Apply Changes**. You can use the **Status** property on the previous screen to check the connection status with GateManager. To exit offline mode, touch **Exit**.

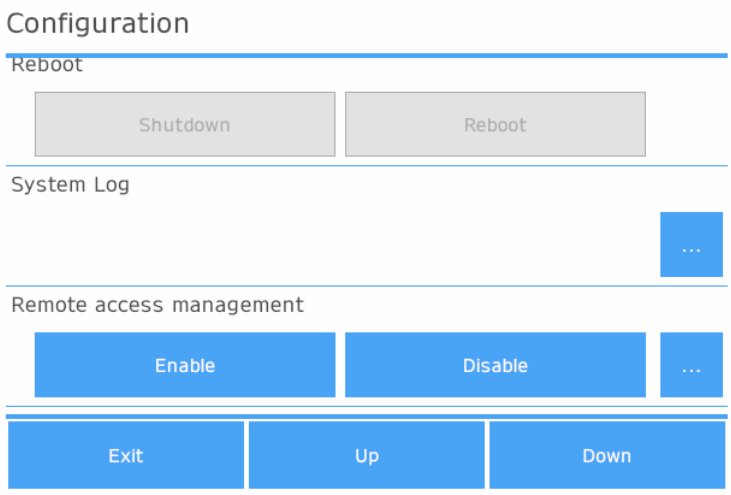
Set up in Hardware Configuration

Steps for models where SiteManager settings are defined in the display unit's Hardware Configuration.

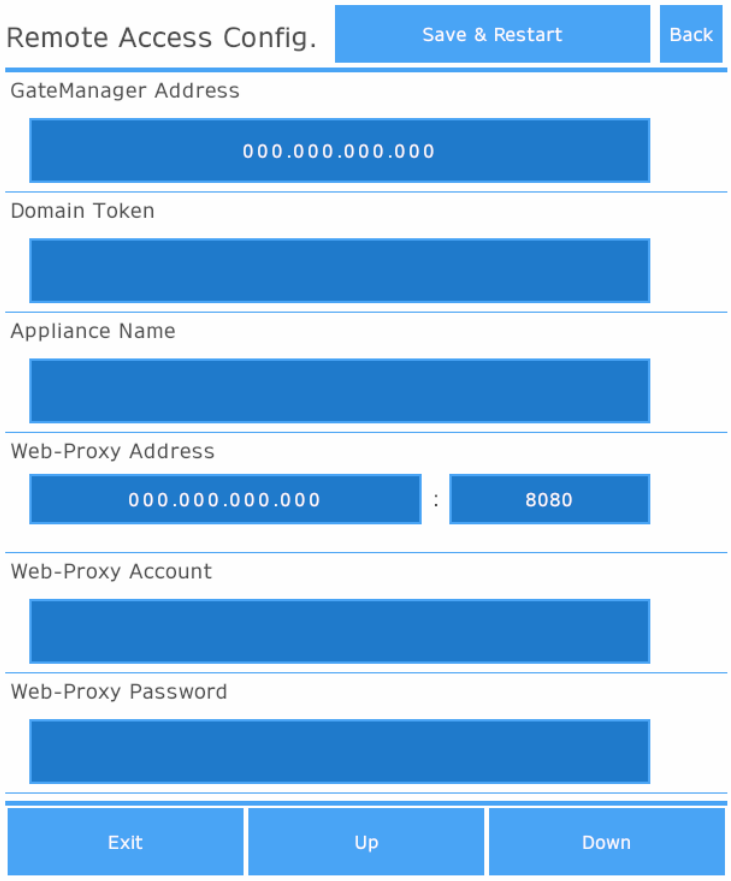
NOTE

- Before setting up Hardware Configuration, enable BLUE's Pro-face Connect setting. For information on entering Hardware Configuration and details of each set up item, refer to the "BLUE User Manual."

1. In the **Hardware Configuration**, from the **Remote access management** menu touch **...**. If the **Remote access management** menu does not display, transfer to the display unit a system with Product Version 2.4.0 or later.

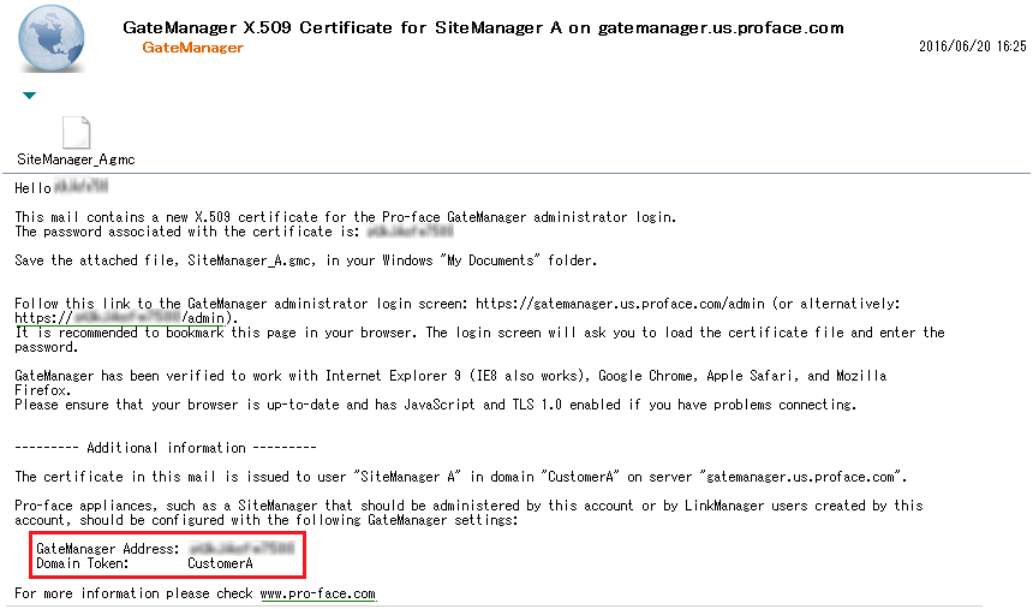


2. Enter the GateManager IP address, password (Domain Token) for connection, and SiteManager's Application Name. The defined SiteManager's Application Name displays on the GateManager.



IMPORTANT

- The information required in this screen is found in the lower section of the e-mail you received from the GateManager with the GateManager X.509 Certificate.



GateManager X.509 Certificate for SiteManager A on gatemanager.us.proface.com

GateManager 2016/06/20 16:25

SiteManager_A.gmc

Hello

This mail contains a new X.509 certificate for the Pro-face GateManager administrator login.
The password associated with the certificate is:

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

Follow this link to the GateManager administrator login screen: https://gatemanager.us.proface.com/admin (or alternatively: https://[redacted]/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 "SiteManager A" in domain "CustomerA" on server "gatemanager.us.proface.com".

Pro-face 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 Address: [redacted]
Domain Token: CustomerA

For more information please check www.pro-face.com

3. If necessary, confirm the proxy server IP address from your network administrator and enter it in the **Web-proxy Address** field.
4. Touch **Save & Restart** to restart the system.
5. In Hardware Configuration, from the **Remote access management** menu touch **Enable**.

NOTE

- When the display unit is restarted, from the **Remote access management** menu touch **Enable** again.

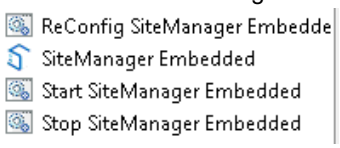
Set up in browser

Steps for models that support setting up SiteManager from a browser.

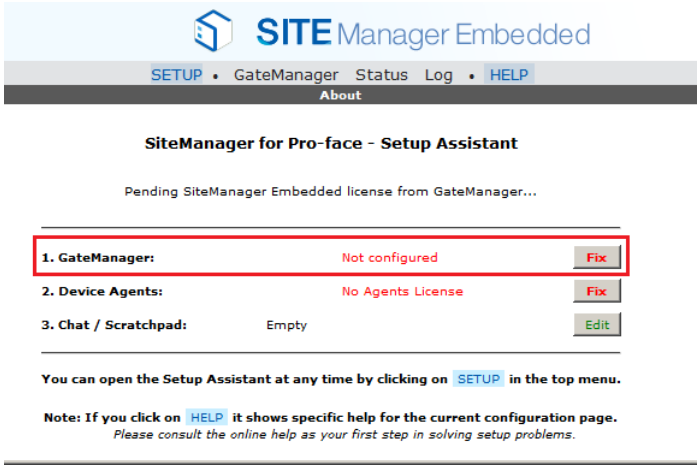
NOTE

- If SiteManager Embedded is not pre-installed on your SP5000 Series Open Box or IPC Series, first download and install the latest update module from our support site.
  http://www.pro-face.com/trans/en/manual/1001.html

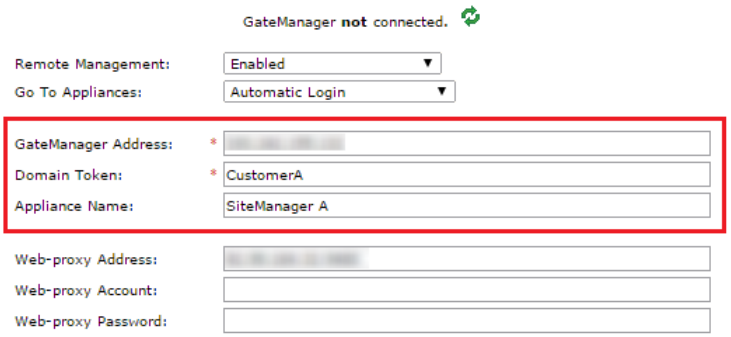
1. Turn off the write filter and click on **All Programs**, **Pro-face**, **SiteManager Embedded**, **Start SiteManager Embedded** in Start menu. SiteManager Embedded setup is started.



2. Subsequently, SiteManager Embedded is started. In the SiteManager Embedded web site, from the **GateManager** setting click the **Fix** button.

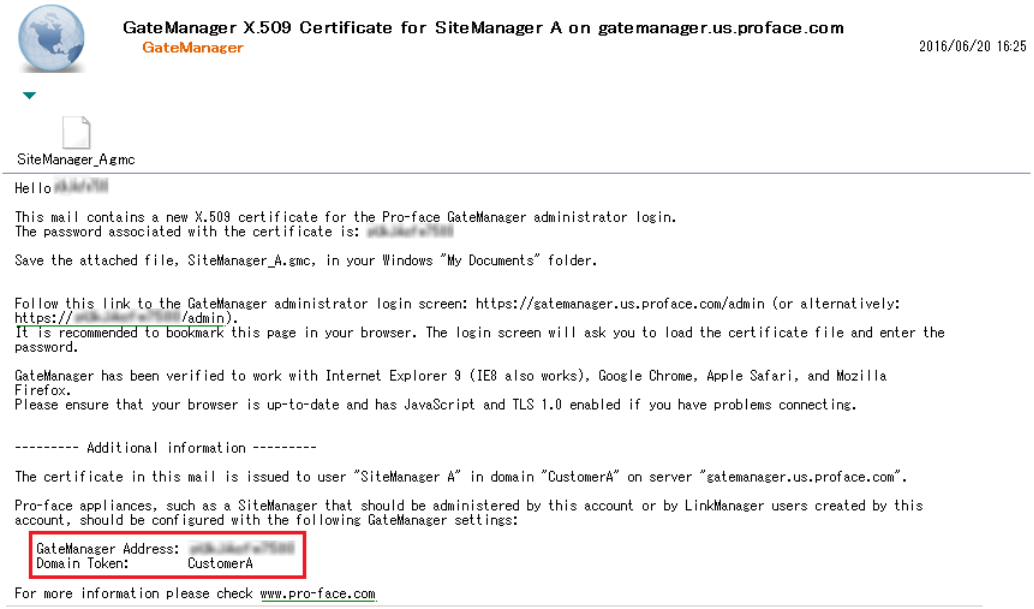


3. Enter the IP address of the GateManager to access, the password (token) required for connection, and the SiteManager name. The defined SiteManager name appears on the GateManager.



IMPORTANT

- The information required in this screen is found in the lower section of the e-mail you received from the GateManager with the GateManager X.509 Certificate.

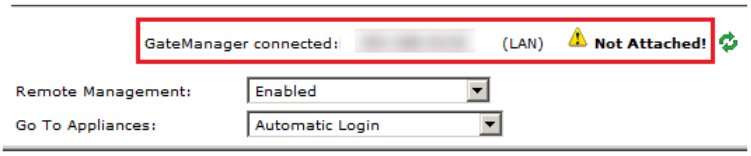


4. If necessary, confirm the IP address of the proxy server with the network administrator, and enter it in the **Web-proxy Address** field.
5. Click **Save** and **Connect**. To check the connection status with GateManager, click the **Refresh** icon.

NOTE

- Connection to the GateManager is possible if the GateManager Administrator has allowed access.

6. After a short while the status should change to this:



SiteManager Embedded set up is now complete and the display unit is ready. Once the unit is connected to a network that has Internet access on this or another site, SiteManager Embedded will automatically connect to the GateManager.

2.3. Creating the GateManager Environment

Log in to GateManager to create LinkManager accounts and assign licenses to SiteManagers.

2.3.1.Authentication and Logging into GateManager

1. Locate the e-mail you received from the GateManager with the **GateManager Certificate**, and save the attached file to your hard disk.

2. Open the link in the same e-mail. (There may be two links with a DNS name and IP address, respectively. You can use either of them.)This will open the login screen of the GateManager:

3. Browse for the certificate you just saved, and enter the password provided in the e-mail.

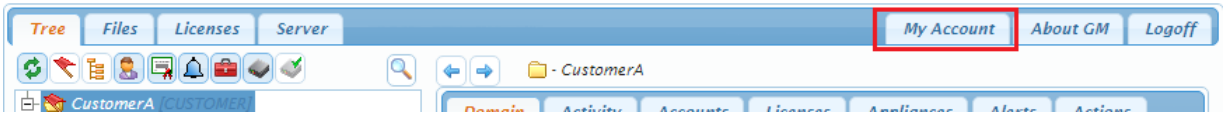
2.3.2.Create LinkManager user account

When LinkManager is a smart device, follow the steps in Create LinkManager Mobile user account.

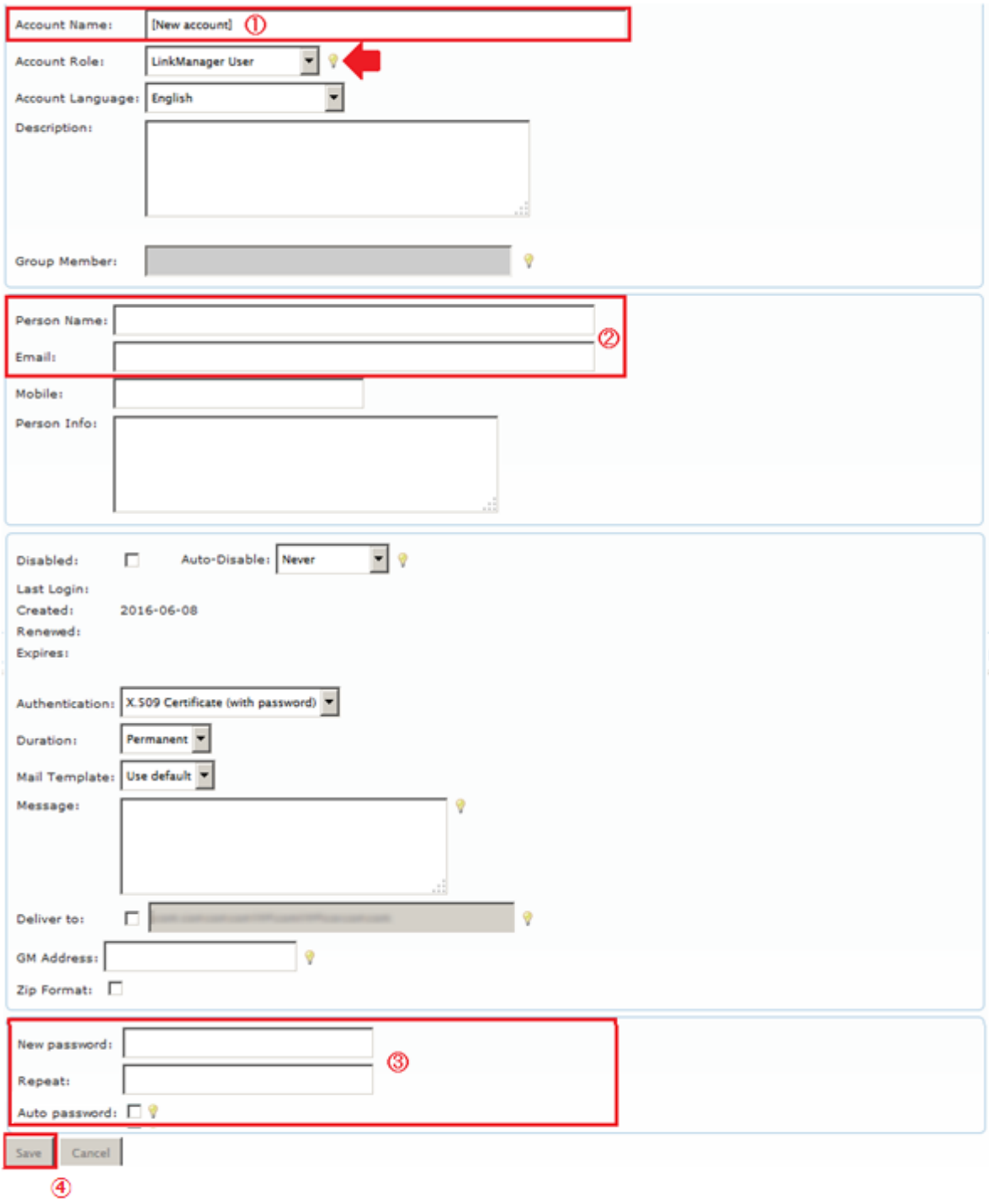
1. When logged in click the **Accounts** tab, and select the **"+"** icon to create a new account.

NOTE

- From **My Account**, in **Personal Account Settings**, when **Show startup Wizard on login** is enabled, logging in to GateManager triggers the Startup Wizard. Follow the instructions in the wizard to continue with the setup.



2. Fill in the following information.



1: Account Name
This will become the file name of the LinkManager certificate file (.lmc)
2: Person Name, Email
Enter the name and email address for whom the account is being created.
3: New password/Auto password
Password is provided to the person associated with the account. For administrator and LinkManager accounts: 12 character alphanumeric password with at least one number, one lowercase character, and one uppercase character. For LinkManager Mobile accounts: 10 character password with lowercase letters followed by digits. You can create your own password with the **New password** command. Send the password by e-mail or notify verbally. **Auto password** creates a random password. Password is sent automatically from GateManager by e-mail.
4: Save
On clicking **Save**, an e-mail with the LinkManager certificate is automatically sent from the GateManager.

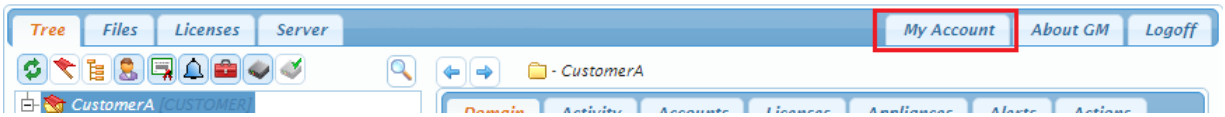
2.3.3.Create LinkManager Mobile user account

The step to create this account is identical to creating the LinkManager user account.

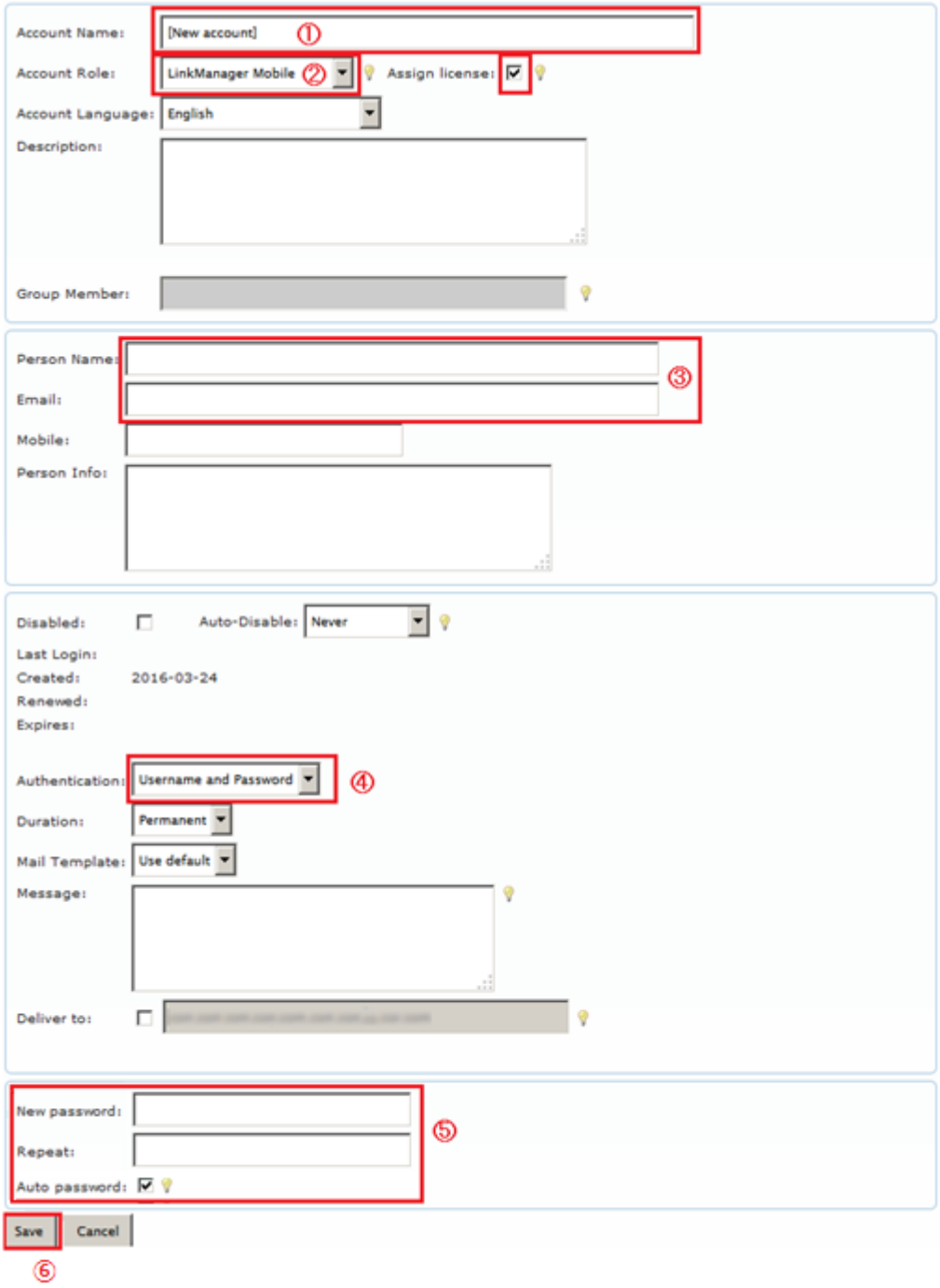
1. Log in to the GateManager portal, and from the Accounts tab select the “+” icon to create a new account.

NOTE

- From **My Account**, in **Personal Account Settings**, when **Show startup Wizard on login** is enabled, logging in to GateManager triggers the Startup Wizard. Follow the instructions in the wizard to continue with the setup.



2. Enter the following details.

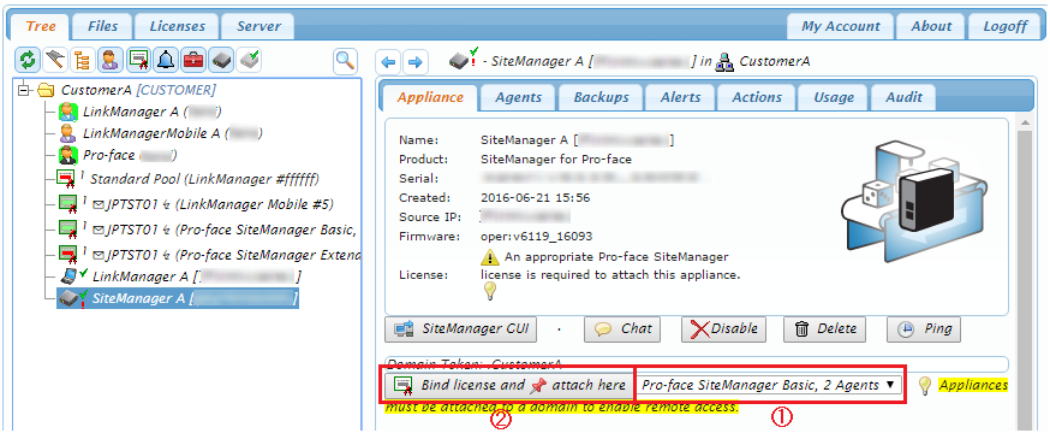


1: Account Name
This will become the login ID for the account.
2: Account Role
Note that the check box **Assign License** appears when selecting this role. When checking this box, this account will allocate the LinkManager Mobile license and subsequently allow remote access by this account (if not checking the box, the account will still be working, but remote access is blocked.)
3: Person Name, Email
Enter the name and email address for whom the account is being created.
4: Authentication
Username and Password are required for log in.
5: New password/Auto password
Password is provided to the person associated with the account. For administrator and LinkManager accounts: 12 character alphanumeric password with at least one number, one lowercase character, and one uppercase character. For LinkManager Mobile accounts: 10 character password with lowercase letters followed by digits. You can create your own password with the **New password** command. Send the password by e-mail or notify verbally. **Auto password** creates a random password. Password is sent automatically from GateManager by e-mail.
6: Save
On clicking **Save**, an e-mail with a link to the LinkManager Mobile login page is automatically sent from the GateManager.

2.3.4.Assigning the license to SiteManager

On the registered SiteManager, an assigned license is required to use Pro-face Connect.

1. If the SiteManager has been configured correctly according to section Set up the GateManager accessed from SiteManager, the SiteManager should appear in the tree view. Place your cursor on it and touch **Bind license and attach here.**



NOTE

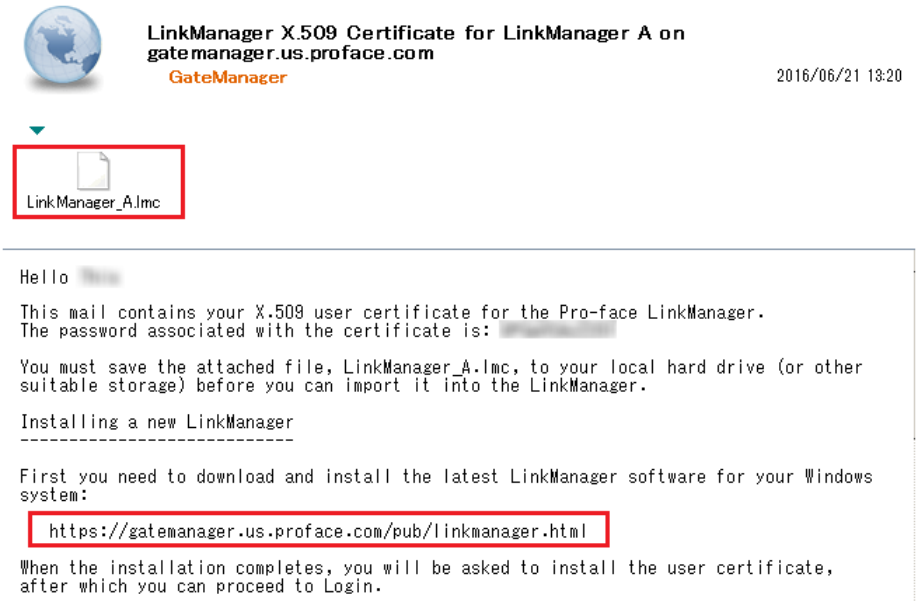
- When the SiteManager that you want to assign the license to do not appear in tree view, check if the SiteManager's Web-proxy Address is set up.

2.4. Creating the LinkManager Environment

Setting up personal computers and smart devices in the office you want to connect to the network.

2.4.1.Authentication and Installing LinkManager

1. The previous step generated an e-mail from the GateManager that included a LinkManager certificate (.lmc). Save the attached certificate to your computer.



2. Download and install the LinkManager software by clicking the appropriate link in the e-mail.

IMPORTANT

- Administrator privileges on the PC are required to install LinkManager.

NOTE

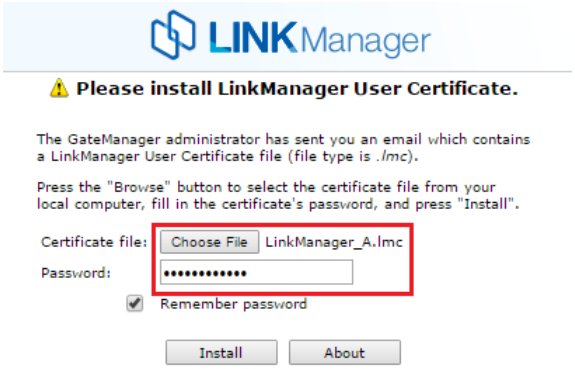
- You can also install LinkManager inside a VMWare virtual machine if the host operating system is Windows 7 and the CPU supports virtualization. You can also run your programming software inside a virtual machine and connect to devices via LinkManager installed on the host operating system if the virtual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

3. After you click **Finish** in the installation wizard, the LinkManager icon in your Windows system tray turns green, and your default web browser opens, showing the LinkManager Web GUI.

NOTE

- If the LinkManager icon remains red for a long time, it could indicate that something on the PC is preventing the LinkManager from starting correctly. Visit our Web site whenever you need help finding a solution.
  http://www.pro-face.com/trans/en/manual/1001.html

4. **Choose File** for the certificate you just saved and enter the password provided in the e-mail.



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

NOTE

- When you cannot log in, confirm the IP address of the proxy server with the network administrator, and use **Add proxy** to set up the Web-Proxy.

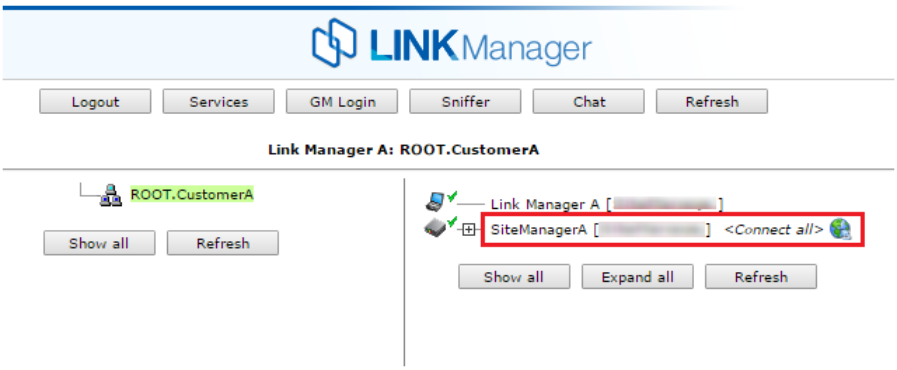
You are now logged in.

2.4.2.Connect to the display unit

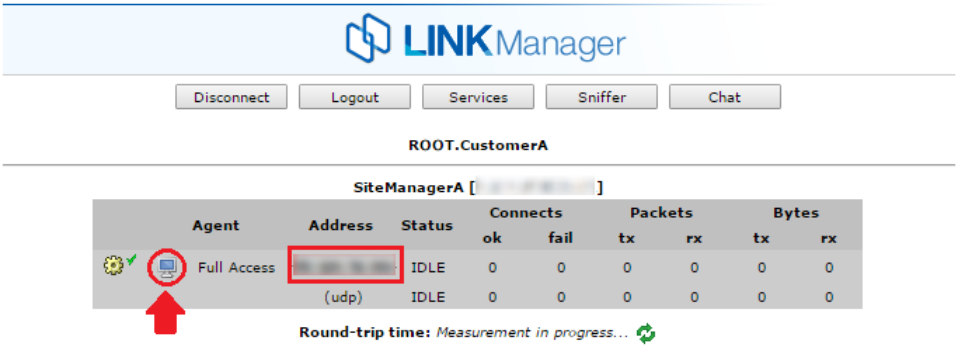
NOTE

- When you connect multiple LinkManager to one SiteManager (agent) at the same time, depending on the application, there may be cases some of the LinkManagers cannot communicate with SiteManager.
  You can avoid this by setting up the SiteManager so it does not allow simultaneous connection of multiple LinkManagers. For more information, refer to the following URL.
  http://www.pro-face.com/trans/en/manual/1050.html

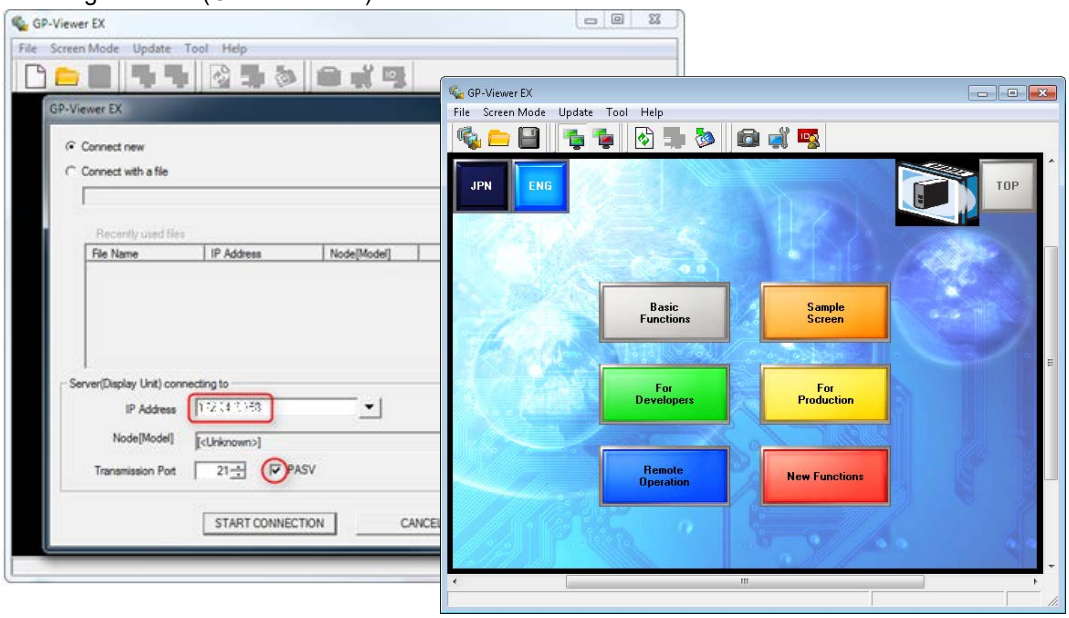
1. Click **SiteManager** <Connect all> to start communication.



2. You are now connected to the IP address of the display unit.

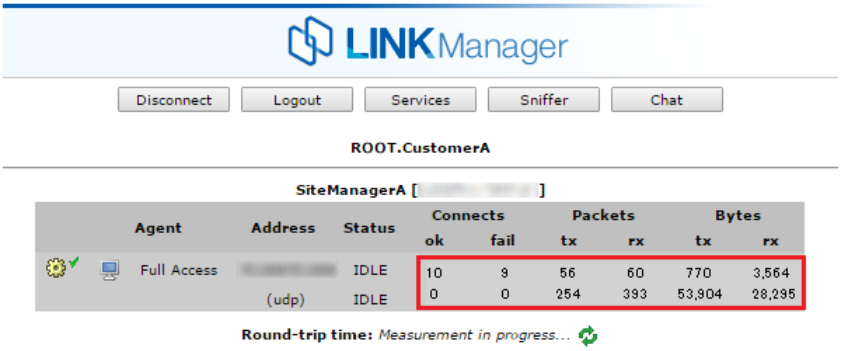


3. You can connect to the application running on the display unit. The following is an example connection using our remote monitoring software (GP-Viewer EX).



NOTE

- To check the volume of TCP/UDP data communication, you can use the LinkManager data counter. (The top part displays TCP, the bottom part UDP data volume.)



1: Connects
ok : Displays number of LinkManager where agent connection successful fail : Displays number of LinkManager where agent connection failed
2: Packets
tx : Displays the amount of data (packets) sent to Agent. rx : Displays the amount of data (packets) received from Agent.
3: Bytes
tx : Displays the total amount of TCP and UDP data (bytes) sent to Agent. rx : Displays the total amount of TCP and UDP data (bytes) received from Agent.

2.5. Creating the LinkManager Mobile Environment

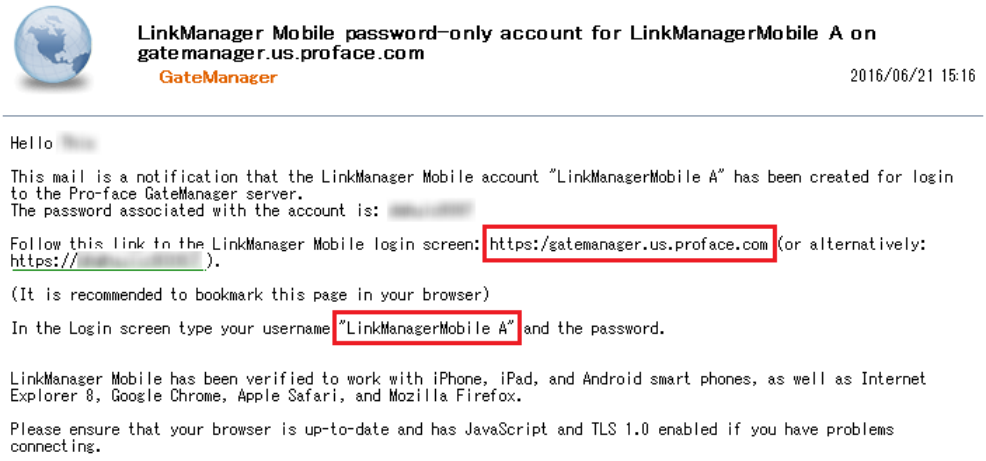
Link Manger Mobile is a “light-weight” version of LinkManager that can be used from most devices with a web browser, such as PCs, Smart phones and tablets.

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

- Web GUI (http/https)
- RDP (MS Remote Desktop) on port 3389
- VNC Servers on port 5900
- Selected APP access mapped via port 5900

2.5.1. Login and connect to LinkManager Mobile

1. In the email that you received, click the 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 LinkManagerMobile A on gatemanager.us.proface.com

GateManager 2016/06/21 15:16

Hello [redacted]

This mail is a notification that the LinkManager Mobile account "LinkManagerMobile A" has been created for login to the Pro-face GateManager server.
The password associated with the account is: [redacted]

Follow this link to the LinkManager Mobile login screen: https:/gatemanager.us.proface.com (or alternatively: https://[redacted]).

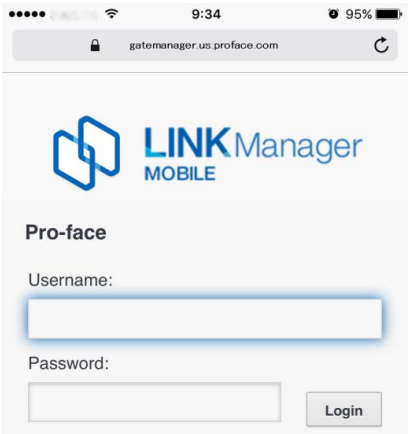
(It is recommended to bookmark this page in your browser)

In the Login screen type your username "LinkManagerMobile A" and the password.

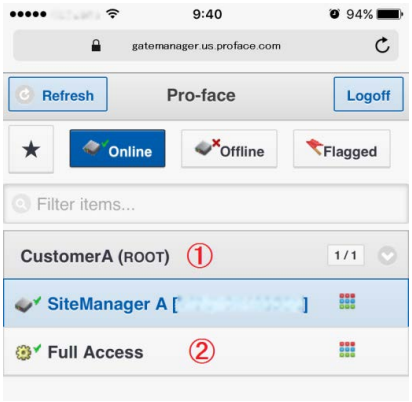
LinkManager Mobile has been verified to work with iPhone, iPad, and Android smart phones, as well as Internet Explorer 8, Google Chrome, Apple Safari, and Mozilla Firefox.

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

2. Login with the user name from the e-mail. The password is provided in e-mail.

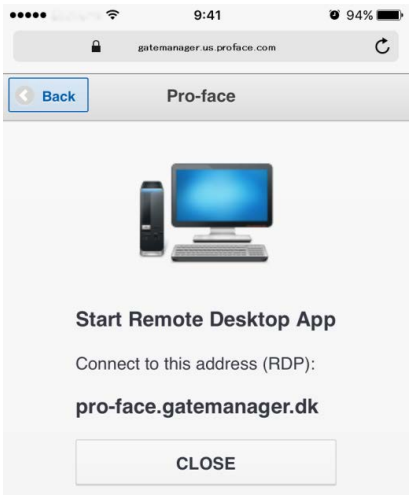


3. Click the **ROOT** bar to display the list of devices. Select **Full Access**.



4. Now click on the RDP button.

5. You are now connected to the display unit with the RDP protocol:



3. SiteManager Embedded Basic - Setting Up Agents

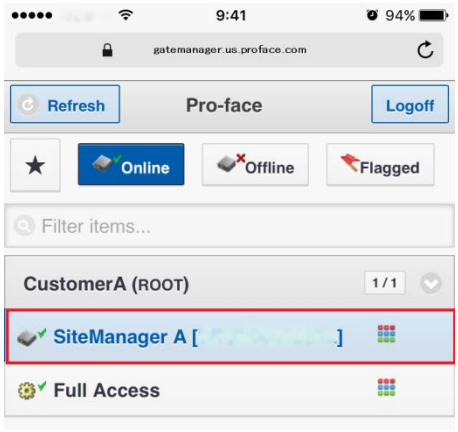
This section describes how to extend SiteManager Embedded Basic to allow access to select services on the Windows computer.

In addition to the default Full Access agent on SiteManager Embedded, you can create agents that allow access to specific services on the computer. You can use this to limit remote access to the computer, or to enable connection buttons on LinkManager or LinkManager Mobile for accessing selected services.

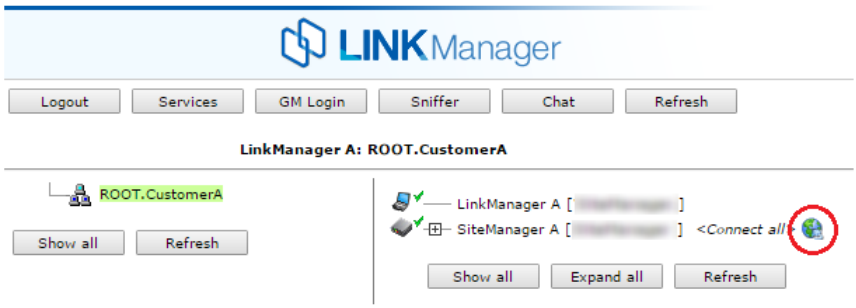
3.1. Configure Device Agents from SiteManager

1. Connect to the Web GUI of SiteManager Embedded, from LinkManager Mobile, LinkManager or from the GateManager Portal:

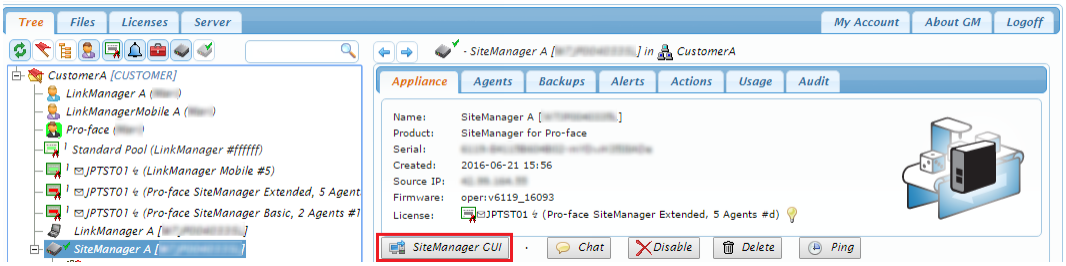
   (1) From LinkManager Mobile select SiteManager and click **WWW**.



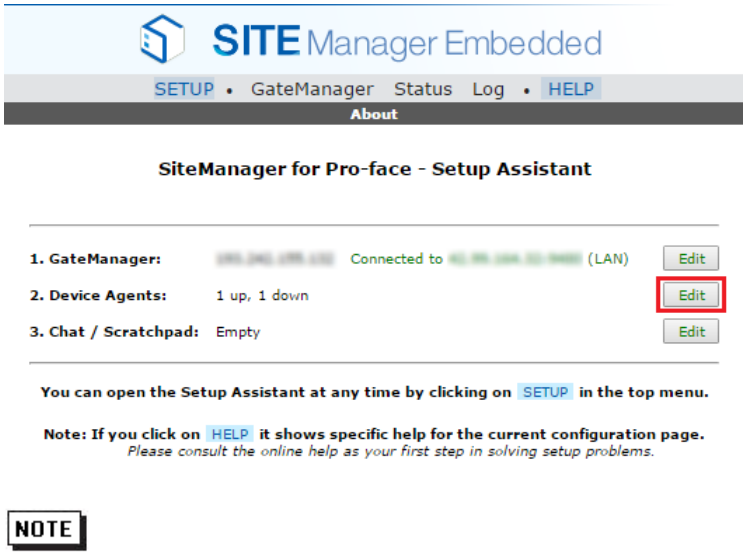
   (2) Or from LinkManager, select the globe icon next to SiteManager Embedded.



(3) Or from the GateManager Portal, click the **SiteManager GUI** button.



2. When connected, the first screen is the Setup Assistant. From **Device Agents**, click the **Edit** button.



NOTE

- The connection is made as a proxy connection via the GateManager over a random port number.

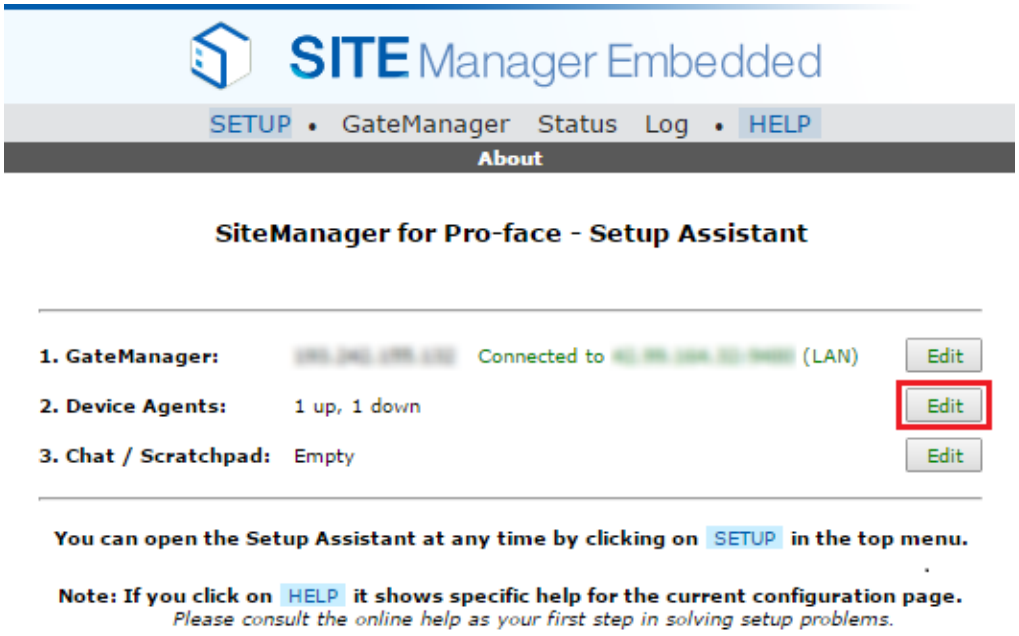
3.2. Enable Connect Buttons for Agents

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

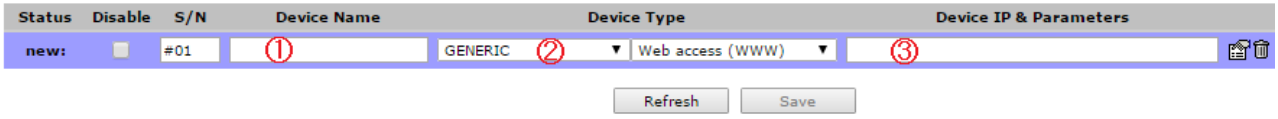
These buttons are not enabled by default as the corresponding service (listen socket), may not be available for the device represented by the Agent.

3.2.1.Creating Agents and Connect Buttons

1. Connect to the SiteManager GUI, and from Device Agents click Edit.

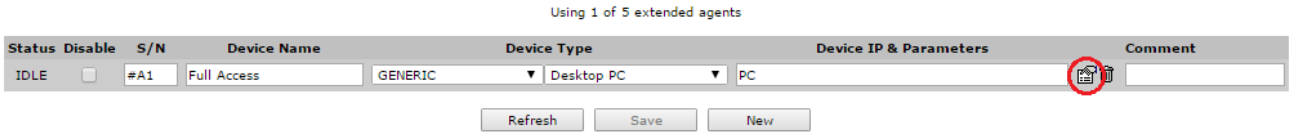


Click **New** and fill in the details.

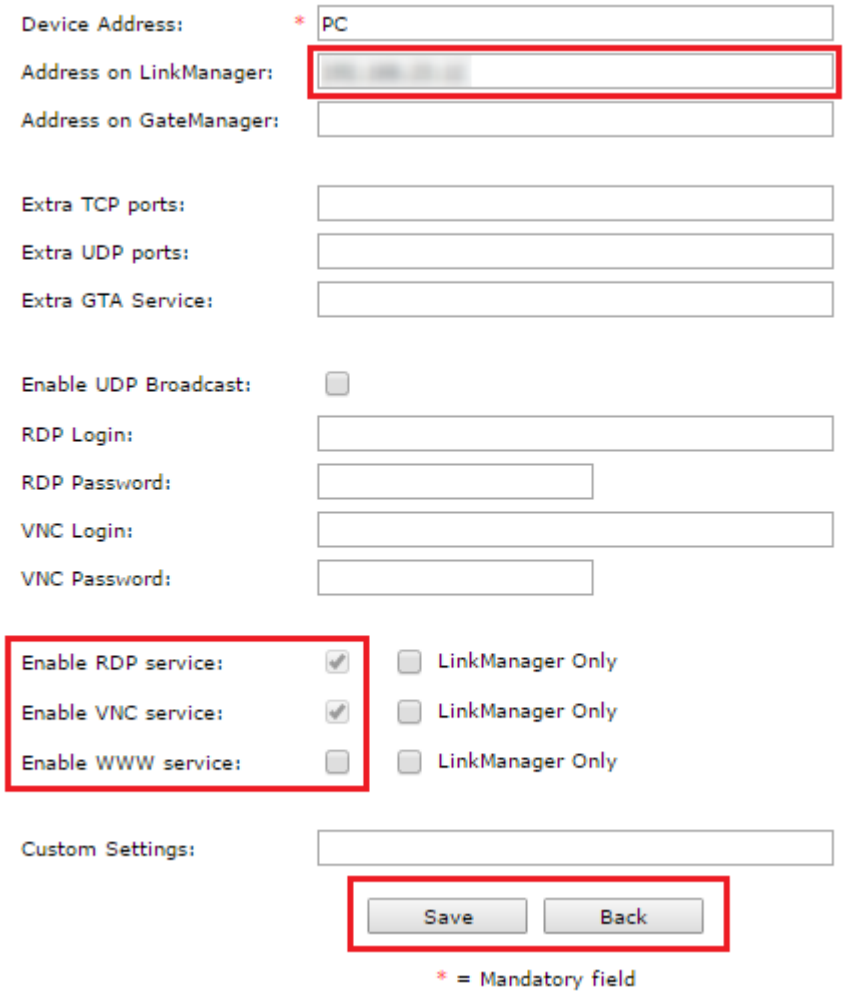


1: Device Name
Enter a recognizable name for the Agent for when you log into LinkManager or LinkManager Mobile.
2: Device Type
Select the type of device. The default (GENERIC) is the state where all the ports are open. Change to the port as used by your application. When using a Pro-face application, select [Pro-face].
3: Device IP & Parameters
Enter the IP address of the device. The IP address must be accessible from the computer / display unit where SiteManager Embedded is installed.

2. Click the **Parameter Details** icon for the Full Access agent.



3. Select **Enable *** service** for the connect button you want to enable, then click **Save** and then **Back**.

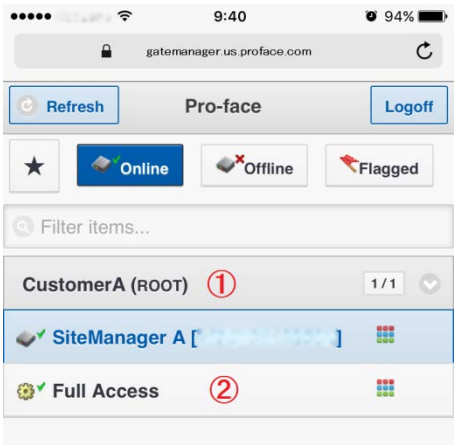


NOTE

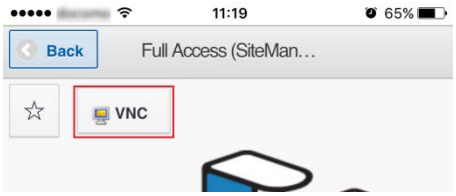
- To use the GP-Pro EX Web Server, also enable **Open WWW using default.htm**. This displays when Device Type is set to Pro-face.
- In Device Address, you can also directly enter the IP address of the device you want to connect.

3.2.2.Connect to VNC Server with LinkManager Mobile

1. In LinkManager Mobile, connect to the **Full Access** agent.



2. You will now see the **VNC** button.



NOTE

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

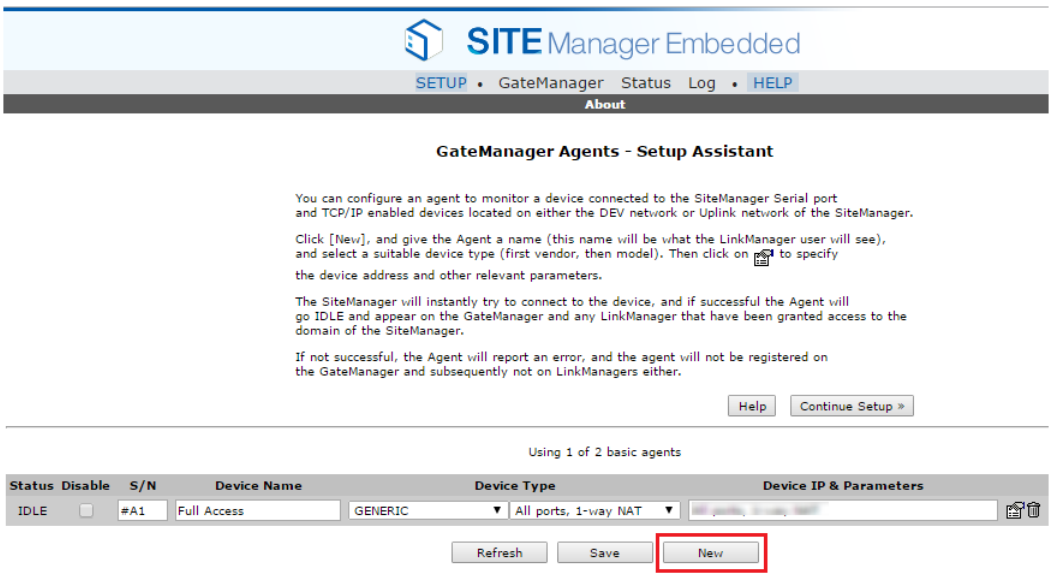
3. Touch the VNC button and LinkManager Mobile creates a connection to the device.

4. Connect to the VNC Client within 60 seconds. Otherwise the connection is closed again, and you would need to repeat the above procedure.

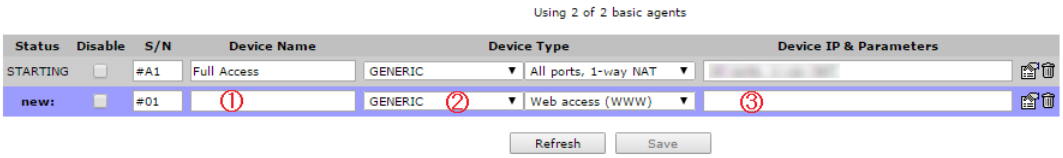
3.3. Using Agents with custom LinkManager Mobile connect buttons

3.3.1.Example: Create a new Agent

1. Select **New**.



2. Fill in the information:



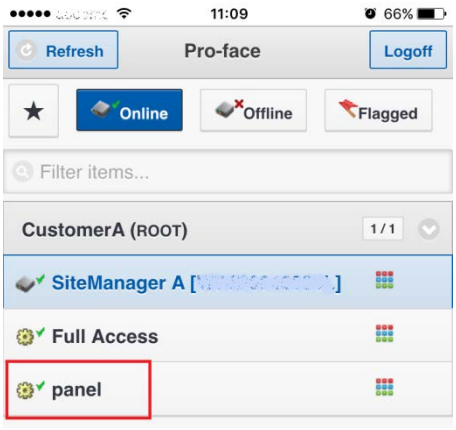
1: Device Name
Type a meaningful name that will describe the agent when logged into LinkManager or LinkManager Mobile.
2: Device Type
Select the Pro-face agent from the scroll bar. In case of SiteManager Embedded the only connection type will be Ethernet. NOTE • Other options could have been **Generic** / **Web access**, which would have limited access to a web server on the computer.
3: Device IP & Parameters
Enter the IP address of the device. The IP address must be accessible from the computer / display unit where SiteManager Embedded is installed.

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

4. You can now close the SiteManager web GUI window.

3.3.2.Connect to the agent with LinkManager Mobile

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



2. If you select the agent, you will see the button specific for the Pro-face agent. Clicking the 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 application, otherwise the connection is closed again, and you would need to repeat the above procedure.

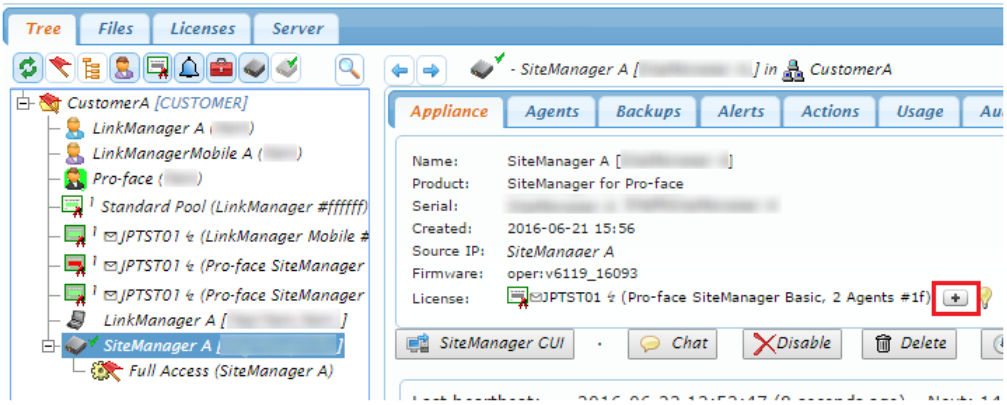
4. SiteManager Embedded Extended – Accessing external devices

4.1. Upgrading SiteManager Embedded Basic to SiteManager Embedded Extended

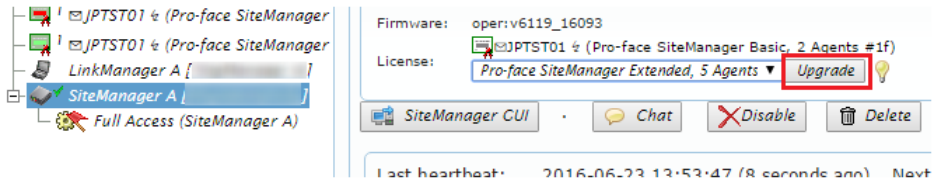
NOTE

- This section assumes you have SiteManager Embedded Basic license, and have received a SiteManager Embedded Extended license. If you already upgraded the license from SiteManager Embedded to SiteManager Embedded Extended, you can proceed to Define device agent for external device.

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

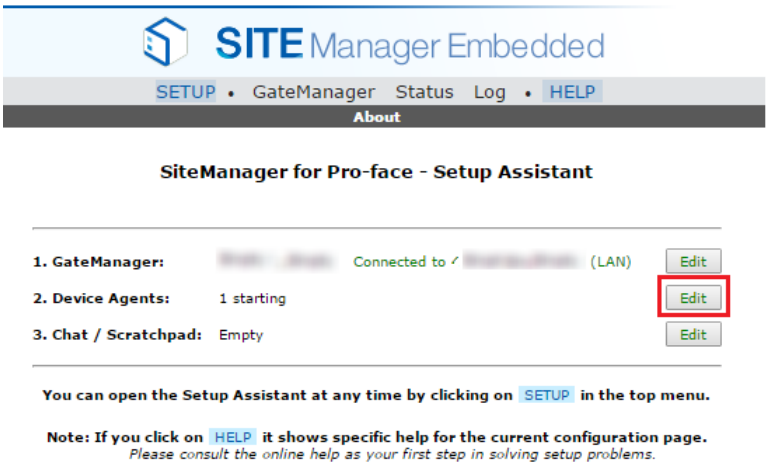


2. Listed are the available licenses. Click **Upgrade** to bind the license.

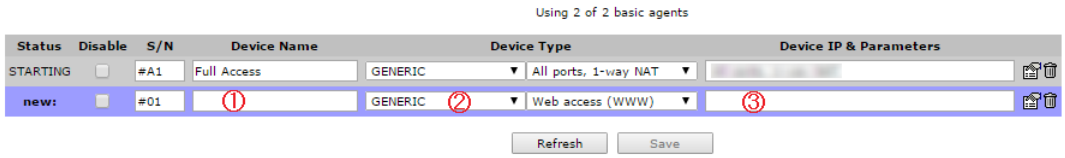


4.2. Define device agent for external device

1. Connect to the SiteManager GUI, and from **Device Agents** click **Edit**.



Select **New** and fill in the details.

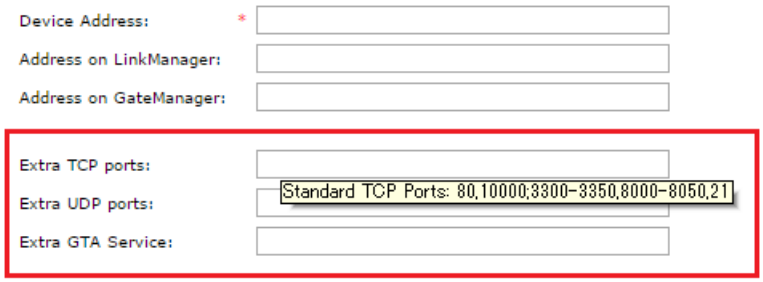


1: Device Name
Fill in the name that appears in LinkManager.
2: Device Type
Select the type of device. NOTE • The default (**GENERIC**) is the state where all the ports are open. Change to the port as used by your application.
3: Device IP & Parameters
Enter the IP address of the device. The IP address must be accessible from the computer / display unit where SiteManager Embedded is installed.

NOTE

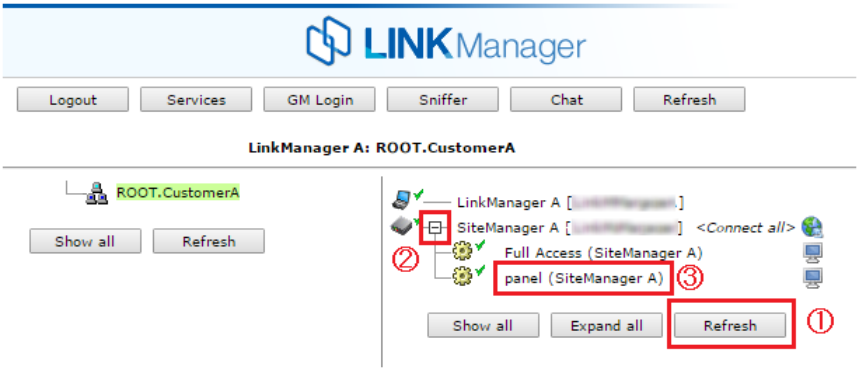
- The standard ports required for access by an agent are already registered. However, if you need to use another port, you can set it up.

  Click the **Parameters Details** icon , and enter the port number. (You can check which standard ports are already set up by hovering the cursor over the Input dialog box.)

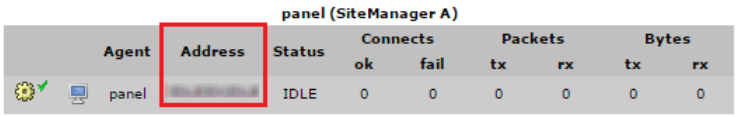


2. Click **Save** and Refresh a couple of times until the **Status** becomes **IDLE**, which indicates that SiteManager Embedded can reach the device.

3. Log in to LinkManager, click **Refresh** to update changes, and click **"+"** to expand and view the agents on the SiteManager. To connect to the new agent, click the agent description.



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



5. The following is an example connection using our remote monitoring software (GP-Viewer EX). Start the remote monitoring software and define the device IP address.