Pro-face
by Schneider Electric

Pro-face Connect
User Guide for Security Setting

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
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 (agents) 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

Preface 2
Trademark Rights 2
Manual Symbols and Terminology 3
Inquiry 4
Table of Contents 5
Introduction 6
Password strength for accounts 7
GateManager Portal login 8
Secure Login Method 8
Create Administrator accounts with X.509 certificate 9
LinkManager Mobile login 10
Secure Login Method 10
LinkManager Windows client 12
Handling certificate when installed in LinkManager 12
SiteManager configuration GUI 13
Login Settings for Remote Access 13

Introduction

Pro-face Connect, consisting of GateManager, SiteManager and LinkManager, is designed to provide a high degree of security while maintaining ease of use.

To that end the Pro-face Connect enforces certain security rules, however you may want to further enforce IT policies for a higher degree of security, or there may be external factors, such as the nature of a browser and its settings that prevent the Pro-face Connect from enforcing or warning the user about potential security threats.

This guide is intended to provide some guidelines for good IT security conduct in managing and operating Pro-face Connect.

Password strength for accounts

There is ongoing debate about what constitutes a strong password.

This combined with the fact that most accounts on a GateManager are based on two factor login, have founded the decision to not make the GateManager enforce high password strength or length when creating accounts.

By release 7.0 of the GateManager, the minimum password strength for manually created passwords follows an algorithm based on the following.

- Upper case characters
- Lower case characters
- Digits (numbers)
- Special characters

By default, a manually created password is enforced to contain at minimum, the following.

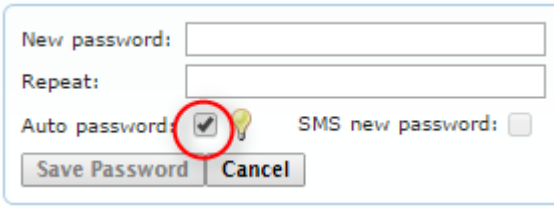
- For passwords 4 to 7 characters long, all of the above must exist
- For passwords 5 to 8 characters long, 3 of the above must exist
- For passwords 9 characters or longer, 2 of the above must exist.

For example, the following passwords are allowed.

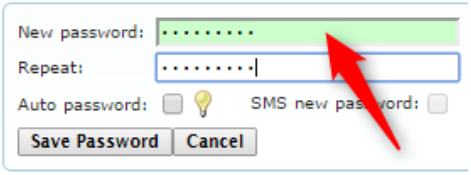
- 1aB#
- 1111aaaaa
- 11aaBBB

To set up a more secure password, create the password following the steps below.

1. Select the **Auto password** check box. This will ensure a password of 12 characters consisting of numbers and lower and upper case letters for administrator and LinkManager accounts, and 10 characters consisting of lower case letters followed by digits for LinkManager Mobile accounts.



2. If you have a reason to define the password manually, at a minimum, set up passwords where the entry field turns green (by combining upper/lower case letters, numbers and symbols). By default, you cannot create a weak password (field color: orange).



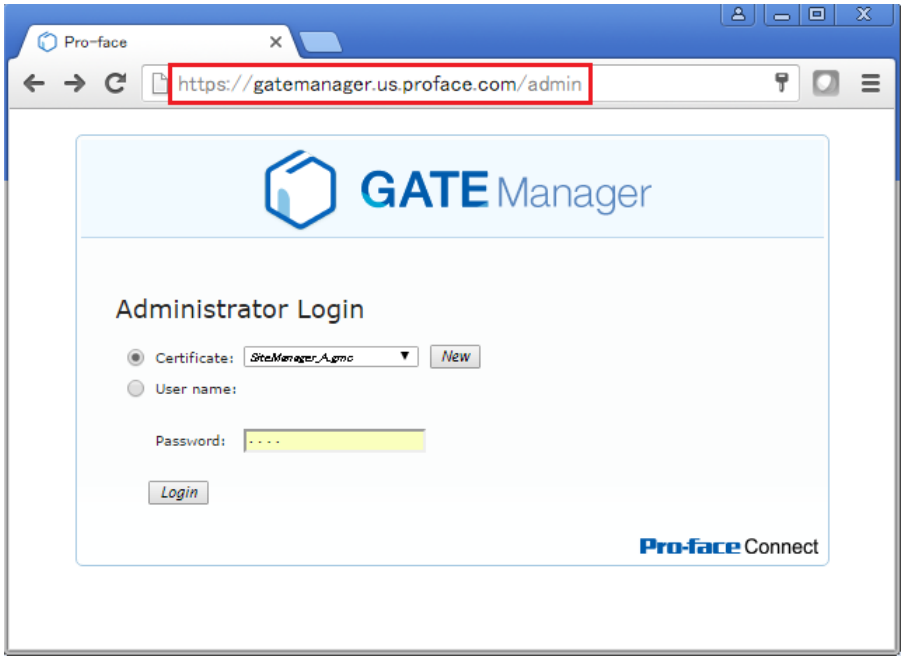
NOTE

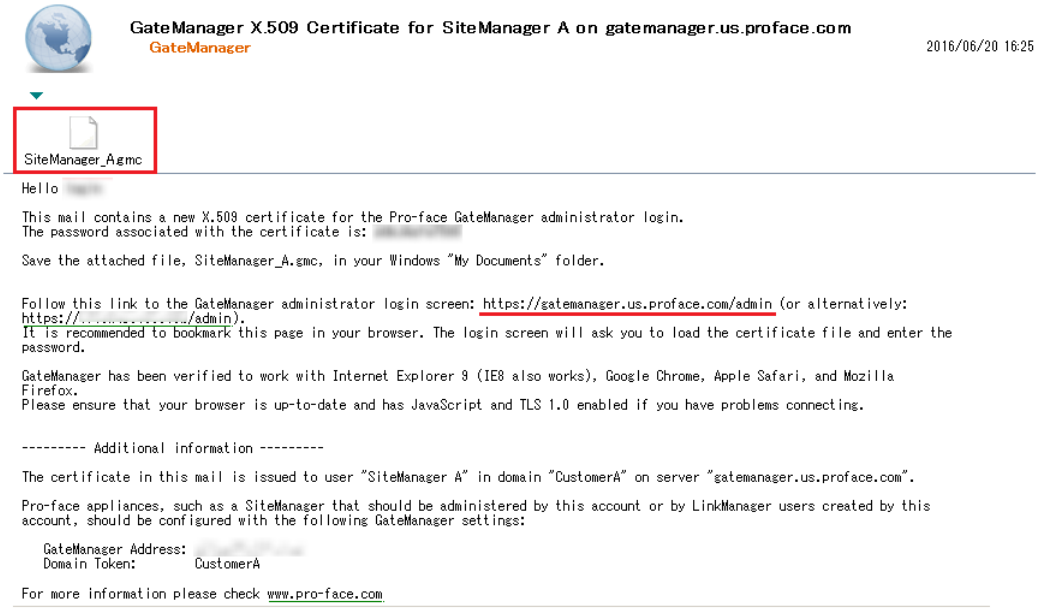
- When a user changes their password from the **My Account** tab, GateManager by default requires minimum 9 characters with letters and numbers for the password.

GateManager Portal login

Secure Login Method

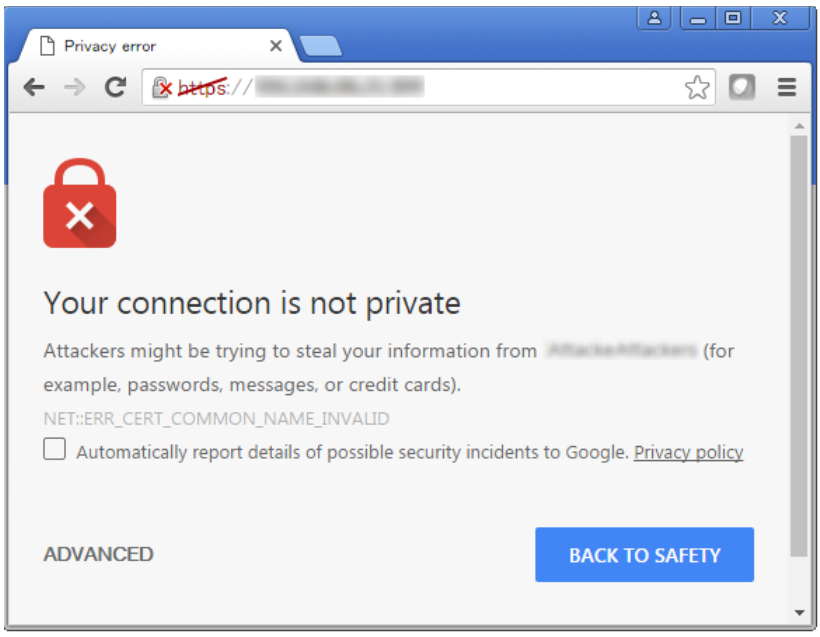
When logging into Pro-face Connect Portal, confirm the address line of the browser indicates a secure website, and that the address line matches that of your account e-mail. Follow this precaution to minimize Man-in-the-middle attacks.





If an https web server certificate has not been installed on the GateManager, temporarily you may have to accept logging in to an un-trusted GateManager server.

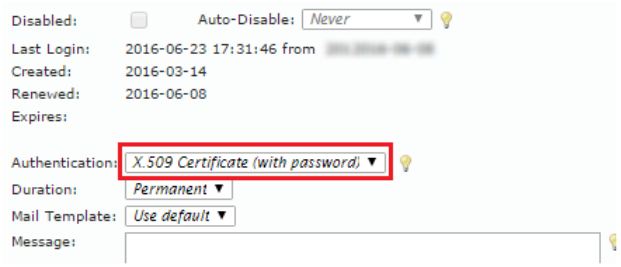
Always verify with your GateManager administrator that this is acceptable.



Create Administrator accounts with X.509 certificate

With GateManager, you can create an Administrator account without a X.509 certificate. Only do this for initial internal testing, before placing the server into production.

Change all Administrator accounts to use X.509 before entering into production.



You may have reasons for creating accounts with Username and Password authentication only–for instance if needing to login from a tablet that cannot store reference files.

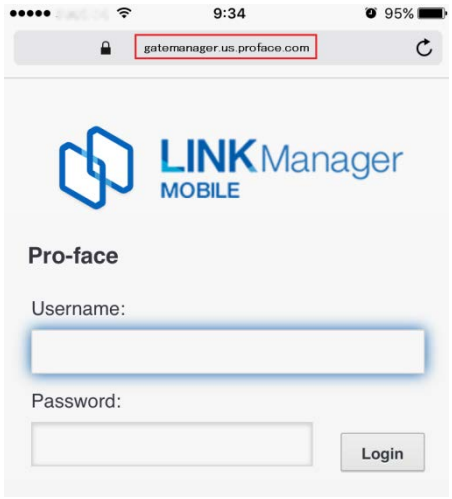
Confirm the account's access is limited to only what is absolutely relevant for the Administrator account.

Do not make a Username/Password only account for a Server administrator account. If you are a Server administrator on your own GateManager, note that a new GateManager installation includes a default temporary Server Administrator account with username/password only. Always follow the instructions in the installation guides to either change or delete this account.

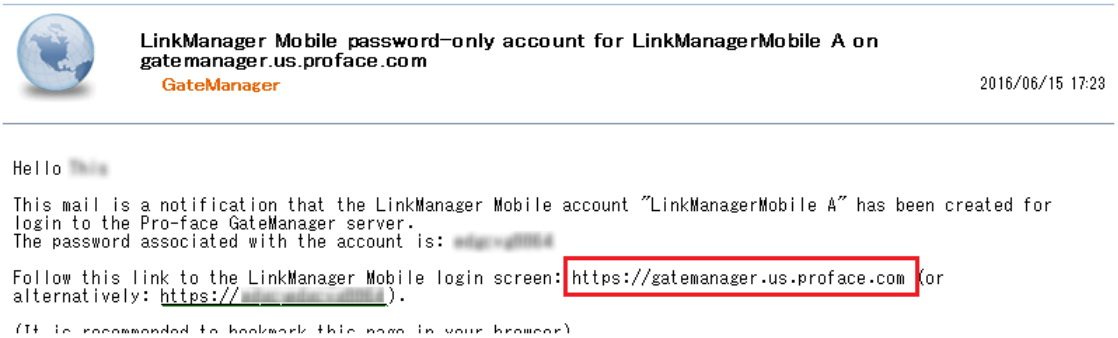
LinkManager Mobile login

Secure Login Method

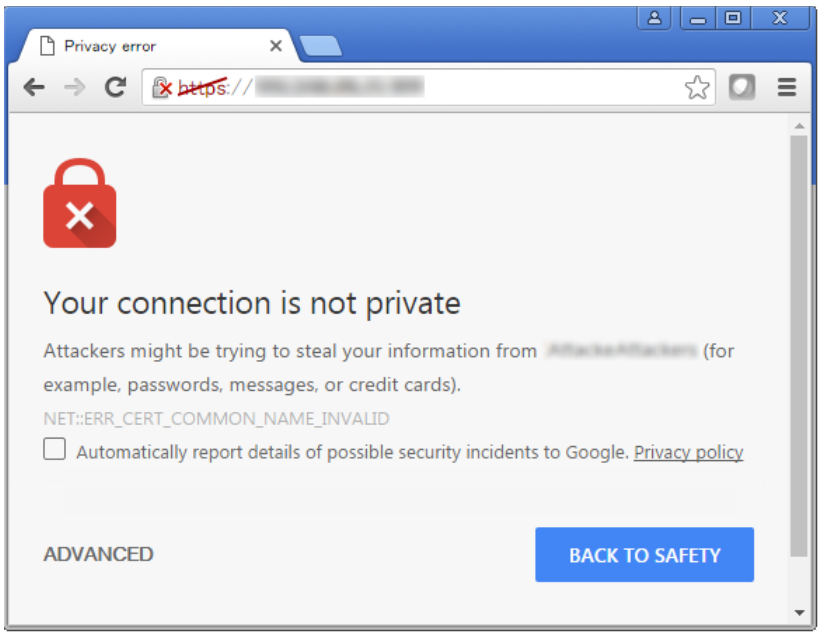
Just as you would with the GateManager Portal login, confirm the address line of the browser indicates a secure website, and that the address line matches that of your account e-mail. Follow this precaution to minimize Man-in-the-middle attacks.



The account e-mail omits the /app/ path, because GateManager automatically launches LinkManager Mobile if the server is accessed without a path.



If an https web server certificate has not been installed on the GateManager, temporarily you may have to accept logging in to an untrusted GateManager server. Always verify with your GateManager administrator that this is OK.

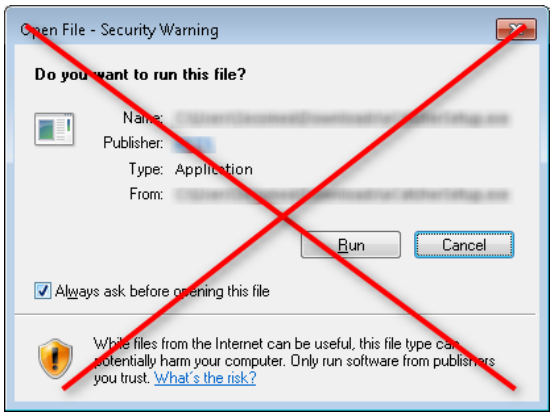

Privacy error
https://
Your connection is not private
Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards).
NET::ERR_CERT_COMMON_NAME_INVALID
Automatically report details of possible security incidents to Google. Privacy policy
ADVANCED
BACK TO SAFETY

LinkManager Windows client

Handling certificate when installed in LinkManager

After the X.509 certificate file (*.lmc) received in the account information e-mail is installed in the LinkManager, delete the certificate from your hard drive.

The LinkManager executable is signed by a certificate that is issued by VeriSign and is preapproved by Windows. As a result, when installing or upgrading LinkManager, the Open File - Security Warning dialog box will not appear. Do not accept such a warning during installation.



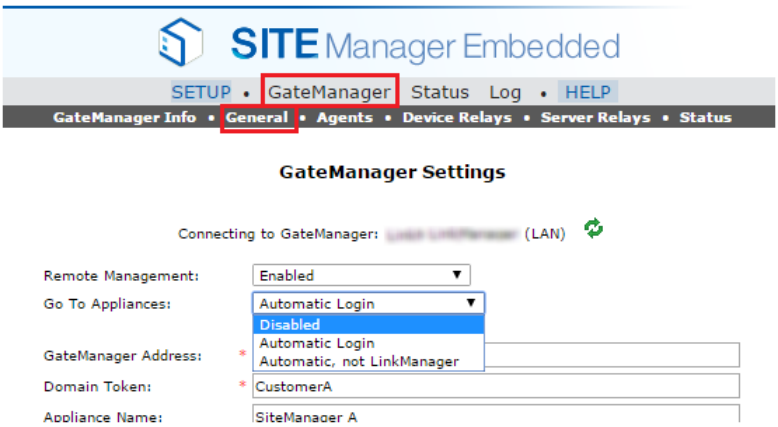
SiteManager configuration GUI

Login Settings for Remote Access

GateManager administrator or LinkManager user with access to the domain where the SiteManager is located, can remotely access the SiteManager GUI.

You can limit access, so remote access to the configuration requires the local password, or you can prevent remote access entirely.

From the menu, select **GateManager** > **General**, click **more>>**, and then change the **Go To Appliance** setting.



NOTE

- Be careful if you are considering this, as your remote service partner may require remote access to assist you in configuring the SiteManager. Additionally all remote access is logged on the GateManager server.