

Pro-face

by Schneider Electric

Pro-face Connect Troubleshooting for LinkManager (Starting up and Connecting)



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.

Copyright (C) 2018.11 Digital Electronics Corporation. All Rights Reserved.

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 |
|---|--|
|  | States precautions and restrictions that must be followed. |
|  | 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. |

| | |
|---|---|
| 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 number of units (agents) you can register differs 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 |
| About the LinkManager | 6 |
| System Requirements and Prerequisites | 6 |
| Troubleshooting Installation | 8 |
| Issues when using more than one network adapter | 8 |
| Issues with rights on the PC | 8 |
| Issues with firewalls or antivirus | 9 |
| Appendix A, LinkManager connection methods | 10 |
| Automatic connection methods | 10 |
| Manually configured Web-Proxy | 10 |

About the LinkManager

LinkManager is software that you can install on Microsoft Windows like any other Windows application.

The LinkManager consists of two components:

1. The LinkManager virtual appliance control module that is visible as an icon in the Windows system tray. The control module menu is accessed by right-clicking the tray icon.
2. The LinkManager virtual appliance that operates in a Vbox engine, separate from the host machine's operating system. It installs its own network layer on a virtual network adapter. The virtual adapter uses NAT mode, which means that it can only be seen from the host PC and therefore does not interfere with anything on the local network. The LinkManager virtual appliance menu is accessed via the web browser that is launched when accessing "Console" from the system tray icon menu.

IMPORTANT

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

System Requirements and Prerequisites

- Any 32 bit/64 bit version of Microsoft Windows Vista, Windows 7, Windows 8.x, or Windows 10. When Intel VT-x is enabled on Windows 7, LinkManager can also run on a virtual machine.
- Intel x86 or compatible processor.
- Minimum 512 MB RAM, dependent on other applications and services installed. The LinkManager virtual appliance reserves 64 MB RAM for its exclusive use.
- Ethernet card with Microsoft Windows or compatible driver installed and attached to a network with a DHCP server. Set up your network to allow outgoing access from applications on a PC. Check Appendix A on how LinkManager accesses the Internet.
- To install the LinkManager, log on to the computer with full administrative privileges.
- The browser GUI used for LinkManager administration, configuration and monitoring uses frames. Therefore, JavaScript must be enabled in the browser.
- When using your LinkManager to access equipment through the GateManager, you need a LinkManager certificate file (.lmc) issued by the GateManager.
- Set up installed antivirus programs to allow installation of a virtual adapter and allow subsequent communication between processes. It is typically not enough just to pause the antivirus program.
- Make sure that your local internet bandwidth is aligned with your data transmission need.
- Standard security requirements:
 1. Protect your computer/tablet with strong passwords (refer to "Pro-face Connect User Guide for Security Setting" chapter "Password Strength for Accounts").
 2. Install antivirus / update security patches on your computer.

- By default, Timeout to disconnect LinkManagers is not active: It is under customer's responsibility to disconnect LinkManagers.

⚠ 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.

Troubleshooting Installation

The symptom for the most typical installation problem is that one of the LinkManager tray icons stays red.

Status of the LinkManager is displayed using icon color.



Red icon – LinkManager is starting or stopped.



Green icon –LinkManager is running.

NOTE

- You can confirm status details by hovering your mouse cursor over the icon.

Issues when using more than one network adapter

If you are often switching between different network adapters on your PC (such as between wireless network and Ethernet) combined with using sleep mode, or your PC is connected with more than one network adapter simultaneously (such as wireless network and Ethernet), you may experience that the LinkManager icon remains red. This is typically due to the LinkManager adapter not getting an IP address from the correct network.

To address this issue, restart the LinkManager (right click the LinkManager tray icon and select Exit, and start it again).

In some cases, you may have to restart the PC to initialize the Windows network stacks.

Issues with rights on the PC

The LinkManager requires the user log in with administrator privileges on the PC where the LinkManager is installed.

Example) When Using Windows 7

1. From the Windows Start menu, open the Control Panel. Or, from the Start menu, click Search, type "control panel" and hit Enter.
2. Go to User Accounts. If using Classic View, go to User Accounts and Family Safety.
3. Browse your users to find the current user, which should be set up as Administrator.

Issues with firewalls or antivirus

1. First stop the personal firewall. However, some personal firewalls continue to block even when stopped. Next, you can try to reconfigure the personal firewall, as shown in the following steps. Only as a last resort, you may have to uninstall the personal firewall completely.
2. Confirm that the LinkManager virtual engine is allowed to communicate by checking that the linkmanager.exe program is not blocked. If the LinkManager still does not work, also check the following:
 1. Confirm the personal firewall has opened UDP port 8888 (all addresses, including broadcast) and TCP port 3. Consult your firewall documentation, or contact your provider. You can limit opening these ports/protocols for the linkmanager.exe.
 2. Confirm personal firewall or antivirus components are not blocking the LinkManager virtual adapter. Enter your Network Connection settings, enter the properties of the LinkManager Adapter, and clear the check box of all items related to antivirus or personal firewall.
 3. Confirm that a third party VPN client is not interrupting the traffic.
3. If there is still an issue, you can check if the LinkManager virtual engine (vBox) is running at all. First stop LinkManager via the tray icon menu (the icon is now red). Hold the Shift key while selecting Start in the LinkManager tray icon menu. Typically, a black console window with a lot of boot messages will appear, indicating the LinkManager virtual machine process is running. If the console window does NOT appear, the virtual machine is not running and there would be one or more log files in the LinkManager installation folder:
C:\Program Files\Pro-face\LinkManager\Machines\LinkManager\Logs

Appendix A, LinkManager connection methods

LinkManager tries several protocols simultaneously to quickly get a working connection to the GateManager.

Automatic connection methods

ACM/PXP (port 11444):

Dedicated port for connecting to the GateManager server. Using a dedicated port is normally preferable as it separates the GateManager related traffic from other out-bound traffic in your network, so you can track the GateManager traffic on your local network and on your Internet connection. Using a dedicated port also means you probably need to open this port in the company firewall, which may collide with corporate policy rules.

HTTPS/TLS (port 443):

Connects to the GateManager using the TLS protocol on port 443. This connection works through firewalls that allow out-going HTTPS connections.

TLS over HTTP (port 80):

Connects to the GateManager using the standard HTTP port 80, but immediately upgrades that connection to a secure TLS connection. This connection method may work through a firewall that only allows out-going HTTP connections.

TLS via Web-proxy:

Connects through a Web Proxy, requesting that Web Proxy to connect to the GateManager on port 443. Once established, the normal TLS protocol is used.

HTTP via Web-proxy:

Connects through a specified Web Proxy (see below), requesting that Web Proxy to connect to the GateManager on port 80. Once established, the connection is upgraded to a secure TLS connection.

Manually configured Web-Proxy

LinkManager searches the Windows registry for information about available web proxies. Such information may originate from a user's configuration of a web browser, or the web browser's detection of the web proxy via the WPAD protocol.

You can manually enter the IP address (and optional port number separated by a colon) of the Web Proxy through which the LinkManager connects to the GateManager.

Alternatively, you can specify a Web-Proxy Auto-discovery (WPAD) URL in the web proxy address field, from which the device can obtain the actual Web-proxy address, for example `http://***.**.*:8080/wpad.dat`.

If the Web Proxy requires authentication from the device, specify the required username and password. Digest, NTLMv2, NTLMv1, and Basic authentication methods are supported (in that order).

For an NTLM-based Web-proxy, the account is typically specified as `DOMAIN\USER` (domain name and user name separated by a back-slash).

The Windows PC's hostname is used as the workstation name in NTLM authentication. If required, you can specify a different workstation name before the account name, separated by a colon, `WORKSTATION:DOMAIN\USER`.

To specify an empty domain, user, or password, write a single # character in the corresponding input field.