

LinkManager™ Startup and Connection Trouble Shooting Guide



This manual describes measures to trouble shoot and fix issues for starting the LinkManager application, or to connect to the GateManager.

Version 2.1, July 2016

Applicable to LinkManager version 6.0 (build 15432 or later)



Table of Contents

Version history	2
1.1. System Requirements and Prerequisites	3
2. Troubleshooting Installation	4
2.1. Issues when using more than one network adapter	4
2.2. Issues with rights on the PC	4
2.3. Issues with firewalls or antivirus	4
2.4. Issues with LinkManager Adapter.	5
Appendix A, LinkManager connection methods	6
Automatic connection methods	6
Manually configured Web-Proxy	6
Notices	7

Version history

- 2.1 Added section 2.4 and version history, and added information about Windows 10

About the LinkManager Application

LinkManager is a software application that runs on MS Windows and installs as any other Windows application.

The LinkManager consist of two components that work completely transparent to the user, and subsequently make the product very user friendly:

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 completely separated from the hosting machine's operating system. It installs its own network layer on a virtual network adapter. The virtual adapter is using NAT mode meaning that it will only be seen from the hosting PC and therefore not interfere with anything on the local network. The LinkManager virtual appliance menu is accessed via a web browser that is automatically launched when accessing "Console" from the system tray icon menu.

1.1. System Requirements and Prerequisites

- Any version of Microsoft Windows XP, Vista, Windows 7, Windows 8.x or Windows 10 (both 32 and 64 bit). LinkManager will also run on these OS'es inside a virtual machine (requires minimum Windows 7 and VT-x enabled in the BIOS). Refer to the vendor specific guides for specific PLC or HMI products for details
- Intel x86 or compatible processor.
- Min. 512 MB RAM depending 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. Your network must allow outgoing access from an application on a PC. Check **Appendix A** for a description on how LinkManager obtains access to the Internet.
- In order to install the LinkManager, you must be logged 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.
- You will need a LinkManager certificate file (.lmc) issued from the GateManager, in order to obtain access to equipment through the GateManager, using your LinkManager.
- An installed antivirus program must allow installation of a virtual adapter and subsequent communication between processes. It is typically not enough just to pause the antivirus program.

2. Troubleshooting Installation

The symptom for the most typical installation problem is, that the LinkManager tray icons either stays red, or remains Yellow (starting)



Red Circle – Grey Switch. The LinkManager is stopped.



Yellow Circle – Grey Switch. The LinkManager is starting.

2.1. Issues when using more than one network adapter

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

You may try to 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 re-initialize the Windows network stacks.

2.2. Issues with rights on the PC

The LinkManager requires that the user has administrator privileges on the PC where the LinkManager is installed.

Windows 7/8 and Vista:

1. Go to Start > Control Panel, or try go to Start > Search, Type “control panel” and hit Enter
2. Go to User Accounts, or if using Classic View this is under User Accounts and Family Safety.
3. Browse your users to find the current user, the account must show the text **Administrator**.

Windows XP:

1. Right click on Start and select Explore.
2. Locate My Computer and right-click and then click Manage, This will show the Computer Management windows.
3. Expand Local Users and Groups.
4. Click Groups, here you find the Administrators.
5. Double click on Administrators. Here, you will find the list of administrators on the computer.

2.3. Issues with firewalls or antivirus

1. You should first try to stop the personal firewall. However, some personal firewalls will retain the blocks even when stopped. In some cases, it is necessary to uninstall it completely. You may not want to do that, and you could therefore try to reconfigure it.
2. Ensure that the LinkManager virtual engine is allowed to communicate. So ensure that the program linkmanager.exe is not blocked. If this still does not work, also check the following:

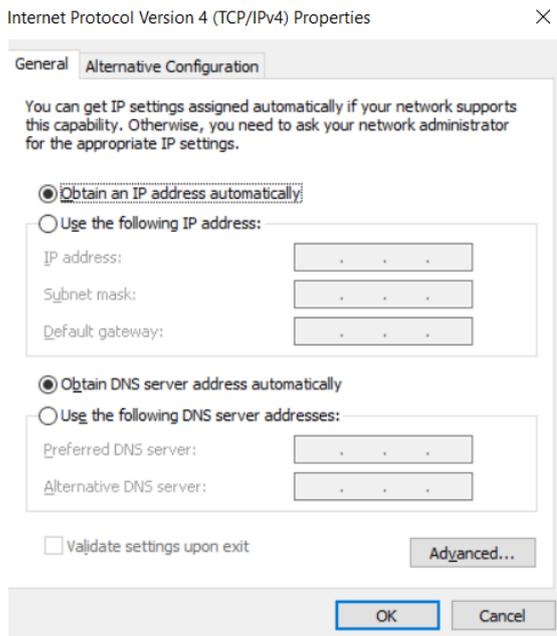
3. Ensure that the personal firewall has opened for UDP port 8888 (all addresses, including broad cast) and TCP port 3. Consult your firewall's documentation, or contact your provider. You can limit opening for these ports/protocols for the linkmanager.exe.
4. Ensure that personal firewall or antivirus components are not blocking the LinkManager virtual adapter. Enter your Network Connections settings and enter the properties of the LinkManager Adapter and uncheck all items that seem to be related to antivirus or personal firewall.
5. Ensure that you do not have a third party VPN client that interrupts the traffic. For instance, the Checkpoint1 SecureClient has been seen doing so. To resolve this, enter your Network Connections settings, enter the properties of the LinkManager Adapter and uncheck the item "Check Point SecuRemote". This will make the LinkManager adapter work, and will have no effect on the SecureClient that can run together with LinkManager.
6. If there still seems to be 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 should be red). Then hold the Shift key pressed while selecting Start in the LinkManager tray icon menu. This should typically give you a black console window with a lot of boot messages, which indicates that the linkmanager virtual machine process is actually running. If the console window does NOT appear, it indicates that the virtual machine is not running. In this case there would be one or more log files in the LinkManager installation folder (typically

C:\Program Files\Secomea\LinkManager\Machines\LinkManager\Logs

These log files may provide some more info, but may also require Secomea support personal to interpret.

2.4. Issues with LinkManager Adapter.

1. The LinkManager will not work with an IP address configured on the TAP adapter. Check settings in Network connections > LinkManager Adapter > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties > Should be set to "Obtain an IP address automatically" and "Obtain DNS server address automatically".



Appendix A, LinkManager connection methods

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

Automatic connection methods

ACM/PXP (port 11444): This is a 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 more easily track the GateManager traffic on your local network and on your Internet connection. But using a dedicated port also means that you will probably need to open this port in the company firewall, which may collide with corporate policy rules.

HTTPS/TLS (port 443): This connects to the GateManager using the TLS protocol on port 443. This should work through firewalls that allow out-going HTTPS connections.

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

TLS via Web-proxy: This 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: This 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

Generally LinkManager will automatically search the Windows registry for information about available web proxies. Such information may originate from a users configuration of a web browser, or the web browsers automatic detection of the web proxy via the WPAD protocol.

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

Alternatively, you may specify a Web-Proxy Auto-Detect (WPAD) URL in the web proxy address field, from which the appliance can obtain the actual Web-proxy address, for example **http://172.16.1.1:8080/wpad.dat**.

If the Web Proxy requires authentication from the appliance, you can specify the necessary 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, i.e. a domain name and a user name separated by a backslash character.

The Windows PC's hostname is used as workstation name in NTLM authentication; if needed, a different workstation name can be specified before the account name separated by a colon, i.e. WORKSTATION:DOMAIN\USER.

If you need to specify an empty domain, user, or password, write a single # character in the corresponding input field.

Notices

Publication and copyright

© **Copyright Secomea A/S 2014-2016**. All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

GateManager™, SiteManager™ and LinkManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we can not guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Secomea A/S shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com