HIRSCHMANN
A BELDEN BRAND

Startup and Connection Trouble-shooting Guide

LinkManager™

Applicable to LinkManager version 5.8
(build 14385 or later)

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

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

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

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

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

Contents

1 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 transparently 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 or Windows 8.x (both 32 and 64 bit). LinkManager will also run on these OS’es inside a virtual machine. Refer to the 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 status as below:

 This tray Icon represent LinkManager is stopped.

 This tray Icon represent 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 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

You should first try to stop the personal firewall. However, some personal firewalls will retain the blocking 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.

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:

Ensure that the personal firewall has opened for UDP port 8888 (all addresses, including broadcast) 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.

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.

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.

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\Hirschmann\LinkManager\Machines\LinkManager\Logs

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

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 outbound 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 outgoing 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 outgoing 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 user's 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.

3 Appendix B: Third-Party Software

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

Firmware/Software for SiteManager, LinkManager and GateManager

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

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

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

4 Appendix C: Further Support

■ Technical Questions

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

You can contact us in the EMEA region at

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

in the America region at

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

in the Asia-Pacific region at

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

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

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

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