

ONESHIELD SECURITY[®]

security solutions you can manage [™]

Quick Install Guide for the Link Manager LM-Product Family Version 1.0

Oneshield Link Manager
Network Management Solutions

This document contains proprietary information relating to Delemont Technology Srl, and is not to be disclosed or used except in accordance with applicable contracts or agreements.

March - 2009

Oneshield Security is a trademarked brand of: Delemont Technology S.r.l.

Headquarters : Venice Gateway for Science and Technology - Via delle Industrie 17/a 30175 Marghera - Venice - Italy

info@oneshieldsecurity.com - www.oneshieldsecurity.com

Page 1 of 11

I. Introduction

The Oneshield LM are powerful network appliances designed to give network applications the bandwidth and redundancy they need. With these appliances the network administrator can add additional WAN services to increase bandwidth and/or implement a redundant WAN infrastructure.

The architecture of the LM product family also allows the implementation of redundant VPN solutions. VPN connections between home-offices and the corporate network, or even between various branch offices are becoming an important part of any business network. The security advantages of such VPNs are well understood, but their reliability and lack of redundancy can often still be a stumbling block. The ability to connect via redundant VPNs over the LM product family removes this problem.



Figure 1 : Link Manager Nano 4 Links

The Oneshield LM hardware and software is developed specifically to address the special needs that the SME customers have; simple reliable equipment that do not offer unnecessary expensive features.



Figure 2 : Link Manager Pico 3 Links

ONESHIELD SECURITY®

security solutions you can manage™

The different products within the family have exactly the same management interface, reducing personnel training costs drastically and easing management of large sites with multiple products.

With their excellent price/performance and their easy to use, intelligent graphical user interface the Oneshield LM products offer minimal total cost of ownership.

In the Oneshield Link Manager architecture, links (or WAN ports) will be grouped into *link pools*. The operation and function of a link pool can be set by selecting one of several pre-defined modes of operation. Depending on the chosen mode of operation, the appliance will either utilize the links (services) simultaneously by balancing the traffic equally, or activate a WAN link when a certain load level is reached on the first link. Another possibility is a complete traffic reroute in the case a WAN link failure.

The powerful architecture of the Oneshield Link Manager allows the definition of streams. This gives the network administrator the possibility to enforce the desired network behaviour, not only at the "physical" link level, but also at the network application (connection, stream) level. The design of the system is based on powerful Oneshield technology, that ensures highest reliability and minimal latency (delay).

In addition to the "outbound" load and link management capabilities the Oneshield Link Manager also offers "inbound" load and link management functions utilizing the integrated DNS server implementation.

Oneshield Security is a trademarked brand of: Delemont Technology S.r.l.

Headquarters : Venice Gateway for Science and Technology - Via delle Industrie 17/a 30175 Marghera - Venice - Italy
info@oneshieldsecurity.com - www.oneshieldsecurity.com

2. Installation

2.1. LM installation introduction

The LM Link Manager Appliances will typically be installed into a 19-inch cabinet. The power cable is connected directly to the rear of the unit. Ethernet connections must then be made to the local network (LAN) and also to the Ethernet ports of the WAN products.

2.1.1. LM package contents

The LM Link Manager contains the following items:

- ▶ 1 LM Link Manager appliance (check the model number on the back of the unit against the documentation)
- ▶ 1 power cable
- ▶ 1 power adapter
- ▶ 1 Quick install guide

You can download the LM PDF manual from www.oneshieldsecurity.com/download

Contact the Oneshield partner where you purchased the product to report missing or improperly functioning items.

2.2. Site requirements

Before you install the Link Manager, make sure the site meets the following requirements:

Mounting Provide a flat table, shelf surface, or an optional 19 in. (48.3 cm) equipment rack. Use an EIA standard equipment rack that is grounded and physically secure.

Power source Provide a power source within six feet (1.8 m) of the installation location. This source must provide 100 VAC to 240 VAC, and 50 Hz to 60 Hz power. Power specifications for the switch are shown in Appendix 6.1. Primary voltage selection within the above ranges is automatic and requires no user action.

Environmental Install the LM Link Manager in a dry area, with adequate air circulation. Avoid placing the LM Link Manager in direct sunlight or near other heat sources, such as hot-air vents. For temperature and humidity specifications, see Appendix 6.1.

Ventilation Do not restrict airflow by covering or obstructing air inlets on the side of the LM Link Manager.

2.3. Connecting to the console port

The LM Link Manager console port is a serial RS-232 interface that provides a connection to a terminal, for performing both monitoring and configuration functions.

The terminal may be a PC or workstation running terminal emulation software, or a terminal configured as a Data Terminal Equipment (DTE) connection. If you connect a terminal to the console port prior to powering on the switch, you can observe the progress and results of the power-on initialization as the LM Link Manager goes through its initialization process.

The console port is a standard RS-232 DTE connection using a male DB-9 connector (see Figure 6.1 for pinouts). This cable must be shielded to comply with emissions regulations and requirements.

2.3.1. Console port (out-of-band) connections

To connect the Link Manager console port to a terminal, do the following:

- a. Connect a VT100 compatible terminal or a PC running a terminal emulation program to the console port. When connecting to a PC, a null-modem cable will be needed. (compatible with the console port pin assignments shown in Appendix 6.2).
- b. Connect one end of the interface cable directly to the LM's console port and tighten the retaining screws.
- c. Connect the other end of the interface cable to a terminal or PC (in some instances, an adapter may be required to make this connection).
- d. From your PC, start the terminal emulation program.
- e. Configure the terminal to the following communication settings: VT100 emulation, 115200 baud, no parity, 8 data bits, 1 stop bit, no flow control, ASCII character set.

2.3.2. Ethernet In-Band Management

The LM Link Manager is delivered with the management IP address set to 10.100.10.100/8 for the MGTM-Ethernet port, that is the **THIRD LAN-Ethernet port, (the third port starting from VGA and/or console port indicated in eth2 on the FRONT panel on LM)**. This IP address should be changed, via the serial console port, to a dedicated IP address within the local subnet schema. This IP address will then be the internal address (LAN) for the *Link Manager*, and will also be used for the web-based management.

Oneshield Security is a trademarked brand of: Delemont Technology S.r.l.

Headquarters : Venice Gateway for Science and Technology - Via delle Industrie 17/a 30175 Marghera - Venice - Italy
info@oneshieldsecurity.com - www.oneshieldsecurity.com

After the IP address has been set, a SSH client should be able to connect to this subnet and can then be used to connect via the Ethernet to the console menu, in the same way as through the serial cable.

2.3.3. Powering the LM Link Manager

The LM Nano, is powered by an external power supply, which must be connected to the connector mounted at the rear of the appliance and to a grounded three-prong wall outlet. See Appendix , “Technical Specifications” for more information regarding specific international power cord requirements. The main power switch located at the rear of the LM Nano must also be turned to the “on” position.

During the initial power cycle, the “Power” lamp on the front panel will light red. During the system boot it will be change to “steady green” when normal operation starts. The “Power” lamp should remain “steady green” now during normal operation. The hardware Ethernet bypass-switch in the LM Nano appliance connects the “LAN” Ethernet port directly to “WANI” Ethernet port when power is removed from the appliance.

The LM-Pico is powered by an external power supply, which must be connected to the power connector on the rear of the unit.

When power is applied, the LM Pico conducts a series of hardware and software tests after bootstrapping to verify operation, the “Power” lamp should light up showing the status of these tests. During the inital power cycle, the “Error” lamp on the front panel will light red. The “Power” lamp should remain “steady green” now during normal operation.

If the power cycle is not as described, check to make sure that the power cable is plugged in correctly, the main switch is “on” and that the power source is good.

When power is applied, the LM appliance conducts a series of hardware and software tests after bootstrapping to verify operation. If a terminal or computer is connected to the console port, the results of the tests, and the bootstrap are displayed on the screen.

2.3.4. Connecting into the Ethernet network

The LM appliances are equipped with a total of five Ethernet RJ45 network interfaces – one LAN Ethernet port and four WAN ports (three on the LM Pico).

The LAN port is connected into the internal network, and is also normally used as the connection over which the management is done. On the LM, each RJ45 Ethernet connector is fitted with two LEDs to show the status of the Ethernet connection. Their functions are listed below in table 5

ONESHIELD SECURITY®

security solutions you can manage™

LED	STATUS	DESCRIPTION
LINK	off	No Ethernet link. No Ethernet cable connected or connection needs to be crossed. The straight CAT5 cable might need to be swapped for a crossed cable, or vice versa.
	green	10/100Mbps Ethernet connection active
ACT	yellow flashing	Ethernet packets activity present
	off	No data being transferred.

Table 1: Ethernet status LED

The interfaces should be connected as described below:

WAN1: Autodetecting 10/100Mbps HDX/FDX Ethernet connection to the first external network. This could be either by a router or directly connected, via the PPPoE protocol, to a DSL splitter. Web-based management is not available via this interface unless specifically enabled (see section 5.4.5).

WAN2: Autodetecting 10/100Mbps HDX/FDX Ethernet connection to the second external network. This could be either by a router or directly connected, via the PPPoE protocol, to a DSL splitter. Web-based management is not available via this interface unless it has been specifically enabled (see section 5.4.5).

WAN3 Autodetecting 10/100Mbps HDX/FDX Ethernet connection to the first external network. This could be either by a router or directly connected, via the PPPoE protocol, to a DSL splitter. Web-based management is not available via this interface unless specifically enabled (see section 5.4.5).

WAN4 (LM Nano 4 Only) Autodetecting 10/100Mbps HDX/FDX Ethernet connection to the second external network. This could be either by a router or directly connected, via the PPPoE protocol, to a DSL splitter. Web-based management is not available via this interface unless it has been specifically enabled (see section 5.4.5).

LAN: Autodetecting 10/100Mbps HDX/FDX Ethernet connection for all *Link Manager* in-band management and also the connection into the internal network. This port has an IP address, and IP netmask as defined via the console menu. The factory IP address for the LAN port is 10.100.10.100 with an IP netmask of 255.0.0.0. After installation, all standard management will be browser-based via the standard HTTP port 80. However, the Ethernet port can also be used when connecting via SSH to the setup menu.

WARNING: operation of the Link Manager depends on continuous link monitoring of the WAN connections. This monitoring is done by regularly sending ICMP ECHO and receiving ICMP ECHO REPLY messages to/from the link gateway, and the check-it addresses.

Firewalls inserted between the Link Manager and the relevant hosts must pass these packets through unchanged, to guarantee proper operation of the Link Manager.

When a Link Manager is placed in a running network, it will typically have to modify the existing data flow from the LAN into the WAN. Hosts and networking equipment will often have stored the existing MAC addresses of the previous gateways, etc. with long life times, and will not request a new one from the Link Manager for a considerable time.

It is therefore important to do one of the following:

- 1) Clear the arp caches on the relevant hosts, and networking products**
- 2) Reduce the timeout time for the host or networking equipment as described in Appendix 6.5**

WARNING: the Ethernet cables used to connect the LM device to other equipments must be shielded and no longer than 10 feet

3. Basic system configuration

To set up the basic system configuration, it is necessary to log into the basic system menu via either the serial port, or SSH connected by the LAN Ethernet port. The factory user name and password are as follows:

USERNAME	admin
PASSWORD	admin

Table 2: Factory password for administration and setup

3.1. Basic configuration menu

Figure 4.1 shows the Basic Configuration menu after logging in using the username and password. The cursor keys or the TAB key can be used to move the cursor to the entry to be changed. It can then be selected by pressing the return key.



Figure 4.1: Standard setup menu

ONESHIELD SECURITY®

security solutions you can manage™

IP Address: The IP address of the LAN Ethernet port. The web management interface and SSH server will also respond at this address. The IP address can be changed later via the web management (see section 5.4.5).

Netmask: The IP netmask of the LAN interface and also the web-based management and SSH server. The IP netmask can be changed later via the web management (see section 5.4.5).

Expert: Select the Expert menu for firmware upgrades, database resets, and configuration import functions.

Save: Save any changes made to the configuration. The *Link Manager* will immediately reboot with the new parameters.

Quit (No Save): Continue operation without changing parameters, or rebooting.

3.2. Expert configuration menu

The expert menu adds extra functions that can be performed from the menu interface but are needed during the standard installation. This mode is entered directly from the standard menu by selecting the “expert” entry. The terminal display in this mode is shown in figure 4.2.

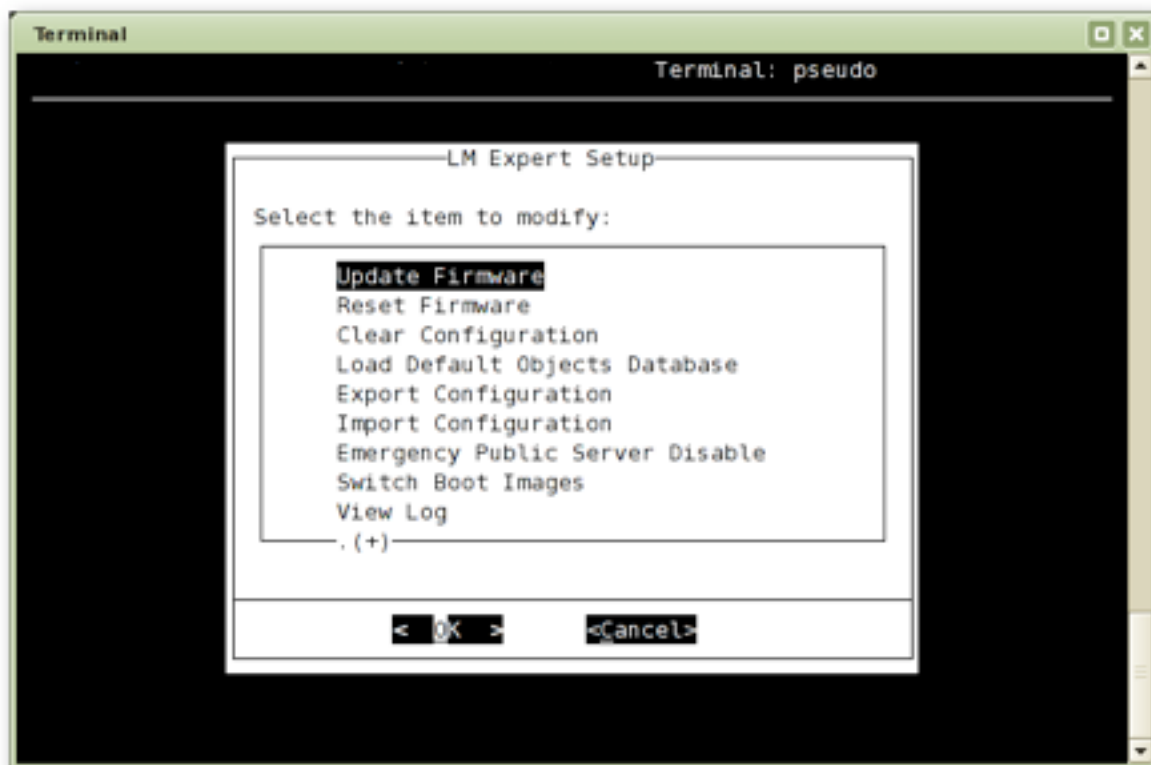


Figure 4.2: Expert setup menu

Update Firmware: The system firmware can be upgraded via the Z-Modem protocol. This is described in detail in Appendix 6.4.

Oneshield Security is a trademarked brand of: Delemont Technology S.r.l.

Headquarters : Venice Gateway for Science and Technology - Via delle Industrie 17/a 30175 Marghera - Venice - Italy
info@oneshieldsecurity.com - www.oneshieldsecurity.com

ONESHIELD SECURITY®

security solutions you can manage™

Reset Firmware: Revert to factory-loaded system firmware.

Clear Configuration: All configurations are reset to the factory defaults. This includes the **admin** password, which is changed back to “admin”. The following parameters are reset to the factory defaults: IP address, netmask, etc. The object database is reset to the initial state.

Load Default Objects Database: Delete the present objects configuration database, and replace it with the factory release. This effectively re-initialises the object database.

Export Configuration: Save a copy of present configuration using the Z-Modem protocol.

Import Configuration: Load a configuration using the Z-Modem protocol.

Switch Boot Images: Switch to the other stored image. This is then selected at the next boot.

View Log: List any system anomalies and events that occurred since last system boot.

System Info: System software version, firmware release, device model, etc.

Main Menu: Return to the standard configuration menu. Note: It will be necessary to scroll down to select this entry.