



Simplify Management of Your IT Equipment and Your Entire Network Infrastructure

The vSLM 2 Secure Management Software is a “master control center” that seamlessly integrates equipment connected by console servers, KVMs, and remote power managers.

Due to the demands of modern day business, network infrastructures continue to grow along with the number of “out-of-band infrastructure” (OOBI) management devices. With Lantronix’ vSLM 2, “managing the management equipment” is no longer a challenge. Through a centralized point of access and common interface, the vSLM 2 enables administrators to quickly and easily access equipment anywhere in the enterprise with just a few mouse clicks.

Consolidated Access and Authentication

The vSLM 2 simplifies administration by offering multiplatform client access through a standard web browser for a single point of consolidated access with simplified views to OOBI management devices and attached equipment. This centralized



vSLM™ 2 Highlights:

- Virtualized central management appliance
- VMware® compatible
- Consolidate management of IT infrastructure
- Maintain a secure central point of access to all equipment
- Reduce troubleshooting and repair time
- Dynamically discover device on local or remote subnet
- Minimize total cost of ownership and administrative resources
- Maximize equipment up-time

authentication minimizes administrative burdens. Additionally, since user account information is maintained in one place, there is no need to maintain separate user-names/passwords for each management device. Users can also be remotely authenticated using LDAP, RADIUS, NIS, Kerberos, and TACACS+.

Reduced Operating Costs

Streamlining overall operations reduces administration and maintenance costs. With consolidated remote access, network administrators can quickly isolate and access problem equipment. This can minimize the impact of system down time and improve employee and company productivity. Additionally, the vSLM 2 reduces total cost of ownership for data center equipment. Automated firmware deployment tools also reduce time and labor.

Simplified and Bulletproof Security

The vSLM 2 helps IT departments adhere to corporate security policies. As a proxy between administrators and OOB management devices, access is well defined and easily controlled, particularly where access is required outside a firewall or NAT-based router. Users are only allowed to access the devices and attached equipment with granted access specific rights for read-only or read/write access, and provisions for remote authentication. To ensure accountability, user access audit logs maintain a record of login success/failure, user login/logout, and port open/close activity. And whether connecting via a web browser or a command line (CLI), 128-bit encryption (SSL/SSH) ensures secure connections to the end-user equipment along with strong authentication.

Features and Specifications

> VMware Compatibility

- ESX
- ESXi
- Workstation



> Hardware Requirements (minimum)

- 3.0Ghz or faster single core speed
- RAM: 2 GB
- Disk Space: 60GB
- Ethernet: 1 Bridged

> Distribution

- Available as a digital download from <http://www.lantronix.com>
- Compressed & zipped OVF & VMDK distributions available

> Trial Period

- 30 day free trial
- License activation required after 30 day expiration

> Warranty

- 90-day limited warranty

Advanced Feature Set

For quick and easy setup, Auto Discovery finds device and port assignment, eliminating the time-consuming task of manual configuration. Auto Discovery supports Lantronix Discovery Protocol (LDP) for SLC Console Servers and SNMP for all other devices. With the click of a button the SLC Update tool automates firmware deployment to console servers. All console messages are captured and stored to the internal hard drive, providing secure and permanent storage. Console logs may be conveniently accessed through the web interface. System configurations can also be saved and restored, providing rapid recovery of inadvertent configuration changes and peace of mind. Dual Ethernet adapters provide connection to OOB management devices on the network, while remote users connect through another, providing greater security.

Web Interface

The screenshot shows the Lantronix SLM web interface. The browser address bar displays <https://172.18.100.22>. The page title is "LANTRONIX SLM". The user is logged in as "sysadmin@SLM4F37". The main content area is titled "Manage 'SLC' Group" and contains a table with the following data:

Name	IP Address	Ethernet Address	Device Type	Location	Model	FW Ver	Last FW Update	Login	Char Key
Gary_SLC48-03	172.18.12.150	00:80:A3:8D:24:C5	SLC		SLC48	5.5		sysadmin	No
Kevin_SLC	172.18.17.145	00:80:A3:89:12:7D	SLC		SLC48	5.4		sysadmin	No
LabSLC	172.18.0.107	00:30:31:FF:FF:54	SLC		SLC32-02	5.4		sysadmin	No
MartinsSLC	172.18.23.110	00:80:A3:89:1E:29	SLC		SLC8	5.4		sysadmin	No
mlslc48	172.18.21.66	00:80:A3:8D:53:29	SLC		SLC48	5.5		sysadmin	No
slc0085	172.18.32.25	00:80:A3:89:00:85	SLC		SLC16	5.4		sysadmin	No
slc0b6d-Gary	172.18.12.200	00:80:A3:89:0B:6D	SLC		SLC48	5.4		sysadmin	No

- Interactive web interface requires no special software.
- Authenticated users only have access to authorized devices.
- Built in SSH Web Client provides secure access.
- Console messages logged for audit and control.

Ordering Information

> **Part Number**
VSLM-02

> **Description**
Secure Management Software License