

Date: December 7, 2006

PCN No.: PCN-068

PRODUCT CHANGE NOTICE: SLM25612N-02 and SLM Firmware Version 2.2

Dear Valued Lantronix Customer,

Lantronix is pleased to announce availability of the SLM25612N-02 replacement for the SLM25612N-01, and updated firmware for the Securelinx™ SLM Management Appliance. Beginning December 12, 2006 the SLM25612N-02 will begin shipping with version 2.2 firmware installed.

Model	Description
SLM	SecureLinx Management Appliance

UPDATE HIGHLIGHTS

Hardware platform:

SLM25612N-02 features include:

- Physically smaller size – allowing the new SLM to utilize less rack space. The new chassis is 14 in. (35.6 cm) deep, compared to the -01 model of 23 in. (58.4 cm) a savings of 9 in. (22.8 cm)
- Larger Hard Drive – for increased storage capacity, a 160GB drive replaces the older 40GB drive.
- Dual 10/100/1000Base-T Ethernet – as compared to the previous model with only 1) 10/100/1000Base-T Ethernet port.
- RoHS-5 Compliant – under the exception for servers and network infrastructure equipment.
- Built-in CD-ROM – to support product updates in a future release.

Feature Set:

SLM version 2.2 adds a number of significant new features, including: key enterprise productivity enhancements, improved ease-of-use, expanded integration with other Lantronix products, and enhanced security. Please see the following page for a summary of the new features.

UPDATE AVAILABILITY

Customers with existing SLMs, electing to take advantage of the new features and capabilities of the v2.2 update, may upgrade their units at no additional charge. An upgrade patch, installation instructions, and release notes will be available on **December 12, 2006** from the Lantronix web site at:

<http://www.lantronix.com/support/downloads.html>

If you have any questions, please contact your local sales representative or Lantronix Customer Support at (866) 649-0721 or (949) 453-3990 x342.

FEATURE SET HIGHLIGHTS

Feature/Enhancement	Description and Benefit
Windows™ Active Directory Remote Authentication	LDAP remote authentication has been enhanced for interoperation with Windows™ Active Directory servers, allowing SLM users to be remotely authenticated via Active Directory.
IP Filtering	The IP Filter allows restrictions to be placed on incoming connections to SLM based on the protocol type, port number or range of ports, and the originating IP address.
Connection Manager	A new Connection Manager, available to users with SLM administrative privileges, displays all connected users and their respective outbound device connections, and allows termination of connected users and their individual outbound device connections.
Interface Fusion	Managed Devices now support a consolidated (or fused) view of end-devices connected by various means. For example, a server connected to both an SLC Console Server and SLP Remote Power Manager, may be managed from a single interface, for both console access and power control, greatly simplifying system administration that requires access/control methods.
IPv6 Support	SLM now includes a dual-stack IPv4/IPv6 architecture, with support for: static IPv6 addressing, IPv6-based ICMP, and incoming IPv6-based SSH connections.
Additional TACACS+ Servers	TACACS+ Remote User Authentication settings have been updated to add two (2) additional TACACS+ servers, for a total of three (3) TACACS+ servers, in environments where multiple TACACS+ servers are employed.
Multiple syslog Server Support	Outgoing syslog messages may optionally be sent to multiple syslog servers (2 max.) for applications requiring redundancy and/or backup of outgoing syslog event messages.
SLP Power Manager Outlet Name Management	For authorized users, the Ethernet Device > Configure tab for SLP Remote Power Managers allows the Name of the respective outlet to be changed remotely via the SLM.
RDP for Windows Managed Devices	Windows-based hosts may now be accessed via Remote Desktop Protocol (RDP) via the optional “Remote Desktop” button in the Managed Device view.
Dial-In and Dial-Out Modem Support	USB and PCI connected modems are now supported for dial-in and dial-out PPP and text connections. At this time, the following modems have been testing for compatibility: MultiTech MultiModem USB V.92 Data/Fax World Modem (part# MT5634ZBA-USB-V92), and the MultiTech MultiModemZPX V.92 Voice/Data/Fax World Modem (part# MT5634ZPX-PCI-U).
Modem Connectivity Check	Remote hosts connected via modem may optionally be periodically checked for connectivity.
New Event Manager Triggers	The Event Manager now supports triggers for: communication loss with polled devices, AC current overload conditions on an SLP Remote Power Manager, and text string matching of SLM internal syslog messages.
SLC SSH Key Management	Public SSH keys, used for Secure Channel connections with managed SLCs, may now be: stored by the SLM, transferred to an SLC, or deleted.

FEATURE SET HIGHLIGHTS (Continued)

New SNMP Traps Recognized	SNMP traps from both the SLK Remote KVM and SLP Remote Power Manager are now fully recognized by the SLM, for use with the Event Manager, and for display within the Trap tab of SLK and SLP Ethernet Device folders.
Auto-Discovery of Lantronix Devices Beyond the Local Subnet	Auto-discovery using Lantronix Discovery Protocol (LDP) now supports multicast IP addressing, allowing discovery of devices beyond the local subnet, as supported by network infrastructure.
Auto-Discovery of Lantronix Devices by IP Address Range	Auto-discovery using Lantronix Discovery Protocol (LDP) now supports IP address ranges, allowing a group of devices to be discovered by IP address range, as defined by a starting IP address and ending IP address.
Lantronix SCSxx00 Auto-Discovery	Auto-discovery will now recognize Lantronix SCSx00/xx00 devices, and place discovered devices in a separate device folder.
Non-Lantronix Discovery Options	Auto-discovery of non-Lantronix devices may optionally be disabled, resulting in no devices being stored in the "Other Devices" folder.
New Ethernet Device Folder Properties	Ethernet Device folders feature new properties that allow individual folders to be: always displayed, never displayed, or only if populated (not empty).
Ignore ICMP Requests	A new configuration option in the Services > Configure folder allows ICMP requests to be ignored, rendering the SLM invisible to external "ping" requests.
SSH v1 Enable/Disable	Incoming SSH v1 connections to the SLM may be disabled, allowing only SSH v2 connections, for enhanced security.
SSH and SSL Updates	As part of ongoing security enhancements, OpenSSH has been updated to version 4.3p2-4, and OpenSSL had been updated to version 0.9.8a-5.2.
SLM Update via Web Browser	Updates may now be uploaded directly from the SLM administrator's computer, using only a web browser, eliminating the need for an intermediary FTP/SFTP server.
SLM Update Management	Updates may now be transferred to the SLM via USB attached storage devices, NFS mounts, or CIFS shares. Once stored on a local folder of the SLM, the updates may be applied.