Security

Allerion Inc.

SUPPORTlink

717 Ridgedale Avenue
East Hanover, NJ 07936 USA

Tel: 201-887-1000
Ext. 2385
Fax: 201-887-9546

SUPPORTlink services helps companies monitor, manage, control, and optimize networks and desktop systems through a spectrum of network management tasks:
Fault management: detecting network faults on managed devices; isolating and resolving the faults in the shortest amount of time possible. Performance management: monitoring performance of managed network devices to determine device thresholds and performance bottlenecks. Change management: providing information to assist in the adding, moving, or deleting of nodes, lines, data-paths, and access devices.
Security administration: reviewing network security, such as user rights, file access and resource access, during system audit and periodic reviews. Resource administration: maintaining an inventory database of managed devices to aid in the diagnosis of network events and assist in the detection and resolution of network faults SUPPORTlink manages all or part of your environment including: servers, peripherals, hubs, bridges, routers, and desktops. SUPPORTlink service is non-obtrusive and can co-exist with SunConnect's Solstice SunNet Manager management platform. SUPPORTlink is offered in two ways: On-Site - Allerion will integrate the SUPPORTlink Network Control Center and the associated management tools on your site, train your personnel in its operation and provide on-going support. Remote - A service bureau approach that allows you the ability to provide first-rate network support without investing resources in network management tools.

Solaris version:
Solstice application/version:
Types of integration: Console Menu Interface, Data File Integration, Uses Agent API, Uses Manager API

Australian Software Innovations Services

ASI-SECURITY

Level 3 51 Rawson Street
Epping NSW 2121
Australia

Tel: 61 2 869-0244
Fax: 61 2 869-0280

ASI-SECURITY maintains a system access security code (password) for each user login ID. ASI-SECURITY forces users to change their security code on a regular basis, based on either the number of days or number of logins elapsed since the last password change. After a specified number of consecutive failed logins, the user ID that fails can be barred from logging in again until the system administrator re-enables the user ID. Users can be barred from logging in if they have not logged within a configured number of days. To assist in the control of out-of-hours access, the system administrator can configure an After Hours access period for weekday and weekend access and prevent specified users from accessing the system during this time. ASI-SECURITY provides control of the format of security codes that are selected by the user to enforce the inclusion of non-alphanumeric characters in the password. Also, ASI-SECURITY can prevent specified user IDs from logging in on more than one terminal or remote line at a time.

The ASI-SECURITY Administration utility is accessible to the System Administrator from the Solstice SunNet Manager Console.

Solaris version:
Solstice application/version:
Type of integration:

Australian Software Innovations Services

LOGMON

LOGMON monitors terminal activity and logs out inactive terminals after a specified period of time. Inactivity time limits can be set on a per user, per group, or terminal id basis. LOGMON provides a solution to the security and resource availability problems arising from unattended or inactive, logged in terminals and workstations. The LOGMON Administration utility is accessible to the System Administrator from the Solstice SunNet Manager Console.

Solaris version:
Solstice application/version:
Type of integration:

Level 3 51 Rawson Street
Epping NSW 2121
Australia

Tel: 61 2 869-0244
Fax: 61 2 869-0280

AxLAN

AxLAN ADMINISTRATOR

AxLAN ADMINISTRATOR is a management and administration tool for LAN Manager networks. It is integrated into Sun Net Manager and later versions of SOLARIS 2.3. AxLAN ADMINISTRATOR offers a GUI interface to manage, secure audit and administrate LAN Manager servers and LAN managers users. AxLAN ADMINISTRATOR is usable with all LAN Manager products (OS/2, UNIX, LAN Server, PATHWorks).

Solaris version: Solaris 2.3
Solstice application/version: Solstice SNM 2.2.2
Types of integration: Console Menu Interface, Data File Integration, Requires Solstice SNM to Run

Centre d'Affaires de Jouy
1, rue du Petit Robinson
78353 Jouy-en-Josas
FRANCE

Tel: 33 (1) 34 65 94 44
Fax: 33 (1) 30 70 60 15
Internet: ogranbou@axlan.oleane.com

Cascade Communications Corporation

Cascade View

Network Management Station for Cascade Multi-ServiceNetwork (Frame Relay, SMDS and ATM) providing backbone for CDPD.

Solaris version: 2.3, 2.4
Solstice application/version: Solstice SEM
Types of integration: Console Menu Interface, Data File Integration, Uses Agent API, Uses Manager API, Requires Solstice SNM or Solstice Enterprise Manager to run

5 Carlisle Rd.
Westford, MA 01886 USA

Tel: 508-692-2600
Fax: 508-692-9214

Computer Associates

CA-Unicenter for Solaris

One Computer Associates Plaza
Islandia, New York 11788 USA

Tel: 516-342-6000
Fax: 516-345-5737

The security system in CA-Unicenter provides centralized user administration for a single machine or network of UNIX computers, with global enforcement of both user access controls and asset access controls. It provides calendar control to ensure assets are available to specific users only during specific hours of specific days. It works with the native Solaris security system and can be implemented in phases, so that migration to the more robust security environment provide can be made easily. It also offers monitoring modes so that defined security rules can be tested in simulation mode, enabling security administrators to check what would happen if full security were implemented, and record the activity of specific users who attempt to circumvent the new security policies.

Security management with CA-Unicenter for Solaris is extremely cost-effective as it allows all security to be policy based. Instead of forcing security administrators to individually set permissions for files and users via access control lists, CA-Unicenter uses a graphical interface with push buttons to define security policies for groups of users and groups of assets. It also offers several more types of control than provided by standard UNIX permissions. The security facility provides protection for all systems management functions, and even prevents superusers from abusing their privileges or by bypassing this security.

Security events and attempted violations are written to a log file which provides a complete audit trail for security administrators and auditors.

Solaris version: 2.3 and 2.4
Solstice application/version: Solstice SNM 2.2
Type of integration: Console Menu Interface

LANNET Data Communications, Ltd

MultiMan/SNM

17942 Cowan
Irvine, CA 92714 USA

Tel: 714-752-6638
Fax: 714-752-6641

MultiMan/SNM provides network management applications that allow network managers to monitor and control LANNET's Ethernet, Token Ring and FDDI based intelligent switching hubs from Solstice SunNet Manager 's management platform.

MultiMan/SNM's Zoomed Hub Management View displays a detailed image of the hub showing the functional status of management objects including modules and ports. Multi-level configuration and control information is provided for the hub, agent, modules, and internal buses. Network connections can be monitored via port to bus and network connectivity maps.

MultiMan/SNM provides a multi-faceted security scheme, enabling the definition of access control at the port and network level. Fault reporting can be performed via custom definitions which allow the setting of color coded fault status, propagation of compound status, and user definable actions.

Solaris version:
Solstice application/version:
Types of integration: Console Menu Interface, Data File Integration, Uses Manager API

Motorola UDS

GlobalView/GV SNMP

Analog modem management; offers configuration security, problem isolation, activity and usage monitoring, graphical user interface; SNMP connectivity via GV/SNMP option, the GlobalView management station MIB.

5000 Bradford Blvd. NW
Huntsville, AL 35805 USA

Tel: 205-430-8855
Fax: 205-726-0617

GlobalView SNMP Management Station MIB:
Motorola UDS has added Simple Network Management Protocol (SNMP) support to its Windows-based GlobalView network management system. GlobalView now offers a management station Management Information Base (MIB) to provide an interface to SNMP managers on the network. In an SNMP environment, a network administrator can address queries and commands to network nodes and devices. The protocol moves management information between SNMP managers and agents to monitor network status and performance, control operating parameters, and report and analyze faults or alarm conditions. The GlobalView software serves as a proxy agent in the SNMP environment, adding its control and comprehensive configuration, diagnostic, security and fault isolation features to enhance the SNMP system.

The GlobalView MIB allows users to incorporate GlobalView into their overall network management scheme, providing network administrators with global alarm notification, alarm processing and alarm threshold configuration. When the SNMP manager detects that an alarm has occurred, the network administrator is able to diagnose the problem quickly by requesting a “snapshot” of all devices with active alarms. This snapshot provides device identification, status, and alarm type information for those devices. GlobalView also provides the network administrator with the capacity for detailed system monitoring. Any device or shelf may be selected for specific information retrieval. The administrator can monitor alarm counts, connection times, connection rates (in bps), device status, even the last number dialed by any device.

Device control features include reset, disconnect, busy out. AT command delivery is provided. Full alarm configuration capabilities allow the network administrator to set individual alarm thresholds as well as determine and set a desired response to each alarm type.

Solaris version: N/A
Solstice application/version: N/A
Type of integration: Uses Agent API

Network Peripherals

NPI Switching Hub Manager

The NPI Switching Hub Manager provides Enhanced SNMP management capabilities utilizing a graphical image of NP’s Switching Hubs, and allowing for point-and-click statistics gathering.

1371 McCarthy Blvd.
Milpitas, CA 95035 USA

Tel: 408-321-7300
Fax: 408-321-9218
Internet: info@npix.com

Solaris version: 2.3, 2.4
Solstice application/version: Solstice SNM 2.2, Solstice SNM 2.2.2
Typess of integration: Console Menu Interface, Data File Integration, Uses Agent API, Uses Manager API

Network-1 Software & Technology, Inc.

NET1-NetPanel

P. O. Box 8370
Long Island City. NY 11101 USA

Tel: 719-590-9611
Fax: 718-590-1559

The NET1-NetPanel product was designed by the Network-1 Corporation to provide a variety of features that enhance the capabilities of the basic NetView product on both the OSF/1 - Alpha and AIX - RS/6000 platforms. The product's primary goal is to simplify the daunting task of managing the enterprise network. NetPanel meets this goal by supplying a powerful instrument-like graphical interface and a sophisticated rule-based inference engine for detecting key network events and trends.

The NetPanel graphical display allows customization of a series of instrument clusters that reflect the current state of various network devices and their attributes. The instruments include a wide variety of meters, gauges, light arrays etc., that can be directly associated to SNMP variables of all, some, or one particular network device (e.g. a router, bridge, repeater hub, etc.) These netpanels are designed and configured for use in the NetPanel Configuration application, while they are tied into the "live" SNMP traffic for real-time display with the NetPanel Display application. Both applications provide the standard Motif Windows environment and use the point and click paradigm for control. There is no practical limit to the number of netpanels that may be displayed at one time.

The NetPanel product is closely tied to the Data Collection application provided by NetView, thus using a central point for defining the SNMP polls of interest to the network manager. SNMP traps (asynchronous event signals from SNMP network devices) are also fully supported by NetPanel and its instrumentation. Historical capabilities allow you to re-play a previously stored data flow via the netpanels to assist in the trend analysis of your network.

NetPanel's inference engine is rule based and allows for the use of either the pre-defined network manager. A rule definition tool is provided that allows for the creation of new items in the rule-base, by using an easy to learn graphical interface. Additional device rules will be sent on a regular basis to those customers under a Network-1 maintenance agreement. These device rules alert the network manager to network events that range in severity from "worth noting" to "critical".

Solaris version: 2.3
Solstice application/version:
Types of integration: Console Menu Interface, Data File Integration, Requires Solstice SNM or Solstice Enterprise Manager to run

Newbridge Networks/Vivid

Vivid System Manager

593 Herndon Pky.
Herndon, VA 22070 USA

Tel: 703-708-5913
Fax: 703-708-5959

The VIVID System Manager is used to configure, monitor and troubleshoot a network consisting of VIVID ATM components such as Workgroup Switches and Ridges, and other SNMP manageable LAN devices. The VIVID System Manager provides an intuitive Graphical User Interface (GUI) for managing local area networks. It provides an object oriented view of the network, with physical representations of the overall network topology as well as individual nodes, slots, ports and paths. Logical views are also available for implementing virtual LANs and physical security. Most operations are menu driven and point-and-click.

The VIVID System Manager provides the user with the tools to detect, isolate and correct network problems when they arise. Alarms and trouble tickets are automatically generated and the user is notified through visible and audible alarms in all relevant network views. Additionally, the System Manager enables the user to monitor and correct potential problems before they occur. A variety of statistics are maintained on all of the VIVID elements (e.g. cells transmitted, cells received, errors, etc.). The System Manager provides a performance management tool for correlating, manipulating, and presenting these statistics. Standard or customizable graphs and reports are available. Virtual LANs allow several users to be logically grouped together independent of physical port location.

The VIVID architecture extends this concept to “virtual subnets” that support concurrent bridging and routing. Virtual subnets allow devices in the same subnet to appear on any physical port, either Ethernet or ATM, located throughout the network. With VIVID Routed LAN Emulation, the network administrator can logically group users into virtual subnets and create filters and firewalls as required. All virtual LAN configuration is performed via the System Manager's GUI. As devices move from port to port the VIVID Route Server automatically discovers the changes and maintains the proper network layer address associations. No manual reconfiguration is required by the network administrator. The System Manager reflects these discovered changes on all relevant network views. This separation of logical addresses from physical ports dramatically simplifies the configuration and administration required in LAN inter networks.

Filtering can be implemented between virtual LAN workgroups. Network managers can administer security based on logical communities of interest as opposed to physical port location. Filters between virtual subnets will remain in effect regardless of where users move.

Port-level bindings are also available, allowing administrators to restrict virtual subnets to specific physical ports or to bind individual ports to an individual host. Switched virtual circuits (SVCs) are dynamically set up and torn down by VIVID ATM Switches based on reachability tables calculated and distributed by the System Manager. The ATM switch uses a fast signaling protocol, SVC Turbo, to dynamically establish SVC connections across a network of ATM switches in a streamlined fashion. Such rapid call setup is critical for emulating connectionless LAN traffic in large networks.

Unlike shared media LANs, where on-demand usage can degrade performance, VIVID LANs with congestion management ensure a predictable service level for all users. Permanent virtual circuits can also be established.

Solaris version: 2.3
Solstice application/version:
Types of integration: Console Menu Interface, Data File Integration, Uses Agent API, Uses Manager API

OpenVision Technologies, Inc.

OpenV*SecureMax

7133 Koll Center Parkway
Pleasanton, California 94566
USA

Tel: 800-223-OPEN or
510-426-6400
Fax: 510-426-6468

OpenV*SecureMax allows you to centrally audit and manage security of your UNIX or VMS systems. It quickly determines the security status of systems on the network and gives detailed attention to those systems that fail to meet your security standards. OpenV*SecureMax's comprehensive reports and analysis tools immediately identify exposures and created corrective scripts so you can close potential security issues and quickly manage on-going changes with exceptions-based reports.

Solaris version: 2.3 and 2.4
Solstice application/version: Solstice EM 1.0 and Solstice SNM 2.2.2
Type of integration: Console Menu Interface

Tripp Lite Manufacturing

UPS SNMP Adapter

500 N. Orleans St.
Chicago, IL 60610 USA

Tel: 312-923-2289
Fax: 312-329-9620

Using the standardized MIB for SNMP communication for UPSS, the SNMP Adapter allows remote management of up to 4 UPSs and 2 peripheral devices, which allows control of AC power remotely. Adding SNMP control can provide an additional layer of fault tolerance to your network. Because the SNMP-2 adapter doesn't require a nearby PC to run monitoring software, it is ideal for UPS systems in hub closets or anywhere along the network wire where power control enhances management control. When used with our new SNMP-2 adapter the Smart Series UPS becomes an intelligent node on the network.

Self-test any UPS on the network to determine battery condition. Through the SNMP-2, UPSs can be remotely controlled on line or time programmed to reboot and/or power- down connected devices, allowing the restart of network components that have locked up. Disaster Planning and Network Control. Tripp Lite's SNMP-2 Adapter can maintain a separate network communication channel via a phone line modem. If the Ethernet cable is disabled, normal communication with key computers, bridges, routers and concentrators is lost. “Out-of-band” phone-line links via the SNMP-2 provide a vital alternate channel able to reboot components and resume critical network operations. Control UPSs and peripherals connected to the SNMP-2, i.e. local alarm systems, TV monitors, other security devices, etc.

Monitor and control ambient temperatures and humidity with the SNMP-2's built-in sensors. HVAC (Heating, Ventilation, Air Conditioning) systems can be controlled remotely by programming Tripp Lite's SNMP-2 to turn them on when conditions exceed programmed set points. Connect up to four Tripp Lite UPS systems at once, allowing control of more components on the network with fewer SNMP adapters. Depending on network size, this can represent a substantial cost savings.

SNMP adapters are typically connected to a UPS that a network manager would want to monitor and control. If the manager chose to turn-off the UPS, that action would cut power to the SNMP adapter, shutting down further communication and preventing subsequent remote turn-on and reboot. Only Tripp Lite's SNMP-2 adapter has a second AC input which can be permanently connected to another power source. This maintains communications and enables the manager to power-up a “sleeping” UPS and power-on connected equipment. PNM (Phil Net Manager) Network Management Application (based on SNM) for Data Communication products manufactured by TRT, allowing heterogeneous products management for LAN/WAN customers.

Solaris version:
Solstice application/version: MIBs may be loaded onto <u>any</u> Solstice SEM or Solstice SNM version
Type of integration: