

# Lucent Security Management Server Security, VPN, and QoS Management Solution



Lucent Security Management Server (SMS) software brings you advanced carrier-grade IP services management at a low total ownership cost. Teaming with Lucent's award-winning VPN Firewall Brick® portfolio, Lucent Security Management Server lets you rapidly provision and manage high-return services for thousands of users in a single console. It integrates firewall, VPN, QoS, VLAN and virtual firewall policy management; provides industry-leading scalability and availability; delivers robust monitoring, logs and reports; and gives you flexible deployment options — all without the costly additional modules or recurring license fees that competitive products require.

## Applications

- Advanced security services
- VPN services for site-to-site and remote access
- Bandwidth management capabilities
- VoIP Security
- Secure data center Web and application hosting
- Storage network security solution
- Mobile data security
- Packet Data Gateway and Packet Data Interworking Functions for Dual-Mode Wireless/Wifi VPN and VoIP/Data Security
- Managed Security Services
- Unlicensed Mobile Access (UMA) and IP Multimedia Subsystem (IMS) Security

## Features

- Fully integrates firewall, VPN, QoS, VLAN, and virtual firewall management
- Comprehensive remote management capabilities with role-based administration
- Flexible management model: controls policies at global, customer, device, interface, VLAN and IP address range levels
- High scalability: supports 20,000 Lucent VPN Firewall Brick units and up to 500,000 simultaneously connected VPN users from one Lucent Security Management Server console.
- Carrier-class reliability: distributable across up to four network operations centers (NOCs) for active/active network redundancy with no single point of failure
- Real time monitoring, robust logging, and customized reporting
- Multiple IP services deployment options: premises-based, network-based, tiered, and data-center architectures

## Benefits

- **One management solution** — single platform provides centralized, comprehensive management of all IP services
- **Low operating costs** — secure remote management reduces need for network reconfigurations, truck-rolls, on-site support; VLAN, virtual firewall, and QoS support included at no extra charge; management efficiencies cut staffing and administrative expenses
- **Simple, economical licensing model** — no ongoing license fees or add-ons required for complete security management
- **Cost-saving growth** — easily migrate from basic to advanced security, VPN, and QoS services
- **Assured business continuity** — native high availability, carrier-class reliability, no advisories or reported vulnerabilities
- **Proven carrier-class performance** — mature product with over 7 years service in the world's largest networks



# Lucent Security Management Server Technical Specifications

## 1. Mode of Operation

Centralizes firewall, virtual firewall, VLAN, VPN and QoS policy management  
Proactively monitors all VPN Firewall Brick® platforms and IPSec Client users  
Provides real-time monitoring, log collection, reporting and alarm generation  
Supports network-based and premises-based deployments

## 2. Performance and Capacity

Supports 1,000 customer groups each with hundreds of unique policies  
Centrally collects up to 15, 000 log records per Lucent Security Management Software or Compute Server for a maximum of 300,000 log records per second.  
Central management of up to 20,000 VPN Firewall Brick® units and 500,000 simultaneously connected VPN users

## 3. Policy Management

Uses a group-based model to manage a collection of devices, security policies, VPN tunnels, and user authentication components as a single entity  
Controls policies at the global, customer, device, interface, VLAN and IP address range level  
Includes preconfigured typical security and VPN policy templates that can be tailored to suit unique requirements  
Uses user-definable Host Groups, Service Groups, Application Filters and User Groups  
Supports global and nested policy objects

## 4. Role-based Administration

Uses two administrative classes:  
Lucent Security Management Server Administrators – full privileges over all groups, devices, policies and users  
Group Administrators – restricted privileges and access only to assigned group(s)  
Supports shared administration with customers  
Local and remote administration via Lucent Security Management Server Remote Navigator utility (included); provides secure access to all Lucent Security Management Server utilities  
Allows concurrent administrators to exchange messages via a real-time messenger service

## 5. Secure 3-Tier Architecture

Lucent Security Management Server to VPN Firewall Brick® platform communications secured with Diffie-Helman and 3DES encryption, SHA-1 authentication and integrity, and digital certificates for VPN Firewall Brick® platform to Lucent Security Management Server authentication  
Lucent Security Management Server Remote Navigator to Lucent Security Management Server communications secured with 3DES encryption and SHA-1 authentication and integrity, and either local password or external database authentication with SecurID or RADIUS servers  
Transfers logs in real-time over reliable and secured connections

## 6. Authentication

Built-in internal database – 10,000 users  
Browser-based authentication allows authentication of any user protocol  
Local passwords, RADIUS, SecurID, X.509 digital certificates  
PKI Certificate requests (PKCS 12)  
User assignable RADIUS attributes  
DoD PKI

## 7. Remote Access VPN Tunnel Management

Supports IKEv1 and IKEv2 remote access VPN, including Lucent IPSec Client software distribution and updates  
Centralizes management of all IPSec Client configurations, including personal firewall settings  
Allows any combination of authentication methods; configurable per user, user group or application  
Supports virtual addresses for tunnel end points  
Allows administrator to terminate specific tunnels when necessary, or terminate all tunnels in a single action

## 8. Site-to-Site VPN Tunnel Management

Provides SLA probes for real-time round trip delay statistics and tunnel status indicators to verify tunnel availability in real-time; configurable with alarm notifications  
Supports virtual addresses for tunnel end points  
Configurable tunnel default settings  
Includes preconfigured VPN policy templates fully integrated with firewall policy  
Supports IKEv1 and IKEv2 site-to-site tunnels

## 9. High Availability/Redundancy

Supports active/active management with up to four geographically distributed servers and real-time database replication  
Internal database automatically backs up to a local and remote disk daily; additional backups can be scheduled at any time  
Backup file contains ALL policy, configuration, and security information for ALL configured devices and policies

## 10. Central Staging with Secure Upgrades

Securely pushes the VPN Firewall Brick® operating system to each device with no truck-rolls or on-site hardware support; maintains ALL sessions during an OS upgrade with a failover pair of VPN Firewall Brick® units

## 11. Application Programming Interfaces (APIs)

Scriptable command line interface  
Parseable ASCII log files (for per-customer reporting)  
Supports SNMP GET v2c (read-only) and SNMP traps v1 and v2c  
TL1 Alarm Interface

## 12. Audit Log Management

VPN Log

Four categories of audit logs created daily:

Firewall Session Logs

Administrative Event Logs

User Authentication Logs

Proactive Monitoring Statistic Logs

Real time logs viewable with Log Viewer; historical logs viewable with Log Viewer or Reporting System (see below).

Log viewing and manipulation follows administrative permissions model

Configurable log file disk management

Automated log scheduling and forwarding for post-processing

## 13. Real-time Log Viewer

Displays log records as received from all VPN Firewall Brick® platforms; messages can be filtered, sorted and highlighted

Includes historical record search capabilities with specified time parameters

## 14. Reporting System

Automatically merges data from geographically distributed log servers

Generates HTML-based reports with full filtering, sorting and scheduling capabilities; configurable per administrator

Reports include sessions over time, policy snapshots, administrator events and configuration changes

Includes preconfigured reports for fast initial deployment

## 15. Customer Specific Report Generation and Delivery

Integrates with the WebTrends Firewall Reporting Suite; uses the WebTrends Enhanced Log Format (WELF)

Fully automates generation and delivery of customer-specific, traffic statistic graphic reports to customers via FTP, e-mail or http server

## 16. Policy Change Control

Records all administrative activity to audit logs

Captures all policy and configuration changes in detailed, user-configurable history files that are secured from tampering/modification and support policy roll-back

## 17. Alarms

Generates alarms based on VPN Firewall Brick® log messages and locally generated log messages from LSMS subsystems; configurable per-administrator

Includes preconfigured alarms for fast initial deployment

Configurable alarm triggers include:

Lucent Security Management Server Error

VPN Firewall Brick® Error

VPN Firewall Brick® Lost/Found

VPN Firewall Brick® Interface Up/Down

Proactive Monitoring Threshold Crossing

VPN Firewall Brick® Redundancy Alarms

Lucent Security Management Server Redundancy Alarms

## 17. Alarms (continued)

Configurable notification methods:

Console Alarm (via the Lucent Security Management Server Remote Navigator)

Email

Out-of-band modem-dialed alphanumeric message sent to pager (via the TAP protocol)

SNMP Trap

SYSLOG Message (with configurable SYSLOG level)

Alarm triggers can be mapped to any combination of notification methods

## 18. Real-Time Status Monitors

Support real-time and historical dynamically-updating text and graphical monitoring

VPN Firewall Brick® monitor – provides windows for each device and aggregate collection of devices; monitors statistics for each physical port, packet, byte, and session; includes Quality-of-Service graphs to monitor throughput and performance relative to configured guarantees and limits

VPN Tunnel monitor – provides status of each VPN tunnel; monitors Service-Level Agreements (SLAs) for VPN tunnel round-trip delay

Administrator and Lucent Security Management Server monitor – views all logged-in administrators and connection statistics; reports connection status of each Lucent Security Management Server in real-time

## 19. Command Line Interface

Allows administrators to script the configuration of many Lucent Security Management Server components and policy objects using a text file-based interface

## 20. SNMP Agent

Accesses limited configuration and statistic information regarding the system and associated VPN Firewall Brick® platforms in a Read-Only fashion via the Lucent Security Management Server. Absolutely NO information may be configured via SNMP. VPN Firewall Brick® platforms do NOT respond to SNMP or any variation thereof. Available in SNMP v2c format.

## 21. VPN Firewall Brick® Remote Console

Provides a secure remote console to any VPN Firewall Brick® model and executes debugging/troubleshooting commands

No policy modifications can be made from this Remote Console or any VPN Firewall Brick® console interface

## 22. Rules Based Routing

Provides capability to configure a rule for HTTP, FTP, or SMTP protocol traffic. Routes all packets matching the rule to a proxy server, router or other device utilizing third party software to perform content filtering functions such as command blocking, URL filtering, and virus scanning. Allows transparent interaction with any third party equipment.

# Lucent Security Management Software Hardware and Software Requirements

## 1. Software Requirements

Sun Solaris™ 2.8, 2.9 or 2.10 on SPARC processors  
Microsoft Windows® 2000 Professional, WindowsR 2000 Server, Windows XP Professional or Windows Server 2003.

## 2. Hardware Requirements

### Sun® workstation for Sun Solaris operating system:

Sun UltraSPARC5 (330MHz processor or better) or better  
512MB of system memory (minimum)  
Swap space at least as large as system memory  
500MB free disk space in file system partition where software is to be installed  
50MB free disk space in root partition  
1 10/100 Ethernet interface  
CD-ROM drive  
3.5" floppy drive, USB port and serial port.  
Video card capable of supporting 1024x768 resolution (65,535 colors)

### Intel®-based workstation (for Microsoft Windows® operating systems noted above)

400 MHz Pentium® Pro processor (minimum)  
512 MB system memory (minimum), higher recommended  
CD-ROM drive  
Swap space at least as large as install system memory  
1 GB free space on an NTFS partition  
3.5" floppy, USB port and serial port.  
1 Ethernet 10/100 card  
Video card capable of supporting 1024x768 resolution (65,535 colors)

## Ordering Information

Lucent SMS 9.1 Package (includes license to manage up to 5 VPN Firewall Brick® products, and 100 simultaneous IPSec Client tunnels)	Part Number 300903176
Lucent SMS 9.1 Redundancy Package (for High Availability applications)	Part Number 300903184
Lucent SMS 9.1 Compute Server Base Package	Part Number 300903192
Additional 5 VPN Firewall Brick® management licenses	Part Number 300903234
Additional 25 VPN Firewall Brick® management licenses	Part Number 300903242
Additional 50 VPN Firewall Brick® management licenses	Part Number 300903259
Additional 100 VPN Firewall Brick® management licenses	Part Number 300903267
Additional 250 VPN Firewall Brick® management licenses	Part Number 300903275
Additional 500 VPN Firewall Brick® management licenses	Part Number 300903283
Upgrade Lucent SMS 9.0 to Lucent SMS 9.1	Part Number 300903200
Lucent IPSec Client	See Lucent IPSec Client data sheet for ordering details

To learn more, please contact your Lucent Technologies Sales Representative or Lucent Sales Business Partner. Or visit our web site at [www.lucent.com](http://www.lucent.com).

This document is provided for planning purposes only and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to the products or services described herein.

Specifications are subject to change without notice.

Windows is a registered trademark of Microsoft Corporation.

WebTrends is a registered trademark of WebTrends, Inc.

VPN Firewall Brick is a registered trademark of Lucent Technologies Inc.

Copyright © 2006  
Lucent Technologies Inc.  
All rights reserved

Lucent SMS v2 08/06

