



PRODUCT BRIEF

SafeNet Security Management Center (SMC) Enterprise Network Security Management Platform

SafeNet Security Management Center (SMC) from Gemalto redefines enterprise network security management with a robust, Web-based management platform that authenticates any number of SafeNet high speed encryptors deployed on the network.

SMC remotely configures, monitors, and performs firmware updates for SafeNet network security products —automatically managing any product that has been integrated into the extensible management center architecture.

Lowest Cost of Ownership

By providing a single management element to administer security across heterogeneous networks, SMC reduces the cost of network security management. Because SMC is easy to install and requires simple ongoing management, administrators spend less time on deployment and troubleshooting, which reduces administrative costs. With SMC's point-and-click interface and configuration wizards, it's easy to visualize, configure, modify, and manage network security.

Benefits

Ease of Installation and Deployment

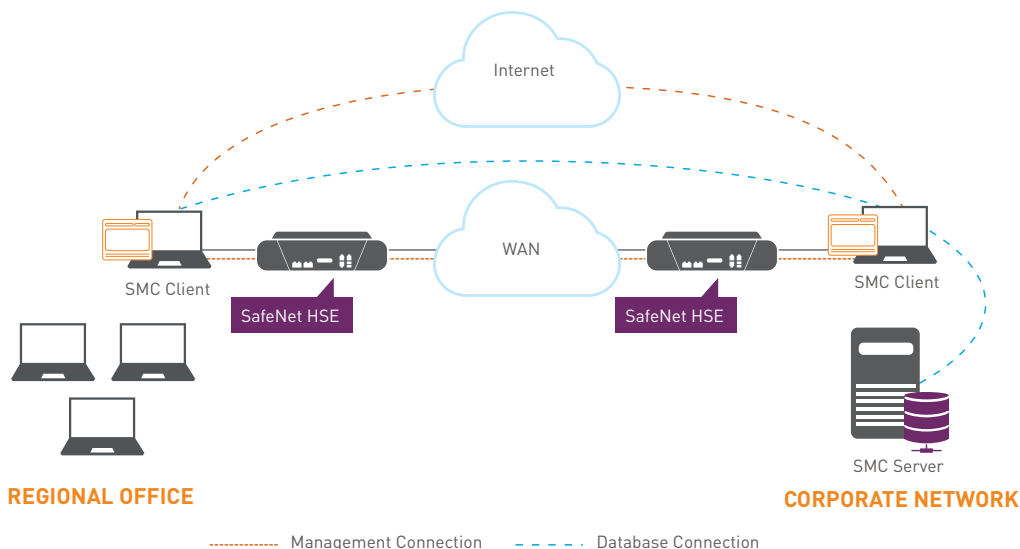
- > 5-minute installation and deployment
- > Zero-footprint, Web-based client. No client installation means no client deployment overhead, no client administration, and no platform dependency
- > Deployment and management of device PKI. No external PKI required

Reduces Management Complexity

- > Comprehensive user management, including configurable role-based access control, user account management, and granular audit logging of all user actions.
- > Batch firmware download - upgrade your entire network in a single operation
- > SNMP Proxy Agent provides northbound SNMP interface to your OSS/NMS

Pervasive System Security

- > SSL, PKI, password enforcement



Secure Operations

SafeNet network security products enable organizations to implement a broad range of security policies that can limit access to specific devices or provide unlimited access to the entire network. The management communication between SMC and the encryptors is through highly secure channel communications, eliminating the possibility of spoofing or eavesdropping.

The internal high-performance relational database provides high availability, and the client-server design allows flexible management for remote administration.

SMC provides full audit trail and event logging of network security activities, including administrator operations and user log-ons and log-offs. This granularity ensures that regulatory compliance requirements are easily met.

Scalability

SMC's simple design allows for the management of thousands of encryptors and can scale to networks of any size. The SNMP architecture provides interoperability with enterprise network management software suites for additional device and network monitoring options. Additionally, SMC has rapid deployment tools that help eliminate the burden of sizeable installations in large organizations.

Technical Specifications

Supported Devices and Clients

- > Ethernet Encryptors
- > SONET Encryptors
- > Conversion Encryptors

Management Protocols

- > SNMP v1, v2, & v3
- > SNMP MIB-II, plus secured

SMC Client Requirements

Supported Browsers

- > Firefox 4 and above
- > Internet Explorer 8 and above

SMC Server System Requirements

- > Microsoft Windows 8, 2012 R2, 7, 2008 R2, Vista
- > Linux Red Hat Enterprise Linux 6.5, 6.6 or CentOS 6.5, 6.6 (64-bit only)
- > Solaris 10, Update 5 and above (64-bit only)
- > Sun SPARC Enterprise Server for Solaris OS
- > Intel Pentium 4 processor (minimum) for Windows OS
- > RAM - 2 GB (minimum) / 4 GB or more recommended
- > Hard Drive - 60 GB (minimum) / 160 GB or more recommended
- > Network interface card

Name	Type	State	Next Execution	Last Exec
Synchronize Alarms	Synchronize Alarms	Normal	10:01 AM	9:48 AM (2 minutes ago) - LOGS
Script Run	Script Run	Normal		Not fired yet - LOGS
SSP/SEE Configuration Backup	SSP/SEE Configuration Backup	Normal		
SSP/SEE Log Backup	SSP/SEE Log Backup	Normal		
Repair Database Tables	Repair Database Tables	Normal	Fri 9:20 AM	
1 download: [CSID: 4510.24.0.020109.14.03.20.03.55.32.tar.gz] to [SEE_BO]	Firmware Download	Completed		Completed - LOGS

Sev	Cr	Adi	Name	Description	Source	Notes	Updated
			NETWORK_LINK	Network port link down indication	SEE-138	None	9:33 AM (10 minutes ago) - Escalate
			LOCAL_LINK	Local port link down indication	SEE-138	None	9:33 AM (10 minutes ago) - Escalate
			LINK	Encryptor link(s) down (speed mismatch or link down)	SEE-138	None	9:33 AM (10 minutes ago) - Escalate
			Communications Down	Last communication attempt failed: Device returned an SNMP error response: status=129, indeterminate	0n4010-desk	None	9:30 AM (13 minutes ago) - Escalate
			Communications Down	Last communication attempt failed: Device returned an SNMP error response: status=129, indeterminate	0n4010-desk	None	Fab 7 4:20 PM (5 days ago) - Escalate
			Connectivity Failed	Server does not have connectivity to 172.16.13.192	0n4010-desk	None	Fab 7 3:13 PM (5 days ago) - Escalate

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: [data-protection.safenet-inc.com](https://www.facebook.com/safenet)

 GEMALTO.COM


security to be free