



# Forcepoint™ Stonesoft® Management Center

**EFFICIENT, CENTRALIZED MANAGEMENT OF FORCEPOINT STONESOFT  
NEXT GENERATION FIREWALLS IN DISTRIBUTED ENTERPRISE ENVIRONMENTS**

Forcepoint Stonesoft Management Center (SMC) provides unified, centralized management of Stonesoft Next Generation Firewalls, in all operational modes across large geographically distributed enterprise environments.

Superior flexibility, scalability, and ease-of-use support dynamic network security environments and aggressive business growth plans. Optimized workflows streamline daily administrative tasks and security management for high efficiency and low TCO.

The SMC also supports third-party devices, gathering event management and status monitoring information for generating detailed reports. This open approach provides administrators with a comprehensive view of their environment.

SMC consists of two components — Stonesoft Management Server and Stonesoft Log Server which can reside on the same or separate servers.

## **HIGH AVAILABILITY**

Today's businesses have zero tolerance for disruption, demanding 24/7/365 access to critical resources. Forcepoint SMC High Availability features enable reliable deployment of extremely resilient management infrastructure with continuous access to log resources.

## **SECURITY MANAGEMENT CLIENT**

Regardless of geographic location, administrators can securely access the SMC with the Management Client. The client provides a simple graphical user interface for configuration, monitoring, logging/alerts, reports, updates, and upgrades to Stonesoft Next Generation Firewalls. The Stonesoft Management Center Client provides administrators with a holistic view of the network and drill-down actions for effective management of your entire security environment.

## **KEY BENEFITS**

- Centralized, single-pane-of-glass management of Stonesoft Next Generation Firewalls in distributed environments.
- Flexibility and scalability for deployment in large distributed enterprise environments.
- High availability supports demanding uptime requirements.
- Efficient workflow automation provides fast and accurate deployment and maintenance of Stonesoft Next Generation Firewalls.
- Provides situational awareness and visibility across your entire network, including branch and remote sites.

**STONESOFT MANAGEMENT CENTER SPECIFICATIONS**

<b>MANAGEMENT SERVER</b>	
<b>Number of Managed Devices</b>	License limited: 2 to 2,000 nodes with one Management Server
<b>Number of Administrators</b>	Unlimited
<b>Number of Elements</b>	Unlimited
<b>Number of Policies</b>	Unlimited
<b>Number of Log Servers</b>	Unlimited
<b>Number of Web Portal Servers</b>	Unlimited
<b>Administrator Authentication</b>	Local database, RADIUS, TACACS+
<b>Device Connections</b>	SSL-encrypted
<b>LOG SERVER</b>	
<b>Number of Supported Devices</b>	Unlimited
<b>Log Records per Second</b>	The high-performance logging system can process more than 500,000 records per second
<b>Device Connections</b>	SSL-encrypted, IPv4/IPv6
<b>Log Storage Size</b>	Unlimited
<b>Number of Log Forwardings per Log Server</b>	Unlimited
<b>FEATURES</b>	
<b>GENERAL</b>	
<b>Management Client</b>	Java-based for Windows and Linux and Java Web Start for Mac.
<b>SMC Application Programming Interface (SMC API)</b>	<ul style="list-style-type: none"> <li>• Documented API enabling easy third-party product and service integration</li> <li>• Uses REST architecture where data can be XML or JSON coded</li> </ul>
<b>Simultaneous Administrators</b>	<ul style="list-style-type: none"> <li>• Several administrators can perform changes at the same time</li> <li>• Critical elements like policies are locked for editing</li> </ul>
<b>High Availability</b>	Supports up to four standby Management Servers
<b>Upgrades</b>	Upgrades and dynamic update packages can be automatically downloaded
<b>Backups</b>	Integrated backup tool for taking backups from the whole system, including all next generation firewall configurations
<b>Navigation</b>	Intuitive browser-like navigation with browsing history, tabs, and bookmarks
<b>Search Tools</b>	Efficient element and references search tools
<b>Quick Filtering</b>	Convenient type-ahead filtering in element lists, tables, and policy cells
<b>Multi-Selection Support</b>	Perform actions and commit changes to hundreds of elements at the same time
<b>System Clean-Up Tools</b>	Enables administrator to easily find which elements and rules are not used
<b>ADMINISTRATION</b>	
<b>Alert Escalations</b>	Allows administrator to forward alerts from the system using email, SMS, SNMP trap, and custom scripts
<b>Alert Thresholds</b>	Automatic alert thresholds for overview statistics
<b>Audit Logs</b>	Extensive audit information about all changes in the system
<b>System Reports</b>	Inventory and audit reports about administrators' activities
<b>Plug-and-Play Installation</b>	Cloud (or USB stick)-based installation with initial policy push
<b>Automated Tasks</b>	Refresh policies; archive, export, and delete logs; make backups with automated tasks
<b>Administrative Domains</b>	Allows division of the environment into isolated configuration domains
<b>Import/Export</b>	XML and CSV export and import with intelligent conflict handling between SMC installations



## STONESOFT MANAGEMENT CENTER SPECIFICATIONS CONTINUED

<b>Remote Upgrades</b>	One-click fail-safe remote upgrade
<b>Administrator Role-Based Access Control</b>	Custom roles can be defined and combined in addition to predefined roles like Owner, Viewer, Operator, Editor and Superuser, to control permissions flexibly and accurately.
<b>License Management</b>	Automatic online license updates and maintenance contract status reports
<b>Troubleshooting Tools</b>	Extensive remote diagnostic capabilities: integrated traffic capture tool, diagnostics, configuration snapshot download from next-generation firewall, and session monitoring views
<b>POLICY MANAGEMENT</b>	
<b>Virtual Contexts</b>	Share same master context across several SMC Administrative Domains — up to 250 virtual contexts, and each has its own policies and routing tables
<b>Hierarchical Policy Management</b>	Policy templates, sub-policies, aliases, and rule comment sections keep the policy organized and understandable
<b>Application Identification</b>	Restrict access based on network and/or client applications: <ul style="list-style-type: none"> <li>• Identify applications by payload, and restrict access accordingly</li> <li>• Use client application information from McAfee Endpoint Intelligence Agent</li> </ul>
<b>URL Filtering</b>	Restrict access by URL categories
<b>Domain Names</b>	Restrict access dynamically by using domain names
<b>User Identification</b>	Create user-based rules either with or without authentication
<b>Zones</b>	Physical interfaces can be tagged with zones and referred to in the policies
<b>Geoprotection</b>	Restrict access by countries or geographical regions.
<b>Inspection Policies</b>	Granular control for deep packet inspection and easy ways to toggle off false positives
<b>Quality of Service (QoS) Policies</b>	QoS class-based policy configuration
<b>Policy-Based File Filtering</b>	Define how files are inspected using McAfee Global Threat Intelligence file reputation, Anti-Malware Scan, and McAfee Advanced Threat Defense
<b>Network Address Translation (NAT)</b>	• Default NAT • Element-based NAT • NAT policies
<b>Policy Validation Tool</b>	Helps administrator find configuration mistakes before policy activation
<b>Policy Snapshots</b>	Allows for exploration and comparison of Stonesoft Next Generation Firewall configuration history
<b>Policy Restoration</b>	A previous policy version can be recovered and uploaded to the next-generation firewall
<b>Rule Usage Optimization Tool</b>	Enables administrators to see how many times each rule has matched within a specified time period
<b>Rule Search Tool</b>	Integrated tool for searching rules in policies
<b>Rule Names</b>	Ability to create rule names that are visible in logs, statistics, and reports
<b>Fail-Safe Policy Uploads</b>	System automatically restores the previous policy version if the new version fails
<b>CONFIGURATION</b>	
<b>Routing</b>	Drag-and-drop routing configuration for the firewalls and specific widgets to add routes and default routes
<b>Dynamic Routing</b>	Advanced OSPF and BGP configuration via intuitive graphical user interface
<b>Automatic Anti-spoofing</b>	Anti-spoofing configuration is created automatically based on routing
<b>Site-to-site VPNs</b>	- Policy-based IPsec VPN - Route-based IPsec VPN and tunneling (GRE)
<b>Remote access VPNs</b>	- IPsec VPN client (Windows) - SSL VPN client (Android, iOS, Mac and Windows) - Clientless SSL VPN Portal
<b>Incident Case Management</b>	Integrated tools for collaborative network incident management
<b>Firewall Element Creation Wizard</b>	Create hundreds of firewall elements through a firewall creation wizard



## STONESOFT MANAGEMENT CENTER SPECIFICATIONS CONTINUED

STATUS, STATISTICS, AND REPORTING	
<b>System Status Monitoring</b>	Real-time status information about network devices and their connections
<b>Appliance Status Monitoring</b>	Graphical view on the hardware status of the appliances
<b>Networks Diagrams</b>	Visualize configurations, topologies, and status connectivity with drawings
<b>Session Monitoring</b>	Dedicated views to monitor connections, VPN security associations (SAs), authenticated users, active alerts, and dynamic and static routes
<b>Overviews</b>	Customize dashboards of network statistics for real-time monitoring
<b>Geolocations</b>	<ul style="list-style-type: none"> <li>• Show the country information for all IP addresses with the help of country flags and geolocation statistics.</li> <li>• Show where network attacks come from</li> </ul>
<b>Reporting</b>	Customize and schedule reports that provide detailed information about network statistics
<b>Web Portal</b>	Lightweight web access to policies, logs, and reports
THIRD-PARTY MANAGEMENT	
<b>Third-Party Device Monitoring</b>	Allows administrator to monitor and view status changes in third-party device availability
<b>Third-Party Device Log Reception</b>	Log parsing and reception in syslog format for third-party devices and out-of-the box support for CEF, LEEF, CLF, and WELF format
<b>NetFlow/IPFIX Reception</b>	Ability to receive and consolidate data in NetFlow v9 and IPFIX formats
<b>Third-Party Device Statistics</b>	Graphical statistics and reports based on third-party log data and simple network management protocol (SNMP) counters
<b>Number of Supported Third-Party Devices</b>	200 per Log Server
<b>Licensing</b>	Each third-party device consumes 0.2 from Management Server license device count
LOGS	
<b>Log Browser</b>	Common log browsing view for all log data
<b>Drag-and-Drop Filtering</b>	Efficient log filtering—drag and drop any log data cell to the Query Panel
<b>Log Statistics</b>	Create log statistics on the fly and see the top trends
<b>Log Visualizations</b>	Find the anomalies in logged traffic in filterable log visualizations
<b>Log Aggregations</b>	Summarize the large amount of filtered log data by any columns
<b>Archiving</b>	Archive logs in multiple directories by using filtering
<b>Backups</b>	Integrated backup mechanism for Log Server configuration and log data
<b>Log Exports</b>	CSV, XML, CEF, LEEF, and McAfee Enterprise Security Manager log exporting; logs can also be exported to PDF and ZIP files directly from the log browser
<b>Log Forwarding</b>	Real-time log redirection in syslog; CEF, LEEF, XML, CSV, IPFIX, NetFlow, and McAfee Enterprise Security Manager formats; configuration for filtering, data type; and log field selection available
<b>Log Data Contexts</b>	Shortcuts to browse different types of logs with dedicated column sets
<b>High Availability</b>	Support for backup Log Server



### STONESOFT ADMINISTRATIVE DOMAIN LICENSE PROVIDES CENTRALIZED MANAGEMENT OF MULTIPLE CUSTOMER ENVIRONMENTS

Managed Security Service Providers (MSSPs) need to reduce the high administrative costs associated with managing multiple servers across multiple domains. Stonesoft Administrative Domain License enables management of multiple customer environments through a single Management Server. Configurations can be reused and shared across domains for rapid and efficient distribution of changes. The

unique architecture of the Administrative Domain License solution simplifies enterprise and MSSP environments, making them easier to maintain. Role-based access management (RBAC) ensures accurate definition of administrator responsibilities and domain access limitations. Domain-based customers can access reports, policy configurations, and logs easily via a secure, lightweight web portal.

### STONESOFT ADMINISTRATIVE DOMAIN LICENSE SPECIFICATIONS

DOMAINS	
Maximum Number of Domains	200
Number of Administrators	Unlimited
Number of Managed Devices per Domain	Unlimited
Number of Elements per Domain	Unlimited
FEATURES	
Configuration Separation	Isolate customer environments to different domains, and make sure that customers' network elements never get mixed up
Configuration Sharing	Share elements such as policy templates for all domains
Access Control	Configure the administrators' visibility and responsibilities with the help of domains
Monitoring	Monitor the status of all granted domains with the help of the domain overview
Customization	Customize the PDF style templates
Migration Tools	Move elements between domains with the integrated "move-to" tool
Import/Export	Import and export elements between different SMC installations and domains
Virtual Contexts	Share the same master context across domain boundaries of up to 250 virtual contexts, which can each have their own policies and routing tables



### STONESOFT WEB PORTAL SERVER

Stonesoft Web Portal Server provides customers, administrators, and management with a lightweight web-based portal for viewing logs, scheduled reports, current policies, and policy change history. MSSP administrators can configure the amount of information displayed on the portal based on customer needs or to reduce support requests.

Stonesoft Web Portal Server supports English, Spanish, and French natively, with the ability to add new languages.

### KEY BENEFITS

- Clientless, read-only access to logs, reports, policies, and policy change history.
- Real-time network status available for defined users.
- Support for mobile devices.

### STONESOFT WEB PORTAL SERVER SPECIFICATIONS

SPECIFICATIONS	
Maximum Number of Concurrent Users	Unlimited
Number of Administrators	Unlimited
Number of Web Portal Users	License Unlimited
User Authentication	Management Server database, RADIUS, TACACS+
Device Connections	SSL-encrypted
FEATURES	
Security Policies	View next-generation firewalls' latest configurations in HTML format
Reports	View reports that are scheduled to be published in the web portal in HTML format
Log Browsing	Browse and filter the logs in HTML format
Log Details	View log event visualizations and other log details in a separate HTML page
PDF Export	Print reports and logs to PDF documents
Announcements	Administrators can specify announcements to be shown in the web portal
Policy Comparison	Compare the different next-generation firewall configuration versions to see if the change request has been implemented
Localization	Web portal supports English, Spanish and French, and can be easily translated to support other languages.
Customization	Customize the look-and-feel of web portals

### CONTACT

[www.forcepoint.com/contact](http://www.forcepoint.com/contact)

### ABOUT FORCEPOINT

Forcepoint™ is a trademark of Forcepoint LLC. SureView®, ThreatSeeker®, TRITON®, Sidewinder®, and Stonesoft® are registered trademarks of Forcepoint LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks and registered trademarks are property of their respective owners.

[DATASHEET\_SECURITY\_MANAGEMENT\_CENTER\_EN] 100030.121916