

Forcepoint Security Management Center

Single-pane administration for maximum visibility across the network

Key Benefits

- › Centralized, single-pane management of thousands of physical or virtual engines across distributed environments
- › Flexibility and scalability for deployment in large enterprise networks
- › High availability option for demanding uptime requirements
- › Smart policies and efficient workflow automation for fast and accurate deployment and maintenance of Forcepoint engines
- › Works with Security Service Edge (SSE) platforms to secure access to web, cloud, and private applications in SASE architectures.
- › User and endpoint context, awareness and visibility across your entire network, from the data center and edge to branch sites and the cloud
- › Choice of software deployment options or appliance
- › The entire SMC functionality is available through SMC API

Forcepoint Security Management Center (SMC) provides unified, centralized management of all models of Forcepoint engines whether physical, virtual or cloud—across large, geographically distributed enterprise environments.

With superior flexibility, scalability and ease-of-use, Forcepoint SMC makes dynamic network security environments more manageable and able to support aggressive business growth plans. Smart policies enable business processes to be expressed in natural terms, while its optimized workflows streamline daily administrative tasks for high efficiency and low total cost of ownership (TCO).

SMC provides 360-degree visibility throughout enterprise networks by gathering event management and status monitoring information from Forcepoint engines and endpoints, enabling interactive investigation as well as generating detailed reports. In addition, Forcepoint SMC can aggregate engine log data from multiple, geographically distributed Forcepoint engine Log Servers for consolidated reporting while maintaining data sovereignty.

High availability

Today's businesses have zero tolerance for disruption, demanding around-the-clock access to critical resources. With Forcepoint's SMC's high availability option, organizations maintain continuous access to log resources for resilient incident analysis and response.

Interactive security management client

Regardless of geographic location, administrators can securely access the Forcepoint SMC through a web browser or the SMC Management Client. This provides a powerful graphical user interface for configuration, monitoring, logging, alerts, reports, updates and upgrades to Forcepoint engines. Forcepoint SMC gives administrators a holistic view of the network and context-driven drill-down actions for fast, effective management of your entire security environment.

Forcepoint SMC Specifications

MANAGEMENT SERVER	
Number of Managed Engines	Licensed: 1 to 3,000 nodes with one Management Server
Number of Administrators	Unlimited
Number of Elements	Unlimited
Number of Policies	Unlimited
Number of Log Servers	Unlimited
Number of Web Portal Servers	Unlimited
Administrator Authentication	Local Database, RADIUS, TACACS+, Client Certificate, Microsoft Active Directory (LDAP), SAML and OpenID
Engine Connections	TLS 1.2 Encrypted and authenticated using X.509v3 Keys and Certificates
LOG SERVER	
Number of Supported Engines	The number of supported engines isn't strictly limited but depends on the size of the hardware
Log Records per Second	The high-performance logging system can receive up to 500,000 records per second
Engine Connections	TLS 1.2 Encrypted and authenticated using X.509v3 Keys and Certificates
Log Storage Size	There's no hard limit, but it depends on the size of the hardware
Native Integration with Third Party Indexing Tools (ElasticSearch and OpenSearch).	Unlimited
GENERAL	
Management interface	Management client or web-based console
SMC Application Programming	Documented API enabling easy third-party product and service integration.
Simultaneous Administrators	Administrators can make changes simultaneously, even when critical elements like policies are locked for editing
Home Screen Dashboards	Customizable home screen dashboards for engines, Multi-Link™ VPNs, network applications and servers
User Monitoring	In addition to the user behavior-related correlations and checks, it provides endpoint security status information and endpoint application statistics
User Monitoring	In addition to the user behavior-related correlations and checks, it provides endpoint security status information and endpoint application statistics
High Availability	Up to four standby management servers
Upgrades	Upgrades and dynamic update packages for managed devices can be automatically downloaded
Backups	Integrated backup tool for taking backups from the whole system, including all managed engines configurations
Navigation	Intuitive browser-like navigation with browsing history, tabs and bookmarks
Search Tools	Efficient element and references search tools with context-sensitive quick actions
Quick Filtering	Convenient type-ahead filtering in element lists, tables and policy cells
Multi-Selection Support	Perform actions and commit changes to hundreds of elements simultaneously
System Clean-Up Tools	Enables administrator to easily find which elements and rules are not used
Application Health Monitoring	Monitor and visually present metrics about the quality of application connections

ADMINISTRATION	
Alert Escalations	Allows administrator to forward alerts from the system using email, SNMP trap and custom scripts
Alert Thresholds	Easy alert thresholds for overview statistics
Audit Logs	All changes to the system are recorded in audit logs
System Reports	Inventory and compliance audit reports about administrators' accounts and activities
Zero Touch Provisioning of Engines	Plug-and-play installation, either via Cloud or USB stick, with initial policy push
Automated Tasks	Automated log data management, archive and retention, backups, upgrades and policy refresh tasks
Administrative Domains	Allows division of the environment into isolated configuration domains
Import/Export	XML and CSV export and import all times, rather than just between installations
Remote Upgrades	One-click fail-safe remote upgrade of the managed engines
Administrator Role-Based Access Control	Custom roles can be defined and combined in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Superuser) to control permissions flexibly and accurately
License Management	Automatic online license updates and maintenance contract status reports
Certificates Management	Consolidated view of all certificates and credentials
Troubleshooting Tools	Extensive remote diagnostic capabilities: integrated traffic capture tool, configuration snapshot download from next generation firewall and session monitoring views

POLICY MANAGEMENT	
Virtual Engine	Share same master context across several SMC Administrative Domains; up to 250 virtual contexts, each with its own policies and routing tables
Hierarchical Policy Management	Policy templates, sub-policies, aliases and rule comment sections keep the policy organized and understandable
Application Identification	<ul style="list-style-type: none"> → Restrict access based on network and/or endpoint applications → Restrict access from/to applications by payload → Allow list/block list by application name and version from Forcepoint Endpoint Context Agent
Change Management	Require review and approval by a second administrator before changes are deployed
URL Filtering	Restrict access by URL categories; supports QUIC and HTTP/3
Domain Names	Restrict access dynamically by using domain names that can be translated to IP-addresses
User Identification	Match user-based rules via transparent user identification or enforcing strong authentication methods
Zones	Physical interfaces can be tagged with zones and referred to in the policies
Geographical Access Control	Restrict access by countries or geographical regions
Inspection Policies	Granular control for deep packet inspection and easy ways to toggle off false positives
Quality of Service (QoS) Policies	QoS class-based policy configuration
Policy-Based File Filtering	Define how files are inspected using file reputation service, Anti-Malware scan and sandboxing.
Network Address Translation (NAT)	<ul style="list-style-type: none"> → Default NAT → Element-based NAT → NAT policies
Policy Validation Tool	Helps administrator find configuration mistakes before policy activation
Local Alternative Policy	Enables switching engine policy without requiring a management connection in emergency situations
Policy Restoration	A previous policy version can be recovered and uploaded to the next generation firewall
Policy Optimization Tool	Multiple admins can edit simultaneously, but critical elements like policies are protected to prevent conflicts
Rule Search Tool	Integrated tool for searching rules in policies
Rule Names	Ability to create rule names that are visible in logs, statistics and reports
Fail-Safe Policy Uploads	System automatically restores the previous policy version if the new version fails

CONFIGURATION	
Routing	Drag-and-drop routing configuration with easy-to-use widgets for adding routes and default routes
Dynamic Routing	Advanced OSPF and BGP configuration via intuitive graphical user interface
Automatic Anti-spoofing	Anti-spoofing configuration is created automatically based on routing
Site-to-site VPNs	<ul style="list-style-type: none"> → Flexible private networking via Policy-based VPN → Route-based VPN → Dynamic SD-WAN Orchestrator
Remote access VPNs	Granular access control for remote endpoints.
ZTNA Application Connector	Enables private applications in internal data centers to connect to Forcepoint ONE's Zero Trust Network Access service so that remote users can access them without a VPN
Endpoint Context Agent Management	Extend access control and visibility to the applications running on endpoints
Firewall Element Creation Wizard	Create hundreds of firewall elements through a firewall creation wizard
Browser-Based User Authentication	Configure and customize an easy browser-based authentication service for users

STATUS, STATISTICS, AND REPORTING	
System Status Monitoring	Real-time status information about engines and their connections
Appliance Status Monitoring	A graphical view of the hardware model and port status of the appliances, with additional details on hardware performance status
Session Monitoring	Dedicated views to monitor connections, VPN security associations (SAs), authenticated users, active alerts and dynamic and static routes
Overviews	Customize dashboards of user and network statistics for real-time monitoring
Geolocations	Show the country information for all IP addresses with the help of country flags and geolocation statistics. Show where network attacks come from
Reporting	Customize and schedule reports that provide detailed information about network statistics

LOGS	
Browser	Granular view for separate log types in addition to common log browsing view for all log data
Intuitive Filtering Tools	Interactive log filtering—drag and drop any log data cell to the Query Panel
Statistics	Create built-in log-based counters and on-demand statistics for reporting, monitoring and alerting
Visualizations	Find the anomalies in logged traffic in filterable log visualizations
Log Analyzer	Aggregate freely on the large amount of filtered log data by any columns
Archiving	Duplicate or archive logs to directories by log data type, time, or filters
Backups	Integrated backup scheduler for Log Server configuration and log data
Exports	CSV, XML, JSON, CEF, LEEF and log exporting; logs can also be snapshot reports
Forwarding	Real-time log redirection in syslog; CEF, LEEF, XML, CSV, JSON, Kafka Topics, NetFlow v9/IPFIX and McAfee Enterprise Security Manager formats; configuration for filtering, data type; and log field selection available
Data Contexts	Shortcuts to browse different types of logs with contextual column sets that are customizable
High Availability	Support for assigning primary and backup Log Servers for each log source

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. Forcepoint Administrative Domain License enables multiple customer environments to be managed 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 Forcepoint Administrative Domain License solution simplifies enterprise and MSSP environments, making them easier to maintain. Role-based access control (RBAC) ensures accurate definition of administrator responsibilities and domain access limitations.

Forcepoint Administrative Domain License Specifications

DOMAINS	
Maximum Number	200
Number of Administrators	Unlimited
Number of Managed Engines	3,000
Number of Elements	Unlimited

FEATURES	
Configuration Separation	Isolate managed environments to different administrative 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	Grant or limit the administrators' access rights to configuration and visibility with the help of separate administrative domains
Monitoring	Monitor the status of all granted domains with the help of the domain overview
Branding	Brand PDF reports with custom 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 Engine	Share the same master context across domain boundaries of up to 250 virtual contexts, which can each have their own policies and routing tables

Forcepoint SMC Appliance

Forcepoint Secure SD-WAN SMC Appliance is an all-in-one dedicated device for configuring, managing and monitoring Forcepoint engines—physical, virtual and cloud-based. Forcepoint SMC provides ease of deployment to get you up and running quickly, combining Forcepoint’s engine management server and log server into a single plug-and-play package running on optimized 1U hardware.

Forcepoint SMC deployment options

There are three ways to deploy Forcepoint SMC: on your systems, on your bare hardware or hypervisor, or as an all-in-one appliance¹.

¹ An SMC software license has to be purchased separately for all 3 deployment options. An appliance alone does not include any licenses.

FORCEPOINT SECURE SD-WAN MANAGER DEPLOYMENT OPTIONS			
COMPONENTS	SOFTWARE	ISO IMAGE	APPLIANCE
SMC Software	●	●	●
Operating System	Customer-supplied	●	●
Hardware/Platform	Customer-supplied	Customer-supplied	●

Forcepoint SMC Appliance Specifications

PERFORMANCE	
Managed Engines	2,000
Maximum Domains	200
Indexed Logs per sec.	80,000
Events per day	6,912,000,000
Log Storage Size	690

Forcepoint SMC Appliance Specifications

PHYSICAL	
Form factor	1U
Processor	2 x Intel Xeon Silver 8 core
Memory	32 GB
Storage (HDD)	Capacity 1.2 TB (2 x 1.2 TB RAID-1), Hot Swappable
Power Supply	2 x 800W (100V~240V) Hot Swappable
Dimensions	26.4" D x 16.9" W x 1.8" H (67 cm D x 43 cm W x 4.5 cm H)
Weight	27.3 lbs. (12.4 kg)
Regulatory & Compliance	FCC / ICES / EN55032 / EN55035 / VCCI BSMI / C-Tick / SABS / CCC / UL / TEC Verified to comply with RoHS Directive

Forcepoint FlexEdge Secure SD-WAN Manager Ordering

ORDERING	ORDERING
Forcepoint FlexEdge Secure SD-WAN Manager (software)	SMCX
Forcepoint FlexEdge Secure SD-WAN Manager (software) 1000 Appliance	SMCAPG5
Forcepoint FlexEdge Secure SD-WAN Manager High Availability	SMCHAX
Forcepoint FlexEdge Secure SD-WAN Manager Additional Log Server	ALSX
Forcepoint FlexEdge Secure SD-WAN Manager Domains (Up to 200 Domains)	ODFSMCX
Forcepoint FlexEdge Secure SD-WAN Manager Web Portal	OWPSX