Symantec
A Division of Broadcom

Product Brief

Management Center Appliance and Virtual Appliance

Improve the Scalability, Security, and Cost Effectiveness of Your Deployments

Key Features

- **Simplify Web Security and Governance:** Define, deploy, and monitor the impact of powerful proxy policies across all sites and devices.
- **Enhance Advanced Threat Defenses:** Eliminate 99.99% of known threats with ProxySG malware categories and Content Analysis System. Streamline investigations by identifying risky users and site access.
- **Reduce Operating Costs:** Provides high availability, while improving overall visibility, and automating common operational tasks.

Introduction

Symantec™ provides Web access control and advanced threat protection for many of the world's largest enterprises. To maximize the value of your Symantec Network solutions, including the powerful ProxySG, you need to be able to quickly and easily roll out, configure, monitor, manage and backup your deployments. Symantec™ Management Center offers a unified management platform that provides the visibility and control you need in one central place. Reduce the time and costs associated with managing your Symantec solutions, including your multi-proxy deployments.

Management Center Unified Management Platform

Management Center is a powerful, unified management platform that gives you centralized visibility for the Symantec network product portfolio. With a single pane of glass, you can see your Symantec deployments, including ProxySG, ASG, SSL Visibility Appliance, Content Analysis System, and Malware Analysis (sandboxing). You can also scale deployments and apply powerful proxy policies throughout your environment that address your specific needs and ensure the consistent application of Web security and governance.

Simplify and Scale Web Security and Governance

Management Center offers centralized visibility and controls to simplify the ongoing management of ProxySG. You can perform the following tasks:

- Configure, manage, and provision ProxySG policies to gain complete control over all your Web traffic.
- Create and deploy policies to multiple devices simultaneously, through the Visual Policy Manager.
- Check consistency between policies and devices.
- Standardize policies across like-purpose devices, with the ability to customize when necessary.

Enhance Advanced Threat Defenses

Management Center makes it simple for you to take advantage of ProxySG malware categories and Content Analysis System to eliminate 99.99% of known threats targeting your organization. You can automate advanced threat protection at the gateway to fortify your network against unknown and advanced malware. You can also streamline investigations and accelerate attack remediation by using the Management Center unified management and reporting capabilities to quickly identify risky users and potentially inappropriate site access.

Figure 1: Get an at-a-glance view of your organizational Web application usage.

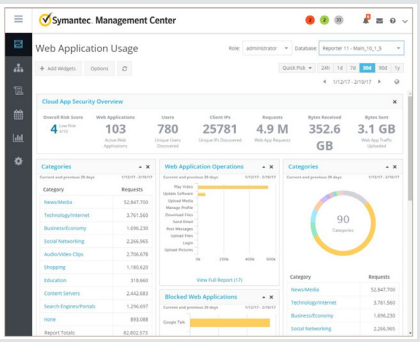
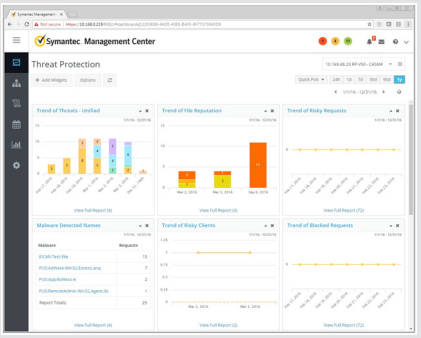


Figure 2: View customizable threat reporting in a unified dashboard.



Reduce Operating Costs

Management Center enables you to automate and streamline operations, saving you precious time and resources. You can report on all your Symantec ProxySG appliances and virtual appliances and receive an up-to-date picture on the health and activity of your other Symantec products to simplify ongoing management. The platform will continue to add product and feature support across the portfolio to continue to increase operational efficiencies. With Management Center, it is easy to do the following tasks:

- **Deploy** – Deploy Management Center as an appliance or virtual appliance to seamlessly integrate and meet the needs of your environment. Centrally manage up to 500 ProxySG appliances, and organize your proxy deployments by purpose, location, department, and more.
- **Specify roles and management tasks** – With object-level access control, you can define users, user groups, devices, and device groups to simplify operations. You have the flexibility to create roles at a very granular, object-level, and apply those roles to individual users or groups. User groups with the same permissions can access, manage, and report on devices within their management area and avoid overlapping duties.
- **Automate operations** – With scripts and job scheduling, you can use Management Center to automate repetitive tasks, including version control and version comparisons. Scripts can be imported from a device and distributed across your device population. You can also reuse key logic across your devices to maximize its utility and minimize the potential for error.
- **Report on device performance** – From Management Center, you can leverage Symantec™ Reporter to collect and analyze logs from all the devices in your Symantec deployment. This information will enable you to access and customize templates to simplify reporting, such as the amount of malware that has been blocked, top threat categories, risky users, and other key metrics. You can also create custom dashboards and reports with widget-based modules to suit your needs.

Maintain a High Availability Environment

For a high availability proxy environment, you can configure device backups and storage to an external server using FTP, HTTP, HTTPS, or SCP. You can monitor hardware diagnostics information, including system metrics, storage usage, temperature, voltage and RPM, to identify and deal with potential issues before they become critical. In the event of a problem, you can click to run hardware diagnostics, power off the appliance and restore factory defaults to resume normal operations and ensure optimal reliability.

Table 1: Management Center (v3.1)

Feature	ProxySG/ASG	CAS	MA	SSLV	SA	RPT	WSS
Inventory and Device Management	●	●	●	●	●	●	●
Health, Monitoring, Status	●	●	●	●	●	●	
Performance Statistics Monitoring	●			●			
Backup and Restore	●	●		●		●	
Image Management	●	●	●	●		●	
License Management	●	●	●	◖	◖	●	
Policy Management and Deployment	●	◖		●		N/A	●
Configuration or Device Sync	●	●	●	●		●	

Table 2: Virtual Appliance Capacity

Management Center	Virtual Appliance						
Capacity	MC-V10-1	MC-V10-10	MC-V10-25	MC-V10-50	MC-V10-100	MC-V10-250	MC-V10-500
Maximum Number of Units Managed	1	10	25	50	100	250	500

Table 3: Hardware Requirements

Server Requirements	2 cores, 8-GB RAM, 100-GB HDD, VMware ESX 5+		
Management Center	S400-20 Appliance		
Capacity	MC-S400-20-100	MC-S400-20-250	MC-S400-20-500
Maximum Number of Units Managed	100	250	500
Disk Drives	3 × 1-TB SAS (effective storage of 1 TB with 2 × RAID1 primary drives and 1× spare drive)		
RAM	16 GB		
Onboard Ports[1]	(2) 1000Base-T Copper ports (with bypass) (2) 1000Base-T Copper ports (non-bypass) (1) 1000Base-T Copper, BMC Management Port		

[1] BMC port is currently disabled

Table 4: Physical Properties

Dimensions and Weight	
Dimensions	572 mm × 432.5 mm × 42.9 mm (22.5 in. × 17.03 in. × 1.69 in.) (chassis only) 643 mm × 485.4 mm × 42.9 mm (25.3 in. × 19.11 in. × 1.69 in.) (chassis with extensions) 1 RU height
Weight (maximum)	Approx. 12.8 kg (28 lbs) ±5%
Operating Equipment	
AC Power	Dual redundant and hot swappable power supplies, AC power 100V to 127V @ 8A/200V to 240V @ 4A/47 HZ to 63 Hz
Total Output Power	450W
Optional DC Power	Input voltage range: 40.5V to 57V Input max current: 22A Total output power: 770W
Thermal Rating	Typical: 1086 BTU/hr, Max: 1381 BTU/hr
Temperature	5°C to 40°C (41°F to 104°F) at sea level
Humidity	20% to 80% relative humidity, non-condensing
Altitude	Up to 3048m (10,000 ft)

Table 5: S400-20 Appliance

Regulations	Safety	Electromagnetic Compliance (EMC)
International	CB – IEC60950-1, Second Edition	CISPR22, Class A; CISPR24
USA	NRTL – UL60950-1, Second Edition	FCC part 15, Class A
Canada	SCC – CSA-22.2, No.60950-1, Second Edition	ICES-003, Class A
European Union (CE)	CE – EN60950-1, Second Edition	EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3
Japan	—	VCCI V-3, Class A
Mexico	NOM-019-SCFI by NRTL Declaration	—
Argentina	S Mark – IEC 60950-1	—
Taiwan	BSMI – CNS-14336-1	BSMI – CNS13438, Class A
China	CCC – GB4943.1	CCC – GB9254; GB17625
Australia/New Zealand	AS/NZS 60950-1, Second Edition	AS/ZNS-CISPR22
Korea	—	KC – RRA, Class A
Russia	CU – IEC 60950-1	GOST-R 51318.22, Class A; 51318.24; 51317.3.2; 51317.3.3
Environmental	RoHS-Directive 2011/65/EU, REACH-Regulation No 1907/2006	
Product Warranty	Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. Symantec Hardware Support contracts available for 24/7 software support with options for hardware support.	
Government Certifications	For further government certification information please contact GTSO-Security-Operations.pdl@broadcom.com.	
More Info	Contact GTSO-Security-Operations.pdl@broadcom.com for specific regulatory compliance certification questions and support	

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-Mgmt-Ctr-PB100 December 14, 2020