Supported Devices & Levels of Support

SIP offers five levels of device support. Each level offers graduating features and functionality in Security Manager and Policy Planner. Please refer to the table below for the level of support offered for your devices.

Level 1: Text-based configuration retrieval is the foundational functionality of Security Manager. Raw retrieval for schedule change detection, comparisons, and change notification features are all built on text-based configuration retrieval.

Level 2: Normalized configuration retrieval. Features that require Level 2 support include configuration comparisons in a normalized display, the display of the device in the network map, database queries, and most reports. Also, real-time change detection using Syslog or CPMI / API polling for Check Point devices.

Level 3: Usage analysis is offered for object and rule usage (both reports and GUI displays), and Traffic Flow Analysis.

Level 4: Behavior analysis is offered for risk analysis, access path analysis (APA), and enhanced rule recommendation features in Security Manager and Policy Planner.

Level 5 / Automation: Ability to take a planned rule and stage it on a device from inside the Policy Planner module. This feature includes the capability to create new rules and place existing objects inside of them. Changes are staged through management stations where applicable, except with ASA where automation is directly against ASA web services.

Note: Our documentation is continuously updated but may not always reflect the latest vendor device versions due to the timing of vendor releases. If your version isn't listed, please contact FireMon Support to verify supported versions.

Caution! **End of Support Notice**: The following devices are no longer supported: Juniper ScreenOS, Juniper ScreenOS VSYS, Juniper SA, and Juniper NSM.

Management Stations

Manufacturer	Device	Version	Level of Support / Comment
Amazon	AWS Account	multi-account discovery	Level 1, 2, & 5
Barracuda	Control Center	v7 (7.2.4), v8	based on managed device level of support
Check Point	R80 CMA /	R80.10 - R80.40	Level 1, 2, 3 & 5

Management Stations (continued)

Manufacturer	Device	Version	Level of Support / Comment
	SmartCenter™		
Check Point	R80 MDS	R80.10 - R80.40	Level 1, 2, 3 & 5
Check Point	R81 CMA / SmartCenter™	R81 - R81.10	Level 1, 2, 3 & 5
Check Point	R81 MDS	R81 - R81.10	Level 1, 2, 3 & 5
Check Point	R82 CMA / SmartCenter™	R82	Level 1, 2, 3 & 5
Check Point	R82 MDS	R82	Level 1, 2, 3 & 5
Cisco	APIC - ACI Manager	4.1	based on managed device level of support
Cisco	Security Manager CSM	4.3 - 4.19+	Level 1, 2, 3
Cisco	Firepower Management Center (FMC)	6.1 - 6.7, 7.0 - 7.1	Level 1, 2, 3 & 5
Cisco	Cloud-Delivered Firepower Management Center (cdFMC)	cloud based	Level 1, 2, 3 & 5
Cisco	ISE	2.2+	based on managed device level of support
Cisco	Meraki	cloud based	based on managed device level of support
Cisco	Viptela vManage		Level 1 & 2
CloudGenix	Controller	cloud based	based on managed device level of support

Management Stations (continued)

Manufacturer	Device	Version	Level of Support / Comment
Forcepoint	Stonesoft Management Center	5.6 - 5.10, 6.0 - 6.7+	Level 1, 2 & 3
Fortinet	FortiManager	4.3.6, 5.0+, 6.0 - 6.4, 7.0 - 7.2	Level 1, 2, 3 & 5
Fortinet	FortiManager - ADOM	4.3.6, 5.0+, 6.0 - 6.4, 7.0 - 7.2	Level 1, 2, 3 & 5
Google	Google Cloud Platform	1.22.13+	based on managed device level of support
HPE / Aruba	EdgeConnect SD WAN	9.1.x	based on managed device level of support
Juniper Networks	Space	19.1R1, 20.1R1	Level 1 & 2
Microsoft	Azure Manager	multi-subscription discovery	based on managed device level of support
Palo Alto	Panorama	8.1.x, 9.0.x, 9.1.x, 10.0. 10.1.x, 11.0	Level 1, 2, 3 & 5
Palo Alto	Prisma Access Cloud Manager / Strata Cloud Manager	cloud based	Level 1, 2 & 3
VMware	NSX-T Manager	3.1+	based on managed device level of support
VMware	NSX-V Manager	vSphere 6.5, NSX 6.2.4 - 6.4, Log Insight 4.0.0 - 4.5	based on managed device level of support
Zscaler	ZIA	Advanced Cloud FW	Level 1, 2 & 3

Firewalls

Manufacturer	Device	1	2	3	4	5	Version / Comment
AhnLab	TrusGuard Series	X	X	X			2.1+
Amazon	VPC	X	X			X	cloud
Barracuda	NGFW	X	X				7.2.4, 8
Check Point	R80, R81, R82 Edge	X	X	X	X	X	R80.10 - R80.40, R81, R81.20, R82
Check Point	R80, R81, R82 Firewall	X	X	X	X	X	R80.10 - R80.40, R81, R81.20, R82
Cisco	ACI	X	X	X			4.1
Cisco	ASA/ASA Context	X	X	X	X	X	7.x, 8.x, 9.x
Cisco	FWSM/FWSM Context	X	X	X	X	X	7.x, 8.x, 9.x
Cisco	Firepower FTD	X	X	X	X	X	6.1 - 6.7, 7.0 - 7.1
Cisco	Firepower FDM	X	X				7.0+
Cisco	Meraki	X	X	X	X	X	cloud
Cisco	Viptela Tenant	X	X				cloud
CloudGenix	ION	X	X	X			cloud
Forcepoint	Enterprise Firewall	X	X	X			8.0+
Forcepoint	Sidewinder	X	X	X			7.0+
Forcepoint	Stonesoft	X	X	X	X		5.6, 5.8, 5.9, 6.1, 6.1, 6.2+
Fortinet	FortiGate Firewall	X	X	X	X	X	FortiOS 4.3.6, 5.0+, 6.0 - 6.4, 7.0 - 7.2

Firewalls (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
Fortinet	FortiGate VDOM	X	X	X	X	X	FortiOS 4.3.6, 5.0+, 6.0 - 6.4, 7.0 - 7.2
Google	VPC Network	X	X				cloud
Hillstone Networks	Firewall	X	X	X			1.22.13+
Huawei	Eudemon Series	X	X	X			4.0+
Huawei	NGFW Series	X	X	X			3.3, 5.3+
Juniper Networks	SRX	X	X	X	X	X	Junos 9.6R1.13+ Automation for SRX, not managed by NSM
Juniper Networks	SRX LSYS	X	X	X	X		Junos 9.6R1.13+
Juniper Networks	QFX	X	X				Junos 12.x - 15.x+
Juniper Networks	VSRX	X	X				Junos 19.1R1, 20.1R1
Linux	IPtables		X	X			Usage support issues -- no rule name references
Linux	NFtables	X	X	X			Usage support issues -- no rule name

Firewalls (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
							references
Microsoft	Azure	X	X	X		X	cloud Usage by Hit Count
Microsoft	Azure Firewall	X	X	X			cloud
Netgate	pfSense	X	X	X	X		2.4.5+
Palo Alto Networks	PA Firewall	X	X	X	X	X	4.0.x, 4.1.2-4.1.10, 5.0-7.1.x, 8.0.x+, 9.0.x, 10.1.x, 11.0
Palo Alto Networks	Prisma Access (single tenant only)	X	X	X			cloud
Palo Alto Networks	VSYS	X	X	X	X	X	4.0.x, 4.1.2-4.1.10, 5.0-7.1.x, 8.0.x, 9.0.x, 10.1.x, 11.0
Riverbed	SteelHead	X					9.1.0
SECUI	BLUEMAX	X	X	X	X	X	
SECUI	MF2	X	X	X			2.0
SECUI	NXG Series	X	X	X			2000
SonicWALL	SonicWALL 6.5.1+	X	X	X			6.5.1+ There is a known bug that we're trying to get the vendor to fix. Duplicate

Firewalls (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
							UUIDs may be seen on rules, which can cause incorrect usage for rules.
SonicWALL	SonicWALL 5.9+	X	X				5.9+, 6.x+, 6.5.1+ No UUID in this version to track usage for Level 3 support. Usage will require SonicWALL firmware: 6.2.7.0-11+
SonicWALL	SonicWALL 5.8	X	X				5.8 No UUID in this version to track usage for Level 3 support
Sophos	XG	X	X				7.x , 8.x,
Sophos	XGS	X	X				Validated that v20.x, and v21.x successfully on-boarded
Stormshield	Stormshield Network	X	X	X			3.2.1+

Firewalls (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
	Security						
TopSec	Firewall	X	X	X			3.3+
VMware	NSX-T	X	X	X	X	X	3.1+
VMware NSX-V	Distributed Firewall	X	X*	X	X	X	6.2, 6.3.1 *Real time change detection is not currently supported for VMware NSX devices
VMware NSX-V	Edge Firewall	X	X*	X			6.2, 6.3.1 *Real time change detection is not currently supported for VMware NSX devices
WatchGuard	Firebox	X	X	X			11.11.2
Zscaler	Cloud	X	X	X			cloud

Traffic Managers

Manufacturer	Device	1	2	3	4	5	Version / Comment
A10	ADC Load Balancer	X	X				4.14, 5.2.x
Blue Coat	ProxySG	X	X	X			5.2, 6.5, 6.6 Usage by Hit Count

Traffic Managers (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
Citrix	Netscaler VPX	X	X	X	X		12.0.53.13.nc+ Usage by Syslog
F5	BIG-IP	X	X	X	X	X	10.x, 11.x - 15.x Policy Planner automation for F5 AFM

Routers / Switches

Manufacturer	Device	1	2	3	4	5	Version / Comment
Arista	EOS & vEOS	X	X				4.22
Cisco	IOS® IOS XE	X	X	X	X	X	11.x+ Minimum version required for Hit Counters: IOS 12.4 (22)T IOS XE Release 3.6S
Cisco	IOS® XR	X	X	X	X	X	5.3.3+
Cisco	IOS® ZFW ZoneBased-FW	X	X	X	X		12.4(6)T
Cisco	Nexus	X	X		X		4.1 - 7.2
Commscope	Ruckus Layer 3 Switches	X	X		X		Normalization of: users, interfaces, routers, network objects, service objects, security objects, nat rules
Dell	Powerswitch S-series	X	X				
Extreme	X Series	X	X				EXOS 22.6.1.4

Routers / Switches (continued)

Manufacturer	Device	1	2	3	4	5	Version / Comment
Networks							
Google	Caprica	X	X				
HPE	Aruba OS-CX	X	X				9.2+
Juniper Networks	EX Series	X	X	X	X		Junos 12.x - 15.x+
Juniper Networks	M Series	X	X	X	X	X	Junos 11.1R4+
Juniper Networks	QFX	X	X		X		Junos 12.x - 15.x+
Nokia	Lucent/Alcatel	X	X				

Log Servers

Manufacturer	Device	Version / Comment
Check Point	Check Point Log Server	NG FP3, R80.10+ DC connects to Log Server over TCP/18184 to receive usage logs.

Communication Protocols

Because the SIP modules are browser-based, HTTPS is the communication protocol. Below are tables listing the various ports used for connecting and their function relating to inbound (ingress) and outbound (egress) communication.

Inbound Communication

Inbound Communication Ports

Port	Type	Connection	Function
22	TCP	SSH	Used to retrieve configuration information from the Data Collector to non-Check Point devices.
50	IP protocol	IPsec ESP	This port is used to authenticate and encrypt data