



Supported Devices and Software Versions for Cisco Security MARS Local Controller 4.3.x and 5.3.x

Revised: September 26, 2008

This document includes:

- [Supported Local Controller Appliances](#)
- [Supported Reporting and Mitigation Devices](#)
- [Interoperable Supporting Services](#)

Supported Local Controller Appliances

The software that supports the Local Controller appliance varies depending on the model of the appliance:

- [Appliance Models Supported with 5.3.x, page 1](#)
- [Appliance Models Supported with 4.3.x, page 2](#)

Appliance Models Supported with 5.3.x

Cisco Security MARS version 5.3.x supports the following Cisco Security MARS Local Controller appliances:

- Cisco Security MARS 25 (CS-MARS-25-K9) —Release 5.3.2 and more recent
- Cisco Security MARS 25R (CS-MARS-25R-K9)—Release 5.3.2 and more recent
- Cisco Security MARS 55 (CS-MARS-55-K9)—Release 5.3.2 and more recent
- Cisco Security MARS 110 (CS-MARS-110-K9)
- Cisco Security MARS 110R (CS-MARS-110R-K9)
- Cisco Security MARS 210 (CS-MARS-210-K9)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

Appliance Models Supported with 4.3.x

Cisco Security MARS version 4.3.x supports the following Cisco Security MARS and Protego Networks MARS Local Controller appliances:

- Cisco Security MARS 20 (CS-MARS-20-K9)
- Cisco Security MARS 20R (CS-MARS-20R-K9)
- Cisco Security MARS 50 (CS-MARS-50-K9)
- Cisco Security MARS 100 (CS-MARS-100-K9)
- Cisco Security MARS 100e (CS-MARS-100E-K9)
- Cisco Security MARS 200 (CS-MARS-200-K9)
- Protego Networks PN-MARS 20
- Protego Networks PN-MARS 50
- Protego Networks PN-MARS 100
- Protego Networks PN-MARS 100e
- Protego Networks PN-MARS 200

Supported Reporting and Mitigation Devices

The following tables list the devices supported upon release of Cisco Security MARS Local Controller 4.3.x and 5.3.x:

- [Router and Switch Devices](#)
- [Firewall Devices](#)
- [VPN Devices](#)
- [Network IDS and IPS Devices](#)
- [Host IDS and IPS Devices](#)
- [Antivirus Devices](#)
- [Vulnerability Assessment Devices](#)
- [Host Operating System Applications](#)
- [Web Server Devices](#)
- [Database Server Applications](#)
- [AAA Servers](#)
- [Syslog Servers and SNMP Devices](#)
- [Wireless Access Points](#)

Also listed are protocols used to retrieve configuration event data and protocols used to mitigate attacks (if supported on the device).

The following support level may be noted:

- **Backward compatible support.** When supporting current major/minor device release, it also supports two prior non-EOL major releases and all minor releases within the support major releases.
 - No device type version supported in web interface; uses existing device type and version.
 - No new data work for this version; uses existing event types and rules.
 - This version may or may not be fully tested. Another version using the same evnets has been tested.

The *Added to GUI As* column identifies how you add the device type using the Cisco Security MARS web interface. The classifications used are defined as follows:

- HW. Indicates that you add the device directly as a hardware-based security device.
- HW-switch. Indicates that you add the device as a module after you define a base switch.
- HW-router. Indicates that you add the device as a module after you define a base router.
- HW-ASA. Indicates that you add the device as a module after you define a Cisco Adaptive Security Appliance.
- host. Indicates that you add this device as a host operating system.
- SW-host. Indicates that you add this device as a software application after you define a base host.
- ODS. Indicates that you add this device as an on-demand security service.

Table 1 Router and Switch Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Router and Switch Devices .							
Cisco Router	Cisco IOS 11.x Cisco IOS 12.2	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	IOS
	Cisco IOS 12.3	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	IOS
	Cisco IOS 12.4 (11) T2	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	IOS
Cisco Router Module	Cisco IOS 12.2	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW-switch	SWITCH-IOS
	Cisco IOS 12.3	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW-switch	SWITCH-IOS
	Cisco IOS 12.4 (11) T2	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW-switch	SWITCH-IOS
Cisco Switch	CatOS 6.x IOS 12.2	Yes	FTP, SNMP, SSH, Telnet	Syslog , NetFlow v1, v5, v7 ³	SNMP	HW	SWITCH-CATOS
	Cisco IOS 12.3	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	SWITCH-CATOS
	Cisco IOS 12.4 (11) T2	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	SWITCH-CATOS
Extreme ExtremeWare	6.x	No	SNMP	Syslog	SNMP	HW	EXTREME
Generic Router	Unknown	No	SNMP	Syslog	n/a	HW	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance
3. NetFlow v7 supports only Catalyst 5000 switches with Sup III and the NFFC and NFFC II cards, which reached end of support in May 2005.

Table 2 Firewall Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Firewall Devices .							
Cisco PIX	6.0, 6.1, 6.2, 6.3	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	PIX
	7.0, 7.0.7 (GD release)	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	PIX7X
	7.2, 7.2.1, 7.2.2, 7.2.3	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	PIX7X
	8.0	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	PIX7X
Cisco Adaptive Security Appliance (ASA)	7.0.1, 7.0.7 (GD release)	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	ASA
	7.2, 7.2.1, 7.2.2, 7.2.3	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	ASA
	8.0	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	ASA
Cisco Firewall Services Module (FWSM)	1.1	No	FTP, SSH, Telnet	Syslog	n/a	HW-switch (IOS 12.2 or CatOS)	FWSM
	2.2, 2.3, 2.3.5,	Yes	FTP, SSH, Telnet	Syslog	n/a	HW-switch (IOS 12.2 or CatOS)	FWSM
	3.1, 3.1.3, 3.1.5, 3.1.6	Yes	FTP, SSH, Telnet	Syslog	n/a	HW-switch (IOS 12.2 or CatOS)	FWSM
	3.2.1.	Yes	FTP, SSH, Telnet	Syslog	n/a	HW-switch (IOS 12.2 or CatOS)	FWSM
Cisco IOS Firewall Feature Set	12.2(T) and later	No	n/a - discovered as part of the router configuration	Syslog	n/a	n/a - add the IOS router	n/a
Juniper NetScreen	ScreenOS 4.0, 5.0	No	SNMP, SSH, Telnet	Syslog	n/a	HW	NETSCREEN

Table 2 Firewall Devices

Check Point Opsec NG and Firewall-1	NG FP3, NG AI (R55), NGX AI (R60) up to build 244	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host	Not supported
	NGX AI (R61, R62)	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host	Not supported
	NGX AI (R65) Backward Comaptible	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host	Not supported
Nokia Firewall (running Check Point)	NG FP3, NG AI (R55), NGX (R60)	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host as CheckPoint	Not supported
	NGX AI (R61, R62)	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host as CheckPoint	Not supported
	NGX AI (R65) Backward Comaptible	Yes	OPSEC-CPMI (SSLCA, CLEAR, ASYMSSLCA)	OPSEC-LEA (from Log Server or Management Server)	n/a	SW-host as CheckPoint	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 3 VPN Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring VPN Devices .							
Cisco VPN 3000 Concentrator	4.0.3, 4.7	No	SNMP	Syslog	n/a	HW	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 4 Network IDS and IPS Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Network-based IDS and IPS Devices .							
Cisco Network IDS	3.1	No	SSH, Telnet	POP	n/a	HW	Not supported
Cisco IDSM	3.1	No	SSH, Telnet	POP	n/a	HW-switch	Not supported
Cisco Network IDS	4.0	No	SSL	RDEP	n/a	HW	CiscoIDS4x
Cisco IDSM	4.0	No	SSL	RDEP	n/a	HW-switch	CiscoIDS4x
Cisco Intrusion Prevention System (IPS), IDSM-2 module	5.0, 5.1	No	SSL	SDEE	n/a	HW, HW-switch	CiscoIPS5x
	6.0, 6.0.1, 6.0.2, 6.0.3	No	SSL	SDEE	n/a	HW, HW-switch	Not supported
Cisco IPS ASA module	5.0, 5.1	No	n/a	SDEE	n/a	HW-ASA	CiscoIPS5x
	6.0	No	n/a	SDEE	n/a	HW-ASA	Not supported
Cisco IOS IPS (software only)	12.3(8)T or later.	No	FTP, SNMP, SSH, Telnet	SDEE	n/a	HW-switch, HW-router	n/a
	12.4(Pi5)	No	FTP, SNMP, SSH, Telnet	SDEE	n/a	HW-router	n/a
McAfee/IntruVert IntruShield	1.5	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
Juniper NetScreen IDP	2.1	No	n/a	Syslog (from IDP Management Server)	n/a	SW-host	Not supported
	3.x (3.0, 3.1)	No	n/a	Syslog (from IDP Management Server)	n/a	SW-host	Not supported
	4.x (4.0, 4.1)	No	n/a	Syslog (from NSM Server) Syslog from IDP Sensor	n/a	SW-host	Not supported
Symantec ManHunt	3.x	No	n/a	SNMP	n/a	SW-host	Not supported

Table 4 Network IDS and IPS Devices

IBM/ISS RealSecure Sensor	6.5, 7.0	No	n/a	SNMP	n/a	SW-host	Not supported
IBM/ISS Site Protector	2.0	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
Snort	2.0, 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8 (use 2.0 in UI)	No	n/a	Syslog	n/a	SW-host	Not supported
Enterasys Dragon	6.x	No	n/a	Syslog (from Manager)	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 5 Host IDS and IPS Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Host-Based IDS and IPS Devices .							
Cisco Security Agent	4.0, 4.5	No	n/a	SNMP (from CSA MC)	n/a	SW-host	Not supported
	5.0, 5.1, 5.2	No	n/a	SNMP (from CSA MC)	n/a	SW-host	Not supported
McAfee Enterscept	2.5, 4.0	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
IBM/ISS RealSecure Host Sensor	6.5, 7.0	No	n/a	SNMP	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 6 **Antivirus Devices**

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Antivirus Devices .							
Symantec Anti Virus	9.x	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
	10.x (10.1, 10.2)	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
Cisco Incident Control System (Cisco ICS), Trend Micro Outbreak Prevention Service (OPS)	1.0	No	n/a	Syslog (from CICC Server)	n/a	SW-host	Not supported
McAfee ePolicy Orchestrator (ePO)	3.5	No	n/a	SNMP (from Management Server)	n/a	SW-host	Not supported
McAfee/Network Associates VirusScan	8.x	No	n/a	SNMP (from Management Server)	n/a	n/a - learn about hosts via the traps provided ePO Server)	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 7 *Vulnerability Assessment Devices*

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Vulnerability Assessment Devices .							
eEye REM	1.0	No	MS SQL	JDBC (from REM server)	n/a	SW-host	Not supported
Qualys QualysGuard	3.x	No	n/a	HTTPS (using XML via API v. 3.3)	n/a	ODS	Not supported
McAfee/Foundstone Foundscan	3.0	No	MS SQL	JDBC (from Management Sever)	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 8 *Host Operating System Applications*

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Generic, Solaris, Linux, and Windows Application Hosts .							
Windows	NT, 2000, 2003	No	n/a	Syslog (from SNARE agent) or MS-RPC event pull	n/a	host	WINDOWS , WindowsNT Windows2000 Windows2003
Solaris	8.x, 9.x, 10.x	No	n/a	Syslog	n/a	host	SOLARIS
Redhat Linux	7.x, 8.x	No	n/a	Syslog	n/a	host	LINUX

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 9 *Web Server Devices*

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Web Server Devices .							
Support logs in common access log, squid log, netscape extended log, and MS-W3C formats.							
Microsoft Internet Information Server	Any earlier than 6.0	No	n/a	Syslog (from SNARE agent)	n/a	SW-host	Not supported
Sun iPlanet	Any	No	n/a	HTTP (from available Web agent)	n/a	SW-host	Not supported
Apache	Any	No	n/a	HTTP (from available Web agent)	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 10 *Database Server Applications*

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Database Applications .							
Oracle Database	9i, 10g, 11g (as generic), Generic	No	TCP	SQLNet (from Host)	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 11 AAA Servers

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring AAA Devices .							
Cisco Secure Access Control Sever (ACS)	3.3, 4.x ³	No	n/a	Syslog (from pnLog Agent)	n/a	SW-host	Not supported
Cisco Secure ACS Solutions Engine	3.3, 4.x	No	n/a	Syslog (from pnLog Agent running on remote logging host)	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance
3. Cisco Secure ACS 4.x support is provided via the pnLog Agent, not through the syslog format found in Cisco Sucre ACS.

Table 12 Syslog Servers and SNMP Devices

Vendor	Supported Versions	SNMP-based Resource Monitoring ¹	Protocol: Configuration Retrieval	Protocol: Event Retrieval ²	Protocol: Mitigation	Add to GUI As	CSV Keyword
See Configuring Generic, Solaris, Linux, and Windows Application Hosts .							
See Syslog Relay Support .							
Generic Devices	Any	No	n/a	SNMP Syslog	n/a	SW-host	Not supported
Syslog relay	Any. Tested with syslog-ng and kiwi servers.	No	n/a	Syslog	n/a	SW-host	Not supported

1. Cisco Security MARS supports only SNMPv1
2. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Table 13 *Wireless Access Points¹*

Vendor	Supported Versions	SNMP-based Resource Monitoring ²	Protocol: Configuration Retrieval	Protocol: Event Retrieval ³	Protocol: Mitigation	Add to GUI As	CSV Keyword
See, Configuring Wireless LAN Devices							
Cisco Wireless LAN Controller	4.1.171.0	No	SNMP	SNMP (from WLAN Controller)	n/a	HW	Not supported

1. Wireless Access Points are supported only on the Cisco Security MARS version 5.3.x.
2. Cisco Security MARS supports only SNMPv1
3. Assume the protocol is configured on the device, unless otherwise noted. In some cases, collector agents are responsible for providing the event data to the MARS Appliance

Interoperable Supporting Services

Supporting services are defined as those network services that extended functionality of Cisco Security MARS. The following table lists those proven, tested, and version specific services.

Table 14 *Interoperable Supporting Services for Cisco Security MARS Local Controller 4.3.x and 5.3.x*

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Products						
See Security Manager Policy Table Lookup from a MARS Event .						
Cisco Security Manager	3.0, 3.1	n/a	HTTPS (policy lookup, not event data)	n/a	SW-host	Not supported
NFS Servers						
Support for Cisco Security MARS configuration and event backups. See Configuring and Performing Appliance Data Backups .						
Microsoft Windows Services for UNIX (SFU) See http://www.interoperabilitybridges.com/ and Configure the NFS Server on Windows .	3.5	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a

Table 14 Interoperable Supporting Services for Cisco Security MARS Local Controller 4.3.x and 5.3.x

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Linux NFS See Configure the NFS Server on Linux .	2, 3 ¹	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a
Network Appliance NetApp-store See Configure the NetApp NFS Server .	FAS270 ver. 7.0.4	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a
External AAA Servers						
Support for user authentication via the RADIUS protocol. See Authenticating MARS Accounts with External AAA Servers .						
Cisco Secure Access Control Server (ACS)	All versions	RADIUS	n/a	n/a	AAA server	n/a
Microsoft Internet Authentication Service (IAS) Server	All versions	RADIUS	n/a	n/a	AAA server	n/a
Juniper Steel belted RADIUS	All versions	RADIUS	n/a	n/a	AAA server	n/a

1. Full support of NFS v4 is not provided, as it may require an additional authentication method.

