



Supported Devices and Software Versions for Cisco Security MARS Local Controller 4.2.x and 5.2.x

Revised: September 9, 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 5.2.x, page 1](#)
- [Appliance Models Supported with 4.2.x, page 2](#)

Appliance Models Supported with 5.2.x

Cisco Security MARS version 5.2.x supports the following Cisco Security MARS Local Controller appliances:

- Cisco Security MARS 110 (CS-MARS-110-K9)
- Cisco Security MARS 110R (CS-MARS-110R-K9)
- Cisco Security MARS 210 (CS-MARS-210-K9)



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

© <year> Cisco Systems, Inc. All rights reserved.

Appliance Models Supported with 4.2.x

Cisco Security MARS version 4.2.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

[Table 1](#) lists the devices supported upon release of Cisco Security MARS Local Controller 4.2.x and 5.2.x. It also identifies what protocols are used to retrieve configuration and event data, as well as the protocol used to mitigate attacks (if that device supports mitigation).



Note

Release 5.2.4 reporting and mitigation device support is identical to Release 4.2.2 reporting and mitigation device support.

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 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.2.x

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Router / Switch Devices						
See Configuring Router and Switch Devices .						
Cisco Router	Cisco IOS 11.x, 12.2	FTP, SNMP, SSH, Telnet	Syslog (from device), NetFlow v1, v5	SNMP	HW	IOS
Cisco Router Module	Cisco IOS 12.2	FTP, SNMP, SSH, Telnet	Syslog (from device), NetFlow v1, v5	SNMP	HW-switch	SWITCH-IOS
Cisco Switch	CatOS 6.x IOS 12.2	FTP, SNMP, SSH, Telnet	Syslog (from device), NetFlow v1, v5, v7 ¹	SNMP	HW	SWITCH-CATOS
Extreme ExtremeWare	6.x	SNMP	Syslog (from device)	SNMP	HW	EXTREME
Generic Router	Unknown	SNMP	Syslog (from device)	—	HW	

Firewall Devices

See [Configuring Firewall Devices](#).

Table 1 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.2.x (continued)

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco PIX	6.0, 6.1, 6.2, 6.3	FTP, SSH, Telnet	Syslog (from device)	—	HW	PIX
Cisco PIX	7.0	FTP, SSH, Telnet	Syslog (from device)	—	HW	PIX7X
Cisco Adaptive Security Appliance (ASA)	7.0.1	FTP, SSH, Telnet	Syslog (from device)	—	HW	ASA
Cisco Firewall Services Module (FWSM)	1.1, 2.2, 2.3, 3.1	FTP, SSH, Telnet	Syslog (from device)	—	HW-switch (IOS 12.2 or CatOS)	FWSM
Cisco IOS Firewall Feature Set	12.2(T) and later	FTP, SNMP, SSH, Telnet	Syslog (from device)	—		
Juniper Netscreen	ScreenOS 4.0, 5.0	SNMP, SSH, Telnet	Syslog (from device)	—	HW	NETSCREEN
Check Point Opsec NG and Firewall-1	NG FP3, NG AI (R55), NGX AI (R60) up to build 244	SSLCA, CLEAR, ASYMSSLCA (OPSEC-CPMI)	OPSEC-LEA (from Log Server or Management Server)	—	SW-host	
Nokia Firewall (running Check Point)	NG FP3, NG AI (R55), NGX (R60)	SSLCA, CLEAR, ASYMSSLCA (OPSEC-CPMI)	OPSEC-LEA (from Log Server or Management Server)	—	SW-host as ChcekPoint	
VPN Devices						
See Configuring VPN Devices .						
Cisco VPN 3000 Concentrator	4.0.3, 4.7	SNMP	Syslog (from device)	—	HW	
Network IDS						
See Configuring Network-based IDS and IPS Devices .						
Cisco Network IDS	3.1	SSH, Telnet	POP (from device)	—	HW	
Cisco IDSM	3.1	SSH, Telnet	POP (from device)	—	HW-switch	
Cisco Network IDS	4.0	SSL	RDEP (from device)	—	HW	CiscoIDS4x
Cisco IDSM	4.0	SSL	RDEP (from device)	—	HW-switch	CiscoIDS4x
Cisco Intrusion Prevention System (IPS), IDSM-2 module	5.0, 5.1	SSL	SDEE (from device)	—	HW	CiscoIPS5x

Table 1 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.2.x (continued)

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco IPS ASA module	5.0, 5.1	—	SDEE (from device)	—	HW-ASA	CiscoIPS5x
Cisco IOS IPS (software only)	12.3(8)T or later.	FTP, SNMP, SSH, Telnet	SDEE (from device)	—	HW-switch, HW-router	
IntruVert IntruShield	1.5	—	SNMP (from Management Server)	—	SW-host	
Juniper Netscreen IDP	2.1	—	SNMP (from Management Server)	—	SW-host	
Symantec ManHunt	3.x	—	SNMP (from Device)	—	SW-host	
ISS RealSecure Sensor	6.5, 7.0	—	SNMP (from Device)	—	SW-host	
Snort	2.0, 2.1, 2.2, 2.3, 2.4, 2.6, (use 2.0 in UI)	—	Syslog (from Device)	—	SW-host	
Enterasys Dragon	6.x	—	Syslog (from Manager)	—	SW-host	
Host IDS						
See Configuring Host-Based IDS and IPS Devices .						
Cisco Security Agent	4.0, 4.5		SNMP (from CSA MC)	—	SW-host	
McAfee Enterccept	2.5, 4.0	—	SNMP (from Management Server)	—	SW-host	
ISS RealSecure Host Sensor	6.5, 7.0	—	SNMP (from Device)	—	SW-host	
Anti-virus						
See Configuring Antivirus Devices .						
Symantec Anti Virus	9.x	—	SNMP (from Management Server)	—	SW-host	
Cisco Incident Control System (Cisco ICS), Trend Micro Outbreak Prevention Service (OPS)	1.0	—	Syslog (from CICC Server)	—	SW-host	
McAfee ePolicy Orchestrator	3.5		SNMP (from Management Server)		SW-host	

Table 1 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.2.x (continued)

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Network Associates VirusScan	8.x	—	SNMP (from Management Server)	—	SW-host	
Vulnerability Assessment						
See Configuring Vulnerability Assessment Devices .						
eEye REM	1.0	MS SQL	JDBC (from REM server)	—	SW-host	
Qualys QualysGuard	3.x	—	HTTPS (using XML via API)	—	ODS	
Foundstone Foundscan	3.0	MS SQL	JDBC (from Management Sever)	—	SW-host	
Host OSes						
See Configuring Generic, Solaris, Linux, and Windows Application Hosts .						
Windows	NT, 2000, 2003	—	Syslog (from SNARE agent) or MS-RPC event pull	—	host	WINDOWS, WindowsNT Windows2000 Windows2003
Solaris	8.x, 9.x, 10.x	—	Syslog (from Device)	—	host	SOLARIS
Redhat Linux	7.x, 8.x	—	Syslog (from Device)	—	host	LINUX
Web Servers						
See Configuring Web Server Devices .						
Microsoft Internet Information Server	Any	—	Syslog (from SNARE agent)	—	SW-host	
Sun iPlanet	Any	—	HTTP (from Cisco Security MARS Agent)	—	SW-host	
Apache	Any	—	HTTP (from Cisco Security MARS Agent)	—	SW-host	
Web Proxy Devices						
See Configuring Web Proxy Devices .						
Network Appliance NetCache	Generic	—	HTTP	—	HW	

Table 1 *Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.2.x (continued)*

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Database Servers						
See Configuring Database Applications .						
Oracle Database	9i, 10g, Generic	TCP	SQLNet (from Host)	—	SW-host	
AAA Servers						
See Configuring AAA Devices .						
Cisco Secure Access Control Sever (ACS)	3.3, 4.x ²	—	Syslog (from pnLog Agent)	—	SW-host	
Cisco Secure ACS Solutions Engine	3.3, 4.x	—	Syslog (from pnLog Agent running on remote logging host)	—	SW-host	
Syslog Servers and SNMP Devices						
See Configuring Generic, Solaris, Linux, and Windows Application Hosts .						
Generic Devices	Any	—	SNMP (from Device) Syslog (from Device)	—	SW-host	

1. 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.
2. Cisco Secure ACS 4.x support is provided via the pnLog Agent, not through the syslog format found in Cisco Sucre ACS.

Interoperable Supporting Services

Supporting services are defined as those network services that extended functionality of Cisco Security MARS. [Table 2](#) lists those proven, tested, and version specific services.

Table 2 *Interoperable Supporting Services for Cisco Security MARS Local Controller 4.2.x*

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Products						
See Policy Table Lookup on Cisco Security Manager .						
Cisco Security Manager	3.0	—	HTTPS (policy lookup, not event data)	—	SW-host	—

NFS Servers

Support for Cisco Security MARS configuration and event backups. See [Configuring and Performing Appliance Data Backups](#).

Table 2 Interoperable Supporting Services for Cisco Security MARS Local Controller 4.2.x

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Microsoft Windows Services for UNIX (SFU) See http://technet.microsoft.com/en-us/interopmigration/bb380242.aspx and Configure the NFS Server on Windows.	3.5	NFS (MARS archive mount, not retrieval of NFS server logs)	—	—	—	—
Linux NFS See Configure the NFS Server on Linux.	2, 3 ¹	NFS (MARS archive mount, not retrieval of NFS server logs)	—	—	—	—

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