



# Supported Devices and Software Versions for Cisco Security MARS Local Controller 4.1.x

Revised: February 15, 2005

This document includes:

- [Supported Cisco Security MARS Devices](#)
- [Supported Reporting and Mitigation Devices](#)

## Supported Cisco Security MARS Devices

Table 1 lists the devices on which Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) Local Controller 4.1.x runs upon release. You can find information about new device support at <http://www.cisco.com>.

**Table 1**      **Supported Devices for Cisco Security MARS Local Controller 4.1.x**

Type of Device	Devices Supported
Protego Networks	
	PN-MARS 20
	PN-MARS 50
	PN-MARS 100
	PN-MARS 100e
	PN-MARS 200
Cisco Systems	
	Cisco Security MARS 20
	Cisco Security MARS 50
	Cisco Security MARS 100
	Cisco Security MARS 100e
	Cisco Security MARS 200



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

© 2005 Cisco Systems, Inc. All rights reserved.

# Supported Reporting and Mitigation Devices

Table 2 lists the devices supported upon release of Cisco Security MARS Local Controller 4.1.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).

The *Added to GUI As* column identifies how you add the device type using the Cisco Security MARS HTML 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 2** Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.1.x

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

**Table 2 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.1.x**

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Adaptive Security Appliance (ASA)	7.0.1	FTP, SSH, Telnet	Syslog (from device)	—	HW	
Cisco Firewall Services Module (FWSM)	1.1, 2.2, 2.3	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 (R60)	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 CheckPoint	
<b>VPN Devices</b>						
See <a href="#">Configuring VPN Devices</a> .						
Cisco VPN 3000 Concentrator	4.0.3, 4.7	SNMP	Syslog (from device)	—	HW	
<b>Network IDS</b>						
See <a href="#">Configuring Network-based IDS and IPS Devices</a> .						
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	
Cisco IDSM	4.0	SSL	RDEP (from device)	—	HW-switch	
Cisco Intrusion Prevention System (IPS), ASA module	5.0, 5.1	SSL	SDEE (from device)	—	HW	
Cisco IPS ASA module	5.0, 5.1	—	SDEE (from device)	—	HW-ASA	
Cisco IOS IPS (software only)	12.3(8)T or later.	FTP, SNMP, SSH, Telnet	SDEE (from device)	—	HW-switch, HW-router	

**Table 2 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.1.x**

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
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	—	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 Entercpt	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	
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	
----------	-----	--------	------------------------	---	---------	--

**Table 2 Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.1.x**

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
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
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	
----------------------------	---------	---	------	---	----	--

**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, 4.0	—	Syslog (from pnLog Agent)	—	SW-host	
---	----------	---	---------------------------	---	---------	--

**Table 2** Supported Reporting and Mitigation Devices for Cisco Security MARS Local Controller 4.1.x

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Secure ACS Solutions Engine	3.3, 4.0	—	Syslog (from pnLog Agent running on remote logging host)	—	SW-host	
<b>Syslog Servers and SNMP Devices</b>						
Generic Devices	Any	—	SNMP (from Device) Syslog (from Device)	—	SW-host	