



# Supported Devices and Software Versions for Cisco Security MARS Local Controller 6.0.x

---

**Revised: December 17, 2009**

This document includes:

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

## Supported Local Controller Appliances

Cisco Security MARS version 6.0.x supports the following Cisco Security MARS Local Controller appliances:

### Generation 2 Hardware

- Cisco Security MARS 25 (CS-MARS-25-K9)
- Cisco Security MARS 25R (CS-MARS-25R-K9)
- Cisco Security MARS 55 (CS-MARS-55-K9)
- Cisco Security MARS 110 (CS-MARS-110-K9)
- Cisco Security MARS 110R (CS-MARS-110R-K9)
- Cisco Security MARS 110RF (CS-MARS-FIPS-K9)
- Cisco Security MARS 210 (CS-MARS-210-K9)

### Generation 1 Hardware

- 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)



---

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

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

- 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 6.0.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 LAN Controller](#)
- [Content Management](#)
- [Interoperable Supporting Services for Cisco Security MARS Local Controller 6.0.x](#)

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 events 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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Router	Cisco IOS 11.x	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	IOS
	Cisco IOS 12.2						
	Cisco IOS 12.3	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5	SNMP	HW	IOS
	Cisco IOS 12.4 (11) T2 <sup>3</sup>	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5, v9 <sup>4</sup>	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 <sup>3</sup>	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5, v9 <sup>4</sup>	SNMP	HW-switch	SWITCH-IOS
Cisco Switch	CatOS 6.x	Yes	FTP, SNMP, SSH, Telnet	Syslog, NetFlow v1, v5, v7 <sup>5</sup>	SNMP	HW	SWITCH-CATOS
	IOS 12.2						
	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, v9 <sup>4</sup>	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. Zone-based policy firewall feature is supported on IOS 12.4(11)T.
4. IOS/CatOS NetFlow v9 support is limited to parsing and storing only the fields that Cisco Security MARS already parses and stores for NetFlow v5/v7. This support is tested on IOS 12.4(11)T.
5. 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**

<b>Vendor</b>	<b>Supported Versions</b>	<b>SNMP-based Resource Monitoring<sup>1</sup></b>	<b>Protocol: Configuration Retrieval</b>	<b>Protocol: Event Retrieval<sup>2</sup></b>	<b>Protocol: Mitigation</b>	<b>Add to GUI As</b>	<b>CSV Keyword</b>
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, 7.2.4	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	PIX7X
	8.0, 8.0.3	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, 7.2.4	Yes	FTP, SSH, Telnet	Syslog	n/a	HW	ASA
	8.0, 8.0.3, 8.0.4	Yes	FTP, SSH, Telnet	Syslog/Secure-syslog	n/a	HW	ASA
	8.1, 8.1.2	Yes	FTP, SSH, Telnet	Syslog/Secure-syslog, NetFlow v9	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, 3.1.7, 3.1.8, 3.1.9	Yes	FTP, SSH, Telnet	Syslog	n/a	HW-switch (IOS 12.2 or CatOS)	FWSM
	3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5	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

**Table 2 Firewall Devices (continued)**

Juniper NetScreen	ScreenOS 4.0, 5.0, 5.4, 6.0	No	SNMP, SSH, Telnet	Syslog	n/a	HW	NETSCREEN, NETSCREEN50, NETSCREEN54, and NETSCREEN60 respectively
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 Compatible	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 Compatible	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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Network IDS	4.0	No	SSL	RDEP	n/a	HW	CiscoIDS4x
Cisco IDSM	4.0	No	SSL	RDEP	n/a	HW-switch	Not supported
Cisco Intrusion Prevention System (IPS)	5.0, 5.1	No	SSL	SDEE	n/a	HW,	CiscoIPS5x
	6.0, 6.0.1, 6.0.2, 6.0.3, 6.1, 6.2 (Backward compatible), 7.0	No	SSL	SDEE	n/a	HW,	CiscoIPS6x
Cisco IDSM-2 module	5.0, 5.1	No	SSL	SDEE	n/a	HW-switch	Not supported
	6.0, 6.0.1, 6.0.2, 6.0.3, 6.1, 6.2 (Backward compatible)	No	SSL	SDEE	n/a	HW-switch	Not supported
Cisco NM-CIDS	5.0, 5.1	No	SSL	SDEE	n/a	HW-router	Not supported
	6.0.x	No	SSL	SDEE	n/a	HW-router	Not supported
Cisco AIM-IPS	6.0.x, 6.1, 6.2 (Backward compatible)	No	SSL	SDEE	n/a	HW-router	Not supported
Cisco NME-IPS	6.1, 6.2 (Backward compatible)	No	SSL	SDEE	n/a	HW-router	Not supported

**Table 4 Network IDS and IPS Devices (continued)**

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 IntruShield	4.1	No	n/a	SNMP	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
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
ISS Proventia	Any	No	n/a	SNMP (through Site Protector as a Management Server)	n/a	As Site Protector agent (learn about Proventia via traps from Site Protector)	Not supported

**Table 4** *Network IDS and IPS Devices (continued)*

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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
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, 6.0 (backward compatible)	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**

<b>Vendor</b>	<b>Supported Versions</b>	<b>SNMP-based Resource Monitoring<sup>1</sup></b>	<b>Protocol: Configuration Retrieval</b>	<b>Protocol: Event Retrieval<sup>2</sup></b>	<b>Protocol: Mitigation</b>	<b>Add to GUI As</b>	<b>CSV Keyword</b>
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, 3.6.x, 4.0	No	n/a	SNMP (from ePO Server)	n/a	SW-host	Not supported
McAfee/Network Associates VirusScan	8.x	No	n/a	SNMP (from ePO Server)	n/a	as ePO agent (learn about hosts via the traps provided by ePO Server)	Not supported
McAfee Host Intrusion Prevention (HIPS)	6.0, 7.0	No	n/a	SNMP (from ePO Server)	n/a	as ePO agent (learn about hosts via the traps provided by 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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
eEye REM	1.0	No	MS SQL	JDBC (from REM server)	n/a	SW-host	Not supported
Qualys QualysGuard	ANY	No	n/a	HTTPS (using XML via API v. 5.1)	n/a	ODS	Not supported
McAfee/Foundstone Foundscan	3.0, 5.0, 6.0	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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
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

**Table 9** *Web Server Devices*

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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
Oracle Database	9i, 10g, 11g, 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 <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Secure Access Control Sever (ACS)	3.3	No	n/a	Syslog (from pnLog Agent)	n/a	SW-host	Not supported
	4.1.3, 4.1.4 4.2	No	n/a	Syslog	n/a	SW-host	SecureACS4 <sup>3</sup>
Cisco Secure ACS Solutions Engine	3.3	No	n/a	Syslog (from pnLog Agent running on remote logging host)	n/a	SW-host	Not supported
	4.1.3, 4.1.4 4.2	No	n/a	Syslog	n/a	HW	SecureACSSE
Cisco NAC Appliance <sup>4</sup>	4.1.3(CAM)	No	Yes	SNMP, Syslog	n/a	HW	NACApp

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. SecureACS can be given as device type for the agent on Windows Host.
4. NAC Appliance has been tested with stand alone CAS and NM Module CAS(Swiffer).

**Table 12 Syslog Servers and SNMP Devices**

Vendor	Supported Versions	SNMP-based Resource Monitoring <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
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 LAN Controller**

Vendor	Supported Versions	SNMP-based Resource Monitoring <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
Cisco Wireless LAN Controller	4.x, 5.x	No	SNMP	SNMP (from WLAN Controller)	n/a	HW	WLANController

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 14 Content Management**

Vendor	Supported Versions	SNMP-based Resource Monitoring <sup>1</sup>	Protocol: Configuration Retrieval	Protocol: Event Retrieval <sup>2</sup>	Protocol: Mitigation	Add to GUI As	CSV Keyword
CSC-SSM module	6.1, 6.2	No	n/a	Syslog	n/a	HW - under ASA	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.

# Interoperable Supporting Services

Supporting services are defined as those network services that extended functionality of Cisco Security MARS. [Table 15](#) lists those proven, tested, and version specific services.

**Table 15** *Interoperable Supporting Services for Cisco Security MARS Local Controller 6.0.x*

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
<b>Cisco Products</b>						
Cisco Security Manager	3.0 <sup>1</sup> , 3.1, 3.2, 3.2.1	n/a	HTTPS (policy lookup, not event data)	n/a	SW-host	Not supported
<b>SFTP Servers</b>						
Support for Cisco Security MARS configuration and event backups and device migration. See, <a href="#">Backup, Recover, Restore, and Standby Server Options</a> .						
Cygwin for Windows See <a href="#">Configure the Cygwin SFTP Server on Windows</a> .	1.5.25-12	SSH	n/a	n/a	n/a	n/a
OpenSSL, Windows XP	0.9.8g 19 Oct 2007	OpenSSH_5.0p1	n/a	n/a	n/a	n/a
OpenSSL, Windows 2000	0.9.8a 11 Oct 2005	OpenSSH_4.3p2	n/a	n/a	n/a	n/a
OpenSSL, Linux	0.9.7a 19 Feb 2003	OpenSSH_3.9p1	n/a	n/a	n/a	n/a
<b>NFS Servers</b>						
Support for Cisco Security MARS configuration and event backups and device migration.						
Microsoft Windows Services for UNIX (SFU) See <a href="http://technet.microsoft.com/en-us/interopmigration/b380242.aspx">http://technet.microsoft.com/en-us/interopmigration/b380242.aspx</a> and <a href="#">Configure the NFS Server on Windows</a> .	3.5	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a
Linux NFS See <a href="#">Configure the NFS Server on Linux</a> .	2, 3 <sup>2</sup>	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a

**Table 15** *Interoperable Supporting Services for Cisco Security MARS Local Controller 6.0.x*

Device Type / Vendor	Supported Versions	Protocol: Configuration Retrieval	Protocol: Event Retrieval	Protocol: Mitigation	Add to GUI As	CSV Keyword
Network Appliance NetApp-store  See <a href="#">Configure the NetApp NFS Server</a> .	FAS270 ver. 7.0.4	NFS (MARS archive mount, not retrieval of NFS server logs)	n/a	n/a	n/a	n/a
<b>External AAA Servers</b>						
Support for user authentication via the RADIUS protocol. See, <a href="#">Authenticating MARS Accounts with External AAA Servers</a> .						
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. Unidirectional support only.
2. Full support of NFS v4 is not provided, as it may require an additional authentication method.

