



Quick Install and Release Notes for Cisco Security MARS Appliance 4.2.2

Revised: July 24, 2009, 78-17805-01

These release notes are for use with the Cisco Security Monitoring, Analysis, and Response System (MARS), Version 4.2.2 running on any Local Controller or on any Global Controller. They provide the following information:

- [Introduction, page 1](#)
- [Supported Hardware, page 2](#)
- [New Features, page 2](#)
- [Upgrade Instructions, page 3](#)
- [Important Notes, page 7](#)
- [Quick Install Notes, page 9](#)
- [Caveats, page 13](#)
- [Product Documentation, page 22](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 22](#)

Introduction

Version 4.2.2 is now available as a patch upgrade to 4.2.1 of your MARS Appliance software. Registered SMARTnet users under the can obtain version 4.2.2 from the Cisco support website at:

<http://www.cisco.com/go/mars/>

And then click the **Download Software** link in the Support box on the right side of the MARS product home page.



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

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

Supported Hardware

Cisco Security MARS Version 4.2.2 supports the following Cisco Security MARS and Protego Networks MARS appliances:

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

Global Controller Appliances

- Cisco Security MARS GC (CS-MARS-GC-K9)
- Cisco Security MARS GCm (CS-MARS-GCM-K9)
- Protego Networks PN-MARS GC
- Protego Networks PN-MARS GCm

New Features

In addition to resolved caveats, this release includes the following new features:

- [Miscellaneous Changes and Enhancements, page 2](#)
- [New Vendor Signatures, page 3](#)

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 4.2.2:

- **Support for Firewall Services Module 3.1.** A new user-selectable option available when adding modules to IOS switch that has been defined as a managed reporting device or mitigation device.
- **Performance Improvements for Windows and Cisco IPS Log Processing.** Three dedicated processes run on the MARS Appliance, two of which replace earlier processes:
 - **csips.** This backend process uses RDEP to pull alerts from IDS 4.0 devices and SDEE to pull alerts from IPS 5.0 devices. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the two former processes named pnids40_srv and pnids50_srv.

- **csiosips**. This backend process uses SDEE to pull alerts from IOS IPS devices using SDEE. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the former process named pniosips_srv.
- **cswin**. This backend process uses MS-RPC to pull alerts from Windows devices. The alerts pulled are then processed and passed on to pnparsr from where they enter the system as all other events do.
- **Enhanced Topology Synchronization between Global and Local Controllers.** A new button on the Global Controller GUI permits the administrator to manually start and stop an improved topology synchronization process from the Zone Controller Information page (**Admin > System Setup > Local Controller Management**). New status messages display progress and facilitate trouble shooting. A new **pnpreset -s** CLI option can restore a Local Controller to Standalone from Monitor mode when the Global Controller cannot completely uncouple from (that is, delete) a Local Controller because of an unreliable network connection.
- **Enhanced Result Format Display for the Custom Column Query.** A query with a Custom Columns result format can now display up to 100,000 results. Previously the maximum (rank returned) was 5,000. If the total results per row exceeds 100 items, MARS provides a link that launches a popup window in which all the results are displayed. Rows with fewer than 100 items can be expanded (and collapsed) for viewing within the same window.

New Vendor Signatures

The following table describes the most recent signatures supported for each product or technology:

Product	Signature Version Supported
Cisco IDS 4.1/IPS 5.x	S244
McAfee Enterecept HIDS 4.1	Agent Version 40-56
ISS RealSecure Network Sensor 7.0	24.43
ISS RealSecure Server Sensor 7.0	24.43
McAfee IntruShield NIDS 1.8	1.8.80.4
Snort NIDS	2.3.3
Netscreen IDP 2.1	Idp2.1r3 Update 254
Enterasys Dragon 6.x	Latest signatures as of 08-15-2006
Symantec Manhunt	3.4.3 Update 53
Qualys QualysGuard 3.x	Latest Knowledge Base XML file as of 02-07-2005
Common Vulnerabilities and Exposures (CVE) Database	Latest as of 09-08-2005

Upgrade Instructions

The MARS upgrade packages are the primary vehicle for major, minor, and patch software releases. As administrator of the MARS Appliance, you should check the upgrade site weekly for patch upgrades. In addition to addressing high-priority caveats, patch upgrade packages update system inspection rules, event types, and provide the most recent signature support.

For detailed instructions on planning and performing an upgrade or install, refer to [Checklist for Upgrading the Appliance Software](#) in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Important Upgrade Notes

To ensure that the upgrade from earlier versions is trouble free, this section contains the notes provided in previous releases according to the release number. Please refer to the notes that pertain to the release you are upgrading from and any releases following that one.

Upgrade to 4.2.2

The following issues can occur during the standard upgrade process of a MARS Appliance:

- If you re-image your MARS Appliance from 3.4.3 to 4.2.2, your 3.x license key does not work on the new image. See CSCsg74922 for details.

The following issues can occur when upgrading your reporting devices:

- If you upgrade your Cisco FWSM modules to software version 3.1.2, you will be unable to parse the events identified in CSCsg31072.

Upgrade to 4.2.1

As identified in CSCse17864, CSCse22610 and CSCse22617, the changes in the case management feature requires that you close all cases before upgrading from MARS 4.1.x to 4.2.1. By closing the cases, you ensure that the device, report, and query information is copied to the case, assuming it still exists in the database.

Upgrade to 4.1.5

No important notes exist for the 4.1.4 upgrade.

Upgrade to 4.1.4

No important notes exist for the 4.1.4 upgrade.

Upgrade to 4.1.3

No important notes exist for the 4.1.3 upgrade.

Upgrade to 4.1.2(2042)

The following notes detail changes to the standard upgrade process:

- If you completed the 4.1.1 to 4.1.2 (2040) upgrade, verify whether the upgrade failed by entering ``pnlog mailto <SMTP server> <sender> <recipient>'` at the CLI. This command mails the MARS Appliance logs to the recipient. Open the e-mailed file attachment, and then open the newest `upgrade*.log` found in `/var/log/`. Successful upgrades from 4.1.1 (2022) to 4.1.2 (2040) include the following line:

```
Opening file:
/etc/data/secondarytables/reports/Report.0.Resource-Issues--IOS-IPS-DTM---All-Events.xml
```

If you do not see this line, then a problem occurred during the upgrade regardless of whether the **version** command reports 4.1.2 (2040).

- To upgrade from 4.1.1 or a *successful* or *unsuccessful* 4.1.2 (2040) to 4.1.2 (2042), download the package, perform the upgrade as defined in [Checklist for Upgrading the Appliance Software](#). If you are upgrading from 4.1.1, you must also execute the following command at the CLI of the upgraded MARS Appliance:

```
script -b patch_or_04_1_16.sh
```

The 4.1.2 (2042) image includes an additional command `script` that cleans the database of the data referenced in CSCsc31386. As a result of running the script, the total upgrade process from 4.1.1 to 4.1.2 (2042) may take much longer than previous releases; it depends on the amount of data stored on the MARS Appliance. For a MARS 200, it could double the normal upgrade time to two hours. To determine whether the script is still running, enter the following command and look for `patch_or_04_1_16.sh` anywhere in the output:

```
sysstatus -n 1 -b
```

Upgrade to 4.1.1

The following notes relate to changes in your system or configuration as a result of upgrading to MARS 4.1.1.

- Prior to the 4.1.1 release, CSA was identified by the device type name *Cisco CSA 4.0*. As part of an upgrade, any Cisco CSA 4.0 devices were renamed as *Cisco CSA 4.x*. This new name includes support for Cisco CSA 4.0 and 4.5.
- The new case management replaces the Escalate Incident functionality in MARS 3.4.4 and earlier. However, escalated incidents are not converted to cases during the upgrade process. Therefore, you must close all open escalations before upgrading to MARS 4.1.1 (CSCsb52057).

Required Upgrade Path

When upgrading from one software version to another, a prerequisite version is always required. This prerequisite version is the minimum level required to be running on the appliance before you can upgrade to the most recent version. [Table 1](#) identifies the upgrade path that you must follow to reach the minimum level required to upgrade to current version.

Table 1 Upgrade Path Matrix

From Version	Upgrade To ¹	Upgrade Package
releases prior to 2.5.6	Contact Cisco Support	n/a
2.5.6	3.1.1	pn-3.1.1.pkg
3.1.1	3.2.1	pn-3.2.1.pkg
3.2.1	3.2.2	pn-3.2.2.pkg
3.2.2 or 3.3.2 Beta	3.3.3*	pn-3.3.3.pkg
3.3.3	3.3.4*	pn-3.3.4.pkg

Table 1 Upgrade Path Matrix

From Version	Upgrade To ¹	Upgrade Package
3.3.4	3.3.5*	pn-3.3.5.pkg
3.3.5	3.4.1*	pn-3.4.1.pkg
3.4.1	3.4.2	pn-3.4.2.pkg
3.4.2	3.4.3	pn-3.4.3.pkg
3.4.3	3.4.4	pn-3.4.4.pkg
3.4.4	4.1.1	csmars-4.1.1.pkg
4.1.1	4.1.2 (2042) + script command	csmars-4.1.2.pkg ²
4.1.2 (2040) without error	4.1.2 (2042)	csmars-4.1.2.pkg ²
4.1.2 (2042)	4.1.3	csmars-4.1.3.pkg
4.1.3	4.1.4	csmars-4.1.4.pkg
4.1.4	4.1.5	csmars-4.1.5.pkg
4.1.5	4.2.1	csmars-4.2.1.pkg
4.2.1	4.2.2	csmars-4.2.2.pkg

1. An asterisk (*) next to a package name in this column identifies that this upgrade must be performed from the command line, as GUI support was lost with the closing of the upgrade.proteogonetwork.com website.
2. To upgrade from 4.1.1 or 4.1.2 (2040) to 4.1.2(2042), please review the special upgrade notes in the *Quick Install and Release Notes for Cisco Security MARS Appliance 4.1.2 (2042)*.

Downloading the Upgrade Package from CCO

Upgrade images and supporting software are found on the CCO software download pages dedicated to MARS. You can access these pages at the following URLs, assuming you have a valid CCO account and that you have registered your SMARTnet contract number for your MARS Appliance.

Top-level page:

<http://www.cisco.com/go/mars/>

And then click the **Download Software** link in the Support box on the right side of the MARS product home page.

Result; The Download Software page loads.

From this top-level page, you can select one of the following options:

- CS-MARS IPS Signature Updates Archives
- CS-MARS IPS Signature Updates
- CS-MARS Patches and Utilities (supplementary files)
- CS-MARS Recovery Software
- CS-MARS Upgrade Packages



Note

If you are upgrading from a release earlier than those posted on CCO, please contact Cisco support for information on obtaining the required images. Do not attempt to skip releases along the upgrade path.

For information on obtaining a CCO account, see the following URL:

- http://www.cisco.com/en/US/applicat/cdcrgrstr/applications_overview.html

Important Notes

The following notes apply to the MARS 4.1.x and 4.2.x releases:

- Do not use DISTINCT or SAME in queries, and do not run multi-line queries in Release 4.2.2. If you run such a query, the system times out after 20 minutes without returning any results. The message “Timeout Occurred” appears instead. You can use DISTINCT and SAME in a Query to create a rule with the Query interface.
- For Symantec AntiVirus, the Symantec agent hostname (AV client computer name) appears in the “Reported User” column of the event data. Therefore, you can define a query, report or rule related to this agent based on the “Reported User” value.
- The False Positive and Query pages (multi-column result format) have changed. You can now query on firing events that triggered false positives within a time interval. Such queries will render events that did not appear on the False Positive page. To ensure performance, the False Positive page only displays false positives from the most recent 10,000 firing events. To view additional false positives, you must perform a query.

The following notes describe new behavior based on the resolution of specific caveats. Be sure to check the upgrade notes for each release for important notes on data migration.

Reference Number	Description
CSCsc50636, CSCsc50652	<p><i>Issues:</i> Backend IPS process runs at 99% CPU when pulling large IP Logs</p> <p>The backend IPS process reaches 1GB in memory used when pulling IP Logs. The process names depending on the version on MARS that is running:</p> <ul style="list-style-type: none"> • In version 4.2.1 and earlier, the process names are pnids50_srv and pnids40_srv. • In version 4.2.2 and later, the process is named csips. <p>These related issues, are specific to pulling IP logs from Cisco IDS/ IPS devices. The symptom is that the backend IPS service consumes the system resources on the MARS Appliance. As an improper configuration of the sensor can significantly degrade the sensor performance as well as that of MARS.</p> <p><i>Workaround:</i> Ensure that settings for IP log creation on the sensor limit the size of the IP log (in terms of number of bytes or number of packets captured). Also, verify that IP packet logging is enabled only for signatures of interest and not for all signatures.</p> <p>In addition, the following release-specific maximums are enforced:</p> <ul style="list-style-type: none"> • In 4.2.1, a 100 file maximum is enforced for the log file queue when the MARS is configured to pull IP log files. Therefore, it may not pull every IP log file. In addition, the complete IP Log file may not be pulled, instead, data is pulled from the file starting 5 minutes before the alert was generated through the end of the file. • In 4.2.2, a 1,000 file maximum (up from 100 in 4.2.1) is enforced for the log file queue when the MARS is configured to pull IP log files. The complete IP Log file may not be pulled, instead, data is pulled from the file starting 1 minute (down from 5 minutes in 4.2.1) before the alert was generated through the end of the file. And last, 100KB is the maximum IP log size that can be pulled from a MARS Appliance.
CSCsb71309	<p><i>Issue:</i> In MARS release 3.4.4 and earlier, queries that are run from a Global Controller that has no results returned from any of the attached Local Controllers will show up as “In Progress” in the GUI.</p> <p>This occurs in a Global Controller/Local Controller environment, and only when a global query returns 0 results from every one of the Local Controllers.</p> <p><i>Workaround:</i> You may have to wait up to 10 minutes for a GC Query status to be marked as “Finished”, after all Local Controllers have finished running the query.</p>
CSCpn02175	<p><i>Issue:</i> Data computed or stored on a standalone MARS while in standalone mode will not be transferred to a Global Controller. Only data computed on an Local Controller that is currently monitored by a Global Controller will be pushed up.</p>
CSCpn02073	<p><i>Issue:</i> After renaming a cloud, clicking the cloud again causes an error.</p> <p><i>Workaround:</i> Refresh the page before clicking a renamed cloud.</p>

Reference Number	Description
CSCpn01270	<p><i>Issue:</i> The free-form search may not work for the following devices:</p> <ul style="list-style-type: none"> • Check Point Opsec NG FP3 • Cisco CSA, 4.0 • Cisco, IDS, 3.1 and 4.0 • ISS, RealSecure, 6.5 and 7.0 • Enterscept Enterscept, 2.5 and 4.0 • IntruVert IntruShield, 1.5
CSCpn00247	<p><i>Issue:</i> The automatic time-out feature built into the GUI does not work when the Summary page is left open with automatic refresh selected.</p> <p><i>Resolution:</i> Please log out of the system when you are no longer using it.</p>

Quick Install Notes

It is recommended that users read the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*. However, for those users who simply want to get the MARS Appliance up and running, the following two topics, taken from the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*, summarize the hardware installation and initial software configuration:

1. [Installation Quick Reference, page 9](#)
2. [Checklist for Initial Configuration, page 10](#)

Installation Quick Reference

[Table 2](#) provides an overview of the installation and initial configuration process. Following installation and initial configuration, see the following publications for information on how to use a browser and the HTML interface to fully configure your MARS Appliance to provide the security threat mitigation (STM) services you want from this installation:

- *User Guide for CS-MARS Local Controller Version 4.2.x*
- *User Guide for CS-MARS Global Controller Version 4.2.x*

Table 2 **Quick Reference**

Task	References in Install Guide
Use the rack mount kit to install the MARS Appliance in a rack.	Installing the MARS Appliance in a Rack
Connect the MARS Appliance to an AC power source.	Connecting to the AC Power Source
Connect network and console cables.	Connecting Cables
Turn on the appliance.	Powering on the Appliance and Verifying Hardware Operation
Verify initial power up.	Powering on the Appliance and Verifying Hardware Operation

Table 2 Quick Reference (continued)

Task	References in Install Guide
Perform initial configuration of the MARS Appliance.	Checklist for Initial Configuration, page 10
Configure the MARS Appliance to monitor reporting devices.	Next Steps

Checklist for Initial Configuration

Initial configuration of the appliance accomplishes several goals:

- Introduces the two user interfaces to MARS: the command line interface (CLI) and the web interface.
- Licenses the appliance.
- Prepares the appliance to monitor and communicate on your network.
- Configures the system time so that event correlation works properly.
- Ensures the system administrative account is configured properly.
- Ensures appliance is running the most recent version of software.

The following checklist describes the tasks required to initially configure your MARS Appliance. Each task might contain several steps; the tasks and steps within should be performed in order. The checklist contains references to the specific procedures used to perform each task.

✓	Task
☐	<p>1. Establish a console connection to the appliance.</p> <p>Initial configuration requires a console connection to access the CLI. You should establish this connection with the power turned off on the MARS Appliance. Three console connection options exist:</p> <ul style="list-style-type: none"> • A direct console connection to the appliance using a keyboard and monitor • A standard serial console connection between a computer and the appliance using a terminal emulation package • An Ethernet console connection between a computer and the appliance using a terminal emulation package <p>After you have chosen and configured your console connection, you must power up the appliance.</p> <p><i>Result:</i> The appliance is powered up and you can see the command line prompt through your console connection.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Establishing a Console Connection

✓	Task
☐	<p>2. Command Line Configuration: Setting the system administrative account's default password and configuring the interfaces.</p> <p>The command line configuration is separated into three tasks, each task being separated by a reboot of the appliance. The first task involves performing three to four procedures:</p> <ul style="list-style-type: none"> • Collect the information required to configure the appliance to operate optimally on your network. • Log in to the appliance and change the password associated with the system administrative account (padmin). • Configure the eth0 network interface, specifying the default gateway and IP address and network mask pair for that interface. • (Optional) Configure the eth1 network interface, specifying the IP address and network mask pair for that interface. <p>Each MARS Appliance has two Ethernet interfaces: eth0 and eth1. The eth0 interface is the dedicated interface used for collecting event data and logs from your network. The eth1 interface is intended for use in an out-of-band management (OOBM) network or for a console connection. Therefore, your default gateway and IP address/mask values should focus on the network connections to be used to monitor the data streams of reporting devices, and these settings should be applied to eth0.</p> <p>Note The MARS Appliance does not allow you to configure both of its interfaces on the same network.</p> <p><i>Result:</i> The default password is no longer associated with the system administrative account and the appliance is more secure. Also, the eth0 is configured to communicate on your network. When you complete the IP address configuration changes for either, the appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Configuring Basic Network Settings at the Command Line • Change the Default Password of the System Administrative Account • Specify the IP address and Default Gateway for the Eth0 Interface • (Optional) Specify the IP Address and Default Gateway for the Eth1 Interface
☐	<p>3. Command Line Configuration.</p> <p>The second task of the CLI configuration involves setting the hostname of the appliance. The hostname is used to uniquely identify which appliance collects a specific log and which appliance fires an inspection rule. This unique identity is especially important in an environment where Global Controller is running. To complete this task, you must:</p> <ul style="list-style-type: none"> • Log in to the appliance using the system administrative account and the new password. • Set the hostname of the appliance. <p><i>Result:</i> The hostname is configured for the appliance. The appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Specify the Appliance Hostname

✓	Task
□	<p data-bbox="186 283 600 315">4. Command Line Configuration.</p> <p data-bbox="227 325 1469 483">The third and final task of the initial CLI configuration involves specifying those settings that help ensure the integrity of the event correlation and complete your network connection, allowing access to the appliance from other hosts on the network. In other words, after you complete this phase, you can connect to and complete the appliance configuration using a non-console connection from any host on your network. To complete this task, you must:</p> <ul data-bbox="235 493 1250 756" style="list-style-type: none">• Log in to the appliance using the system administrative account and the new password.• Set any additional static routes.• Set the clock.• Set the NTP server settings.• Set the DNS domain name.• Connect the appliance to the network (that is, plug in the Cat 5 cables.) <p data-bbox="227 766 1469 861"><i>Result:</i> Now you have network connectivity. You can access the CLI interface using an Secure Shell (SSH) client on any host that can reach the appliance, and you can log in to the web interface to complete the initial configuration.</p> <p data-bbox="227 871 535 903">For more information, see:</p> <ul data-bbox="235 913 673 1050" style="list-style-type: none">• Specify the Time Settings• Set Up Additional Routes• Completing the Cable Connections

✓	Task
☐	<p>5. Complete initial configuration using the web interface.</p> <p>After you have completed the cable connections to the MARS Appliance, defined the required network connection settings, and specified any additional default routes, you can start the web interface configuration process. Verify the configuration settings of your browser before configuring the MARS Appliance (see Web Browser Client Requirements).</p> <p>During this phase, you configure the following:</p> <ul style="list-style-type: none"> • Appliance license • Zone identification (Global Controller only) • E-mail server identification • DNS addresses • E-mail address for the system administrative account (pnadmin) • TACACS/AAA login prompt settings <p><i>Result:</i> You have configured your appliance to communicate on the network, properly correlate events, and issue system e-mails to a monitored e-mail address.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Completing the Configuration using MARS web interface • Licensing the Appliance • Verifying and Updating Network Settings • Specifying the DNS Settings • Configure E-mail Settings for the System Administrative Account • Configure TACACS/AAA Login Prompts
☐	<p>6. Upgrade the appliance to the most recent software version.</p> <p>The software version determines the currency of signatures, system inspection rules, features, and bug fixes. An important part of your security solution is ensuring that you maintain the most up-to-date software on the MARS Appliance. This process involves preparing an upgrade strategy and selecting a method, determining your current version, identifying the most recent version, and downloading and applying all intermediate versions of the software.</p> <p><i>Result:</i> The appliance is running the most recent version of software.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Checklist for Upgrading the Appliance Software

Caveats

This section describes the open and resolved caveats with respect to this release.

- [Open Caveats - Release 4.2.2, page 14](#)
- [Resolved Caveats - Release 4.2.2, page 19](#)
- [Resolved Caveats - Releases Prior to 4.2.2, page 22](#)

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://www.cisco.com/support/bugtools>

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Open Caveats - Release 4.2.2

The following caveats affect this release and are part of supported devices or compatible products:

Reference Number	Description
CSCsg31072	Connection IDs in %FWSM-6-30201x are too big. getting parser error
CSCsf31561	FWSM 3.1 syslogs FWSM-3-717001 till FWSM-4-717031 have missing colon
CSCsf29424	MARS servlet can differentiate the interfaces to improve match accuracy
CSCsg00377	show resource usage command reports incorrect connection usage
CSCsg31072	MARS not able to parse %FWSM-6-30201x syslog from FWSM3.1 devices
CSCsg35110	MARS Global Controller cannot import a Local Controller SSL security certificate if the LC zone name contains a forward slash character (/)

The following caveats affect this release and are part of MARS.

Reference Number	Description
CSCsg13767	SuperV doesn't detect/restart processes
CSCsg10787	CATOS discovery failing.
CSCsg08166	Unable to discover ASA 7.0 Error:There is no Error Log for this Device
CSCsg06339	Getting a Timeout Occured error when running a query with != as service
CSCsg04079	Lotus Notes client gets JavaScript error with emailed MARS report
CSCsf99844	wrong values for current connections using CLI "show resource usage"
CSCsf98682	windows 2003 pulling: should proceed if pulling appl/system evt log fail
CSCsf32615	Archiving can fill the / partition, disabling the Mars

Reference Number	Description
CSCsf31228	Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031
CSCsf31228	Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031
CSCsf31207	Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs
CSCsf31207	MARS doesn't support new/changed FWSM 3.1.3 maintenance release syslogs
CSCsf31121	Exception in Case Management code when deleting a report
CSCsf30116	Event Rate on the Top Destination Port graph is not correct
CSCsf26715	Inaccuracy in per-context memory utilization for multi-context devices
CSCsf18192	Slow rendering of the GC Summary page
CSCsf12825	GUI should prevent edit/delete of system-context PIX/ASA 7.0 devices
CSCsf11651	Device resource monitoring incorrectly samples 5 sec CPU instead of 5 min
CSCsf06819	eEye: vulnerabilities are not displayed for some (old) hosts
CSCsf04540	MARS: Javascript Error w/ Email Report-5496: document.getElementById
CSCse99039	Redundant tab add available module under Device type Cisco IOS 12.2
CSCse98029	Occasionally corrupted event data enters into MARS database
CSCse91636	csv report contains a number (session Id probably) and not event type
CSCse88764	can't access a ftp server with a user ID/password including @
CSCse85973	Deleted windows custom parsing templates show up in the SW apps dropdown
CSCse85564	Cannot add devices to a report which has more than 35 devices.
CSCse84962	eEye: MARS does not remove resolved vulnerabilities from host info
CSCse82042	Change the Device Type Version for FWSM
CSCse82022	Unable to view reports starting with #sign in csv format
CSCse82017	View HTML option for reports turns back to default report format - csv
CSCse78738	FWSM ifspeed incorrectly reported as 0 for per-context vlan interfaces
CSCse78089	Unable to upgrade CS-Mars via GUI
CSCse73868	pnrestore command should support end-time argument in the command line
CSCse73788	MARS rediscovers Juniper Netscreen firewalls with wrong OS
CSCse60240	CS-Mars - report for old events include real-time events
CSCse56632	when adding a device and adding more than 50 monitored networks, browser
CSCse54976	Some incidents are not written to DB
CSCse54808	The time stamp shown by the pndbusage command is incorrect.
CSCse52782	can't change run-time to day for "Resource Issues: Server - Top Reporting
CSCse52217	Customer gets pink box in GenericHostDeviceEditManagement.jsp
CSCse51438	Login session timeout not detected when a real-time (LLV) query resumes
CSCse49004	MARS 4.1.5 does not correctly parse IDS/IPS AIC FTP signatures
CSCse45884	LLV query causes client CPU to go to 100%
CSCse45018	MARS is unable to parse NetScreen 5.x syslogs
CSCse42953	CS-Mars - unable to show L2 path when source and destination in same net

Reference Number	Description
CSCse39426	superV & pnparsers restarts causes interruption in log pulling
CSCse38565	Re-importing Symantec AV client CSV doesn't work
CSCse38356	Windows pulling gets stuck for one IP due to invalid content in evt log
CSCse35758	Inability to trace when first and last event occurred on a query
CSCse35758	Inability to trace when first and last event occurred
CSCse35420	Interface error rate formula needs correction in the source code
CSCse34600	configurable SNMP timeout support
CSCse34407	Query Tab -> Multi column query returns wrong results.
CSCse33688	no events under Cisco Switch-IOS 12.2
CSCse33172	Invalid id used in DbClient::retrieve() 0
CSCse32600	Exception with Query All Matching Sessions or All Matching Events
CSCse32591	dealing with duplicate hostnames in VA import
CSCse31722	Cloud toggle only works on first page of reporting devices
CSCse29860	UTC and GMT time zone missing
CSCse26964	CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS
CSCse23191	Disable 'No Pager' cmd sent by MARS to PIX, ASA, FWSM firewalls
CSCse23176	MARS Global Controller not producing alerts when losing LC communication
CSCse23051	viewing report of query type of MAC addresses report got pink box
CSCse22838	can't find priority for CSA NT-Event-Log events
CSCse21936	Daylight savings time affects the custom parser's received time field
CSCse21626	Clicking activate is not taking effect
CSCse20593	CSM device type could not be added one time (OK most times)
CSCse18865	scalability issues in "My Reports" page
CSCse18816	UI takes 99% CPU, hanging browser and slowing system while expanding all
CSCse17936	5K Lines Custom Query fails
CSCse13038	CS-Mars - learning of McAfee agents with invalid names
CSCse11258	After group is deleted, items under "All" group not shown
CSCse10945	Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)
CSCse09127	Failed load from csv returns incorrect status
CSCse03237	Changes made to GC network groups are not propagated to active LC rules
CSCse03097	CheckPoint LEA record comes to MARS later and later
CSCse00668	rule definition changes can lead to empty reports
CSCse00626	IP Management -> device group displays hosts only
CSCsd96067	5k query report emails sizes
CSCsd96048	Case management email sizes with multiple 5k reports attachments
CSCsd95582	Both successful/failed mitigation reports show same results
CSCsd92916	CS MARS - Raw Ip Addresses in Custom Query email have incomplete URL

Reference Number	Description
CSCsd92285	Security Dev Edit page does not check for existing ip address conflict
CSCsd89457	Incorrect handling of time range for rules that fire periodically
CSCsd86896	Clicking the clear button when editing the query type doesn't work
CSCsd84350	CS-MARS/CSM: Cred change on CSM side not checked.
CSCsd84094	using rules in query/report definitions
CSCsd74283	changing report-result retention limit
CSCsd73486	Mars: Not able to recognize the event type for ISAKMP and IPsec messages
CSCsd69137	Default Group in Scheduler need to be made to Run On Demand
CSCsd69063	Reported User with single-quote (') causes oracle error
CSCsd61749	pnrestore doesn't restore static routes or ntp settings
CSCsd53173	Retrieve raw messages doesn't properly update the progress percentage
CSCsd48231	inaccurate total number of retrieved events/sessions displayed by Query
CSCsd37005	user must be able to change own password
CSCsd28590	CS-MARS - Inactive Reporting Device Rule is not configurable
CSCsd25868	CS-MARS Inactivity report is not updated in netflow processing
CSCsd22832	Attempt to remove IP subnet from IP Management fails, with error
CSCsd15695	Summary dashboard showing incorrect statistics for false positives
CSCsd13969	resetting italics for GUI links
CSCsd06302	device name with single quote causes pink box
CSCsc97963	Netscreen logical interfaces (vlan intf) not discovered
CSCsc91572	Multiple target ports in IDS event show up as 'port 0' in query
CSCsc78878	snort signature 2570 incorrectly mapped
CSCsc58485	5 tuple information missing from downloaded raw log file
CSCsc48498	CS-MARS: Upgrade from 3.4.x fails
CSCsc46884	free form reported user input for rules, reports
CSCsc42396	CS-MARS Viewing IP of grouped sessions throws Exception, no Time var
CSCsc15590	MARS not including all events in a report, query returns events fine
CSCsc04484	LC Rule/Report list shows empty after deletion of GC group
CSCsb80082	Deleting a LC w/o exchanging certs doesn't reset mode to Standalone
CSCsb77550	CSV re import of CSA and Symantec agents unsuccessful
CSCsb67871	Got System Error In GC After Re-installed New Version In LC
CSCsb64587	After GC restore, LC certificate missing
CSCsb15330	Path calculation broken due to out-of-sync event IDs
CSCsb12137	MARS - SQL maximum open cursors exceeded resulting in blank reports
CSCpn03077	GC, sys error when adding a LC which was added to GC already
CSCpn03074	CS-Mars GC - Incident page - View & Show buttons do not work
CSCpn03057	Copied rules have shortened year in front, which is confusing (ex. 0

Reference Number	Description
CSCpn03052	JBoss 'OutOfMemoryError ' when accessing Management/Event Management
CSCpn02976	GC:LC - Communication issues after time zone change
CSCpn02973	Not able to downgrade a security analyst to Notification only user
CSCpn02968	Network group search is not working for "All IP addresses
CSCpn02901	GC/LC, rule does not display user <cxu> but allows such cfg
CSCpn02883	Event management search works only for event description
CSCpn02869	Rules editing: changing entry for select window pulldown after error
CSCpn02804	Replay History feature not working correctly
CSCpn02688	GC/LC: gc lc displayed diff time rage for the same global report
CSCpn02666	Batch Query Results with one item returned -> no data in graph in em
CSCpn02656	System error occurs when # of java connections runs out
CSCpn02653	(FA Credco) No way to specify "!Keyword" without a good "keyword"
CSCpn02594	LC: Path/Mitigate link throws up a pink box after the device has bee
CSCpn02574	Time change on system causes GC/LC communication problem
CSCpn02566	rebooting mars while it is upgrading cause the box not accessible
CSCpn02558	"Agent" didn't be removed correctly
CSCpn02549	JavaScript Error from ViewReport when clicking Edit/Clear
CSCpn02511	need to fix errors in affected os
CSCpn02470	Server csv function could not handle special characters in password
CSCpn02414	GC/LC user rule is too long to fit into a page if keyword is long
CSCpn02410	rule was not fired because Oracle log used upper case for user
CSCpn02398	XML escaping errors in Keyword Search in Rule
CSCpn02385	Applied \$TARGET01 for GC Query Source IP resulted in "resultCounter
CSCpn02383	IIS parsing must be separated from Windows log
CSCpn02333	LC: After pnrset -g, should clear out former zone's information
CSCpn02251	License: Upon entry of 100 license onto 100e, need to restart pnpars
CSCpn02177	Docs: Filesystem Check after 22 reboots
CSCpn02061	Saving .csv files under WinXP SP2 results in .htm extension
CSCpn02011	discovery for special passwd 1"1 failed
CSCpn01489	BQ: Query summary doesn't mention "severity" if it's a criterion
CSCpn01438	Batch Query: Under high load, some batch queries may not complete
CSCpn01416	Select: Temp paging fix on Notification-SNMP page
CSCpn01398	Unable to shutdown an interface
CSCpn01382	Security device type hosts don't show up in IP management
CSCpn01319	pnrset command does not cause reboot
CSCpn01293	Host OS listing needs cleaning
CSCpn01219	Cleanup script for invalid /etc/qpage.conf entries

Reference Number	Description
CSCpn01134	Cloud name input box accepts invalid characters
CSCpn01051	Browser: Open non-supported browser to MARS causes other browsers to
CSCpn01045	Archiving: Need better error message
CSCpn00908	"Domain" in Configuration page - no use
CSCpn00610	Backend logs can be out of order in the view page
CSCpn00596	RelNote: Events and Sessions counts can be out of synch
CSCpn00586	nasl message text needs to be changed
CSCpn00455	Graph doesn't refresh when a cloud is renamed
CSCpn00293	using TAB in editing fields
CSCpn00259	Setting Logging Level for "GUI" to "Trace" and saving -> "Debug"
CSCpn00212	Graphgen crashes when there are many non-existent devices
CSCpn00183	Adding devices w/o "Activate" can cause "messy" graph
CSCpn00173	Nessus should check pre-NAT address instead of Post-NAT address
CSCpn00166	Inconsistent behavior for "ANY" in Rules and Queries
CSCpn00146	Identical reports differed by slashes and dashes result in conflicts

Resolved Caveats - Release 4.2.2

The following customer found or previously release noted caveats have been resolved in this release.

Reference Number	Description
CSCsf97193	Needs to mark denied IPS/IDS events as system defined false positives
CSCsf30130	15 unknown device events for FWSM3.1
CSCsf28294	destination and source ip are switched for syslog %FWSM-6-302013
CSCsf26873	Exception occurs when trying to sync a suspended LC
CSCsf26869	The status is not correct after clicking 'Suspend' button
CSCsf26867	Not to refresh the Zone page after clicking the Topo Sync button
CSCsf26749	pnparser stops processing events from Checkpoint devices
CSCsf26648	csips and csiosips modules are not brought up after upgrading
CSCsf25347	On demand report always in progress
CSCsf25071	Upgrade and install pkg should include updated scripts
CSCsf23388	Set shorter timeout value
CSCsf23252	missing source and destination ip for %FWSM-6-315011
CSCsf21669	The Next button on Incidents page only works once.
CSCsf21661	Details button on Local Controller Management page causes GC hanging
CSCsf20160	GC Port 8444 does not respond.
CSCsf19891	Mars not able to purge older reports (ORA-01654 error)

Reference Number	Description
CSCsf19751	pnparser stops processing events from all devices on some restarts
CSCsf19675	inactive access-list didn't be parsed correctly
CSCsf18695	Mars is pulling events when the device credentials are wrong
CSCsf18308	rebuild the rpcclient2 binary for 4.2.2 phase 2 build
CSCsf18199	The error message doesn't indicate the wrong device type
CSCsf15731	Two system contexts shown after discovery with hostname changed
CSCsf14373	improve java.io.StreamCorruptedException handling in GC/LC communication
CSCsf12428	pnparser needs to set correct device event types, related to CSCpn03044
CSCsf11625	Some PIX 6.3 events are not being parsed by MARS
CSCsf02057	"pnreset -j" malfunctioning on GC
CSCsf01907	MARS 4.2.1 fails to parse NAC message with blank hostname
CSCsf01761	Netflow five tuple wrongly reversed for certain unidirectional flows
CSCsf00530	Upgrade libcurl version to 7.15.4
CSCse99322	MARS stops functioning after listener.log reaches 2 GB in size
CSCse97518	Internal Beta customer gets pink box in IncidentDetails.jsp
CSCse95602	pnlog mailto does not package all the logs
CSCse89628	paging error when view recent incidents other than ' within one hour
CSCse89415	NAC syslog HOST=AUTHORIZED triggers Host Posture Validation Rejected
CSCse87332	SNMP RO community string error for pnmac not showing problem client IP
CSCse81985	MARS code in dead-lock condition with IP logging turned on for IDS
CSCse80762	netflow from 'Cisco Switch-CatOS ANY' device type is dropped
CSCse79191	Enable MARS 20R to be managed by a GC.
CSCse76930	FWSM 3.1 Support
CSCse76304	MARS GC - Device list pink box when searching All zones for a device
CSCse72333	[CSIRT] MARS GC won't display Summary page - too many incidents
CSCse72302	[CSIRT] MARS GC won't display Incidents page - too many incidents
CSCse68305	Top User Report incorrectly recognizes ??? as a username
CSCse61179	parsing error for PORT_SECURITY-2-PSECURE_VIOLATION event syslog message
CSCse56473	High pnparser CPU usage in processUserInfo thread
CSCse55634	System Error when viewing User confirmed false positives - huge agent id
CSCse55575	Discovery from Topology Map records two device types for one device
CSCse55090	PIX/ASA 7.0 syslog parsing error for message number 415006
CSCse53573	false alarm error in janus_log: corruption in shared buffer
CSCse53541	Customer gets pink box in ViewReport.jsp
CSCse53492	Customers get pink box in SubmitDevicePage.jsp
CSCse53424	MARS CSM error message spelled incorrectly: "occured
CSCse53407	IP TO VAL: errors while inserting entries into the table

Reference Number	Description
CSCse52169	Customers get pink box due to ReportChart.jsp
CSCse51311	Copyright date on license agreement page is stale
CSCse50890	Customer gets pink box in AddRoute.jsp
CSCse50859	Customer gets pink box cancelling creating a service group
CSCse49992	An unknown device type for FWSM
CSCse48877	XSS vulnerability in CS-MARS GUI
CSCse40803	Parsing error for FWSM-3-106011
CSCse37274	CS-MARS Parsing error for ASA and PIX Syslog Message ID 713052
CSCse35845	notification user should not be listed in case owner dropdown filter
CSCse22751	Case mgmt fails to 'Expand All' for attached report
CSCse20469	Custom Column Query: total number doesn't match after Expand +
CSCse11072	event/session retrieve inefficient when overlapping partitions exist
CSCse11059	Customer gets pink box in IPManagement defining existing object
CSCse08771	Customer gets pink box in Incidents
CSCse07425	JVM is using up to 1.5 GB on a GC
CSCse06057	Custom Columns query output missing some info
CSCse05822	re-sizing Oracle tablespaces for CS MARS 20, ORA-1654
CSCse03082	add device time in CheckPoint raw message
CSCse00251	process_inlinerep_srv ignores Rule Groups as selection/filtering criteria
CSCsd97886	Oracle Audit log retrieval: Time synchronization issue
CSCsd97115	GUI error logs with user_id = 201
CSCsd85123	CS-MARS unable to parse PIX-4-400036: IDS:6052 DNS high error
CSCsd84124	Sudden Increase in Traffic anomaly doesn't always attach 30 sessions
CSCsd61563	no new event written in MARS, pnparsers stops writing data, sb not full
CSCsd47801	MARS fails to collect all events from IPS devices
CSCsd43484	CS-MARS Events from CSA MC shows invalid eventText field
CSCsd35692	pnesloader gets stuck, stops processing event sb data, with low cpu usage
CSCsd29496	Expand All within incident and add to case --- expanded view is not stored
CSCsd29193	CLI: The sysstatus command allows a user to write to the file .toprc
CSCsd25002	entering IP addresses in free format
CSCsd24729	FWSM-4-313004, FWSM-4-106100 not parsed correctly
CSCsd10627	MARS fails to re-establish communication with IPS appliance
CSCsc65771	MARS doesn't correctly handle protocol field in message FWSM-4-500004
CSCsc63433	Missing datawork for Windows Security Events related to group membership
CSCsc59275	PIX/ASA: 4 new event types, 1 parsing errors
CSCsc49248	Drop rule for Inactive CS-MARS Reporting Device does not work.
CSCsc22331	Incorrect event grouping for FWSM translation messages

Reference Number	Description
CSCsc15667	MARS need to restart processes to connect to IDS sometimes
CSCsc03387	MARS does not parse: FWSM-4-405001
CSCsb41606	Could not subscribe to events: out of subscriptions
CSCpn02938	Multi-thread support for pulling events from IPS/IDS/Windows

Resolved Caveats - Releases Prior to 4.2.2

For the list of caveats resolved in releases prior to this one, see the following documents:

http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html

Product Documentation

For the complete list of documents supporting this release, see the release-specific document roadmap:

- *Cisco Secure MARS Documentation Guide and Warranty*

http://www.cisco.com/en/US/products/ps6241/products_documentation_roadmaps_list.html

Lists document set that supports the MARS release and summarizes contents of each document.

For general product information, see:

<http://www.cisco.com/go/mars>

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

© 2007 Cisco Systems, Inc. All rights reserved.