



Quick Install and Release Notes for Cisco Security MARS Appliance 4.2.1

Revised: July 24, 2009, 78-17784-01

These release notes are for use with the Cisco Security Monitoring, Analysis, and Response System (MARS), Version 4.2.1 running on either a Local Controller or on a Global Controller. They provide the following information:

- [Introduction, page 1](#)
- [New Features, page 1](#)
- [Upgrade Instructions, page 8](#)
- [Important Notes, page 11](#)
- [Quick Install Notes, page 12](#)
- [Caveats, page 16](#)
- [Product Documentation, page 43](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 44](#)

Introduction

Version 4.2.1 is now available as a patch upgrade to 4.1.5 of your MARS appliance software. Registered SMARTnet users under the can obtain version 4.2.1 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.

New Features

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

- [Cisco Security Manager \(Security Manager\) Policy Lookup Integration, page 2](#)




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

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

- [Increased Ease of Deployment via Relayed Syslog Handling Feature, page 4](#)
- [Low-Latency, Real-Time Event Query, page 4](#)
- [XML Incident Notification, page 4](#)
- [Disk Usage via CLI, Events, Inspection Rules, and Reports, page 5](#)
- [Improved Performance of Software Upgrades, page 5](#)
- [Low-End Monitoring Solution: MARS 20R, page 5](#)
- [Distributed Threat Management \(DTM\) Enhancements, page 5](#)
- [Case Management Enhancements, page 6](#)
- [Using ISS Site Protector to Configure ISS NIDS and HIDS, page 6](#)
- [Miscellaneous Changes and Enhancements, page 7](#)
- [New Vendor Signatures, page 8](#)

Cisco Security Manager (Security Manager) Policy Lookup Integration

This feature allows you to map a traffic-related syslog message back to the firewall policy that triggered the syslog, thus helping you to fix firewall configuration-related network problems, configuration errors, and to fine-tune existing firewall policies.

Policy lookup is achieved by integrating MARS, the monitoring product and Security Manager, the device management product. The MARS web interface now includes a new Security Manager Policy Table Lookup icon  in the session/event display for all syslog events related to traffic. When you click this icon, MARS securely connects to Security Manager, retrieves the policy list, and displays it with the access rule that triggered the traffic syslog selected.


This integration enables policy lookup for the following device types:

- Cisco IOS 12.x
- Cisco PIX 6.x and 7.0
- Cisco Switch-IOS 6.x
- Cisco ASA 7.0
- Cisco FWSM 2.x

**Note**

This feature is available beginning with MARS 4.2.1 and Security Manager 3.0. In Security Manager 3.1, you can open the MARS web interface.

The following caveats exist for the Security Manager integration:

Reference Number	Description
CSCse03254	<p><i>Issue:</i> Inconsistent population of CSM icon for ICMP messages</p> <p><i>Description:</i> The same events received by MARS can display the Security Manager Policy Table Lookup icon  inconsistently between the low-latency, real-time event query and standard queries, such as sessions ranked by time. Specifically, the icon will not appear in the low-latency, real-time query, but it may appear in queries against sessionized events.</p> <p>This behavior is expected. When MARS receives events, they are parsed, sessionized, written to an event shared buffer, and then written to the database. Because sessionization takes time, sometimes keeping an event in cache for 2 minutes, the low-latency event query displays events right after parsing, but before sessionization. Displaying the event at this point allows the low-latency query to achieve a close to real-time effect. For some events, parsing cannot determine some part of the 5-tuple data, such as a destination address. Later, sessionization later fills in such missing data using configuration data. As a result, the 5-tuple data displayed by the low-latency event query can be different from values stored in the database, which are used to populate the standard queries.</p> <p><i>Workaround:</i> None.</p>
CSCse19392	<p><i>Issue:</i> CSM: Policy query for ICMP traffic</p> <p><i>Description:</i> An error can occur with the policy query if you discover a device configuration with Security Manager but do not submit it in Security Manager. The following error message is an example of this issue:</p> <pre data-bbox="480 982 1503 1140"><190>2312080: *May 9 23:50:02.199: %SEC-6-IPACCESSLOGDP: list permit-all permitted icmp 10.2.3.8 -> 10.4.21.2 (0/0), 1 packet An error occurred while querying policies from Cisco Security Manager. Reason: Failed to retrieve policy information from CSM. Reason: Cisco Security Manager Internal error: Failed to get interfaces in the device! The device LC2DTM was discovered by CSM without any errors.</pre> <p><i>Workaround:</i> Before you perform policy queries, verify that all discovered devices have been submitted in Security Manager.</p>
CSCse20041	<p><i>Issue:</i> CSM policy query icon for NetFlow events</p> <p><i>Description:</i> The Security Manager Policy Table Lookup icon displays for NetFlow events even though they are not triggered by an ACL. This extra event data allows you to determine whether there is a policy permitting that traffic, which ensures you are able to tune accordingly.</p> <p>Note Because this is NetFlow data, it may not match the exact ACL or match multiple ACLs.</p> <p><i>Workaround:</i> None.</p>
CSCse20691	<p><i>Issue:</i> CSM:Policy query icon</p> <p><i>Description:</i> The Security Manager Policy Table Lookup icon displays only for those events with 5-tuple event data (source and destination address, protocol, source and destination port). In the MARS web interface, the all matching events query displays the text “session five tuple” for events with no 5-tuple event data. These events will not have a policy query icon.</p> <p><i>Workaround:</i> None.</p>

Increased Ease of Deployment via Relayed Syslog Handling Feature

You can rapidly deploy MARS by forwarding messages from existing syslog-ng or Kiwi syslog servers. This feature eliminates the network and device changes required to insert MARS into an operational network. You no longer have to configure each network device to publish its syslog messages directly to MARS, which saves time, avoids device change approval processes, preserves packet processing performance of the network devices, and ensures that daily network operations proceed uninterrupted.

**Note**

Solaris/Linux syslogd is not supported as its message format does not include the host and timestamp information for the device that originates the message.

This relay feature also allows the correlation and inspection of syslog messages from reporting devices, such as those on the DMZ, for which corporate policies might prohibit the existence of or connection to configuration information.

If your network devices already publish syslog messages to syslog-ng or Kiwi syslog servers, simply configure those servers to forward messages to the MARS Appliance and identify the syslog servers in MARS. MARS parses the syslog messages generated by the following devices: Cisco PIX, Cisco IOS, Cisco CatOS, Cisco ASA, Cisco FWSM, Cisco VPN 3000, Cisco Secure ACS, Snort IDS, Juniper/Netscreen firewalls, Solaris, Redhat Linux, and Microsoft Internet Information Server (ISS). For other devices, you can define custom log parsers.

The MARS Appliance can begin processing and storing the events while you define the reporting devices using the MARS web interface. You still must define the reporting device by IP address and device type in MARS to ensure proper event correlation; however, you are not required to configure device to publish syslog messages directly to MARS.

Low-Latency, Real-Time Event Query

MARS can now display incoming raw events in real-time with a real-time event viewer query option. Previous releases of MARS had a real-time event query that sessionized and stored events before displaying them. This could incur delays of at least 2 minutes. The real-time raw event viewer operates in memory and has a 5-second delay. All parsed raw events are passed to the sessionizing module for further analysis.

To access the real-time event viewer, define a new query with **All Matching Events**, or **All Matching Event Raw Messages** as the Result Format, then select **Raw events** as the Real Time parameter.

XML Incident Notification

The new XML incident notification feature enables automated workflow integration with help desk and ticketing systems. XML incident notification is configured as an alert action of a rule. An XML data file is e-mailed to a specified recipient or group when the rule fires.

Based on the published schema (XSD file), you can develop custom parsing scripts to drive your ticketing or help desk system. You can also compress the e-mailed XML data file using gzip compression. XML incident notification benefits are as follows:

- The XML data file includes all information related to the incident that can be seen on the web interface, except for Path/Mitigation information
- Recipients do not have to log in to MARS to view the incident data

- The XML schema definition allows integration of the XML notifications with third-party applications

Disk Usage via CLI, Events, Inspection Rules, and Reports

To address the operational planning needs of storage and archive, MARS 4.2.1 includes two new CLI commands that provide database and disk usage information. It also includes a new event, inspection rule, and report to provide the information and notify the administrators of upcoming purging events.

The two new commands are **dbusage**, which identifies current database usage and future allocation plans through either unused partitions or purging of oldest data, and **diskusage**, which displays the amount of disk space available on all partitions.

The new event, *CS-MARS DB partition filling up causing the next partition to be purged soon*, notifies the administrators when the current partition is 75% full and switching to the next partition will result in data being purged from a previously used partition. The system inspection rule and report allow you to monitor when this event fires. The inspection rule is *System Rule: CS-MARS Database Partition Usage*, and the report is *Resource Utilization: CS-MARS-All Events*.

Improved Performance of Software Upgrades

Because MARS relies on frequent signature updates to stay abreast of the most recent known attacks and issues, software updates are an integral part of any operational plan. Even on small appliances that monitor low volume traffic, this upgrade can consume valuable time, both as system downtime and in terms of administrative monitoring and verification.

Beginning with release 4.2.1, the software upgrade uses binary differential updates rather than complete image updates. As a result, both signature update and system patch performance is greatly improved.

Low-End Monitoring Solution: MARS 20R

The MARS 20R provides the same functionality as the MARS 20 with the restriction of accepting only 50 events per second and 1,500 NetFlow flows per second. It is restricted to operate as a standalone Local Controller and cannot be managed by a Global Controller. This entry-level product is positioned as a low-cost replacement for Monitoring Center for Security found in the VMS 2.x suite. However, it is orderable through regular channels. No upgrade option exists for this model.

Distributed Threat Management (DTM) Enhancements

The system parameters controlling the DTM features of MARS now provide improved control and the ability to specify the frequency of synchronization and default action of the N signatures being reported as active on Cisco.com/MySDN. Specific enhancements are as follows:

- (Enhancement) Signature Inactivity Interval For Deletion. Users can now specify the time period for which signatures are kept on IOS IPS routers with IPS support before they are deleted. This setting replaces the previous DTM Deletion Interval setting.
- (New) Top N Signature Pulling Interval From CCO (default 15 minutes). MARS pulls the CCO Top N signatures each time this interval expires. MARS then pushes these Top N signatures to all DTM-enabled IOS routers. (any IOS router that included in any DTM Rule action).

- (New) Top N IPS Signature Action. Applies a global action to the Top N signatures retrieved from CCO. This action is applied only to the CCO Top N Signatures.
- (New) Support for NATed IOS IPS devices. Previously, MARS did not support IOS IPS devices that did not reside on a network that was directly connected to the eth0 interface of the MARS Appliance. This feature enables access to IOS IPS devices that reside behind NATed gateways.
- (Enhancement) Support for additional signature actions. The notification action for DTM now includes the deny attackers and deny flow actions, which are applied to the signatures published to the IOS IPS routers that are targets of the notification.

Case Management Enhancements

The following enhancements to case management are included in the MARS 4.2.1 release:

- The filter, *Open Cases*, displays all open cases.
- In releases before 4.2.1, information was copied to a case when it was closed. This timing allowed the possibility that information might be deleted before the case was closed. Now, information is copied as it is attached to the case.
- In releases before 4.2.1, you could e-mail a case to its owner only. Now, you can e-mail a case to anyone who has an account in MARS, and you can select multiple recipients.
- The ability to show and hide attachments. In 4.2.1, two view buttons appear on the Case Management page: *Show All* and *Show Included*. The default view is *Show All*, which displays all information associated with the case and is consistent with previous releases. *Show Included* allows you to display only those attachments that are selected.
- In releases before 4.1.5, query results were limited to 100 entries. In release 4.1.5, the limit was increased to 5,000. If the number of results is larger than the paging size, you are presented with a popup window that identifies how many results there are, the paging size, and prompts you to specify how many to display. The upper limit of 5,000 results in a query still exists; however, you can reduce the number of results if the paging size is greater than the number of records.
- You can no longer edit a closed case or change the name of the case. You can view, e-mail it, and add a comment.

A general issue with case management still exists where attachments can take while to appear in the case, particularly if that attachment is large. Therefore, if you add something to a case but the attachment does not appear when you review the case, allow some time to pass and try again. It simply takes a while for large attachment to be associated with the case.

Using ISS Site Protector to Configure ISS NIDS and HIDS

MARS supports ISS NIDS and HIDS event retrieval via SNMP. However, when configuring ISS RealSecure sensors (NIDS) and hosts (HIDS), you must configure each active signature to send an alert to the MARS Appliance. This task can be tedious because you must configure each sensor and after each signature upgrade, as an upgrade resets the redirect configuration. You can simplify this task by using the ISS Site Protector management console to define these changes globally and apply them to each sensor.

ISS Site Protector 2.0 allows you to centrally manage SNMP alert destinations, such as the MARS Appliance, for group policies. You can then push these group policies to all desired host and network sensors. For each ISS signature update, you must specify the MARS Appliance as an SNMP alert destination before you apply the downloaded signatures to sensors using Site Protector.

**Note**

The configuration was qualified using an ISS Proventia G100 appliance (NIDS) and Site Protector 2.0 (Management Console).

Miscellaneous Changes and Enhancements

The following changes and enhancements are the result of caveats fixed in the 4.2.1 release:

- **Feedback button behavior changes.** The Feedback button now sends an e-mail to the logged on user, who can forward it to the appropriate support personnel. If the logged on user does not have an e-mail address configured, a pop-up window instructs the user to define one.
- **Pink Box behavior changes.** A pink box appears when a system error in the web interface is detected. In releases before 4.2.1, you could send the error log and related information to Cisco using the Report Error button. In the 4.2.1 release, you can choose to e-mail the error log directly to Cisco TAC. The log can be attached to an existing TAC case, which requires that you provide a valid TAC case number or create a case.
- **Device version upgrade support.** Previously, if you upgraded the software version of a support device, you could not reflect that change in MARS. To do so, you had to delete the old device and then add a new device with the correct software version. In the 4.2.1 release, the Change Version button appears on the Security and Monitoring Devices page, allowing you to identify such changes on defined reporting devices.
- **Severity of a syslog changed in the originating device.** In the 4.2.1 release, MARS ignores the severity of the event in the message while parsing IOS, PIX, and FWSM messages. This enhancement allows you to change the severity of a syslog server without breaking the MARS parser. This change addresses issues defined in CSCpn03044.
- **Blocked packet from the sensor can now be seen.** In releases before 4.2.1, MARS made no indication whether an IPS device blocked a detected attack. In the 4.2.1 release, MARS displays “Block-YES” in IPS raw message if the reporting device blocked the attack. This enhancement allows you to generate reports on the attacks that are blocked by an IPS device. This change addresses issues defined in CSCsb70121.
- **Discovery of Symantec agents.** In the 4.1.4 release, MARS learned, through discovery, of agents managed by Cisco Security Agent and McAfee ePO management consoles. In the 4.2.1 release, this functionality has been extended to the Symantec AntiVirus management console. This change addresses issues defined in CSCsc30044.
- **Automatically add Reporting IP as part of the SNMP Discovery process.** In the 4.2.1 release, MARS defines the Reporting IP of devices discovered during the discovery processes. This change addresses issues defined in CSCsc50789.
- **Alert if MARS is dropping events.** A system inspection rule, *System Rule: Resource Issue: CS-MARS*, has been defined that alert when the MARS Appliance begins to drop events rather than process them due to system resource limitations, such as exceeding storage capacity, dropped events due to rate limits being exceeded, capacity limitations, and so on. This feature applies to standard events and NetFlow records. Four new event types (found in the Info/HighUsage/CS-MARS group) are included in the rule definition. These event types identify the following:
 - First dropped event in one hour
 - Dropped event count in one hour
 - First dropped NetFlow in one hour
 - Dropped NetFlow count in the hour

A new System: CS-MARS Issue report, *Resource Issues: CS-MARS - All Events*, is provided to summarize these notifications. These changes address issues defined in CSCsc33942:

- **Configurable event summary display on the Summary > Dashboard page.** Previously, MARS displayed the last 24 hours of statistical event information. You can now select the interval for displaying summary event results. Choose from the past day, two days, week, month, or year.

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	S229
McAfee Enterccept HIDS 4.1	Agent Version 40-56
ISS RealSecure Network Sensor 7.0	24.36
ISS RealSecure Server Sensor 7.0	24.36
McAfee IntruShield NIDS 1.8	1.8.75.4
Snort NIDS	2.3.3
Netscreen IDP 2.1	Idp2.1r3 Update 254
Enterasys Dragon 6.x	Latest signatures as of 06-01-2006
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 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 4.2.1

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
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

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 4.2.1 release:

- Do not to use DISTINCT or SAME in queries, and do not run multi-line queries in Release 4.2.1. If you run such a query, the system time outs 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.

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 12](#)
2. [Checklist for Initial Configuration, page 12](#)

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
Perform initial configuration of the MARS Appliance.	Checklist for Initial Configuration, page 12
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 (pnadmin). • 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="228 285 638 310">4. Command Line Configuration.</p> <p data-bbox="269 327 1507 485">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="282 501 1284 753" style="list-style-type: none"><li data-bbox="282 501 1284 531">• Log in to the appliance using the system administrative account and the new password.<li data-bbox="282 548 667 577">• Set any additional static routes.<li data-bbox="282 594 467 623">• Set the clock.<li data-bbox="282 640 626 669">• Set the NTP server settings.<li data-bbox="282 686 618 716">• Set the DNS domain name.<li data-bbox="282 732 1110 762">• Connect the appliance to the network (that is, plug in the Cat 5 cables.) <p data-bbox="269 774 1507 863"><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="269 879 570 909">For more information, see:</p> <ul data-bbox="282 926 708 1043" style="list-style-type: none"><li data-bbox="282 926 605 955">• Specify the Time Settings<li data-bbox="282 972 605 1001">• Set Up Additional Routes<li data-bbox="282 1018 708 1047">• 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 (padmin) • 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 4.2.1, page 17](#)
- [Resolved Caveats - Release 4.2.1, page 35](#)
- [Resolved Caveats - Releases Prior to 4.2.1, page 43](#)

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 4.2.1

The following caveats affect this release.

Reference Number	Description
CSCse56692	<p><i>Issue:</i> Policy query should not be case sensitive with interface names</p> <p><i>Description:</i> The policy table lookup feature in MARS is case sensitive when performing queries that match against interface names, such as <i>outside</i> and <i>Outside</i>. The two names are considered exclusive by MARS, while they are equivalent in Security Manager. As a result, name logged in the syslog event may not match the name in Security Manager. Syslog message lowercase all interface names.</p> <p><i>Workaround:</i> Use lowercase for all interface names an in the definition of interface roles in Security Manager.</p>
CSCse56473	<p><i>Issue:</i> High pnparsr CPU usage in processUserInfo thread</p> <p><i>Description:</i> One pnparsr consumes 99% of the CPU for extended periods of time. As a result, you may notice:</p> <ul style="list-style-type: none"> • Events continue to be processed and saved into database but reported users contained in events are not extracted. • Therefore, rules/queries/reports that match on reported users in events will not produce correct results. <p><i>Workaround:</i> None.</p>
CSCse54808	<p><i>Issue:</i> The time stamp shown by the pndbusage command is incorrect</p> <p><i>Description:</i> Two consecutive uses of the pndbusage command display a different current partition starting time.</p> <p><i>Workaround:</i> None.</p>

Reference Number	Description
CSCse53573	<p><i>Issue:</i> false alarm error in janus_log: corruption in shared buffer</p> <p><i>Description:</i> MARS processes use a shared buffer for event and incident data. Data is written in the form of fixed sizes where the size depends on the MARS Appliance model and whether type of shared data. Previously, the maximum size was 100,000, and therefore, an error message such as “corruption in shared buffer: encountered a large (>=100000) length chunk component, currentSize = 220260” would indicate data corruption that results in MARS skipping some events or incidents. However, fixing the defect CSCse24869 increased the maximum size to 300000 and therefore an error printed in the logs for data larger than 100000 is a false alarm as it can legitimately occur.</p> <p><i>Workaround:</i> You can safely ignore this error message when it refers to a chunk size smaller than 300,000.</p>
CSCse51438	<p><i>Issue:</i> No GUI message to indicate a real-time event viewer timeout</p> <p><i>Description:</i> The real-time event viewer session will timeout if paused for more than 30 minutes. No error message will appear to indicate that the real-time event viewer is inoperative. Because the MARS login session timeout is also 30 minutes, you are directed to the MARS login screen when you click any GUI control after 30 minutes. After you login to MARS, the behavior is as follows depending on the GUI control you clicked:</p> <ul style="list-style-type: none"> • Tab—a blank page appears with a URL similar to the following: https://172.16.16.16/Query/LLRTQueryStop.jsp?requestType=STOP&maxRows=40 • Submit button—The default Query Event Data dialog appears. • Resume button —MARS displays the contents of a buffer then stops. The buffer contains the events that were not yet displayed when you clicked Pause. • Restart button—MARS clears the paused display and does not display new events. <p><i>Workaround:</i> Click Clear and submit a new real-time event viewer query.</p>
CSCse45884	<p><i>Issue:</i> Real-Time (raw events) query causes client CPU to go to 100%</p> <p><i>Description:</i> At a high rate of incoming events, i.e., 100 events per second, the low latency query page consumes 100% of the CPU on the web interface client.</p> <p><i>Workaround:</i> None.</p>
CSCse40803	<p><i>Issue:</i> Parsing error for FWSM-3-106011</p> <p><i>Description:</i> MARS fails to parse the FWSM syslog message “Error Message %FWSM-3-106011: Deny inbound (No xlate) string”.</p> <p><i>Workaround:</i> None.</p>
CSCse40779, CSCse23051	<p><i>Issue:</i> Query: Save as report with Mac Addr report criteria throws an Exception</p> <p><i>Description:</i> If you create a report using the query type: MAC addresses report, an exception (pink box) occurs.</p> <p><i>Workaround:</i> None.</p>
CSCse38565	<p><i>Issue:</i> Re-importing Symantec AV client CSV doesn't work</p> <p><i>Description:</i> If you import Symantec AntiVirus agents into the MARS web interface using the CSV file format and then delete those agents, you cannot re-import them. Attempts to re-import will result in the error, “Error Occurred: Status: DbDevice”, and none of the agents will be created.</p> <p><i>Workaround:</i> None.</p>

Reference Number	Description
CSCse34600	<p><i>Issue:</i> CPU utilization is not reported for PIX device</p> <p><i>Description:</i> When you select Yes in the Monitor Resource Usage box of the General tab for a PIX device, the CPU utilization is not reported for that device.</p> <p><i>Workaround:</i> None.</p>
CSCse34407	<p><i>Issue:</i> Query Tab > Multi column query returns wrong results.</p> <p><i>Description:</i> When running a multi-column (custom column) query for a short duration of time, the results returned might contain a lot more data than actually expected.</p> <p><i>Workaround:</i> For correct results, run a regular query inline. In other words, do not choose custom column option for Result Format.</p>
CSCse33688	<p><i>Issue:</i> no events under Cisco Switch-IOS 12.2</p> <p><i>Description:</i> With an IOS switch device, received logs should appear under Cisco Switch-IOS 12.2, However, they are being sorted under Cisco IOS 12.2 instead. In addition, under Management > Event Management, if you select Cisco Switch-IOS 12.2, no events appear.</p> <p><i>Workaround:</i> There is no work around to the incorrect sorting. To see the logs received from a Cisco Switch-IOS device, query using Cisco IOS 12.2 instead.</p>
CSCse32591	<p><i>Issue:</i> dealing with duplicate hostnames in VA import</p> <p><i>Description:</i> While importing VA data from any one of the supported devices, MARS does the following:</p> <ol style="list-style-type: none"> 1. For each device included in the report, MARS checks whether a device with the same name exists in the database. 2. If the device with the same name already exists in the database, then MARS changes the name of the new device according to the convention “devicename (count)”, where “count” is the number of devices that exist in the database and have the same “devicename” substring. Using the new “devicename (count)” name, MARS adds the device to the database. <p>This issue is that when importing data about a given device, such as a router with multiple interfaces, MARS defines multiple, separate devices.</p> <p><i>Workaround:</i> None.</p>
CSCse31722	<p><i>Issue:</i> Cloud toggle only works on first page of reporting devices</p> <p><i>Description:</i> You cannot expand or collapse devices within a cloud on pages other than the first page in the Security and Monitor Devices page. If you select this option on the second or later pages, the first page is displayed.</p> <p><i>Workaround:</i> None.</p>
CSCse29860	<p><i>Issue:</i> UTC and GMT time zone missing</p> <p><i>Description:</i> In 4.1.5, the UTC standard is no longer available as an option for setting the clock on the MARS Appliance.</p> <p><i>Workaround:</i> None.</p>

Reference Number	Description
CSCse23176	<p><i>Issue:</i> MARS Global Controller not producing alerts when losing Local Controller communication</p> <p><i>Description:</i> The Global Controller is not generating alerts when it loses communication with the Local Controller. The user must determine this manually.</p> <p><i>Workaround:</i> At the command line on the Global Controller, run pnlog to determine whether the Local Controller is generating “Data timed out errors” or to run tcpdump to verify the Local Controller communication.</p>
CSCse22751	<p><i>Issue:</i> Case management fails to 'Expand All' for attached report</p> <p><i>Description:</i> The Expand All option may not display sub-events that are attached to case. For example, if you attach the results of a batch query for all matching sessions to an existing case, where the results returned more than 5,000 sessions and so only the page displayed was added).</p> <p><i>Workaround:</i> None.</p>
CSCse21936	<p><i>Issue:</i> Daylight savings time affects the custom parser's received time field</p> <p><i>Description:</i> The hour string in the parsed value field of user-created templates, shows an hour after the actual log timestamp on and after daylight savings time. (April 2, 2006)</p> <p><i>Workaround:</i> None.</p>
CSCse21626	<p><i>Issue:</i> Clicking activate is not taking effect</p> <p><i>Description:</i> After disabling some DTM rules and enabling others, clicking Activate does not effect the changes.</p> <p><i>Workaround:</i> If Activate does not work, perform a pntstop and then a pntstart operation at the command line.</p>
CSCse20593	<p><i>Issue:</i> CSM device type could not be added one time (OK most times)</p> <p><i>Description:</i> Rarely, when adding a Cisco Security Manager device type, a run-time scripting error occurs. This issue appears when there is a timeout situation in either the parent or child browser window, or when one window is unexpectedly closed.</p> <p><i>Workaround:</i> This issue rarely occurs. To work around the issue, repeat the add operation.</p>
CSCse18865	<p><i>Issue:</i> scalability issues in My Reports page</p> <p><i>Description:</i> If you have a large number of reports (e.g., 70 or more) on the My Reports page, and displaying them takes a long time.</p> <p><i>Workaround:</i> None.</p>
CSCse18816	<p><i>Issue:</i> UI takes 99% CPU, hanging browser and slowing system while expanding all</p> <p>The client window (Internet Explorer) becomes unresponsive, the cursor state shows the application is processing information and remains in this state for 5+ minutes and/ or Windows marks the browser as 'Not Responding'. This issue occurs when the user clicks the '+' sign or 'Expand All' in the query results page where >1000 events are grouped together based on the query criteria.</p> <p><i>Workaround:</i> The following options are available:</p> <ul style="list-style-type: none"> • Instead of using Expand All, expand one group at a time. • To resolve the hung process. close the client (Internet Explorer) or kill the process using Task Manager and open a new window to re-run the query.

Reference Number	Description
CSCse17936	<p><i>Issue:</i> 5K Lines Custom Query fails</p> <p><i>Description:</i> In some cases, custom query can result in errors on the rendered page, as well as an incomplete page appears. In the known cases, this issue appears to have been the result of using the “raw message” field in the custom query.</p> <p><i>Workaround:</i> Removing the raw message column from the Query resolves the issue. This issue does not appear in all custom queries that include the raw message field.</p>
CSCse17864, CSCse22610, CSCse22617	<p><i>Issue:</i> Device info was lost after migration</p> <p><i>Description:</i> Case Management migration from 4.1.x to 4.2.x can result in lost reports, queries, and devices that are associated with open cases.</p> <p><i>Workaround:</i> Close all Case Management cases before migrating to 4.2.x. 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.</p>
CSCse13038	<p><i>Issue:</i> CS-MARS - learning of McAfee agents with invalid names</p> <p><i>Description:</i> McAfee ePO agents with non-ASCII hostname/character set, that are imported automatically into MARS 4.1.4 and later, will add devices with invalid names. Events reported from such agents may have:</p> <ul style="list-style-type: none"> • An invalid device name in the reporting device column • Invalid characters in raw message. <p>This issue is caused by the lack of I18N support in the current MARS release. The following are likely causes of this issue:</p> <ul style="list-style-type: none"> • Invalid characters in the raw message sent from the ePO agent • ePO agent names that contain some additional text, such as date or time <p><i>Workaround:</i> Identify such invalid devices in MARS web interface and delete them periodically.</p>
CSCse11258	<p><i>Issue:</i> After group is deleted, items under All group not shown</p> <p><i>Description:</i> This is a minor/cosmetic defect, as the delete is performed correctly, but the display is incorrect.</p> <p><i>Workaround:</i> Click the tab again, or any other selection that leads to a page refresh, to see all items in the All group.</p>
CSCse10945	<p><i>Issue:</i> Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)</p> <p><i>Description:</i> Graphs on the Summary Dashboard, Network Status, and My Reports pages can change display sizes when using a multi-head display. This issue can appear on both the Global Controller and Local Controller when the display period is in minutes. The content displayed is correct, however, the size of the display changes.</p> <p><i>Workaround:</i> Do not use a multi-head display.</p>
CSCse09127	<p><i>Issue:</i> Failed load from csv returns incorrect status</p> <p><i>Description:</i> When a Load from csv operation fails, no errors are reported. Instead, the status is reported as OK. This issue appears when the user has configured an FTP server that does not allow passive transfer. The symptom is that the status is reported as OK, but there are no devices loaded in the MARS web interface.</p> <p><i>Workaround:</i> Other than using an FTP that supports passive transfer, no work around exists.</p>

Reference Number	Description
CSCse03134	<p><i>Issue:</i> More control is needed over retrieve raw messages and cleanup</p> <p><i>Description:</i> Repeated use of the `Retrieve Raw Messages` feature results in the following error message:</p> <pre>ava.io.IOException: No space left on device.</pre> <p>This occurs if `Retrieve Raw Messages` is used excessively within a short period of time.</p> <p><i>Workaround:</i> None. These files are cleaned up automatically after 2 weeks time.</p>
CSCse00668	<p><i>Issue:</i> rule definition changes can lead to empty reports</p> <p><i>Workaround:</i> You can avoid this issue by defining a Rule Group for every rule that is to be used in a scheduled report.</p>
CSCse00626	<p><i>Issue:</i> IP Management device group displays hosts only</p> <p><i>Description:</i> The View > Host option on Management > IP Management page filters all devices defined on the Security and Monitor Devices page from the IP Management page, including from Device groups, which in itself is expected behavior. However, this introduces an inconsistency as any type of device can be added to a Device Group through the Edit/Add Group button. After clicking Submit, the group lists only the Host entries, typically a subset of all devices belonging to a group, and this can be confusing to the user.</p> <p><i>Workaround:</i> To view the actual contents of a group, Select a device group and click the Edit Group button.</p>
CSCse00251	<p><i>Issue:</i> process_inlinerep_srv ignores Rule Groups as selection/filtering criteria</p> <p><i>Description:</i> Rule groups are ignored as selection criteria in an inline report.</p> <p><i>Workaround:</i> You can avoid this issue by defining a Rule Group for every rule that is to be used in a scheduled report.</p>
CSCsd96070	<p><i>Issue:</i> Data refreshes can take a long time when attempting to view the report data associated with that case.</p> <p><i>Description:</i> Due to the issues identified in CSCsd96067, viewing all of the data contained in a case that contains multiple reports can take a long time to load.</p> <p>By default, reports attached to cases limit their results to 25 per page. Due to each report having its own paging value and the issues identified in CSCsd96067, attempting to view all of the data in each report attached to a case by changing to paging to something larger can take a long time.</p> <p><i>Workaround:</i> Limit the number of reports attached to a case and restrict the number of events returned to only that which is required. A general issue with case management exists where attachments can take while to appear in the case, particularly if that attachment is large. Therefore, if you add something to a case but the attachment does not appear when you review the case, allow some time to pass and try again. It simply takes a while for large attachment to be associated with the case.</p>
CSCsd96067	<p><i>Issue:</i> Report e-mails can become large when selecting the raw message format for all matching events.</p> <p><i>Description:</i> Because MARS now allows reports to return up to 5000 events, rather than the previous limit of 1000 events, the report size can be much larger than previously experienced (10-15 MB, depending on the data returned).</p> <p><i>Workaround:</i> To avoid this issue, define exact report parameters and restrict the number of events returned to only that which is required.</p>

Reference Number	Description
CSCsd96048	<p><i>Issue:</i> When using case management, choosing to e-mail case data can generate very large e-mails.</p> <p><i>Description:</i> Due to the issues identified in CSCsd96067, choosing to e-mail a case that contains multiple reports can compound the problem of large e-mails.</p> <p><i>Workaround:</i> Limit the number of reports attached to a case and restrict the number of events returned to only that which is required.</p>
CSCsd95582	<p><i>Issue:</i> Both successful/failed mitigation reports show same results</p> <p><i>Description:</i> For 4.1.5 release, a query based on either the “CS-MARS Host Mitigation - Failure - All Events” or “CS-MARS Host Mitigation - Success - All Events” report retrieve all events associated with a session, which explains why both report types display both failed and successful raw messages.</p> <p><i>Workaround:</i> None.</p>
CSCsd93235, CSCsd10627	<p><i>Issue:</i> MARS can take up to 1 hour to connect to all IPS devices (when there are 60 or more devices) the first time the process comes up. This issue can appear after a power cycle.</p> <p><i>Workaround:</i> None.</p>
CSCsd92285	<p><i>Issue:</i> MARS does <i>not</i> perform a duplicate IP address check in the Admin > Security and Monitor Devices page</p> <p><i>Description:</i> In the 4.1.5 release, MARS does <i>not</i> perform a duplicate IP address check for agents, sensors, and firewalls matching one of the following host-based applications:</p> <ul style="list-style-type: none"> • CheckPoint Opsec NG FP3 • Cisco CSA 4.x • Enterasys Dragon 6.x • Entercept Entercept 2.5 • Entercept Entercept 4.0 • IntruVert IntruShield 1.5 • NetScreen IDP 2.1 • Symantec Anti Virus 9.x <p>As such, avoid using a duplicate IP addresses to prevent event correlation issues with your MARS Appliance. In addition, when you add or edit a new host using the Security and Monitor Devices page, no duplicate IP address checks are performed. Avoid using existing IP address as the host IP address when adding or editing a host.</p> <p><i>Workaround:</i> MARS does perform a duplicate IP address check on the IP Management page. We recommend that you add or edit the IP address of hosts using this page and that you add components to such defined hosts using the Security and Monitor Devices page. You must manually avoid the use of duplicate IDs when defining the host-based reporting devices listed above.</p>

Reference Number	Description
CSCsd89457	<p><i>Issue:</i> Incorrect handling of time range for rules that fire periodically</p> <p><i>Description:</i> To reduce false positives, the first time a rule first a time interval of 5 minutes must elapse before events being received can trigger the rule to fire again. After the second time a rule fires, the time interval is extended to 10 minutes. The fire count value is reset to 0 when no event that matches the rule is received within a past window of <time range> seconds.</p> <p>For rules that fire once every 5 or 10 minutes, events greater than the rule count can accumulate, which is by design. Among these accumulated events, the first <count> number of events in an offset should be within the time range of the rule; however, this is not true and the result is a a higher false positive rate for incidents.</p> <p><i>Workaround:</i> None.</p>
CSCsd86896	<p><i>Issue:</i> When editing the query type, clicking Clear does not work.</p> <p><i>Description:</i> When editing a query type, clicking Clear can actually commit changes to the query type definition rather than clearing any changes made by the user.</p> <p><i>Workaround:</i> None.</p>
CSCsd84350	<p><i>Issue:</i> CS-MARS-Cisco Security Manager Integration: Credentials change on Cisco Security Manager side not checked.</p> <p><i>Description:</i> This issue exhibits when the following conditions are met:</p> <ol style="list-style-type: none"> 1. Enter matching Security Manager credentials in MARS to match that in Security Manager server. 2. Query a “traffic log” related event that has the Security Manager icon enabled. 3. Check to see that the access rule lookup is functioning. 4. Go to Security Manager server and through CiscoWorks, delete the user set in MARS from Security Manager server. 5. Do not click any “Test Connectivity” on MARS side after the Security Manager server modification. 6. Again query the “traffic log” related event that has the Security Manager icon enabled. 7. Access rule lookup is still successful though Security Manager credentials is invalid. <p><i>Workaround:</i> In the MARS web interface, click Admin > Security and Monitor Devices, and then select the Security Manager device, click Edit and then click Test Connectivity after deleting the Security Manager user, but before performing the access rule lookup. The credentials check is performed and fails the subsequent lookup as it should.</p>
CSCsd84094	<p><i>Issue:</i> Problems occur when a report definition contains a rule as a selection criteria and the rule definition is later changed.</p> <p><i>Description:</i> This issue occurs as each changed rule is provide a new rule ID. The old rule ID is inactivated so that it does not fire, but the report definition points to the stale ID rather than the new ID created when the rule definition was changed. As a result of this stale reference, no results appear for the affected reports even though a new query based on the same criteria returns results.</p> <p><i>Workaround:</i> Use rule groups, instead of direct rule reference, in report definitions. The group will always point to the current rule definition instead of pointing to a stale rule definition.</p>

Reference Number	Description
CSCsd79730	<p><i>Issue:</i> Device Groups created on Global Controller do not show up in Global Controller drop down list of groups</p> <p><i>Description:</i> If you define a Device Group in Global Controller, the group is propagated to its monitored Local Controllers, but the new group does not appear in the Select Group list on the Management > IP Management page of the Global Controller web interface.</p> <p><i>Workaround:</i> None.</p>
CSCsd74283	<p><i>Issue:</i> Report results are purged after a fixed time period.</p> <p><i>Description:</i> In releases 4.1.4 and earlier, report results were retained in the database for up to 365 days. However, as of 4.1.5, the maximum number of stored report results was increased from 100 to 1,000 for ranking reports and 1,000 to 5,000 for event/session reports. As a result, the retention period was reduced to 3 months for MARS 20 and MARS 50 models and to 6 months for the MARS 100, MARS 200, MARS GC, and MARS GCm models.</p> <p><i>Workaround:</i> None.</p>
CSCsd69137	<p><i>Issue:</i> Default Group in Scheduler need to be made to Run On Demand</p> <p><i>Description:</i> The Default Group in Scheduler is currently set to run on 1st day of every month. Any devices/Networks added in the web interface or discovered are automatically added to this group. Thus, this discovery often returns more devices than desired.</p> <p>The default behavior of this group is such that MARS learns of additional networks through user input and each discovery operation. Therefore, this default scheduled group can progressively discovery new devices via subsequent discoveries.</p> <p><i>Workaround:</i> Under Admin > System Setup > Topology/Monitored Device Update Scheduler, edit the Default Discovery Group and change the schedule to Run On Demand Only.</p>
CSCsd69063	<p><i>Issue:</i> A MARS custom parser cannot parse a reported user field that contains a single quote (') character.</p> <p><i>Workaround:</i> None.</p>
CSCsd61749	<p><i>Issue:</i> pnrstore does not restore some configuration settings</p> <p><i>Description:</i> Settings that are specific to the operating system and not configurable within the MARS HTML interface are not stored in the database, and therefore, they are not restored during pnrstore operation.</p> <p>For example, pnrstore command does not restore static routes or NTP server settings defined at the CLI.</p> <p><i>Workaround:</i> Manually re-enter these settings from the command line.</p>
CSCsd53173	<p><i>Issue:</i> Retrieve raw messages doesn't properly update the progress percentage</p> <p><i>Description:</i> When retrieving raw messages using Admin > System Maintenance > Retrieve Raw Messages, a percentage complete is displayed. This interface is not properly updated.</p> <p><i>Workaround:</i> Please wait for the task to complete.</p>

Reference Number	Description
CSCsd22832	<p><i>Issue:</i> Some networks cannot be removed from the IP Management tab of the Management section of the Web interface.</p> <p><i>Description:</i> The attempt fails with error message: “You cannot delete this network as it is used in discovery.”</p> <p>The error occurs when trying to delete a network that was added into the MARS automatically during device discovery. Those networks cannot be deleted in currently available versions.</p> <p><i>Workaround:</i> None.</p>
CSCsc90480	<p><i>Issue:</i> MARS Incident notification options are not configurable</p> <p><i>Description:</i> Currently when MARS sends out incident notifications via e-mail, you cannot configure the types of links it sends out. As a result, it can send out links that are not reachable/invalid if the DNS name of the MARS Appliance cannot be resolved by the e-mail client.</p> <p><i>Workaround:</i> None.</p>
CSCsc59363	<p><i>Issue:</i> Multi-line rules are difficult to edit.</p> <p><i>Description:</i> Editing multi-line rules can be confusing, particularly if you want to remove a line from a rule.</p> <p><i>Workaround:</i></p> <ol style="list-style-type: none"> 1. In the line above the line that you wish to remove, click on the link taking you to the “Severity” cell. 2. Click Next. A dialog box appears, prompting whether you are finished defining the rule conditions. 3. Click Yes. A warning message appears stating that the subsequent lines will be removed from the rule. 4. To remove all lines underneath the selected one, click OK to confirm the warning.
CSCsc50636, CSCsc50652	<p><i>Issues:</i> pnids50_srv process runs at 99% CPU when pulling large IP Logs pnids50_srv process reaches 1GB in memory used when pulling IP Logs</p> <p>These related issues, are specific to pulling IP logs from Cisco IDS/ IPS devices. The symptom is that the pnids50_srv and pnids40_srv services consume 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, 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.</p>

Reference Number	Description
CSCsc49248	<p><i>Issue:</i> A drop rule for “inactive reporting device” does not work.</p> <p><i>Description:</i> There are six internally generated event types in CS-MARS 4.1.x:</p> <ol style="list-style-type: none"> 1. Sudden traffic increase event 2. Resource high usage event 3. Inactive reporting device detection event 4. VA integration event 5. Mitigation result event 6. DTM event <p>Events generated for items 4, 5 and 6 are processed against drop rules. However, items 1, 2 and 3 cannot be dropped as they are not processed against drop rules by design. Items 1, 2 and 3 record the history of what happened on the network and are retained in the database.</p> <p><i>Workaround:</i> You can delete the inactive device from CS-MARS or ensure that it is reachable by CS-MARS. For other event types, there is no work around.</p>
CSCsc23874	<p><i>Issue:</i> Resource Utilization reports are incorrectly available to be run as a query.</p> <p><i>Workaround:</i> Do not attempt to run any of the following reports as an On Demand query or to use them as part of a user-defined group:</p> <p>Resource Utilization:</p> <ul style="list-style-type: none"> • Bandwidth: Inbound - Top Interfaces Resource • Utilization: CPU - Top Devices Resource • Utilization: Bandwidth: Outbound - Top Interfaces Resource • Utilization: Concurrent Connections - Top Devices Resource • Utilization: Errors: Inbound - Top Interfaces Resource • Utilization: Errors: Outbound - Top Interfaces Resource • Utilization: Memory - Top Devices

Reference Number	Description
CSCsc04484	<p><i>Issue:</i> The rule or report list on a Local Controller (LC) appears empty after deleting a Global Controller (GC) report or rule group.</p> <ol style="list-style-type: none"> From the Rules or Reports page in the GC HTML interface, create a rule or report group with some elements in it. Activate to push the group down to the monitored LC. From the Rules or Reports page of a LC HTML interface, select the newly-created GC group in the filter list. <p><i>Result:</i> The members of that group are listed.</p> <ol style="list-style-type: none"> Select the Summary page. Select the Rule or Report page. <p><i>Result:</i> The group is still selected as the “filter” for that page</p> <ol style="list-style-type: none"> Select the Summary page. In the GC HTML interface, delete the rule/report group. Activate to push changes down to the monitored Local Controllers. In the LC HTML interface, navigate back to rule/report page. <p><i>Result:</i> The filter list has “All” selected, but no rules or reports appear on the page.</p> <p><i>Workaround:</i></p> <ol style="list-style-type: none"> Select another option in the filter list, and then All. <p><i>Result:</i> The list of all rules/reports appears.</p>
CSCsb80082	<p><i>Issue:</i> When you remove/delete a Local Controller from a Global Controller, the Local Controller should revert to the Standalone mode. However, if you add the Local Controller to the Global Controller and delete it before you exchange certificates between the two appliances, then the mode does not revert.</p> <p><i>Workaround:</i> You can work around this issue by ensuring that you always import the certificate from the Local Controller before you attempt to remove it from the Global Controller.</p>
CSCsb77550	<p><i>Issue:</i> Re-importing CSA or Symantec agents fails.</p> <p>When the user tries to agents from a CSV seed file, the following error message appears:</p> <pre>Error Occurred: Status: DbDevice</pre> <p><i>Result:</i> The error message fails.</p> <p><i>Workaround:</i> If you import an agent list once, you must manually synchronize the agent list. To re-import the list of agents will not work.</p>
CSCsb71309	<p><i>Issue:</i> In Cisco Security Monitoring, Analysis and Response System (MARS) release 3.4.4 and earlier, queries that are run from a Global Controller (GC) which have no results returned from any of the attached Local Controllers (LCs) will show up as “In Progress” in the GUI. This occurs in a GC/LC environment, and only when a global query returns 0 results from every one of the LCs.</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 LCs have finished running the query.</p>

Reference Number	Description
CSCsb67871	<p><i>Issue:</i> After re-installing a Local Controller, the zone and device data is lost in the Global Controller.</p> <p><i>Workaround:</i> Before you re-install (using a Recovery DVD) a Local Controller, you must delete that Local Controller and zone from the managing Global Controller.</p>
CSCsb64587	<p><i>Issue:</i> After Global Controller restore, the Local Controller certificates are missing.</p> <p><i>Workaround:</i> After restoring a Global Controller, you must re-import the certificates of each managed Local Controller before communications are restored.</p>
CSCpn03077	<p><i>Issue:</i> Global Controller generates a system error when you add a Local Controller that was added already</p> <p><i>Workaround:</i> Before adding a Local Controller, verify that you have not previously added it to the Global Controller. If you do encounter this error, restart the GUI by closing your web browser and logging in again.</p>
CSCpn03074	<p><i>Issue:</i> On the Incidents page of a Global Controller, the View and Show buttons do not work for incidents pushed up from the monitored Local Controllers.</p>
CSCpn03057	<p><i>Issue:</i> Copied rules have shortened year in front, which is confusing (e.g., 05.04.19) When you duplicate a system rule, the newly created rule has a timestamp appended to it. The date format is unclear, but it is YY.MM.DD.</p>
CSCpn03052	<p><i>Issue:</i> JBoss 'OutOfMemoryError' when accessing Management/Event Management tab.</p> <p><i>Workaround:</i> Avoid using the 10,000 items per page on the Event Management page.</p>
CSCpn02976	<p><i>Issue:</i> GC:LC - Communication issues after time zone change. After initial configuration, if you change the timezone of a communication GC:LC, there may be problems with communications between the GC and LC.</p> <p><i>Workaround:</i> If you notice that the Local Controller appears offline, verify that at least 10 minutes have passed since the appliances rebooted. Alternatively, you can jump start the communication by navigating to Admin > Local Controller Management in the Global Controller user interface.</p>
CSCpn02973	<p><i>Issue:</i> Not able to downgrade a Security Analyst to Notification only user. When you define a user account with the Security Analyst role, you cannot downgrade that role to Notification only.</p>
CSCpn02968	<p><i>Issue:</i> Network group search is not working for "All IP addresses". If you select All IP addresses as the search space, the results may be inconsistent with the expected results.</p>
CSCpn02901	<p><i>Issue:</i> GC/LC, rule does not display user <cxu> but allows such cfg</p> <p><i>Workaround:</i> Avoid using special characters in the keyword search for rules. The list of special characters not supported is as follows:</p> <ul style="list-style-type: none"> • less-than (<) &lt; • greater than (>) &gt; • ampersand (&) &amp;
CSCpn02883	<p><i>Issue:</i> Event management search works only for event description. You cannot search on other fields, such as Event ID.</p>

Reference Number	Description
CSCpn02869	<p><i>Issue:</i> Rules editing: changing entry for select window drop-down list after error message results in the state not being saved.</p> <p><i>Workaround:</i> This issue appears when you have attempted to define an invalid rule and an error message appears. For example, while editing a user inspection rule”</p> <ol style="list-style-type: none"> 1. Click Sources field. 2. Remove all sources. 3. Click Submit. <p><i>Result:</i> Dialog box appears and prompts “please select one”.</p> <ol style="list-style-type: none"> 4. In the select window drop-down list, select “All Devices” <p><i>Result:</i> Rule submission window appears and contains a blank Sources field.</p> <p>To work around this issue, click one of the top tabs to cancel your work and redo your edit without submitting an invalid rule (as shown in Step 3).</p>
CSCpn02804, CSCse33172	<p><i>Issue:</i> Replay History feature not working correctly.</p> <p><i>Description:</i> When you configure a query that triggers replay history, the results are usually incorrect. The following cases will trigger a replay history:</p> <ul style="list-style-type: none"> • a multi-line query that uses AND or Followed By • a query that uses the \$ variables, such as \$EventType, \$Device1, etc. • a query uses NOT EQUAL TO a service <p>If you define an invalid query, MARS returns a “TimeOut Error” message. You may also receive the error message “Invalid id used in DbClient::retrieve(),” depending on the query.</p> <p><i>Workaround:</i> None.</p>
CSCpn02688	<p><i>Issue:</i> Viewing a report on a Global Controller and viewing the corresponding report on the Local Controller may differ in time slightly.</p>
CSCpn02666	<p><i>Issue:</i> The email sent when a batch query completes may not have data in the graph if the query only returns one result.</p>
CSCpn02656	<p><i>Issue:</i> Leaving the browser on the Summary page for an extended period of time (several days) may occasionally run into an error.</p> <p><i>Workaround:</i> Refresh the page to return to the GUI.</p>
CSCpn02653	<p><i>Issue:</i> No way to specify “!Keyword” without a good “keyword”</p> <p><i>Workaround:</i> Keyword search requires two keywords to use the “NOT” operator. For example, you cannot specify `NOT nimda`; instead, you must specify something like `virus NOT nimda`.</p>
CSCpn02594	<p><i>Issue:</i> Clicking on the Path/Mitigate link in an incident that was fired from a device that has since been deleted may result in an error.</p>
CSCpn02574	<p><i>Issue:</i> Having different times on the Global Controller and its associated Local Controllers may cause synchronization problems.</p> <p><i>Workaround:</i> Use the CLI to configure NTP or manually set the date and time to be the same on the Global Controller and Local Controllers.</p>
CSCpn02566	<p><i>Issue:</i> Rebooting the MARS while the box is in the upgrading state may cause system configuration errors.</p>

Reference Number	Description
CSCpn02558	<p><i>Issue:</i> After adding and deleting an agent or sensor to a host, adding a sensor with the same name and type as the previously deleted one back to that host will not work.</p> <p><i>Workaround:</i> Use a different agent/sensor name the second time around.</p>
CSCpn02549	<p><i>Issue:</i> When viewing report results, clicking on “Edit” or “Clear” in the query summary at the top of the page results in a JavaScript error.</p> <p><i>Workaround:</i> Click directly on the “Report type” link to edit the query.</p>
CSCpn02511	<p><i>Issue:</i> In migrating “Microsoft, Windows, Generic” device type to three new Windows device types, errors in affected OS could affect data migration and cause confusion about appropriate selection.</p> <p><i>Workaround:</i> When migrating data, you should make the following mappings for the OS name:</p> <ul style="list-style-type: none"> • Map “2000” to “Windows 2000” • Map “Windows 2000 Professional Server” to either “Windows 2000 Professional” or “Windows 2000 Server” after verifying the data. • Map “NT” to “Windows NT” • Map “Microsoft Windows NT 4.0” to “Windows NT”. <i>Microsoft</i> should be in vendor field and <i>4.0</i> should be in version field.
CSCpn02470	<p><i>Issue:</i> Using passwords with the “,” (comma) or “”” (quote) characters may cause problems with loading devices from csv files.</p> <p><i>Workaround:</i> Avoid using passwords with these characters for the time being.</p>
CSCpn02414	<p><i>Issue:</i> Long keyword strings in rules or reports can cause parts of the GUI layout to be pushed out of the browser window's edges.</p>
CSCpn02410	<p><i>Issue:</i> The MARS stores reported user names in a case-sensitive fashion. Devices that report case-insensitive user names can behave counter-intuitively if they report names inconsistently.</p>
CSCpn02398	<p><i>Issue:</i> Reserved XML characters are not supported in the Keyword Search on the Rule page</p> <p><i>Workaround:</i> Avoid using special characters in the keyword search for rules. The list of special characters not supported is as follows:</p> <ul style="list-style-type: none"> • less-than (<) &lt; • greater than (>) &gt; • ampersand (&) &amp;
CSCpn02385	<p><i>Issue:</i> Applying \$VAR variables to queries on a Global Controller causes GUI errors and may not return correct results.</p>
CSCpn02383	<p><i>Issue:</i> An IIS web server cannot be added to the MARS as a generic web server. When configuring the MARS to receive IIS logs, adding generic web server in Reporting Applications does not work.</p> <p><i>Workaround:</i> Choose windows operating system under general tab.</p>

Reference Number	Description
CSCpn02333	<p><i>Issue:</i> After performing a “pnreset -g” (which cleans up the GC data on the LC - a copy will be made of all GC data used by rules and reports while all other GC data will be deleted), the LC still shows the old zone name by which it was monitored from the GC. When adding that LC back to a GC that was re-installed from the recovery DVD, problems can occur if the zone names for the GC and LC do not match the ones used before.</p> <p><i>Workaround:</i> Use the same “old” GC name during the GC configuration. Use the same zone names when re-adding LCs to the GC.</p>
CSCpn02251	<p><i>Issue:</i> After upgrading from a MARS 100e to MARS 100, pnstop and pnstart need to be run for the change to take effect.</p>
CSCpn02177	<p><i>Issue:</i> Every 22nd reboot, the MARS file system is checked for consistency. This takes time to complete, and happens before connecting to the network. While this is happening, it may appear that the box simply isn't starting.</p> <p><i>Workaround:</i> Attach a console to the MARS to verify that checking is happening if the system does not seem to start after a reboot.</p>
CSCpn02175	<p><i>Issue:</i> Data computed or stored on a standalone MARS while in standalone mode will not be transferred to a GC. Only data computed on an LC that is currently monitored by a GC 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>
CSCpn02061	<p><i>Issue:</i> Saving CSV files from reports with IE 6 under Windows XP SP2 causes the file to default to an .htm extension, not .csv extension.</p> <p><i>Workaround:</i> Select “All types” from the drop-down list while saving, and rename the file to have a .csv extension.</p>
CSCpn02011	<p><i>Issue:</i> Certain special characters do not work in password fields. The characters are " ' ; (double-quote, single-quote and semi-colon).</p> <p><i>Workaround:</i> Use passwords that do not contain these characters.</p>
CSCpn01489	<p><i>Issue:</i> Query summary doesn't mention “severity” if it's a criterion</p> <p>When the user configures a batch query with a severity as one of the criteria (Red, Yellow, Green), this criterion doesn't appear in the “query summary” of the batch query page. However, the query is run with the correct criteria. When the results are viewed, the severity can be seen in the query details at the top of the page.</p>
CSCpn01438	<p><i>Issue:</i> When running batch queries under a high system load and over a time range containing a large amount of data, the batch query might not complete. If the Progress Completed status stays at 0% for an extended period of time (a day), try stopping any other batch queries you have running or stopping and resubmitting your batch query with narrower criteria. If neither of these works, please contact Cisco Support.</p>
CSCpn01416	<p><i>Issue:</i> Select: Temp paging fix on Notification-SNMP. All pages that display large numbers of items need to have paging implemented.</p> <p><i>Workaround:</i> Use the search window to locate desired object.</p>
CSCpn01398	<p><i>Issue:</i> Unable to shutdown an interface: the customer should be able to shutdown an interface on CLI or GUI.1.</p> <p><i>Workaround:</i> Do not connect the second network interface to your network.</p>

Reference Number	Description
CSCpn01382	<i>Issue:</i> When you create a new group (MANAGEMENT > IP Management > Add Group) with a combination of Networks, Devices, and IP addresses and then select that group from the pull-down menu, only the Networks in the group appear, even though the Devices and IP addresses are in the group.
CSCpn01319	<i>Issue:</i> The pnrset command indicates that system will reboot after execution, however the system does not reboot. Also, you may find that the cursor does not return from the command—it is locked in the status indication (a string of periods). <i>Workaround:</i> Before running the pnrset command, you must disconnect the appliance from the network by unplugging the Ethernet cable from the appliance. Disconnecting it from the network ensures that the cursor will return from the command upon completion. In addition, you must manually reboot the appliance using the reboot command when the cursor returns from the pnrset command.
CSCpn01293	<i>Issue:</i> When administering MARS, it is possible to select an unsupported OS from the pull-down menu when adding or editing a host for logging. If you select an OS that does not contain the string “Microsoft Windows” or “Sun Solaris” when you save the Pull host log or Receive hostlog parameters, (for example, if you select “Sun Cobalt”), then the GUI does not work correctly.
CSCpn01270	<i>Issue:</i> The free-form search may not work for the following devices: <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 • Enterecept Enterecept, 2.5 and 4.0 • IntruVert IntruShield, 1.5
CSCpn01219 (re-opened)	<i>Issue:</i> If you create a user in the MARS GUI and select New Provider but do not enter a Pager number, qpage.com fails to run because it has an empty entry, and pnmonitor continually tries to restart the daemon that attempts to access qpage.com. <i>Resolution:</i> Open each user profile and click Submit to ensure all the required fields are populated.
CSCpn01134	<i>Issue:</i> The cloud name input box accepts invalid characters. To reproduce this behavior, click on the Large Graph link on the Hotspot graph. Click on a cloud. Click Change name and enter invalid characters into the input field (for example, ~!# or ###). Sometimes the page returns an error message such as error: Error: Invalid or No Security Perimeter. The graph rendering fails with the IE status bar message “not well formed, line #:column#”.
CSCpn01051	<i>Issue:</i> Logging into a MARS from a non-supported browser and leaving the GUI open will prevent other users from logging into that MARS. <i>Resolution:</i> If you log in to MARS using a supported browser and see a message saying that your browser is unsupported, please check if another user has logged into the MARS with an unsupported browser and not closed his browser window.
CSCpn01045	<i>Issue:</i> Entering an incorrect IP address or directory path for the data archiving feature will result in a cryptic error message. <i>Resolution:</i> If you see a message of type “Status: PN-0002: No message for PN-0216” after configuring data archiving, please click “Back to Archiving” and check your IP address and directory.

Reference Number	Description
CSCpn00908	<p><i>Issue:</i> “Domain” in Configuration page - no use</p> <p><i>Workaround:</i> This issue was overcome by other events. This field no longer exists, however, you can specify the e-mail domain on the Configuration page to identify the default domain from which e-mail notifications are delivered by the appliance.</p>
CSCpn00610	<p><i>Issue:</i> Backend logs can be out of order in the view page because the numbers are reused. Timestamps should be used as report identifiers.</p>
CSCpn00596	<p><i>Issue:</i> On a freshly installed machine starting to get events and sessions, you can get a negative Data Reduction where there are more sessions than events. This is due to the fact that events are written to the database more frequently than sessions.</p> <p><i>Resolution:</i> Wait for some time to pass, as events gradually outnumber sessions this number will become increasingly accurate.</p>
CSCpn00586	<p><i>Issue:</i> If you are investigating a false positive, and you see a message telling you that a service has crashed, this could be due to vulnerability scanning by the MARS appliance. You may have to re-start the service.</p> <p><i>Resolution:</i> It is strongly recommended that you patch the security hole to eliminate this vulnerability.</p>
CSCpn00455	<p><i>Issue:</i> If clouds are renamed through diagrams, the system might not display those names.</p> <p><i>Resolution:</i> Here are some work around steps to rename clouds:</p> <ol style="list-style-type: none"> 1. Click the cloud you want to rename. 2. Enter in the new name in the text field near the top of the popup window. 3. Click “Change”. 4. Once it's done, click “Close”. 5. Click the “Large Graph” button in the Hotspot Graph. 6. Return to the Summary page.
CSCpn00293	<p><i>Issue:</i> When tabbing over three-digit entries in IP fields on the Configuration Information page, the cursor can disappear.</p> <p><i>Resolution:</i> Use your mouse to move between fields on this screen when editing IP addresses.</p>
CSCpn00259	<p><i>Issue:</i> On the Setting Runtime Logging Levels page, if you set the level for GUI to Trace and save, it is saved as Debug.</p> <p><i>Resolution:</i> Do not change settings on the Setting Runtime Logging Levels page without a Cisco Support representative.</p>
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>
CSCpn00212	<p><i>Issue:</i> Diagrams on the Summary pages occasionally do not display.</p> <p><i>Resolution:</i> Exit the browser. The next time you log on, the diagrams should have re-drawn.</p>
CSCpn00183	<p><i>Issue:</i> Adding many devices (more than 20) without activating those devices can cause messy output in the diagrams.</p> <p><i>Resolution:</i> Click the Activate button after adding many devices.</p>
CSCpn00173	<p><i>Issue:</i> Nessus should check pre-NAT address instead of Post-NAT address.</p>

Reference Number	Description
CSCpn00166	<i>Issue:</i> The use of ANY in queries and rules is slightly inconsistent. When selecting ANY in the Query page, if other items are selected at the same time for that field, the ANY is ignored. When selecting ANY on the Rules page, if other items are selected at the same time for that field, the other items are ignored and ANY is the selection.
CSCpn00146	<i>Issue:</i> Identical reports differed by slashes and dashes result in conflicting reports. When you have reports with identical names differing only by slashes (/) and dashes (-), running and viewing the reports causes them to get confused and point at the other. <i>Resolution:</i> Do not use slashes or dashes in your rule configuration.

Resolved Caveats - Release 4.2.1

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

Reference Number	Description
CSCse54819	Need to add more annotations to notification schema file
CSCse53491	Anomaly detection: incident should fire but does not
CSCse52649	'pnrestore -m 5' fails to restore late night backup
CSCse52205	janus.conf not upgraded when restoring to an upgraded mars box
CSCse51404	Slow device loading causes processes to be restarted repeatedly
CSCse50303	pn_event_type_range initial value correction
CSCse48719	Pull out a disk. The disk error notification is not received by pndadmin
CSCse47753	Should display OS version and Patch
CSCse47646	JBoss installation allows remote command execution
CSCse47379	Batch query on GC returns no results
CSCse47111	Nowhere to input long description of an event_type_info
CSCse46123	Change made to DNS config from GUI doesn't take effect
CSCse45962	avoid pink-box on the GC Incident page when mapping info is missing
CSCse45895	Real-Time (raw events) blocks and fails to display new events
CSCse45886	postfire lagging behind writing incidents
CSCse45878	Missing 'ANY' option in the OS vendor drop down list
CSCse45846	postfire drops sub-incidents
CSCse45793	Potential for process_event and process_postfire to get out of sync
CSCse45789	Report Group : Batch query reports listed as System Reports.
CSCse44384	3ware controller write cache was turned off
CSCse43729	add desc to service TCP and UDP/5401: "CSA communication
CSCse43576	Case Management attach Networks Ranked by Session report get Pink Box
CSCse43291	Device name not updated in janus.conf on mars20r
CSCse39959	event ID 3002476 does not had a description associate to it
CSCse38778	Device Event Type Vendor Info has bad link for many Cisco devices

Reference Number	Description
CSCse38776	Email of case with multiple 5K reports fails to be received
CSCse38668	System should allow deleting pn_config_sync_log with audit_log_id < 1000
CSCse36971	clicking the icon "q" on display will change the query to sessionized
CSCse36851	GC/LC: reported user became ANY after GC on demand report is pushed to LC
CSCse36639	Java Null pointer exception for LLRTRRequest
CSCse35742	Real-Time (raw events) fails to display device name for dynamically created devices.
CSCse35313	DTM: Signature Inactivity Interval for deletion - NEVER option
CSCse34746	"Reported User" condition doesn't work in process_inlinerep_srv reports
CSCse34575	incidents fired by system are not pushed to the GC
CSCse34309	Real-Time (raw events): on Real-Time (raw events) scrolling page, change the default speed to fast mode
CSCse34146	Real-Time (raw events): on select query page, raw events option should be the first one
CSCse34138	Real-Time (raw events): on scrolling page, pause button should be at right side
CSCse33144	HTML Page is directed to null when adding a device with existing IP
CSCse31732	changing raw event query condition will change the query to sessionized
CSCse29259	javaDbImportExport is not consistent for class DbDeviceType
CSCse29185	pnparser crashes with 2k/s pix events when verifying CSCsd67636
CSCse28847	windows pulling very slow if one server is down/unavailable
CSCse28774	New rule/report group data missing/incorrect on upgraded box
CSCse27195	pnrestore blocked
CSCse26385	popup unclosed after emailing case if attached records are more than 500
CSCse25614	Log Parser does not parse 609001 and 609002 correctly from ASA-PIX
CSCse24791	can't attach big query report from inline submit
CSCse23078	attached incident is lost after data is purged
CSCse23070	view report of query type of detailed NAC report got pink box
CSCse22827	CSM icon should not be displayed on events from unknown reporting devices
CSCse22614	QualysGuard case not handled in False Positive confirmation page
CSCse22578	attached incident info was lost after migration for the open cases
CSCse21965	XML incident notification doesn't include all matched rule offsets
CSCse21955	ACS RADIUS accounting messages get sessionized incorrectly
CSCse21950	Transfer bytes in incident archive files are zero
CSCse21845	Real-Time (raw events) Query: Blank src/dst IP/port columns
CSCse21559	"Reported User" condition doesn't take effect
CSCse21417	View report save from query(event Type ranking) wrong color of 1st rank
CSCse21340	Must update Help --> About --> Documentation URL for 4.2
CSCse20764	CSM: Policy query with test connect failure
CSCse20736	Restart of syslogd is needed on a linux box after configuring it
CSCse20702	Incorrect reporting device showing in the unknown events query

Reference Number	Description
CSCse20691	CSM:Policy query icon
CSCse20493	Symantec AntiVirus Server config guide needs addition of controller's ip
CSCse20312	IDP-side Configuration missing controller's ip address
CSCse20242	mars not processing certain device (routerToLab) syslog messages
CSCse20041	CSM policy query icon for netflow events
CSCse20014	SigTool, EventTypes, going backwards in Add gets pink box
CSCse19472	pndbusage command accepts arguments without complaining
CSCse19392	CSM: Policy query for ICMP traffic
CSCse19203	process memory exceeded and pnesloader was killed on mars20r
CSCse18978	found extra line in updateAK xml file
CSCse18873	The detail report result didn't be added to a case
CSCse18851	pinkbox in case management after show all
CSCse18782	migration doesn't work at all
CSCse18240	DOC: cs-mars doesn't handle vpn paths
CSCse17939	ssh root login incorrectly allowed
CSCse17880	Incorrect service handling in low latency (real time) viewer
CSCse17864	Device info was lost after migration
CSCse17777	5K Query - Pink box in query for all matching sessions
CSCse17403	Configuration can persist on Community Strings and Networks page
CSCse17345	Pink box on GC when viewing devices by zone
CSCse17089	CS-MARS Installation Guide - VGA and Serial Ports swapped in diagram
CSCse16262	Improve msg displayed when click policy icon but CSM configured
CSCse16007	The output of pndbusage shows a wrong timestamp
CSCse15994	The '?' question mark did not trigger the command usage display
CSCse15303	pnarchiver - ORA-01455: converting column overflows integer datatype
CSCse15015	"Query on this ..." icon missing for event type in raw event query.
CSCse14666	Real-Time (raw events): Fails to display five tuple for IDS/IPS/IOSIPS events
CSCse14655	Real-Time (raw events) - displays Trigger packet/ Context Data/ IP Log in wrong format
CSCse14634	low latency real time viewer: alignment of src ip /port and dest ip / port
CSCse13971	Incident archived files could be lost in certain conditions
CSCse13922	Selecting "Raw Events" from RT pulldown erroneously disables widgets.
CSCse13904	low latency real time viewer: restart won't start from now (current time)
CSCse13359	archiver failing to archive report results data
CSCse12452	Mars - legend on graph is off by one color with full size graphs
CSCse11036	Oracle event/session partition purging is incorrect
CSCse10933	Sigtool create report: Filter does not show report created.
CSCse07865	DOC: can't do keyword searches on pix url logs

Reference Number	Description
CSCse07579	Sigtool Vulnerability Add: Cannot perform add.
CSCse07405	Protocol name should match the types we support
CSCse06197	Sigtool System Setup: Default IP address incorrect.
CSCse06051	Null Pointer Exception on Low latency real time viewer when backend ...
CSCse04786	“Realtime viewer temporarily unavailable” Error popup
CSCse04705	pnrestore cannot restore os from other models to MARS20 model
CSCse03448	CS-Mars - special characters not supported in activation key field
CSCse03254	Inconsistent population of CSM icon for ICMP messages
CSCse01818	low latency real time viewer doesn't display all of events
CSCsd96095	Sigtool Event Type Group Add: Leading/Trailing spaces in event group.
CSCsd96070	Case mgmt emails with multiple 5k reports aren't useable
CSCsd96033	Sigtool Event Group Delete: Problem if event not selected.
CSCsd92161	Customer gets pink box in UserConfirmedFalsePositivePage.jsp
CSCsd88081	Customer pink box at URL /Admin/Devices/SubmitDevicePage.jsp
CSCsd87778	[CSIRT] Incidents should link to device name instead of IP in GC
CSCsd86925	Top N signatures are not updated on DTM
CSCsd86719	Raw event query type changed to sessionized after condition is set
CSCsd86706	"Raw Events" displayed when other filter is selected
CSCsd83991	CS-MARS/CSM: Lookup of denial event found different ACL
CSCsd83692	CS-MARS/CSM: Credentials change for CSM not checked.
CSCsd83688	CS-MARS/CSM: Credentials: password change not checked.
CSCsd81330	Processing VPN events before pix events caused unknown event type for pix
CSCsd80458	Error in PnParsedEvent serialization could cause event data corruption
CSCsd79114	Small number of Raw Events are not displayed in real time
CSCsd79072	“Raw Events” selection missing when query is modified again
CSCsd79063	Deleting reports without activating causes inlinerep_srv to stop working
CSCsd78717	Cannot add an IDSM with same reporting IP as switch to a Switch device
CSCsd77422	Sigtool Pattern add: In edit mode if pattern is selected.
CSCsd77402	Sigtool Pattern add: Return from add after problem occurs.
CSCsd77398	Sigtool Pattern add: Save with empty value pattern.
CSCsd76965	Sigtool Appl add: Appl texts disappeared after modifying dev os.
CSCsd76960	Sigtool Appl add: Can't delete device os.
CSCsd76957	Sigtool Appl add: Leading/trailing spaces in Device OS Name.
CSCsd76956	Sigtool Appl add: Device OS "Name" accepts blank input.
CSCsd76932	Sigtool Appl add: Should label mandatory device os vendor field.
CSCsd76007	Device doesn't update its Device type list after new Application add on
CSCsd75950	Sigtool Delete Service Group: Problem after service group deletion.

Reference Number	Description
CSCsd72868	Sigtool Add Event Type Group: spaces in event group type name
CSCsd72169	DOC - LC 4.1 logging emblem instructions are confusing
CSCsd72022	network didn't been added into group
CSCsd71954	Sigtool Add Event Type Group: Problem from empty event type description
CSCsd71897	Sigtool Event Filter by Sev: Sev text missing in Event Types display.
CSCsd71818	Sigtool Event Type Edit: Should prompt duplicate event type name
CSCsd71817	Sigtool Event Type Create: Abbreviations in event map
CSCsd71815	Sigtool Event Type Create: Name mismatch (Event Type vs Event ID)
CSCsd71809	Sigtool Event Type Create: Should prompt duplicate event type name
CSCsd71805	Sigtool Event Type Create: Missing mandatory info should trigger message
CSCsd71794	Sigtool Event Type Create: Cancel button refinement
CSCsd71787	Sigtool Event Type Create: Model/Version choices initially not available
CSCsd70108	Sigtool edit device type: No message when device type can't be saved
CSCsd70087	Sigtool add device type: No message when missing information.
CSCsd70042	Sigtool add device type: No message for device types that can't be added
CSCsd70000	Sigtool device type delete: No message for device that can't be deleted.
CSCsd68896	Sigtool view report group: System Reports emptied after group access.
CSCsd68810	File permissions on two files incorrect
CSCsd67636	pnparser cpu goes 99% in sessionization for traffic of 1 k/sec
CSCsd67492	Sigtool delete rule: "Delete" button is not present.
CSCsd67474	Sigtool rule edit: Edited rule should be saved.
CSCsd65943	process_inlinerep_srv goes to 99% CPU
CSCsd64438	pnparser crashed at 2.5k/s for relayed syslog and stops receiving events
CSCsd63437	Many "false alarm" errors in Rule/Report import into CS-MARS
CSCsd62251	Incorrect parsing for all Windows MSSQL event pushing
CSCsd60252	MS SQL error 18453 should be in "Trust" group
CSCsd59102	rpcclient2 is incorrect in the current CD packages
CSCsd59044	Error in 4.2.1 db schema script
CSCsd54625	SigTool: Editing Event Type doesn't save changes
CSCsd54620	SigTool: Can't delete report
CSCsd54614	SigTool: services don't appear in service group selection window
CSCsd54597	SigTool: System Error when creating new Vulnerability
CSCsd54541	SigTool: Can't create Application
CSCsd54144	A closed case can be re-open.
CSCsd53037	Customer feedback reports pink box adding a user
CSCsd51554	pink box on GC local controller management page
CSCsd49703	Popup a window with all of device names when discovering an IOS device

Reference Number	Description
CSCsd48577	graphgen cannot be started on some MARS boxes
CSCsd48460	TopN: pull interval and URL cannot be retrieved from DB
CSCsd48097	Processes restart continuously if pnparses creates shared buffers first
CSCsd47251	extra space in the name of "DTM_TOPN_SIG_ACTION" in pn_sys_param table
CSCsd46831	CS-Mars - need to specify exact version support for Check Point firewall
CSCsd35354	Anomaly Profiling does not include denies and other non-pix flow events
CSCsd35158	Should not send feedback to protego-feedback.
CSCsd33735	MARS need remove quotation marks from the ACL name passed to CSM
CSCsd31984	Dam account has default password
CSCsd31972	CS-MARS CLI Privilege Escalation
CSCsd31202	mars internal protocol numbers
CSCsd29152	Password found in shell script
CSCsd28493	View Case document selection doesn't work after e-mail report results
CSCsd28491	View Case document selection doesn't work after e-mail query reports
CSCsd28487	View Case document selection doesn't work after e-mail device info
CSCsd28482	View Case document selection doesn't work after e-mail sessions
CSCsd28393	View Case Document selection doesn't work after e-mail incidents
CSCsd28307	attached incident doesn't be shown in the first e-mail
CSCsd28246	There are two users as pndadmin in "Admin" user group
CSCsd28200	"select All" button doesn't work as expected
CSCsd28192	can't keep selected user group(s), or users
CSCsd27874	e-mail to pndadmin twice if selecting "Admin" user group
CSCsd26018	PnParser uses more than High CPU doing sessionization from FWSM events
CSCsd25395	Fix GUI errors caused by 0 id in report database tables
CSCsd25151	adding indexes to optimize DbClient::retrieveParserDeviceInfo()
CSCsd25144	Need to add CPU check for pnesloader and mem check for graphgen
CSCsd25027	device list page got pink box when there is no device agent exists
CSCsd24864	GUI Devices add/edit SW Vuln. Assessment Info does not show device name
CSCsd23721	FWSM events parsing error
CSCsd22430	CSM integration: interface name not parse correctly for FWSM events
CSCsd22299	Got "parsing error" in the syslog-ng relayed solaris syslogs
CSCsd20988	An invalid session can be added to the current active case
CSCsd20976	An invalid incident can be added to the current active case
CSCsd20967	The pink box is shown when adding an invalid case
CSCsd15308	ICMP Type not parsed for event PIX-n-106100
CSCsd14963	switch.csv doesn't work
CSCsd13966	case history is located among the attachments, not the last one

Reference Number	Description
CSCsd10764	It's meaningless to attach a session twice or more through gui
CSCsd10754	It's meaningless to attach an incident twice or more through gui
CSCsd10718	It's meaningless to allow attaching a device twice or more through gui
CSCsd09771	A report can be added by not clicking "Add This Report
CSCsd09761	A session can be added by not clicking "Add This Session
CSCsd09745	the changed e-mail subject is back to default value after changing filter
CSCsd09739	Adding device info can't be done if click "more" then "submit
CSCsd09722	Device Info is added by not clicking "Add Device Info
CSCsd09705	Adding an Incident can be done by not clicking "Add This Incident
CSCsd09693	Reference case can't be done right way if I click "more" then "submit
CSCsd09662	Reference case can be done by not clicking "Reference This Case
CSCsd08503	Report - Not Healthy - All Events missing from NAC group
CSCsd00682	MARS needs to handle null value returned from CSM DeviceQuery
CSCsc95485	QualysGuard support: need to add missing part in postfire
CSCsc94043	Include time attribute and value in raw message from IDS/IPS/IOSIPS
CSCsc89884	MARS does not pull log from a windows box if both pull/push are checked
CSCsc87879	CS-MARS - SDEE subscriptions are dropped
CSCsc80185	Unknown Events seen by MARS from PIX and FWSM
CSCsc79646	make GC "Security and Monitor Device" page more robust
CSCsc67926	CSM response parsing error
CSCsc67806	DTM: csdam process syslog sending leaves hanging resources
CSCsc66154	GC rule incidents aren't pushed up after modifying the rule on the LC
CSCsc65845	XML Notification with Incident details
CSCsc59395	ASA parsing gives wrong event types for a few event types
CSCsc57192	Unable to add inline reports to a case
CSCsc54966	fqdn not displayed for some devices on security and monitoring info page
CSCsc50791	MARS needs to provide CSM the interface names for policy query
CSCsc50789	Add Reporting IP to auto discovered devices.
CSCsc50787	MARS needs to provide CSM the ICMP code as part of the policy query
CSCsc50187	Policy display doesn't handle white-spaces in object names properly
CSCsc50175	Some FW inspect syslog messages are not parsed by CS-MARS
CSCsc47258	Need an alert to CS-MARS when current partition is getting full
CSCsc46900	enhance fixed (24 hr) stat values in Summary page to menu
CSCsc46892	a special report for NAC
CSCsc40930	XML parsing for IOS-IPS doesn't include changes/ fixes for IPS 5.x
CSCsc40721	There are several unfunctional buttons in E-mail for Case Mgmt
CSCsc36969	MARS needs to provide CSM 'Action' information from the syslog message

Reference Number	Description
CSCsc36957	MARS needs to provide CSM ACL Name from the syslog message
CSCsc35671	windows pulling could get stuck and block pulling for all other machines
CSCsc34091	Unparsed FWSM 2.3 log messages
CSCsc33942	create alert on dropped event threshold
CSCsc31561	Test connectivity on IOS IPS leads to name change for parent IOS
CSCsc31386	Uninitialized agent_id for unknown reporting device sending netflow
CSCsc30816	NO CSM Access Rule Lookup ICON on the raw message query page
CSCsc30044	Symantec AV Dynamic Agent Creation
CSCsc30033	Windows Application Log Pulling
CSCsc27856	FR - CS-Mars - multiple email addresses for email case button
CSCsc25189	CSM Integration task: paging support for the MARS Policy Query UI
CSCsc24704	Error occurred while querying policies from CSM for ICMP events
CSCsc23631	Scheduled reports with only a != don't work
CSCsc22088	syslog ID 109023 - User must authenticate first - not recognized by MARS
CSCsc22055	syslog ID 313004 - Denied ICMP - not recognized by MARS
CSCsc21724	MARS needs to get SDEE errors in addition to alerts
CSCsc20839	Syslog Relay (Proxy) support in MARS
CSCsc20831	DTM: Current Top N signature pull from CCO
CSCsc20816	IIS Site Protector support
CSCsc08886	Nice to allow user to remove things from Case Management cases
CSCsc07741	If Viewing closed Case, then do refresh, get an email sent
CSCsc07680	CS-Mars - Default Oracle passwords created for SYS and SYSTEM users
CSCsc06218	802.1x GUI host info incorrect
CSCsc06086	Policy Tag from CheckPoint Logs need to be in Raw Message
CSCsc05980	There is a system error when viewing purged data
CSCsc05948	There is a system error when viewing the cases that have data purged
CSCsc05908	The data is lost which is attached in the closed case
CSCsc04637	Closing a Case does not deselect it
CSCsc03230	Not all of query results were added in the case document
CSCsb97824	Seed File load need to support IDS/IPS device type
CSCsb88410	IP to value needs to assign same time value for ACS entries
CSCsb87935	keyword search doesn't work in reports that run in process_inlinerep_srv
CSCsb71298	GC queries less than 10 minutes are always In Progress
CSCsb70130	IDS context information should be displayed after decoding
CSCsb70121	IDS alert vlan id, action information should be in raw message
CSCsb52032	Improved handling of purged data attached to cases
CSCsb23722	Test connectivity failed for a qualys guard device

Reference Number	Description
CSCpn03046	oracle pulling timer modification does not take effect
CSCpn03044	Parser need to ignore the sev number X in PIX_X_YYYYYY syslog
CSCpn03041	PIX7.0, parsing error %PIX-4-411001/411002
CSCpn03019	Load Security Device from CSV has invalid device name
CSCpn02623	sudden traffic increase does not process ICMP events
CSCpn02587	CSV for different type of windows
CSCpn02322	Device type / version change for at least a selected set of device(s)
CSCpn00066	New Version of devices

Resolved Caveats - Releases Prior to 4.2.1

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.