



Quick Install and Release Notes for Cisco Security MARS Appliance 4.2.5

Revised: July 24, 2009, OL-12961-01



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

These release notes are for use with the Cisco Security Monitoring, Analysis, and Response System (MARS), Version 4.2.5 running on any Local Controller or on any Global Controller. They provide the following information:

- [Introduction, page 1](#)
- [Supported Hardware, page 2](#)
- [New Features, page 2](#)
- [Upgrade Instructions, page 3](#)
- [Important Notes, page 10](#)
- [Quick Install Notes, page 12](#)
- [Caveats, page 16](#)
- [Product Documentation, page 23](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 24](#)

Introduction

Version 4.2.5 is now available as a upgrade to 4.2.4 (2428) or 4.2.4 (2432) of your MARS Appliance software. Registered SMARTnet users under the can obtain version 4.2.5 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.



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

© 2007 Cisco Systems, Inc. All rights reserved.

Supported Hardware

Cisco Security MARS Version 4.2.5 supports the following Cisco Security MARS and Protego Networks MARS appliances:

Local Controller Appliances

- Cisco Security MARS 20 (CS-MARS-20-K9)
- Cisco Security MARS 20R (CS-MARS-20R-K9)
- Cisco Security MARS 50 (CS-MARS-50-K9)
- Cisco Security MARS 100 (CS-MARS-100-K9)
- Cisco Security MARS 100e (CS-MARS-100E-K9)
- Cisco Security MARS 200 (CS-MARS-200-K9)
- Protego Networks PN-MARS 20
- Protego Networks PN-MARS 50
- Protego Networks PN-MARS 100
- Protego Networks PN-MARS 100e
- Protego Networks PN-MARS 200

Global Controller Appliances

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

New Features

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

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

Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 4.2.5:

- **Support for Extended Daylight Savings Time.** On March 11, 2007, the United States will adjust to Daylight Saving Time (DST) three weeks earlier than previous years and will end one week later on November 4, 2007. As per the Energy Policy Act of 2005, MARS supports this change in 4.2.4.
- **Bug fixes.** For the list of resolved issues, see [Resolved Caveats - Release 4.2.5, page 21](#).

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	S272
McAfee Enterecept HIDS 4.1	Agent Version 40-56
ISS RealSecure Network Sensor 7.0	24.55
ISS RealSecure Server Sensor 7.0	24.55
McAfee IntruShield NIDS 1.8	2.1.57.3
Snort NIDS	2.4 (12-15-2006)
Juniper Networks IPS/ Netscreen IDP 2.1	2.1r7
Enterasys Dragon 6.x	Latest signatures as of 2-20-2007
Symantec Manhunt	3.4.3 Update 59
Symantec NIDS	4.0 Update 69
Qualys QualysGuard 3.x, 4.x	Latest Knowledge Base XML file as of 1-15-2007
Common Vulnerabilities and Exposures (CVE) Database	Latest as of February 2007

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 regularly 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 4.2.5

The 4.2.4(2432) patch was released to address an issue with the MARS system timezone patch in 4.2.4 (2428). The 4.2.5 update includes the patch, and therefore, you are not required to apply the 4.2.4(2432) patch if you are currently running 4.2.4 (2428). This issue, detailed in CSCsi08897, only affects a few timezones; therefore, many customers would never experience the issue.

Upgrade to 4.2.4

No important notes exist for the 4.2.4 upgrade.

Upgrade to 4.2.3

The 4.2.3 upgrade package is approximately 1.6 GB due to the large number of signatures updated and due to the inclusion of a patch to the database software, which was added to address CSCsg02873. Downloading the PKG file may take up to 7 times longer than previous packages.



Note

Enable archiving on the MARS Appliance for two to three days *before* you perform you attempt to upgrade from 4.2.2 to the 4.2.3 release. This precaution is strongly recommended in case reinstallation is required due to any encountered errors.

To upgrade from 4.2.2 to 4.2.3, follow these steps:

Step 1 Verify that your MARS Appliance does not have hard drives that are degraded or rebuilding by performing the following steps:

- a. At the CLI, enter the following command:

```
raidstatus
```



Tip

For more information on accessing the CLI, see the “Establishing a Console Connection” section in Chapter 5, Initial MARS Appliance Configuration, of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

For more information on the `raidstatus` command, see “`raidstatus`” in Appendix A, Command Reference of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

- b. Verify that hard drives are neither in rebuilding nor degraded status. If they are, please wait until all hard drives have finished rebuilding before attempting an upgrade.

Step 2 Verify that the MARS Appliance has at least 3GB of space available on the partition /u01 by performing the following steps:

- a. At the CLI, enter the following command:

```
diskusage
```

One of the lines should describe the /u01 partition:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/md3        16G   4.6G   10G   31% /u01
```

For more information on the `diskusage` command, see “`diskusage`” in Appendix A, Command Reference of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

- b. Verify at least 3 GB available is available (the example has 10G available).

A nightly process runs to clean up any files that accumulate on this partition. If you have less than 3 GB, there is an issue with your appliance that you must resolve prior to upgrading.

Step 3 Perform the software upgrade. The CLI method is **strongly recommended**.



Note While the GUI upgrade works, it does not show progress of the upgrade. Use the CLI instead to ensure the progress of the update is known. **Do not** reboot the appliance until the upgrade has completed.

For more information on performing the upgrade using the command line, see the following information:

- “Checklist for Upgrading Appliance Software” in Chapter 6, Administering the MARS Appliance of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.
“pnupgrade” command in Appendix A, Command Reference of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.
- “Upgrading from the CLI” in Chapter 6, Administering the MARS Appliance of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

Step 4 After the automatic system reboot, verify the upgrade by performing the following steps:

- a. At the CLI, enter the following command:

pnstatus

For more information on the pnstatus command, see “pnstatus” in Appendix A, Command Reference of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

- b. Verify that all processes are running.

If some processes are not running, you must troubleshoot that issue before proceeding with the upgrade.

- c. Enter the following command:

pnupgrade log

For more information on the pnupgrade log command, see “pnupgrade” in Appendix A, Command Reference of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x*.

- d. Verify that the output looks like the following:

```
[pnadmin]$ pnupgrade log
-----
 4.2.2 2303  --> 4.2.3 2403
-----
1 Preparing upgrade start
  1.1 Load the step table start
  1.1 Load the step table end
  1.2 Stop pnmonitor start
  1.2 Stop pnmonitor end
  1.3 Stop jboss start
  1.3 Stop jboss end
  1.4 Stop other applications start
  1.4 Stop other applications end
1 Preparing upgrade end
2 Upgrade OS start
  2.1 Patch OS start
  2.1 Patch OS end
  2.2 Patch Oracle start
  2.2 Patch Oracle end
2 Upgrade OS end
```

```

3 Upgrade schema start
  3.1 Run upgrade schema script start
  3.1 Run upgrade schema script end
  3.2 Backup schema script start
  3.2 Backup schema script end
3 Upgrade schema end
4 Upgrade MARS applications start
  4.1 Untar MARS executable binary start
  4.2 Untar MARS executable binary end
  4.3 Modify janus.conf start
  4.3 Modify janus.conf end
  4.4 Swap MARS executable binary start
  4.4 Swap MARS executable binary end
  4.5 Run post-unpack-deployment start
  4.5 Run post-unpack-deployment end
4 Upgrade MARS applications end
5 Upgrade data start
  5.1 Start jboss start
  5.1 Start jboss end
  5.2 Importing signature data start
  5.2 Importing signature data end
  5.3 Missing-id fix start
  5.3 Missing-id fix end
5 Upgrade data end
6 reboot ...
Upgrade from 4.2.2 2303 to 4.2.3 2403 finished.

```

If the log does not include the “Upgrade from 4.2.2 2303 to 4.2.3 2403 finished” line, then a problem occurred during the upgrade regardless of whether the **version** command reports 4.2.3 (2403).

Special Note for Post Upgrade of a Global Controller/Local Controller Deployment

In a Global Controller/Local Controller deployment upgraded from 4.2.2 to 4.2.3, the communication states between the Global Controller and one or more Local Controllers can be out of sync. This issue is detailed in CSCsh38818.

The Global Controller identifies the Local Controller as Active, and the Local Controller identifies itself as Offline. Toggling “Suspend/Resume” from the Global Controller’s Local Controller Management page toggles both states, causing the Global Controller to consider the Local Controller as Suspended while the Local Controller considers itself as Online and resumes pushing information to the Global Controller.

This “out of sync” state affects Global Controller/Local Controller deployments that are upgraded from 4.2.2 to 4.2.3.

To determine whether a Global Controller/Local Controller pair is in this error state, follow these steps:

-
- Step 1** The Global Controller and all associated Local Controllers are upgraded from 4.2.2 to 4.2.3 (see upgrade instructions in [Upgrade to 4.2.3, page 4](#)).
 - Step 2** Log into the Global Controller web interface, and select **Admin > System Setup >- Local Controller Management**.
 - Step 3** For each Local Controller, select the Local Controller checkbox and click **Details**.

- Step 4** Verify that there is a discrepancy between the status on the Global Controller and the status of the Local Controller. Specifically, the status on the Global Controller shows that an Local Controller is “Active”, while the Local Controller web interface shows that the Local Controller is Offline in the header - “CS-MARS Local Controller (Offline)”. Confirm the Local Controller status by logging into the Local Controller via its web interface.
- Step 5** Note each Local Controller that is in this “out of sync” state.

Once the error has been identified, follow these steps to exit the error state:

-
- Step 1** Log into the Global Controller web interface, and select **Admin > System Setup >- Local Controller Management**.
- Step 2** Select each Local Controller that is in this “out of sync” state, and click **Suspend/Resume**. Repeat until all Local Controllers in this “out of sync” state have been suspended.
- You can verify that the Global Controller sees each Local Controller as “Suspended” by clicking “Details” for that Local Controller to see if it shows that the Local Controller is no longer Offline - “CS-MARS Local Controller: [hostname]/[zone name]”
- Step 3** On the Local Controller Management page of the Global Controller web interface, select **Refresh Rate “1 minute”** from the pull-down menu.
- Step 4** Select **Admin > System Maintenance > License Key**, and verify that the correct number of Local Controllers (20/50s, and 100/200s) are counted by the Global Controller under “used”.
- Step 5** Select **Admin > System Setup > Local Controller Management** in the Global Controller browser window
- Step 6** Perform [Step 7](#) through [Step 10](#) for each Local Controller that is in this “out of sync” state.
- Step 7** Open an SSH shell to the Local Controller, and enter the following command:
- ```
pnreset -j
```
- Step 8** Enter **yes** to confirm the pnreset operation.
- Step 9** Within 20 seconds of entering the pnreset -j command, switch back to the Global Controller browser window and click the browser refresh button every 3 seconds until the Status message for that Local Controller displays “Not responding”. This is needed to re synchronize communication between the Global Controller and Local Controller.
- Step 10** Wait for the Local Controller Management page to refresh and verify that the Local Controller's status is now “Active” and the web interface for that Local Controller shows the Local Controller is Active (not Offline). Confirm the Local Controller status by logging into the Local Controller via its web interface.
- 

## Upgrade to 4.2.2

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

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

The following issues can occur when upgrading your reporting devices:

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

## Upgrade to 4.2.1

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

## Upgrade to 4.1.5

No important notes exist for the 4.1.4 upgrade.

## Upgrade to 4.1.4

No important notes exist for the 4.1.4 upgrade.

## Upgrade to 4.1.3

No important notes exist for the 4.1.3 upgrade.

## Upgrade to 4.1.2(2042)

The following notes detail changes to the standard upgrade process:

- If you completed the 4.1.1 to 4.1.2 (2040) upgrade, verify whether the upgrade failed by entering ``pnlog mailto <SMTP server> <sender> <recipient>'` at the CLI. This commands 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.

csmars-4.2.2.pkg

**Table 1** Upgrade Path Matrix

| From Version               | Upgrade To <sup>1</sup>       | 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 <sup>2</sup> |
| 4.1.2 (2040) without error | 4.1.2 (2042)                  | csmars-4.1.2.pkg <sup>2</sup> |
| 4.1.2 (2042)               | 4.1.3                         | csmars-4.1.3.pkg              |
| 4.1.3                      | 4.1.4                         | csmars-4.1.4.pkg              |
| 4.1.4                      | 4.1.5                         | csmars-4.1.5.pkg              |
| 4.1.5                      | 4.2.1                         | csmars-4.2.1.pkg              |
| 4.2.1                      | 4.2.2                         | csmars-4.2.2.pkg              |
| 4.2.2                      | 4.2.3                         | csmars-4.2.3.pkg <sup>3</sup> |

**Table 1 Upgrade Path Matrix**

| From Version           | Upgrade To <sup>1</sup> | Upgrade Package  |
|------------------------|-------------------------|------------------|
| 4.2.3                  | 4.2.4 (2428)            | csmars-4.2.4.pkg |
| 4.2.4 (2428) or (2432) | 4.2.5                   | csmars-4.2.5.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 \(2042\)](#).
3. The 4.2.3 upgrade package is approximately 1.6 GB due to the large number of signatures updated and due to the inclusion of a patch to the database software. Downloading the ISO image may take longer than previous packages.

## 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](http://www.cisco.com/en/US/applicat/cdcrgrstr/applications_overview.html)

## Important Notes

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

- Do not use DISTINCT or SAME in queries, and do not run multi-line queries in Release 4.2.5. 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.

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

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

| Reference Number | Description                                                                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSCpn02073       | <i>Issue:</i> After renaming a cloud, clicking the cloud again causes an error.<br><i>Workaround:</i> Refresh the page before clicking a renamed cloud.                                                                                                                                                                                          |
| CSCpn01270       | <i>Issue:</i> The free-form search may not work for the following devices: <ul style="list-style-type: none"> <li>• Check Point Opsec NG FP3</li> <li>• Cisco CSA, 4.0</li> <li>• Cisco, IDS, 3.1 and 4.0</li> <li>• ISS, RealSecure, 6.5 and 7.0</li> <li>• Enterecept Enterecept, 2.5 and 4.0</li> <li>• IntruVert IntruShield, 1.5</li> </ul> |
| CSCpn00247       | <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.<br><i>Resolution:</i> Please log out of the system when you are no longer using it.                                                                                                            |

## 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 13](#)

## 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. | <a href="#">Installing the MARS Appliance in a Rack</a>                    |
| Connect the MARS Appliance to an AC power source.               | <a href="#">Connecting to the AC Power Source</a>                          |
| Connect network and console cables.                             | <a href="#">Connecting Cables</a>                                          |
| Turn on the appliance.                                          | <a href="#">Powering on the Appliance and Verifying Hardware Operation</a> |

**Table 2** Quick Reference (continued)

| Task                                                       | References in Install Guide                                                |
|------------------------------------------------------------|----------------------------------------------------------------------------|
| Verify initial power up.                                   | <a href="#">Powering on the Appliance and Verifying Hardware Operation</a> |
| Perform initial configuration of the MARS Appliance.       | <a href="#">Checklist for Initial Configuration, page 13</a>               |
| Configure the MARS Appliance to monitor reporting devices. | <a href="#">Next Steps</a>                                                 |

## 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><b>1. Establish a console connection to the appliance.</b></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"> <li>• A direct console connection to the appliance using a keyboard and monitor</li> <li>• A standard serial console connection between a computer and the appliance using a terminal emulation package</li> <li>• An Ethernet console connection between a computer and the appliance using a terminal emulation package</li> </ul> <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"> <li>• <a href="#">Establishing a Console Connection</a></li> </ul> |

| ■ | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ | <p><b>2. Command Line Configuration: Setting the system administrative account's default password and configuring the interfaces.</b></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"> <li>• Collect the information required to configure the appliance to operate optimally on your network.</li> <li>• Log in to the appliance and change the password associated with the system administrative account (pnadmin).</li> <li>• Configure the eth0 network interface, specifying the default gateway and IP address and network mask pair for that interface.</li> <li>• (Optional) Configure the eth1 network interface, specifying the IP address and network mask pair for that interface.</li> </ul> <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><b>Note</b> 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"> <li>• <a href="#">Configuring Basic Network Settings at the Command Line</a></li> <li>• <a href="#">Change the Default Password of the System Administrative Account</a></li> <li>• <a href="#">Specify the IP address and Default Gateway for the Eth0 Interface</a></li> <li>• (Optional) <a href="#">Specify the IP Address and Default Gateway for the Eth1 Interface</a></li> </ul> |
| ■ | <p><b>3. Command Line Configuration.</b></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"> <li>• Log in to the appliance using the system administrative account and the new password.</li> <li>• Set the hostname of the appliance.</li> </ul> <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"> <li>• <a href="#">Specify the Appliance Hostname</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| ■ | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ | <p data-bbox="228 281 638 310"><b>4. Command Line Configuration.</b></p> <p data-bbox="269 325 1507 483">The third and final task of the initial CLI configuration involves specifying those settings that help ensure the integrity of the event correlation and complete your network connection, allowing access to the appliance from other hosts on the network. In other words, after you complete this phase, you can connect to and complete the appliance configuration using a non-console connection from any host on your network. To complete this task, you must:</p> <ul data-bbox="282 499 1286 751" style="list-style-type: none"><li>• Log in to the appliance using the system administrative account and the new password.</li><li>• Set any additional static routes.</li><li>• Set the clock.</li><li>• Set the NTP server settings.</li><li>• Set the DNS domain name.</li><li>• Connect the appliance to the network (that is, plug in the Cat 5 cables.)</li></ul> <p data-bbox="269 768 1507 861"><i>Result:</i> Now you have network connectivity. You can access the CLI interface using an Secure Shell (SSH) client on any host that can reach the appliance, and you can log in to the web interface to complete the initial configuration.</p> <p data-bbox="269 877 570 907">For more information, see:</p> <ul data-bbox="282 924 708 1041" style="list-style-type: none"><li>• <a href="#">Specify the Time Settings</a></li><li>• <a href="#">Set Up Additional Routes</a></li><li>• <a href="#">Completing the Cable Connections</a></li></ul> |

| ■ | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ | <p><b>5. Complete initial configuration using the web interface.</b></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 <a href="#">Web Browser Client Requirements</a>).</p> <p>During this phase, you configure the following:</p> <ul style="list-style-type: none"> <li>• Appliance license</li> <li>• Zone identification (Global Controller only)</li> <li>• E-mail server identification</li> <li>• DNS addresses</li> <li>• E-mail address for the system administrative account (padmin)</li> <li>• TACACS/AAA login prompt settings</li> </ul> <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"> <li>• <a href="#">Completing the Configuration using MARS web interface</a></li> <li>• <a href="#">Licensing the Appliance</a></li> <li>• <a href="#">Verifying and Updating Network Settings</a></li> <li>• <a href="#">Specifying the DNS Settings</a></li> <li>• <a href="#">Configure E-mail Settings for the System Administrative Account</a></li> <li>• <a href="#">Configure TACACS/AAA Login Prompts</a></li> </ul> |
| ■ | <p><b>6. Upgrade the appliance to the most recent software version.</b></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"> <li>• <a href="#">Checklist for Upgrading the Appliance Software</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Caveats

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

- [Open Caveats - Release 4.2.5, page 17](#)
- [Resolved Caveats - Release 4.2.5, page 21](#)
- [Resolved Caveats - Releases Prior to 4.2.5, page 23](#)

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 4.2.5

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

| Reference Number | Description                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| CSCsf31561       | FWSM 3.1 syslogs FWSM-3-717001 till FWSM-4-717031 have missing colon                                                                          |
| CSCsg00377       | show resource usage command reports incorrect connection usage                                                                                |
| CSCsg35110       | MARS Global Controller cannot import a Local Controller SSL security certificate if the LC zone name contains a forward slash character ( / ) |
| CSCsf31401       | MARS query does not highlight rules inside any policy group named Local                                                                       |

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

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsi13353       | Timezone Indiana-Pulaski County shows up as GMT in GUI                   |
| CSCsi09318       | Mars - Using IE7, any query over 2 mins to process result in error       |
| CSCsi07719       | Pnlog mailto is sending old error logs from the MARS                     |
| CSCsi06290       | no option for user to chose if they want to stay in GMT timezone         |
| CSCsi03686       | CS-MARS - HTML/XML tags are not escaped when displaying packet context   |
| CSCsi03658       | CS-MARS - IOS Discovery via Telnet/SSH fails with \$hostname in banner   |
| CSCsh99201       | MARS-Scheduled ranking report with ACTION filter produces empty results  |
| CSCsh98408       | Not displaying events from FWSM forwarded by an intermediate syslog-ng   |
| CSCsh97060       | MARs says it can delete up to 500 at a time but only lets you delete 50. |
| CSCsh94361       | TCP SYN Host Sweep On Same Dest Port causes high number false positives  |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsh93759       | Rules/reports with large queries not working                             |
| CSCsh89885       | Mitigation command not display properly in 4.2.4                         |
| CSCsh89445       | GUI allow users create rule without putting rule name                    |
| CSCsh84304       | show inventory command displays info on removed drives                   |
| CSCsh83068       | Report and query return no results under device type ANY                 |
| CSCsh82939       | MARS failed to restart if the hostname is changed after a restore        |
| CSCsh77508       | MARS is not displaying CSM icon for access-list syslog with severity 0   |
| CSCsh73553       | USB Keyboard does not work while re-imaging with DVD                     |
| CSCsh69765       | CLI date/time/ntp commands should reboot if time change exceeds 30 mins  |
| CSCsh68503       | ISS SNMP trap: need to parse another format for ICMP type/code fields    |
| CSCsh63444       | Rules should not correlate events unrelated different sources/dest       |
| CSCsh58754       | 4.2.2->4.2.3 upgrade sometimes stalls, succeeds after repeated tries     |
| CSCsh57236       | Unknown Reporting Device was missing on GC's DB pn_device table          |
| CSCsh56931       | Rule engine does not capture certain patterns over long time ranges      |
| CSCsh55822       | CLI Upgrade needs to be run in the background                            |
| CSCsh52537       | Repeated upgrades 4.2.2->4.2.3 fills hard drive                          |
| CSCsh51271       | GC is unable to update LC's device name under admin/LC management        |
| CSCsh44179       | Connection Errors cause inability to select zone in incident/rule edit   |
| CSCsh42151       | GUI Summary pg shows #events < #sessions & negative data reduction rate  |
| CSCsh39200       | MARS charts only display the data for few days                           |
| CSCsh35953       | MARS unable to add similar named contexts from different fwsm            |
| CSCsh31780       | CS-MARS: Duplicate device name checking is case-sensitive                |
| CSCsh29243       | MARS Device Type label needs to reflect support for IOS 12.2 and later   |
| CSCsh22871       | User can create a device named ANY                                       |
| CSCsh14454       | server.log can grow unbounded with in a single day                       |
| CSCsh01671       | Upgrade scripts need to report errors back to user for suitable action   |
| CSCsg98026       | pnlogagent causes acs log files to add (01) to file name                 |
| CSCsg91816       | Query for ICMP port 0 shows UDP/TCP results                              |
| CSCsg88601       | pnparser may automatically restart shortly after midnight                |
| CSCsg86481       | CS-MARS parsing error for ASA7.0 msg 302018                              |
| CSCsg83055       | parsing error for FWSM-n-302003 and FWSM-n-302004                        |
| CSCsg80475       | All incidents purged if event-session partition table is corrupted.      |
| CSCsg79246       | Getting a blank window when adding a device in IE 7                      |
| CSCsg75303       | GC: If chose LC specific device in rule, it doesn't pass to LC correctly |
| CSCsg74922       | MARS: License invalid after re-image from 3.4.3 to 4.2.2                 |
| CSCsg73786       | Devices should not be added to MARS if Discovery is unsuccessful         |
| CSCsg70386       | SSL uses key less than 1024                                              |

| Reference Number | Description                                                                  |
|------------------|------------------------------------------------------------------------------|
| CSCsg69859       | SNMP Layer 2 Discovery Error, when community string has been corrected.      |
| CSCsg66801       | Activity: All Events and NetFlow report chart is missing on summary page     |
| CSCsg64951       | Certain ASA 7.0 syslogs do not get parsed by MARS                            |
| CSCsg60114       | System error when generating NAC report                                      |
| CSCsg47022       | CS-MARS - Incorrect Start Times on Retrieved Raw Message Files               |
| CSCsg41549       | MARS discovery issues with Loopback IP on IP Unnumbered interfaces.          |
| CSCsg41027       | MARS - Retrieve Raw Messages Fails at 0%                                     |
| CSCsg38029       | high CPU usage in pnparser due to checkpoint NAT rules                       |
| CSCsg26352       | Getting a internal server error when trying to access a incident on GC       |
| CSCsg26225       | Graphs/Images do not show up in case related report emails using Lotus Notes |
| CSCsg20987       | CSMARS DTM sdf files are sent with invalid format                            |
| CSCsg20408       | FW-6-SESS_AUDIT_TRAIL Parsing Error                                          |
| CSCsg16843       | MARS reporting misleading licensing problem while trying to add a LC.        |
| CSCsg14082       | Default query Changed in system defined report                               |
| CSCsg13767       | SuperV doesn't detect/restart processes                                      |
| CSCsg10787       | CatOS telnet discovery failing.                                              |
| CSCsg08166       | Unable to discover ASA 7.0 Error: There is no Error Log for this Device      |
| CSCsg06339       | Getting a Timeout Occurred error when running a query with != as service     |
| CSCsg04079       | Lotus Notes client gets JavaScript error with emailed MARS report            |
| CSCsf96634       | MARS cannot discover new route added to a router                             |
| CSCsf31228       | Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031          |
| CSCsf31207       | Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs      |
| CSCsf31121       | Exception in Case Management code when deleting a report                     |
| CSCsf20103       | csips and csiosips occasionally crashing                                     |
| CSCsf18192       | Slow rendering of the GC Summary page                                        |
| CSCsf06019       | Generic Router UI must support multiple reporting applications               |
| CSCsf04540       | MARS: Javascript Error w/ Email Report-5496: document.getElementById         |
| CSCse99039       | Redundant tab add available module under Device type Cisco IOS 12.2          |
| CSCse98029       | Occasionally corrupted event data enters into MARS database                  |
| CSCse91636       | MARS - not all columns seen in CSV reports generated using custom column     |
| CSCse88764       | can't access a ftp server with a user ID/password including @                |
| CSCse85973       | Deleted windows custom parsing templates show up in the SW apps dropdown     |
| CSCse85564       | Cannot add devices to a report which has more than 35 devices.               |
| CSCse82042       | Change the Device Type Version for FWSM                                      |
| CSCse82022       | Unable to view reports starting with #sign in csv format                     |
| CSCse82017       | View HTML option for reports turns back to default report format - csv       |
| CSCse78089       | Unable to upgrade CS-Mars via GUI                                            |

| Reference Number | Description                                                               |
|------------------|---------------------------------------------------------------------------|
| CSCse73788       | MARS rediscovers Juniper Netscreen firewalls with wrong OS                |
| CSCse60240       | CS-Mars - report for old events include real-time events                  |
| CSCse56632       | Browser hangs if a device is added with more than 50 monitored networks   |
| CSCse54976       | Some incidents are not written to DB                                      |
| CSCse52782       | Can't change run-time to day in "Resource Issues: Server - Top Reporting" |
| CSCse52217       | Customer gets pink box in GenericHostDeviceEditManagement.jsp             |
| CSCse51438       | Login session timeout not detected when a real-time (LLV) query resumes   |
| CSCse45884       | LLV query causes client CPU to go to 100%                                 |
| CSCse45018       | MARS is unable to parse NetScreen 5.x syslogs                             |
| CSCse42953       | CS-Mars - unable to show L2 path when source and destination in same net  |
| CSCse38565       | Re-importing Symantec AV client CSV doesn't work                          |
| CSCse38356       | Windows pulling gets stuck for one IP due to invalid content in evt log   |
| CSCse35758       | Inability to trace when first and last event occurred on a query          |
| CSCse33688       | no events under Cisco Switch-IOS 12.2                                     |
| CSCse32600       | Exception with Query All Matching Sessions or All Matching Events         |
| CSCse32591       | dealing with duplicate hostnames in VA import                             |
| CSCse31722       | Cloud toggle only works on first page of reporting devices                |
| CSCse27948       | pink box when do query - ORA-01555: snapshot too old exception            |
| CSCse26964       | CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS                  |
| CSCse23191       | Disable 'No Pager' cmd sent by MARS to PIX, ASA, FWSM firewalls           |
| CSCse23176       | MARS Global Controller not producing alerts when losing LC communication  |
| CSCse23051       | viewing report of query type of MAC addresses report got pink box         |
| CSCse22838       | can't find priority for CSA NT-Event-Log events                           |
| CSCse21626       | Clicking activate is not taking effect                                    |
| CSCse20593       | CSM device type could not be added one time (OK most times)               |
| CSCse18865       | scalability issues in "My Reports" page                                   |
| CSCse18816       | UI takes 99% CPU, hanging browser and slowing system while expanding all  |
| CSCse17936       | 5K Lines Custom Query fails                                               |
| CSCse13038       | CS-Mars - learning of McAfee agents with invalid names                    |
| CSCse11258       | After group is deleted, items under "All" group not shown                 |
| CSCse10945       | Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)   |
| CSCse09127       | Failed load from csv returns incorrect status                             |
| CSCse03237       | Changes made to GC network groups are not propagated to active LC rules   |
| CSCse03134       | More control is needed over retrieve raw messages and cleanup             |
| CSCse03097       | CheckPoint LEA record comes to MARS later and later                       |
| CSCse00668       | rule definition changes can lead to empty reports                         |
| CSCse00626       | IP Management -> device group displays hosts only.                        |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsd93480       | FOLLOWED-BY in rules has looser constraints than desirable               |
| CSCsd92916       | CS MARS - Raw Ip Addresses in Custom Query email have incomplete URL     |
| CSCsd90181       | increasing pprestore robustness                                          |
| CSCsd89457       | Incorrect handling of time range for rules that fire periodically.       |
| CSCsd86896       | Clicking the clear button when editing the query type doesn't work.      |
| CSCsd73486       | Mars: Not able to recognize the event type for ISAKMP and IPsec messages |
| CSCsd69063       | Reported User with single-quote (') causes oracle error                  |
| CSCsd61749       | pprestore doesn't restore all of the system config                       |
| CSCsd53173       | Retrieve raw messages doesn't properly update the progress percentage    |
| CSCsd48231       | inaccurate total number of retrieved events/sessions displayed by Query  |
| CSCsd37005       | user must be able to change own password                                 |
| CSCsd28590       | CS-MARS - Inactive Reporting Device Rule is not configurable             |
| CSCsd22832       | Attempt to remove IP subnet from IP Management fails, with error         |
| CSCsd20196       | User and System Scheduled Reports fail to display data                   |
| CSCsd15695       | Summary dashboard showing incorrect statistics for false positives       |
| CSCsd13969       | resetting italics for GUI links                                          |
| CSCsd06302       | device name with single quote causes pink box                            |
| CSCsc97963       | Netscreen logical interfaces (vlan intf) not discovered                  |
| CSCsc95831       | log messages of MARS processes stopped being written into backend log    |
| CSCsc91572       | Multiple target ports in IDS event show up as 'port 0' in query          |
| CSCsc90480       | MARS Incident notification options are not configurable                  |
| CSCsc78878       | snort signature 2570 incorrectly mapped                                  |
| CSCsc73832       | Drop rule inactive for events received by netflow in CS-MARS             |
| CSCsc58485       | 5 tuple information missing from downloaded raw log file                 |
| CSCsc48498       | CS-MARS: Upgrade from 3.4.x fails                                        |
| CSCsc42396       | CS-MARS Viewing IP of grouped sessions throws Exception, no Time var     |
| CSCsc23874       | Resource Utilization reports shouldn't be exposed to load as on demand   |
| CSCsc15590       | MARS not including all events in a report, query returns events fine     |
| CSCsc04484       | LC Rule/Report list shows empty after deletion of GC group               |
| CSCsb80082       | Deleting a LC w/o exchanging certificates doesn't set mode to Standalone |
| CSCsb77550       | CSV re import of CSA and Symantec agents unsuccessful                    |

## Resolved Caveats - Release 4.2.5

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

| Reference Number | Description                                                               |
|------------------|---------------------------------------------------------------------------|
| CSCsi08897       | CS-MARS - CLI may display incorrect timezone after 03/11/07 DST change.   |
| CSCsh96976       | Datawork for 4.2.5                                                        |
| CSCsh88897       | race condition in pnparsers triage handling caused syslog processing stop |
| CSCsh83470       | DB function to convert unix time to readable string for convenience       |
| CSCsh78439       | Gc to LC: edited user rule not in rule group when passed to LC            |
| CSCsh72483       | "<=" character showing up in OS entries                                   |
| CSCsh71162       | Doc enhancement Mars GC push down IP Mgr group to active LCs              |
| CSCsh68374       | Need to update Oracle shared_pool_size to match recommended settings      |
| CSCsh64155       | MARS is not sending all the parameters to CSM for ASA acl syslog          |
| CSCsh56499       | Mars should learn FWSM dynamic nat from syslog for sessionization         |
| CSCsh56214       | GC User group not removed from LC when LC deleted from GC                 |
| CSCsh54049       | Custom column query: cache is not cleared from option page                |
| CSCsh47461       | 'Details' button does not return                                          |
| CSCsh46868       | Custom column query not returning data                                    |
| CSCsh38818       | GC-LC upgrade 4.2.2->4.2.3 results in inverted online-offline status      |
| CSCsh36853       | overflow condition in FileSystemFull function (pnbfs.cpp)                 |
| CSCsh32558       | custom column query: for acs event log, reported user is missing          |
| CSCsh29555       | MARS-3-100039 syslog not sent after a successful VA data import           |
| CSCsh18265       | null drop rule causes parse error in the GUI                              |
| CSCsh13261       | syslog related to upgrade through GUI sends invalid syslog messg          |
| CSCsh11027       | clicking 'next' button for IOS hangs up on GC                             |
| CSCsg99611       | CS-MARS - Radio buttons are confusing on Retrieve Raw Messages page       |
| CSCsg98822       | A device on GC( pushed from LC) is not deleted even after deleting LC     |
| CSCsg93306       | Hosts List on MARS not consistent with discovered Qualys device list      |
| CSCsg86757       | Using telnet discovery wrongly merged VLAN1 info into VLAN13 info.        |
| CSCsg86481       | CS-MARS parsing error for ASA7.0 msg 302018                               |
| CSCsg83055       | parsing error for FWSM-n-302003 and FWSM-n-302004                         |
| CSCsg76793       | Suspended LC still communicates with GC                                   |
| CSCsg71475       | Submitting Unconf. FP Firing Event only query generates system error.     |
| CSCsg67502       | Incident->False Positive note is grammatically incorrect                  |
| CSCsg66099       | Devices from deleted LC should be removed from the GC                     |
| CSCsg64951       | Certain ASA 7.0 syslogs do not get parsed by MARS                         |
| CSCsg52502       | FWSM 3.1: parsing does not resolve predefined name to IP in Auriga-2      |
| CSCsg44725       | need to downgrade log level of CSA snmp trap errors in backend log        |
| CSCsg39552       | Certain FWSM 2.3 syslogs give parsing errors/unknown event type in 4.2.2  |
| CSCsg37886       | error log exception when user_id is 201 (with Case Management)            |

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsg26225       | Graphs/Images do not show up in case related report emails              |
| CSCsg20514       | Mars backend processes need to save backtraces on a crash for debugging |
| CSCsg10787       | CatOS telnet discovery failing.                                         |
| CSCsg04079       | Lotus Notes client gets JavaScript error with emailed MARS report       |
| CSCsf20103       | csips and csiosips occasionally crashing                                |
| CSCsf06819       | vulnerabilities not updated for hosts reported by deleted eEye console  |
| CSCse84962       | eEye: MARS does not remove resolved vulnerabilities from host info      |
| CSCse39426       | frequent superV & pnparsers restarts cause log processing to fail       |
| CSCse27948       | pink box when do query - ORA-01555: snapshot too old exception          |
| CSCsd48097       | Event processing may stop if pnparsers creates shared buffers first     |
| CSCpn03005       | Loading Resource Util report as On-Demand query produces a system error |

## Resolved Caveats - Releases Prior to 4.2.5

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](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](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.