



Release Notes for Cisco Security MARS Appliance 4.3.5

Revised: July 24, 2009, OL-16727-01



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 4.3.5 running on any supported Local Controller or Global Controller as defined in [Supported Hardware, page 2](#). They provide the following information:

- [Introduction, page 1](#)
- [Supported Hardware, page 2](#)
- [New Features, page 2](#)
- [Upgrade Instructions, page 3](#)
- [Documentation Errata, page 13](#)
- [Important Notes, page 13](#)
- [Quick Install Notes, page 16](#)
- [Caveats, page 20](#)
- [Product Documentation, page 28](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 29](#)

Introduction

Version 4.3.5 is now available as an upgrade to 4.3.4 of your MARS Appliance software. Registered SMARTnet users under the can obtain version 4.3.5 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

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

Supported Hardware

Cisco Security MARS Version 4.3.5 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 4.3.5:

- **Update to intrusion prevention, and intrusion detection, and vulnerability assessment signature sets.** This release includes new vendor signatures, updating the 3rd-party signature support. For more information on the updates, see [New Vendor Signatures, page 2](#)
- **Bug fixes.** For the list of resolved issues, see [Resolved Caveats - Release 4.3.5, page 28](#).

New Vendor Signatures

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

Revised in 4.3.5	Product	Signature Version Supported
Intrusion Prevention and Detection Signatures		
Yes	Cisco IDS 4.0, Cisco IPS 5.x, Cisco IOS 12.2	Current through S330 signature release.
Yes	Snort NIDS 2.6.1	Current through the April 8, 2008 signature release. Latest signature mapped: 13664.
Yes	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 28.050 Release date: April 8, 2008
Yes	McAfee IntruShield NIDS 1.5 and 1.8 McAfee Network Intruvert v. 2.5, 4.0	4.1.24.5 Release date: April 7, 2008
Yes	McAfee Enterecept HIDS 2.5, 4.0	Current through the April 11, 2008 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R55)	Current through the April 8, 2008 signature release
Yes	Netscreen IDP 2.1, 3.0, 3.1, 4.0, 4.1	Signature version: 4.1. Release date: April 10, 2008
Yes	Symantec NIDS, v 4.0	Signature package: 95 Release date: April 11, 2008
Yes	Enterasys Dragon 6.x, 7.x	Current through the April 10, 2008 signature release.
No. EOS.	Symantec Manhunt 3.x (See Symantec NIDS, v 4.0.)	3.4.3 Update 59 Current through the May 24, 2007 signature release.
Vulnerability Scanner Signatures		
Yes	Qualys QualysGuard ANY	Current through the April 11, 2008 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6 ¹	Current through the April 10, 2008 signature release.
Yes	Foundstone, version 3.x	Current through the April 15, 2008 signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the April 17, 2008 definition update.
Miscellaneous Support		
No	Oracle 11g	Support for new AUDIT_ACTIONS.

1. eEye REM 1.0 is supported in 4.2.x.

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 to the release number. Please refer to the notes that pertain to the release you are upgrading from and any releases following that one.

General Notes



Warning

You must adhere to the required upgrade path defined in [Required Upgrade Path, page 11](#).

The MARS Appliance performs a file system consistency check (fsck) on all disks when either of the following conditions is met:

- If the system has not been rebooted during the past 180 days.
- If the system has been rebooted 30 times.

The fsck operation takes a long time to complete, which can result in significant unplanned downtime when rebooting the system after meeting a condition above. For example, a MARS 50 appliance can take up to 90 minutes to perform the operation.

Upgrade to 4.3.5

No important notes exist for the 4.3.5 upgrade.

Upgrade to 4.3.4

No important notes exist for the 4.3.4 upgrade.

In addressing *CSCsm57453: Incident not created for some of same events*, the behavior now differs between 4.3.4 and 5.3.4. In the x.3.3 releases, incident firing was throttled at 100 incidents for event bursts from a vulnerability assessment (VA) reporting device. In 5.3.4, incidents firing throttles at over 430 incidents, and in 4.3.4, the incidents firing throttles at just over 220 incidents.

Upgrade to 4.3.3

No important notes exist for the 4.3.3 upgrade.

Upgrade to 4.3.2

The following important notes apply to the upgrade from 4.3.1 to 4.3.2:

- **Release-Note for CSCsk19730/CSCsk12130**

If you've edited a system rule on a Global Controller, you may encounter one of two conditions where the rules on the Global Controller are out of sync with those on the Local Controller.

Symptom: The edited rule in the Global Controller disappears from the list of rules on the Local Controller. (CSCsk12130)

Condition: The user edited a rule on the Global Controller and then upgraded to a different version of the MARS system software and then added of a new Local Controller to the Global Controller.

Symptom: A rule that was edited in the Global Controller looks as if it is an empty rule in the Local Controller and be inactive. (CSCsk19730)

Condition: This occurs under in some cases where a Local Controller is added to a newly upgraded Global Controller.

Work Arounds: If the Local Controller is deleted from and re-added to the Global Controller under x.3.2, the issue should resolve itself. However, in conditions with a large topology or many custom rules, we recommend contacting technical support for a work around that avoids the need to delete and re-add the Local Controller.

Another possible work around if the number of edited rules are small is to edit and make further changes to the rule and activate. In this case, the issue should be resolved for that rule.

- **Upgrade of IOS 12.3 and 12.4 devices.** In previous releases, these devices were supported under the IOS 12.2 release when defining the device type in theMARS web interface. After you upgrade to 4.3.2, the next discovery of such a device will automatically upgrade the version to its correct value.

For example, an IOS 12.4 device is added to MARS 4.3.1 as 12.2 and after the upgrade to 4.3.2, when the discovery occurs for that device, the device type is automatically updated to IOS 12.4. The same is true for devices that are running IOS 12.3. However, if you have not enabled device discovery, use the Change Version feature to change between IOS 12.2, 12.3, and 12.4.

- **Wireless LAN Controller Support is restricted to the 5.3.x train.** To enable support for wireless access points via the Cisco Wireless LAN Controller, you must use the 5.3.2 or later software, which also restricts the appliance models that can be used.
- **Juniper/NetScreen IDP 3.x and 4.x Support is incomplete.** While device support has been added, the signature/data work portion of these devices will be provided in a future release of MARS software.
- **Renaming of QualysGuard 3.x device type.** During the upgrade, any QualysGuard devices defined under Security and Monitoring Devices will changed their device type from QualysGuard 3.x to QualysGuard ANY.

Upgrade to 4.3.1

Beginning with the 4.3.1 and 5.3.1 releases, the dynamic IPS signature updates (if enabled) is an aspect of the version of software running on a MARS Appliance. Therefore, in addition to running the same MARS software versions on the Global Controller and Local Controller, the IPS signature version must match or the communications fail.

In a Global Controller-Local Controller deployment, configure the dynamic signature URL and all relevant settings on the Global Controller. When the Global Controller pulls the new signatures from CCO, all managed Local Controllers download the new signatures from the Global Controller.

In addition, CSCsk90015 states that any reporting device representing a Cisco ACS 3.x device that exists prior to the 4.3.1 upgrade is deleted during the upgrade. To resolve the issue after upgrade, you must the remove the reporting device from the host and re-add that device again as Cisco Secure ACS 3.x.

An example process is as follows:

1. Click **Admin > Security and Monitor Devices**, select the host with Cisco ACS 3.x as a reporting application and click **Edit**.

2. Select the **Reporting Applications** tab, and then blank link and click **Remove**.
3. After removing the blank link, re-add Cisco Secure ACS 3.x application to that host and click **Activate**.

Upgrade to 4.2.8

No important notes exist for the 4.2.8 upgrade.

Upgrade to 4.2.7

No important notes exist for the 4.2.7 upgrade.

Upgrade to 4.2.6

No important notes exist for the 4.2.6 upgrade.

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 6](#)).
 - 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 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.



**Note**

For example, if you are upgrading to 4.3.5 from 4.2.8, you must follow the upgrade path from 4.2.8, to 4.3.1, 4.3.2, 4.3.3, 4.3.4, and then to 4.3.5. You must upgrade to all intermediate releases in sequence.

**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> |
| 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              |
| 4.2.5                      | 4.2.6                         | csmars-4.2.6.pkg              |
| 4.2.6                      | 4.2.7                         | csmars-4.2.7.pkg              |
| 4.2.7                      | 4.2.8                         | csmars-4.2.8.pkg              |
| 4.2.8                      | 4.3.1                         | csmars-4.3.1.pkg              |
| 4.3.1                      | 4.3.2                         | csmars-4.3.2.pkg              |
| 4.3.2                      | 4.3.3                         | csmars-4.3.3.pkg              |
| 4.3.3                      | 4.3.4                         | csmars-4.3.4.pkg              |
| 4.3.4                      | 4.3.5                         | csmars-4.3.5.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)

## Documentation Errata

- CSCsl14244. User guide does not discuss role of Nessus in the MARS system.  
To determine whether specific incidents are false positives, MARS uses Nessus 2.x GPL plug-ins and custom scripts mapped to specific MARS event types. MARS does not use Nessus to perform vulnerability assessments or related reporting.
- CSCsk77546. Discovery Device with SSH 512 module not supported.  
The OpenSSH client used by MARS does not support modulus sizes smaller than 768. For example, you cannot discover a device using a SSH login that has 512-byte key.

## Important Notes

The following notes apply to the MARS 4.1.x, 4.2.x, and 4.3.x releases:

- If the client system used to access the MARS GUI is not on the same side of the NAT boundary as the a MARS appliance and the Security Manager server, you can perform policy lookup in read-only mode. However, you cannot start the Security Manager client from the read-only policy lookup table to modify matching policies. The client system must be on the same side of the NAT as the MARS appliance and the Security Manager if you want to the Security Manager client from MARS to modify the matching policy.
- Security Manager client must be on the same side of the NAT boundary as the MARS appliance and the Security Manager server to query MARS events from policies.
- The performance of the Summary Page degrades when too many reports are added under My Reports. The smaller the number of reports under My Reports, the faster the Summary page loads. To ensure adequate performance, limit the number of reports to 6. This issue is partially described in CSCse18865.
- Do not to use DISTINCT or SAME in queries, and do not run multi-line queries in Release 4.3.5. 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> |
| CSCpn02175             | <p><i>Issue:</i> Data computed or stored on a standalone MARS while in standalone mode will not be transferred to a Global Controller. Only data computed on an Local Controller that is currently monitored by a Global Controller will be pushed up.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CSCpn02073             | <p><i>Issue:</i> After renaming a cloud, clicking the cloud again causes an error.</p> <p><i>Workaround:</i> Refresh the page before clicking a renamed cloud.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| CSCpn01270             | <p><i>Issue:</i> The free-form search may not work for the following devices:</p> <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             | <p><i>Issue:</i> The automatic time-out feature built into the GUI does not work when the Summary page is left open with automatic refresh selected.</p> <p><i>Resolution:</i> Please log out of the system when you are no longer using it.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Quick Install Notes

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

1. [Installation Quick Reference, page 16](#)
2. [Checklist for Initial Configuration, page 16](#)

## 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> |
| 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 16</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="228 285 638 310"><b>4. Command Line Configuration.</b></p> <p data-bbox="269 327 1503 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><li data-bbox="282 548 667 577">• Set any additional static routes.</li><li data-bbox="282 594 467 623">• Set the clock.</li><li data-bbox="282 640 630 669">• Set the NTP server settings.</li><li data-bbox="282 686 618 716">• Set the DNS domain name.</li><li data-bbox="282 732 1110 762">• Connect the appliance to the network (that is, plug in the Cat 5 cables.)</li></ul> <p data-bbox="269 774 1503 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">• <a href="#">Specify the Time Settings</a></li><li data-bbox="282 972 605 1001">• <a href="#">Set Up Additional Routes</a></li><li data-bbox="282 1018 708 1047">• <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 4.3.5, page 21](#)
- [Resolved Caveats - Release 4.3.5, page 28](#)
- [Resolved Caveats - Releases Prior to 4.3.5, page 28](#)

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 4.3.5

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

| Reference Number                | Description                                                              |
|---------------------------------|--------------------------------------------------------------------------|
| <b>Cisco Security Manager</b>   |                                                                          |
| CSCso16735                      | xCSM: P->E with CS Mgr credentials fails in cross-launched CSM client    |
| CSCsm94630                      | Policy query icon is not shown at times in Real time viewer              |
| CSCso11900                      | Keyword field dimmed in Query page after events lookup from Security Mgr |
| CSCsm96376                      | Policy lookup icon not shown if device is deleted from MARS              |
| CSCsm14585                      | Read-only policy page takes a long time to display for realtime events   |
| CSCsm92008                      | Security Manager not reachable error displayed after long time           |
| CSCsm94537                      | Policy lookup icon not shown for a device deleted and readded to MARS    |
| CSCsl54107                      | Security Manager policy lookup for ICMP connection teardown syslog fails |
| CSCsm43237                      | Minimum password length for Security Manager account in MARS             |
| CSCso38232                      | Host not shown in topology graph if Security Manager is added on it      |
| CSCsf31401                      | MARS query does not highlight rules inside any policy group named Local  |
| <b>Firewall Services Module</b> |                                                                          |
| CSCsl27574                      | FWSM Syslog message FWSM-6-302013 with wrong Real and Mapped IP          |

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

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsq69190       | 4.3.5 eth1 IP address not migrated to 5.3.5                              |
| CSCsq33307       | Custom device still shows up in the device list even after deleting it   |
| CSCsq33040       | On LC seeing pn_statistics_data with zone set to 0 (sometimes)           |
| CSCsq29469       | MARS: Detailed NAC report with keyword query has empty columns           |
| CSCsq23660       | Telnet to port 22 returns SSH Banner                                     |
| CSCsq23060       | Entries with ID 0 exist in database in some tables                       |
| CSCsq15630       | Confirmed false positive did not show in GUI                             |
| CSCsq07542       | CS-MARS Incident path graph connects to wrong cloud/gateway              |
| CSCsq05336       | MARS - Large Number of Reported Users, Query user selection fails        |
| CSCsq01029       | MARS Gen1 - Need Message Pointing to Failed Drive for Replacement        |
| CSCso97681       | Host name appears inconsistently on Incident Vector Topology             |
| CSCso93030       | IP Management not displaying group associations when using Device Group  |
| CSCso89940       | MARS: User-Name in raw message not populating user column in NAC report  |
| CSCso87624       | MARS IOS Discovery failure when banner has number/pound (#) symbols      |
| CSCso86201       | Vulnerabilities found against MARS unit                                  |
| CSCso80923       | Specific Patter From a Customer Parser is Not Synced to LC               |
| CSCso80816       | Dashboard to report relations fail to replicate LC/GC                    |
| CSCso73998       | Editing User Group From Rules/Action Menu Clears Group Members           |
| CSCso72148       | Host name Any can be added via VA scan report in MARS                    |
| CSCso70178       | shared buffer does not update write_stop_time correctly                  |
| CSCso62981       | Gen 2: Raw Message Retrieve doesn't work due to different time zone used |
| CSCso61036       | LC/GC Sync: Improve handling of config pull on update                    |
| CSCso60384       | TR/RR not present in results for All Matching Events - LLV raw events    |
| CSCso59056       | pnrestore throws the warning of archive version 0                        |
| CSCso54308       | LC stops communicating to GC, stack dump shows stuck in Version Check    |
| CSCso53066       | DbInterface's interface_index value's precision has to be 10             |
| CSCso50724       | pnparser memory leak in parsing error handling caused restart by superV  |
| CSCso43238       | LC pull of updated GC rule fails if rule has been edited at LC           |
| CSCso40549       | L2 path through 7600 with VRF give error message                         |
| CSCso39840       | Sud incr. in traf raw msg should have std deviation instead of variance  |
| CSCso38232       | Host not shown in topology graph if Security Manager is added on it      |
| CSCso32099       | Some ISS events parsing error on MARS                                    |
| CSCso28421       | AAA: When adding AAA server cannot select existing ACS                   |
| CSCso27861       | Sym Agent load thru seed file returns ArrayIndexOutOfBoundsException     |
| CSCso09952       | MARS shows unknown reporting IP:0.0.0.0 for events from WL controller    |
| CSCso01260       | Loading hosts from seed file does not fill interface information on MARS |

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsm95233       | host appears in edit, but not view of group                             |
| CSCsm92836       | Large interface index causes SQL errors during DB save of interfaces    |
| CSCsm81377       | Mars 4.3 - not able to set custom POSIX timezone opt 11                 |
| CSCsm75403       | Network groups ignored in query                                         |
| CSCsm60645       | MARS dropping some events                                               |
| CSCsm56006       | PIXIASA70 - Event parsing errors                                        |
| CSCsm55954       | detailed NAC report table header does not show in the schedule report   |
| CSCsm55938       | PIXIASA: Event parsing errors                                           |
| CSCsm48603       | config change report didn't capture cat6k/vpn3k config change events    |
| CSCsm45118       | CSA Events in MARS appear as hex characters                             |
| CSCsm40349       | rare crashing issue due to file system check/memory short               |
| CSCsm38062       | MARS change wrong device type when use SNMP as access type              |
| CSCsm28714       | Need CLI/UI method for retrieving log files                             |
| CSCsm09021       | Wrong query interval if leave one field blank                           |
| CSCsm09020       | "missing_zone_info" incidents show up in the GC                         |
| CSCsl77531       | Device monitor uses excessive memory, repeatedly restarted by superV    |
| CSCsl58359       | exporting data use pnext requires more TEMP tablespace                  |
| CSCsl58216       | MARS Layer 2 path and mitigation issues with IOS 12.3 and 12.4 version  |
| CSCsl41494       | Network_group object with DB ID of 0 (zero) causes system error in GUI  |
| CSCsl31143       | MARS restore process fails on 4.3.1                                     |
| CSCsl14244       | The User guide is not talking anything about the Nessus version         |
| CSCsl11647       | Pnupgrade hanging at the last step - Updating database schema           |
| CSCsl04692       | Reported user is not parsed for windows event id: 680                   |
| CSCsk92543       | CS-MARS: Custom Column Report Device Column Blank .                     |
| CSCsk85267       | pnparser crashes related to CheckPoint Opsec library                    |
| CSCsk85174       | MARS - 5 tuple information missing from raw IDS events from NFS archive |
| CSCsk80647       | pnupgrade is not displaying next fsck scenario                          |
| CSCsk70744       | Upgrade OpenSSL version                                                 |
| CSCsk39645       | GUI doesn't check duplicate agent ip address when adding application    |
| CSCsk27999       | Java error when clicking on Configuration Information page              |
| CSCsk27276       | MARS: Isolated Networks in Topology due to 'ip unnumbered' Interface    |
| CSCsk26308       | pink error when listing devices while scalability script running        |
| CSCsk12489       | operator role can not resubmit report                                   |
| CSCsk12421       | Netflow config wrongly mixed up with traffic anomaly configuration      |
| CSCsk11592       | ids didn't get monitored networks from msfc if discover ids first       |
| CSCsk08028       | Real time multi column query is not working.                            |
| CSCsk04282       | MARS failed to import 1000 hosts vulnerabilty information               |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsj96592       | Adding LC with version lower than 4.3.1 should version mismatch err      |
| CSCsj92673       | pink box appears when adding query/Report into Cases                     |
| CSCsj90875       | Inline/Batch query: result mismatch on Matched Rule Ranking              |
| CSCsj90505       | Inline/Batch query not match on NAT connection report                    |
| CSCsj87207       | GUI cannot show the full topology because of constant process crash      |
| CSCsj69985       | Syslogrelay is accepting same IP for both source and collector           |
| CSCsj68087       | MARS Discovery fails to take the context information of ASA from 7.2-7.0 |
| CSCsj67626       | Raw message query type schedule report missing some raw message events   |
| CSCsj67037       | pnparser / postfire / process_event_srv crashed in func test             |
| CSCsj66955       | scheduled discovery is scheduled at wrong time                           |
| CSCsj60272       | Special characters should not be allowed in device name(MARS)            |
| CSCsj51240       | Paging does not work for report right after adding it to a case.         |
| CSCsj42467       | LC not showing up on certificate page                                    |
| CSCsj31990       | pnparser: to avoid flooding log file                                     |
| CSCsj28376       | Box may not be able to reboot after recovery, under certain conditions   |
| CSCsj23845       | CS-MARS Action filter doesn't work if not associated with incidents      |
| CSCsj20697       | LC did not get added to GC so unable to generate syslogs.                |
| CSCsj15512       | Update reports when handling deletion of hosts                           |
| CSCsi96921       | IPSDynamicSigUpdate attempts to connect to CCO with no credentials       |
| CSCsi93283       | Mismatch between query and report results for source port ranking.       |
| CSCsi91734       | Mismatch in results between query and report for All Matching Events     |
| CSCsi86420       | with 60% event rate capacity, query events ranked by time takes 20 min   |
| CSCsi76255       | Custom log template pattern messed up when add a LC to GC                |
| CSCsi69310       | security hole happens if users close browsers without click logout       |
| CSCsi68126       | For multiple context mode, inbound/outbound error reports are incorrect. |
| CSCsi65960       | L2 mitigation has problem finding path                                   |
| CSCsi65713       | Index needs to be removed for the pn_report_result table                 |
| CSCsi62384       | The performace test kills all the process during the weekend run         |
| CSCsi52731       | mars reboots w/o asking for confirmation after user clicked cfg update   |
| CSCsi51999       | Edit SW based Application device need submit twice                       |
| CSCsi50024       | IPS is not visible in Global Zone Hot Spot Graph                         |
| CSCsi49474       | Mismatch results between query and report (custom column)                |
| CSCsi49419       | The application hangs, while getting the results for a query.            |
| CSCsi49396       | Mismatch in results between query & report when query based on desti. IP |
| CSCsi49330       | Mismatch in results between query and report when query is based on user |
| CSCsi49285       | Mismatch in results between query and report.                            |
| CSCsi44427       | Enh: Make HTML report output the same as CSV output                      |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsi29398       | CS-Mars does mitigate to the proper endpoint                             |
| CSCsi18757       | CS-MARS - Request to have the "ssldump" command in the MARS CLI.         |
| CSCsi15769       | NLS_LANG variable should be updated in environment                       |
| CSCsi13100       | gui.sh dev build makes different JBOSS web.xml than make release         |
| CSCsi11312       | pn_incident_log and pn_report_log should be archived                     |
| CSCsi07186       | User can input unsupported characters in AAA device name                 |
| CSCsi03658       | CS-MARS - IOS Discovery via Telnet/SSH fails with \$hostname in banner   |
| CSCsh97060       | MARs says it can delete up to 500 at a time but only lets you delete 50. |
| CSCsh89445       | GUI allow users create rule without putting rule name                    |
| CSCsh83068       | Report and query return no results under device type ANY                 |
| CSCsh73553       | MARS DVD imaging does not support USB keyboard                           |
| CSCsh67828       | Custom Column Query filtered by reporting device missing results         |
| CSCsh52537       | Repeated upgrades of oracle fills hard drive                             |
| CSCsh44351       | CSM multiple hostname matches failed to return multiple hosts            |
| CSCsh14454       | server.log can grow unbounded with in a single day                       |
| CSCsh00013       | Case Management: history does indicate change of ownership               |
| CSCsg91816       | port 0 in 'Top Destination Ports' misleading                             |
| CSCsg82600       | some syslog results in unknownDET with 'Activate                         |
| CSCsg80475       | All incidents purged if event-session partition table is corrupted.      |
| CSCsg79246       | Getting a blank window when adding a device in IE 7                      |
| CSCsg76958       | FR: Recognize either CIPS network variables or have CSMARS net variables |
| CSCsg73786       | Devices should not be added to MARS if Discovery is unsuccessful         |
| CSCsg64119       | rule's keyword editor treats NOT as binary rather than unary             |
| CSCsg54313       | ORA-01654: unable to extend index .                                      |
| CSCsg47022       | CS-MARS - Incorrect Start Times on Retrieved Raw Message Files           |
| CSCsg26352       | Getting a internal server error when trying to access a incident on GC   |
| CSCsg20987       | CSMARS DTM sdf files are sent with invalid format                        |
| CSCsf99844       | wrong values for current connections using CLI "show resource usage      |
| CSCsf99767       | provide encoding selection for adding agent to device/host               |
| 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                 |
| CSCsf27568       | keyword search query can't display big-5 encoding raw msg                |
| CSCsf26715       | Inaccuracy in per-context memory utilization for multi-context devices   |
| CSCsf15781       | Database table columns do not match with the archive file columns        |
| CSCsf12825       | GUI should prevent edit/delete of system-context PIX/ASA 7.0 devices     |
| CSCsf11651       | Device resource monitor incorrectly samples 5 sec CPU instead of 5 min   |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsf06141       | high CPU usage in pnparsersessionization                                 |
| CSCsf06019       | Generic Router UI must support multiple reporting applications           |
| CSCse98029       | Occasionally corrupted event data enters into MARS database              |
| CSCse91636       | MARS - not all columns seen in CSV reports generated using custom column |
| CSCse85972       | Unresolved symbol in Java build (though did not stop building)           |
| CSCse82042       | Change the Device Type Version for FWSM                                  |
| CSCse82022       | Unable to view reports starting with #sign in csv format                 |
| CSCse78738       | FWSM ifspeed incorrectly reported as 0 for per-context vlan interfaces   |
| CSCse78089       | Unable to upgrade CS-Mars via GUI                                        |
| CSCse54808       | The time stamp shown by the pndbusage command is incorrect.              |
| CSCse51642       | IPlanet Unknown Device Event Type Parsing Error                          |
| CSCse45884       | LLV query causes client CPU to go to 100%                                |
| CSCse44509       | On demand report progress shows negative value                           |
| CSCse42953       | CS-Mars - unable to show L2 path when source and destination in same net |
| CSCse38565       | CSV-Re-importing Symantec AV client CSV doesn't work                     |
| CSCse38356       | Windows pulling gets stuck for one IP due to invalid content in evt log  |
| CSCse34600       | configurable SNMP timeout support                                        |
| CSCse34407       | Query Tab -> Multi column query returns wrong results.                   |
| CSCse33688       | No Event Types listed under Cisco Switch-IOS 12.2                        |
| CSCse33172       | Invalid id used in DbClient::retrieve() 0                                |
| CSCse31722       | Cloud toggle only works on first page of reporting devices               |
| CSCse27948       | pink box when do query - ORA-01555: snapshot too old exception           |
| 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                   |
| CSCse10945       | Summary Page Graphs Spontaneously Change Displayed Size (w/ multi-head)  |
| CSCse09127       | Failed load from csv returns incorrect status                            |
| CSCse00626       | IP Management -> device group displays hosts only.                       |
| CSCsd95582       | Both successful/failed mitigation reports show same results              |
| CSCsd89457       | Incorrect handling of time range for rules that fire periodically.       |
| CSCsd86896       | Clicking the clear button when editing the query type doesn't work.      |
| CSCsd84350       | CS-MARS/CSM: Credentials change on CSM side not checked.                 |
| CSCsd74681       | OS 4.0: FlexLM License                                                   |
| CSCsd61749       | pnprestore doesn't restore all of the system config                      |
| CSCsd06302       | device name with single quote causes pink box                            |
| CSCsc95831       | log messages of MARS processes stopped being written into backend log    |
| CSCsc90480       | MARS Incident notification options are not configurable                  |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsc59363       | Need improvement to GUI for multi-line rules                             |
| 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                    |
| CSCsb67871       | Got System Error In GC After Re-installed New Version In LC              |
| CSCpn03057       | Copied rules have shortened year in front, which is confusing (ex. 0     |
| CSCpn03052       | JBoss 'OutOfMemoryError' when accessing Management/Event Management      |
| CSCpn02976       | GC:LC - Communication issues after time zone change                      |
| CSCpn02973       | Not able to downgrade a security analyst to Notification only user       |
| CSCpn02968       | Network group search is not working for "All IP addresses                |
| CSCpn02901       | GC/LC, rule does not display user <cxu> but allows such cfg              |
| CSCpn02869       | Rules editing: changing entry for select window pulldown after error     |
| CSCpn02804       | Replay History feature not working correctly                             |
| CSCpn02666       | Batch Query Results with one item returned -> no data in graph in em     |
| CSCpn02656       | System error occurs when # of java connections runs out                  |
| CSCpn02653       | No way to specify "!Keyword" without a good "keyword                     |
| CSCpn02574       | Time change on system causes GC/LC communication problem                 |
| CSCpn02566       | rebooting mars while it is upgrading cause the box not accessible        |
| CSCpn02558       | "Agent" didn't be removed correctly                                      |
| CSCpn02549       | JavaScript Error from ViewReport when clicking Edit/Clear                |
| CSCpn02511       | need to fix errors in affected os                                        |
| CSCpn02470       | Server csv function could not handle special characters in password      |
| CSCpn02414       | GC/LC user rule is too long to fit into a page if keyword is long        |
| CSCpn02410       | rule was not fired because Oracle log used upper case for user           |
| CSCpn02398       | XML escaping errors in Keyword Search in Rule                            |
| CSCpn02385       | Applied \$TARGET01 for GC Query Source IP resulted in "resultCounter     |
| CSCpn02383       | IIS parsing must be separated from Windows log                           |
| CSCpn02251       | License: Upon entry of 100 license onto 100e, need to restart pnpars     |
| CSCpn02177       | Docs: Filesystem Check after 22 reboots                                  |
| CSCpn02061       | Saving .csv files under WinXP SP2 results in .htm extension              |
| CSCpn01438       | Batch Query: Under high load, some batch queries may not complete        |
| CSCpn01398       | Unable to shutdown an interface                                          |
| CSCpn01382       | Security device type hosts don't show up in IP management                |
| CSCpn01319       | pnreset command does not cause reboot                                    |
| CSCpn01219       | Cleanup script for invalid /etc/qpage.conf entries                       |
| CSCpn01134       | Cloud name input box accepts invalid characters                          |

| Reference Number | Description                                                     |
|------------------|-----------------------------------------------------------------|
| CSCpn01045       | Archiving: Need better error message                            |
| CSCpn00908       | "Domain" in Configuration page - no use                         |
| CSCpn00586       | nasl message text needs to be changed                           |
| CSCpn00455       | Graph doesn't refresh when a cloud is renamed                   |
| CSCpn00293       | using TAB in editing fields                                     |
| CSCpn00212       | Graphgen crashes when there are many non-existent devices       |
| CSCpn00183       | Adding devices w/o "Activate" can cause "messy" graph           |
| CSCpn00173       | Nessus should check pre-NAT address instead of Post-NAT address |

## Resolved Caveats - Release 4.3.5

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

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsq68939       | adding gen-1 LC to a gen-2 GC runs into error                            |
| CSCsq30468       | x.3.5 packages have different IPS signature levels                       |
| CSCsq23405       | LC/GC Configuration Pull causes unnecessary Activation                   |
| CSCso71201       | FTP upgrade started from GUI or CLI does not work.                       |
| CSCso69721       | Mars 4.3 - Some IPS events showing up with no event type                 |
| CSCso67351       | CS-MARS: IPS Sig 5733 Maps to "WWW IIS Internet Printing Overflow" event |
| CSCso45101       | ASA 8.0.3 : Parsing Errors for some messages                             |
| CSCso02939       | Replace IPS signature link                                               |
| CSCsm98909       | MARS - Firewall Syslog ID 111008 Event Type name is misleading           |
| CSCsm93557       | LC/GC Not replicating large report result sets > 1000 elements           |
| CSCsm79939       | IP address in "More info of this device " is incorrect for Netscreen 5.0 |
| CSCsk02989       | GC is not usable when LC has lots of deleted devices                     |
| CSCsc97963       | Netscreen logical interfaces (vlan intf) not discovered                  |

## Resolved Caveats - Releases Prior to 4.3.5

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.

